



11. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

Vorbemerkungen zum Sprachgebrauch

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

Impressum

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

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

Redaktionsschluss: 17.05.2016

Bildnachweis: TLfDI

11. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

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

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

Erfurt, im Mai 2016

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

Inhaltsverzeichnis

1	Schwerpunkte im Berichtszeitraum	24
2	Allgemeine Entwicklungen im Datenschutz.....	28
2.1	Überblick.....	28
2.2	Wann dürfen öffentliche Stellen einen externen Daten- schutzbeauftragten haben?	32
2.3	Thüringer Gesetz zur Ausführung des Bundesmeldege- setzes (BMG)	32
2.4	Datenerfassung beim Waffenregister – verkantet?	33
2.5	Wissensdurstige Meldebehörde – nach dem neuen Bundesmeldegesetz	35
2.6	Endlich eine Orientierungshilfe zur Videoüberwachung ..	37
3	Europäischer und Internationaler Datenschutz	41
3.1	Safe Harbor – Anlegen verboten.....	41
3.2	Die Datenschutzgrundverordnung: Trilog beendet und alles auf Anfang!	43
3.3	Die JI-Richtlinie – war da was?	47
4	Neue Medien – Rundfunk – Telekommunikation	51
4.1	Melderegisterdaten für ARD, Günter Jauch und Co.?	51
4.2	Löschung von Google-Suchergebnissen	52
4.3	16 Millionen Zugangsdaten geraubt – was nun?.....	54
4.4	Datenschutz und Medienprivileg	56
4.5	Falschparkern auf der Spur – Knöllchen durch die „Wegeheld“-App?	58
4.6	Facebook-Fanpage – seit Safe-Harbor-Entscheidung Rechtmäßigkeit noch unsicherer	59
4.7	Telemediengesetz (TMG) – zeitgemäß ?	61
5	Kommunales	64
5.1	Bloßstellung in der Schankwirtschaft – öffentliche Auslegung von Beschwerdeschreiben.....	64
5.2	Jagdbehördliches Lauschen im Nebenzimmer – ausnahmsweise erlaubt – Türen zum Nebenraum sollten grundsätzlich geschlossen werden	65
5.3	Facebook als Informationsquelle für Steuerprüfer	66
5.4	Stadt ist neugierig: Wer wohnt in der Seniorenresidenz? .	68

5.5	Stadt will immer wieder wissen, wie Jugendliche ticken! – Datenschutz bei Jugendstudien	69
5.6	Karnevalswagen als Beweis unrechtmäßiger Datenübermittlung?.....	72
5.7	Bevor „das Kind in den Brunnen fällt“: besser vom TLfDI beraten lassen!.....	73
5.8	Datenerhebung mittels Mülltonne? – Aufkleber mit personenbezogenen Daten.....	74
5.9	Schatten der Vergangenheit – „Ex-Stasi“ im Stadtrat durch den TLfDI „outen“?	77
5.10	„Werbepost“ vom Oberbürgermeister – leider ohne Rechtsgrundlage und Einwilligung!.....	78
5.11	Keine Meldedaten für den Großvater: nicht lustig, aber datenschutzkonform	81
5.12	Aushändigung einer Meldebescheinigung an Nichtberechtigte	83
5.13	Besonderer Meldeschein: Bayerisches Muster vom TLfDI abgelehnt	85
5.14	Nachbarstreitigkeiten und kein Ende in Sicht? – Einhalt durch Datenschutz! – Zum melderechtlichen Auskunftsanspruch.....	87
5.15	Unterschriftensammlung – auch hier gilt der Datenschutz	88
5.16	Thüringer Landeswahlordnung – Klappe, die Vierte (Änderung).....	91
5.17	Leck im Rathaus Nordhausen? – personenbezogene Daten im Netz	92
5.18	Mit Speck fängt man Mäuse – Stadtwerke bieten Anreize für werbliche Nutzung von Kundendaten	93
5.19	Video(attrappen)gaga 1	94
5.20	Die Nadel im Heuhaufen – wie findet man einen datenschutzkonformen Entsorger?	96
5.21	Dürfen personenbezogene Daten von Wahl-Kandidaten ins Internet?	97
5.22	Eine amtliche E-Mail als lehrreiches Eigentor.....	99
5.23	Hunger des Landratsamtes Saale-Orla-Kreis auf Grundsteuerdaten	100
5.24	Mystery-Check im Thüringer Wald	102
5.25	Nachweis einer Amtspflichtverletzung: TLfDI stößt an Grenzen bei sich widersprechenden Aussagen	105

5.26	Halter – Fahrer – Ehegatte – Familienangehörige: Wann ist der Abgleich mit dem Blitzer-Foto unzulässig?	107
5.27	Rechtswidrige Datenübermittlung – der geblitzte künftige MP?	109
5.28	Geblitzt – wer darf Daten auswerten?	111
5.29	Personenbeziehbarkeit von Daten zu einem Stadtentwicklungskonzept	112
5.30	Rathaus-Videokamera: dieses Mal nicht so gaga!	113
5.31	Videogaga 2 in Piesau	114
5.32	„Brennende“ Datenschutzprobleme bei der Auftragsdatenverarbeitung – Zur Notwendigkeit eines Auftragsdatenverarbeitungsvertrages	115
5.33	Offene Unterstützungslisten bei der Kommunalwahl	117
5.34	Widerspruch zum Widerspruch – auf das Widerspruchsrecht muss angemessen hingewiesen werden.....	118
5.35	Der mitteilsame Oberbürgermeister – Vorsicht bei Pressemitteilungen	120
5.36	Eichsfelder Wurst oder Datenschutz bei Internetumfragen... ..	125
5.37	Hundezensus	127
5.38	Captain Chaos als Nächster bitte ... – Datenschutz bei elektronischen Anzeigetafeln	129
5.39	Gemeinderatsmitglieder wollen es wissen: Gehaltshöhe von Geschäftsführern kommunaler Unternehmen. Geht das?	130
5.40	Grenzen des Auskunfts- und Akteneinsichtsrechts nach § 13 Thüringer Datenschutzgesetz	132
5.41	Kommunale Eigenbetriebe: BDSG oder ThürDSG?.....	133
5.42	Global Positioning System (GPS) für Kommunalbedienstete	135
5.43	Weitergabe einer Telefonnummer zur Verfolgung einer Ordnungswidrigkeit	137
5.44	Fotosafari im Schlafzimmer oder eine mitteilsame Waffenbehörde.....	138
5.45	Individuelle Hilfeplanung: Datenverarbeitung nur bei datenschutzgerechter Einwilligungserklärung	140
5.46	Beschlüsse von Stadtratssitzungen können grundsätzlich im Netz veröffentlicht werden!	142
5.47	Keine Telefonauskünfte an Unbekannte!	143
5.48	Keine Umfrage ohne Datenschutzhinweis	144
5.49	Offene Briefe vom Finanzamt.....	146

5.50	Grabstelleninhaber wider Willen	148
5.51	Zulässigkeit des Verfahrens E-POSTBUSINESS-BOX	149
5.52	Wie viel Arbeitszeit braucht der Datenschutzbeauftragte?.....	150
5.53	Dürfen Stadtratsmitglieder die Gehälter der kommunalen Bediensteten überprüfen?.....	152
5.54	Streaming me softly? – Der Öffentlichkeitsgrundsatz in der ThürKO erfasst noch immer keine Live-Übertragung von Stadtratssitzungen	155
5.55	Verarbeitung von Einkommensdaten zur Festsetzung von Hortgebühren	158
5.56	Datenübermittlung im Verwaltungsverfahren	159
5.57	Pfändung nur bei Kenntnis der Bankverbindung zulässig!	161
5.58	Facebook weckt behördliche Überwachungsfantasien....	163
5.59	Durch und durch Datenschutz	167
5.60	„Datenskandal“ bei den Kraftwerken Gera – personenbezogene Daten auf der Müllkippe	169
6	Personaldaten	172
6.1	Datenleck bei Betriebsratswahl.....	172
6.2	Darf der behördeninterne Datenschutzbeauftragte den Personalrat kontrollieren?	174
6.3	Zeitungsnotiz zur „krankheitsbedingten“ Schließung eines Amtes	177
6.4	Mitarbeiter: Bitte lächeln!	178
6.5	Bewerberunterlagen: Einsicht für alle Personalratsmitglieder?.....	180
6.6	„Pranger 2.0“ – Amtsleiter stellt sensible Daten von Mitarbeiterin ins Intranet	182
6.7	Mitarbeiter im GPS-Dauer-Fokus	182
6.8	Übermittlungsbefugnis des Amtsarztes – keine Generalvollmacht!.....	184
6.9	GPS: nicht vom richtigen Weg abkommen	186
6.10	Bewerbungen per E-Mail	189
6.11	Elektronische Personalakte	191
6.12	Fingerabdruckscanner zur Arbeitszeiterfassung?.....	193
6.13	Fragebögen zur Mitarbeiterbefragung	194
6.14	Wenn sich Beschäftigte über andere Beschäftigte beschwerten: ein Datenschutzproblem?	197

6.15	Schutz: Daten oder Kanzlerin? – Datenübermittlung anlässlich des Besuchs der Bundeskanzlerin	199
6.16	Verfahren „Interamt“ (Onlineverfahren mit Speicherung und Verarbeitung der Bewerberdaten)	202
6.17	Datenschutz im Stadtrat – was darf bei Disziplinarverfahren übermittelt werden?.....	204
6.18	Geheime Personalakten?	206
6.19	Lehrerdaten für die Schuljahresanalyse	210
6.20	Anmeldepflicht für Prostituierte?.....	212
7	Polizei	214
7.1	Aktenplanschlüssel "2124 Landfahrer": fragwürdige Sondererfassung von Sinti und Roma durch Thüringer Polizeibehörden?.....	214
7.2	Interessenkollisionen beim Polizeiärztlichen Dienst.....	216
7.3	NSU-Untersuchungsausschuss des Thüringer Landtags – Beweise vs. Datenschutz	218
7.4	Klick und Blick – mit erheblichen Konsequenzen! – INPOL-Abfrage nur bei Erforderlichkeit	220
7.5	Rasterfahndungen in Thüringen – nicht ohne TLfDI	222
7.6	Unerlaubt und daher beanstandet – Abfrage personenbezogener Daten durch die Polizei	223
7.7	Verwechslung beim Strafbefehl	225
7.8	Bei rechtmäßiger Wohnungsdurchsuchung kann auch der TLfDI nicht mehr helfen	226
7.9	Datenabfrage oder keine Datenabfrage – das ist hier die Frage	227
7.10	Drehort Hörsaal – und Action! – Videogaga 3 – Aufzeichnung einer Dienstversammlung	228
7.11	Prüf- und Löschfristen der Polizei – Fortsetzung folgt ...	231
7.12	Mysteriöses Auftauchen personenbezogener Daten – War die Polizei involviert?	232
7.13	Abgefragt – Abfrage von Meldedaten durch die Polizei	233
7.14	Einnahme von Verwarngeldern als „olympische Disziplin“ der Polizei?.....	234
7.15	DNA-Datei und Datenschutz	236
7.16	Zentrum für Überwachung	238
7.17	„Body-Cams“ für den modernen Polizisten – chic, aber auch zulässig?	239
7.18	Polizist verkauft Privat-PC mit Dienst-Daten	240

7.19	Fallbearbeitungssystem der Polizei – auch hier gilt Datensparsamkeit	241
7.20	Beglaubigte Personalausweiskopien – zukünftig nicht mehr nötig	243
7.21	Polizeiliche Erfassung von Ausweisdaten per Smartphone- Foto?	244
7.22	Kennzeichenerfassung auf Hotelparkplatz	246
7.23	Polizei vs. Polizei – Verfahren bei Dienstaufsichts- beschwerden.....	247
8	Verfassungsschutz	251
8.1	Bekanntgabe personenbezogener Daten durch das Amt für Verfassungsschutz – nicht ohne den TLfDI	251
8.2	Kontrolle der Antiterrordatei	252
9	Finanzwesen.....	254
9.1	Auf Bewährtes vertrauen – keine Geburtsdaten in Konten- daten nutzen	254
9.2	Neugier auf Kontodaten von Kollegen.....	255
9.3	Wenn der Bankautomat spricht.....	256
9.4	Videoüberwachung in Sparkassen –kein Videogaga	258
9.5	Datenschutz im Falle einer Gesamtrechtsnachfolge	260
9.6	Besondere Leistungskontrolle in der Thüringer Landesfinanzdirektion.....	261
9.7	Drittes Gesetz zur Änderung des Thüringer Gesetzes zur Regelung des Kirchensteuerwesens – alles datenschutzrechtlich ok?	263
10	Justiz	265
10.1	Mitnahme von Gerichtsakten? Datenschutz trotz gesetzlich beschränkter TLfDI-Kontrolle	265
10.2	Videoüberwachung oder Zaun? – Was ist bei der Flüchtlingsaufnahmeeinrichtung angemessen?	267
10.3	Datenflüsse an die Staatsanwaltschaft – auf die Rechtsgrundlage kommt es an!	268
10.4	Dienstlich oder privat – falscher Adressat; wendet sich jemand als Privater an eine öffentliche Stelle, muss an die Privatadresse geantwortet werden	270
10.5	Gesetzentwurf zur Aufbewahrung von Notariatsunterlagen – nicht ohne Datenschutz	271

10.6	Ja, wer lauscht denn da in der JVA!?	274
10.7	Übermittlungssperre für Staatsanwaltschaft	278
10.8	Anforderung von Ausländerakten zur Anerkennung ausländischer Entscheidungen in Ehesachen	280
10.9	Zugang zu Gefangenendaten des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT)	282
10.10	Neufassung des Thüringer Maßregelvollzugsgesetzes	284
10.11	Den Wächtern auf der Spur	287
10.12	Auch für eine unklare Übergangsregelung läuft einmal die Zeit ab – zur Veröffentlichung von beeidigten Dolmetschern im Internet	288

11 Arbeit, Gesundheits- und Sozialdatenschutz, Frauen und Familien 291

11.1	Logo arbeitssuchend? Jobcenter verwenden kein spezielles Logo	291
11.2	Originalunterlagen für das Jobcenter?	293
11.3	Datensucht im Jobcenter	294
11.4	Datenabgleich durch Jobcenter	296
11.5	Immer wieder Kontoauszüge für das Jobcenter	297
11.6	Vorsicht bei der Akteneinsicht	299
11.7	E-Health-Gesetz des Bundes	301
11.8	Mobile-Health-Dienste (mHealth) – der Datenmarkt boomt!	303
11.9	Maßregelvollzug: Besuch nur mit Drogenscreening?	306
11.10	Wenn der Arzt kommt – Erfassung von Einsatzdaten des kassenärztlichen Notdienstes	308
11.11	Diagnose des Arztes auf dem Rezept: Geheimnisverrat gegenüber der Beihilfestelle	309
11.12	Privatadressen von Ärzten: Herausgabe durch Krankenhaus?	311
11.13	Rücksendung von Arztrechnungen und Rezepten an eine andere Beihilfeberechtigte	312
11.14	Schließung eines Krankenhauses – Infektionsgefahr für Patientendaten? – Zur ordnungsgemäßen Archivierung	314
11.15	Darf der Hausarzt alles wissen?	315
11.16	Vernichtung von Patientendaten – gut gemeint, aber	317
11.17	Überlassung von Patientenakten an ein Archiv im Sinne des Thüringer Archivgesetzes?	319

11.18	Die Thüringer Krankenhäuser – Heilung in Sicht.....	321
11.19	AlertsNet: Bei Keimen im Blut fließen Daten gut!	323
11.20	Datenschutz vs. Auskunftsrecht	325
11.21	Datenerhebung der Gemeinsamen Prüfungseinrichtung bei Thüringer Ärzten.....	326
11.22	Spender-Anamnesebogen für Angehörige von Organspendern	328
11.23	ARMIN soll Patienten schützen	330
11.24	Einsichtnahme in Todesbescheinigungen für eine wissenschaftliche Studie	332
11.25	Grenzenlose Datenerhebung bei Einschulungsuntersuchungen des Kinder- und Jugendärztlichen Dienstes der Gesundheitsämter?	334
11.26	Datenbohrung bei der Kassenzahnärztlichen Vereinigung Thüringen.....	336
11.27	Auch zukünftig nur anonyme Daten für die Bundesärztestatistik	337
11.28	Vertretung des Amtsarztes durch Private – die Zweite ...	338
11.29	Klinisches Krebsregister Thüringen.....	340
11.30	Ist die Arztqualifikation auch echt?	342
11.31	Elektronische Gesundheitskarte: runde Sache oder Runder Tisch?	343
11.32	Betriebliches Eingliederungsmanagement, ein daten- schutzrechtliches Minenfeld.....	345
11.33	Das Postgeheimnis gilt weiterhin! – Versendung von personenbezogenen Daten per Brief kein Datenschutzverstoß	347
11.34	Auch Sozialbehörden dürfen nicht alles wissen.....	348
11.35	Ein Jugendamt tat sich schwer, Auskunft zu erteilen.....	350
11.36	Aushang von Dienstplänen im Pflegeheim	351
11.37	Sozialdatenübermittlung an die Staatsangehörigkeitsbehörden.....	353
11.38	Akteneinsicht beim Jugendamt – ein schwieriges Unterfangen?	356
11.39	Wohngeld nur für gläserne Bürger?	358
11.40	Datenerhebung zur Aufnahme von Klienten anderer Sozialhilfeträger	361
11.41	Datenschutz und Sorgerechtsstreitigkeiten	363
11.42	Sozialhilfe auf falschem Konto: Datenschutz leitet auf richtiges Konto um.....	364

11.43	Illegaler Datenhandel auch bei Thüringer Behörden? – Zur Anwerbung von neuen Krankenversicherten	366
11.44	Das Jugendamt hat alles richtig gemacht	367
11.45	Sozialdatenschutz im Eilverfahren.....	369
11.46	Anonymisierung von Pflegedienstmitarbeitern zum Zweck der Entgeltsatzverhandlungen	371
11.47	Medizinische Diagnose in Behördenbescheid – kein Problem	374
11.48	Wohin mit dem Schriftverkehr zum Betrieblichen Eingliederungsmanagement (BEM)?	375
11.49	Löschungsresistente Daten im Gesundheitsamt	376
11.50	Auskunft zu und Löschung von Sozialdaten	377
11.51	Thüringer Verordnung über die statistischen Angaben für die Gleichstellung von Frauen und Männern nach dem Thüringer Gleichstellungsgesetz	379
11.52	Auskünfte über Kontenbewegung	380
11.53	Digitalisierung von Akten im Schwerbehindertenrecht ..	383
11.54	Todesursachenrecherche	385
11.55	Vaterschaftsfeststellung durch das Jobcenter?	386
11.56	Jugenderburschaften und Datenschutz	387
11.57	Datenerhebung bei Minderjährigen nur mit Einwilligung der Eltern?	389
11.58	Sperren statt löschen	390
11.59	Mütter und Hebammenleistungen – Befragung „entbindet“ nicht von Datenschutz	392
11.60	Gesundheitsdaten von Asylbewerbern	394
11.61	Einwilligungserklärung und damit Verzicht auf Ausübung des Grundrechts der informationellen Selbstbestimmung durch Minderjährige?	396
11.62	Anonyme Krankenhäuser	398
12	Infrastruktur und Landwirtschaft	401
12.1	Bekanntnis zur freiheitlichen demokratischen Grundordnung bei Ausschreibungen.....	401
12.2	Smarte Heizung – Datenleck?	402
12.3	LPG – nicht datengeschützt	404
12.4	Bodennutzungshaupterhebung	405
12.5	Veröffentlichung personenbezogener Daten in Überwachungsberichten der Immissionsschutzbehörde im Internet	406

12.6	Grundstücksgrenzen sind auch personenbezogene Daten	408
12.7	Thüringen in 3-D.....	410
12.8	Videouüberwachung im ÖPNV – Videogaga 4	411
12.9	PKW-Maut ohne flächendeckende Datenerhebung	413
12.10	Amtshilfe wegen MPU-Gutachten.....	414
12.11	Das Wageninnere: von Interesse auch für die Ordnungskräfte	415
12.12	Im Tower alles im Blick – Videogaga 5 – Videouüberwachung am Flughafen	416
12.13	Video im Bus – kein Muss – Videogaga 6.....	419
12.14	Tunnelblick	420
12.15	Erforschung der Energieeffizienz	422
12.16	Wolf unter Beobachtung – zu Wildkameras	425
13	Wirtschaft, Wissenschaft und digitale Gesellschaft ...	428
13.1	Auch Handwerkskammer unterliegt Auskunftsanspruch	428
13.2	Datenübermittlung einer Handwerkskammer ohne Einverständnis des Betroffenen.....	429
13.3	Widersprechende Angaben zur Einhaltung des Datenschutzes bei der GFAW mbH Erfurt	430
13.4	Gewerbedaten im Internet – nicht für unsichere Drittstaaten bestimmt!	432
13.5	Verarbeitung von Teilnehmerdaten bei EU-geförderten Projekten	434
13.6	Feuer (daten-) frei – Datenerhebung beim Bezirksschornsteinfeger	436
14	Bildung, Jugend, Sport	438
14.1	Arbeitskreis (AK) Datenschutz und Bildung	438
14.2	Unterarbeitskreis Datenschutz und Schule.....	441
14.3	Medienbildung tut not – TLfDI sorgt für Futter!	444
14.4	Medienschulen in Thüringen – kein Auslaufmodell!.....	446
14.5	Lernmanagementsystem neu denken!	447
14.6	Datenschutz im Hort	448
14.7	Schüler unter Beobachtung? – Videogaga 7	450
14.8	Handreichung zur Schulsozialarbeit.....	452
14.9	Erhebung von personenbezogenen Daten im Kultusbereich – zur Integration erforderlich	454
14.10	Anhörung zum Entwurf der Thüringer Fachschulordnung für die Bildungsgänge im Sozialwesen (ThürFSO-SW) .	455

14.11	Kein Muster für Schulleistungsuntersuchungen.....	456
14.12	Noten gehen nur die Betroffenen etwas an	457
14.13	Tresen-Lösung im Prüfungsamt	459
14.14	Betrugsverdacht bei Klausur – Einsicht in Smartphoneverläufe zulässig?.....	460
14.15	E-Mail zwischen Schule und Schulamt.....	461
14.16	Fakten, Fakten, Fakten: www.youngdata.de – nicht nur für Jugendliche!	462
14.17	Hänseleien bei der Bekanntgabe von Schulnoten vor der Klasse	463
14.18	Lehrkräfte führen privates Girokonto zu Schulzwecken?.....	464
14.19	Schülerdaten im Netz	465
14.20	Soziale Netzwerke in der Ausbildung im Vorbereitungsdienst für die Lehrämter	467
14.21	Weltweite Veröffentlichung von Schülernamen und Abiturprüfungszeiten	468
14.22	Elektronisches Klassenbuch: datenschutzrechtlich nicht ohne	470
14.23	Alte Klassenbücher: Oldies sind datenschutzrechtlich keine Goldies	472
14.24	BAföG21, Dialog21 und Kasse21	473
14.25	Novellierung des Thüringer Gesetzes über Schulen in freier Trägerschaft	474
14.26	Schule erhebt Gesundheitsdaten	475
14.27	Schüler an den Pranger gestellt: nichts dazu gelernt!.....	477
14.28	Datenschutzrechtliches O. K. für Schulportal?	478
14.29	Datenunfall bei Schülern? – Prüfung einer Panelstudie ..	480
14.30	Schule – Videogaga 8	481
14.31	Sicheres soziales Netzwerk für Thüringer Schulen!	483
14.32	Schweigepflichtentbindung an einer Schule	485
14.33	Schulunterricht online	486
14.34	Daten-Wolken auch für Schulen?	489
14.35	Behördliche Datenschutzbeauftragte an Schulen	490
14.36	Veröffentlichung personenbezogener Daten des Promovenden	494
14.37	Sicherheitslücken bei „thoska“	495
14.38	Prüfungsamt mit medizinischen Fähigkeiten?	497
14.39	Erhebung von Täternamen bei sexueller Gewalt?.....	498
14.40	Lehrer-Apps: kritisch	500

15	Entwicklungen der automatischen Datenverarbeitung ...	503
15.1	Verschlüsselung mit TrueCrypt	503
15.2	Ein Schritt vor, zwei zurück – ist die Verschlüsselung politisch wirklich gewollt?.....	505
15.3	Betriebssysteme mit Cloud-Anbindung – immer online .	507
15.4	Problem: Biometrische Gesichtserkennung	510
15.5	Verschlüsselung hilft nicht immer – auf die inneren Werte kommt es an	512
15.6	Ein neues „Labor“ beim TLfDI – Prüfung von Apps.....	513
15.7	IT-Sicherheitsgesetz nicht ohne Datenschutz!	514
15.8	Happy Birthday – die elektronische Gesundheitskarte wird 10 Jahre alt	517
15.9	Cloud-Computing 2.0 und Safe Harbor	518
15.10	Newsletter – immer datenschutzgerecht?	519
15.11	eIDAS – was ist das?	521
15.12	Kindergartengruppe 2.0 – Unvernunft der Großen zulasten der Kleinen.....	523
15.13	E-Government und Informationstechnik (IT) in der Thüringer Landesverwaltung	527
15.14	Straßenpanoramafahrten	528
15.15	YouNow – All know!.....	530
15.16	Daten gelöscht? – Datenschutzgerechte Entsorgung von Hardware.....	531
16	Technische Entwicklung in der Thüringer Landesverwaltung.....	533
16.1	Integrierte Teilhabeplanung nun als App	533
16.2	Optimierung eines Beihilfe-Kontrollverfahrens oder fragwürdiger Zugriff auf personenbezogene Daten von BALVI iP?	535
16.3	Oben ohne – Drohne!	537
16.4	Heimarbeit für Finanzbeamte.....	538
16.5	Windows XP – baufällig	540
16.6	Die Telemedizinplattform Thüringen – ein Blick in die Zukunft der Patientenversorgung	542
17	Vorträge – Der TLfDI ist unterwegs!.....	544

Anlagen**Entschlieungen der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder am 27./28. Mrz 2014 in Hamburg**

Anlage 1	Beschftigtendatenschutzgesetz jetzt!	546
Anlage 2	„Gewhrleistung der Menschenrechte bei der elektronischen Kommunikation“	548
Anlage 3	„Gewhrleistung der Menschenrechte bei der elektronischen Kommunikation“	550
Anlage 4	„ffentlichkeitsfhndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“	556
Anlage 5	Entschlieung der Konferenz der Datenschutzbeauftragten des Bundes und der Lnder zur Struktur der knftigen Datenschutzaufsicht in Europa	559
Anlage 6	„Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“	562
Anlage 7	Unsere Daten sicherer machen - wir selbst haben es in der Hand!	564

Entschlieungen zwischen den Konferenzen 2014

Anlage 8	Keine Vorratsdatenspeicherung in Europa!- Neue Mstbe fr den Datenschutz.....	567

**Entschlieungen der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder am 8./9. Oktober 2014 in Hamburg**

Anlage 9	Effektive Kontrolle von Nachrichtendiensten herstellen!	569
Anlage 10	Marktmacht und informationelle Selbstbestimmung	571
Anlage 11	Unabhngige und effektive Datenschutzaufsicht fr Grundrechtsschutz unabdingbar	573
Anlage 12	Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen	575
Anlage 13	Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert.....	578

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

Anlage 14	Datenschutz erfordert unabhängige Kontroll- behörden	580

Entschliefungen zwischen den Konferenzen 2014/2015

Anlage 15	Keine PKW-Maut auf Kosten des Datenschutzes! .	583
Anlage 16	Anforderungen an den Schutz der Datenübermittlun- gen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern	584
Anlage 17	Anforderungen an den Schutz der Datenübermittlun- gen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern (Anlage)	585
Anlage 18	Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!	593
Anlage 19	Keine Cookies ohne Einwilligung der Internetnutzer...	595

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

Anlage 20	Datenschutz nach „Charlie Hebdo“ Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristi- scher Bedrohung!	597
Anlage 21	Datenschutzgrundverordnung darf keine Mogelpackung werden!	599
Anlage 22	Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA	601
Anlage 23	Verschlüsselung ohne Einschränkungen ermöglichen..	602
Anlage 24	IT-Sicherheitsgesetz nicht ohne Datenschutz!	604
Anlage 25	Mindestlohngesetz und Datenschutz	607
Anlage 26	Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich	609
Anlage 27	Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten	611

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

Anlage 28	Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!	613

Entschlieungen zwischen den Konferenzen 2015

Anlage 29	Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken	615

**Entschlieungen der 90. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder am 30. September/1. Oktober 2015
in Darmstadt**

Anlage 30	Cloud-untersttzte Betriebssysteme bergen Datenschutzrisiken.....	617
Anlage 31	Verfassungsschutzreform bedroht die Grundrechte	619

**Beschluss der obersten Aufsichtsbehrden im Datenschutz im
nicht-ffentlichen Bereich (Dsseldorfer Kreis am 15./16.
September 2015)**

Anlage 32	Videberwachung in ffentlichen Verkehrsmitteln	621

Pressemitteilungen 2014

Anlage 33	Das Auto – Black Box auer Kontrolle	633
Anlage 34	 28 BDSG – nicht verzagen!	635
Anlage 35	EuGH kippt Richtlinie zur Vorratsdatenspeicherung – Hasse: Ein guter Tag, auch fr den Thringer Datenschutz	636
Anlage 36	Arbeitskreis Datenschutz und Bildung am 2. und 3. Juni 2014 beim Thringer Landesbeauftragten fr den Datenschutz und die Informationsfreiheit in Erfurt	638
Anlage 37	Arbeitskreis Datenschutz und Bildung in Erfurt richtungsweisend	639

Anlage 38	Videogaga: Europäischer Perspektivenwechsel ! ...	641
Anlage 39	EuGH-Urteil: „Recht auf Vergessen“ vs. Archive? – Nein!	643
Anlage 40	Nokia ante portas	644
Anlage 41	Datenverschlüsselung geht zur Schule! Ich mach's mit Safer Mail	645
Anlage 42	Keine PKW-Maut auf Kosten des Datenschutzes! .	646
Anlage 43	„Videogaga als Video“ Kurzfilm zur Videoproble- matik als Modul für den Schulunterricht	647
Anlage 44	In's Netz gegangen – Facebook Fortsetzung: Sachstand & Hinweise	648
Anlage 45	Weihnachtsgeschenk für den Datenschutz!	649
Anlage 46	Safe the Date "Safer Internet Day" am 10.02.2015 - Medienkunde als eigenes Schulfach -Neuland in Sicht?	650

Pressemitteilungen 2015

Anlage 47	Elektronische Gesundheitskarte ist nun Pflicht!	651
Anlage 48	Non vitae, sed scholae discimus?	653
Anlage 49	Krankenkasse als Fitnesscoach?	654
Anlage 50	Reminder "Safer Internet Day" am 10.02.2015 - Medienkunde als eigenes Schulfach - Neuland in Sicht?	655
Anlage 51	TLfDI fordert: Deutschland oben ohne – Drohne! .	656
Anlage 52	Sind sie noch da?	658
Anlage 53	YouNow – All know!	662
Anlage 54	Neuer Beirat beim TLfDI: Frischer Wind!	664
Anlage 55	Bei Anruf – Betrug!	665
Anlage 56	Datenschutzkonferenz verabschiedet Entschließung gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten	667
Anlage 57	Fingerabdruckscanner in der Schule – Finger weg! - TLfDI nimmt eingesetztes System unter die Lupe -	669
Anlage 58	Schutzbund der Senioren und Vorruheständler e.V. WANTED! Gesucht werden: Maus-Liebhaber!	670
Anlage 59	Windows 10 – Fenster zur Privatsphäre	671
Anlage 60	Aktenlager in Immelborn - Desaster mit Lerneffekt	672
Anlage 61	SeniorenComputerClub Erfurt – Start gelungen	674
Anlage 62	Unsafe harbor Datenschutzbeauftragter Dr. Hasse:	

	Der EuGH hat den „unsicheren Hafen“ endlich geschlossen	675
Anlage 63	Kein Wildwuchs mehr bei Videoüberwachung im ÖPNV	677
Anlage 64	NEU: Digitale Selbstverteidigung – Youngdata hat die Tipps für Kids	678
Anlage 65	Revolution beim 13. Arbeitskreis Datenschutz und Bildung Wow – das ging ab:	679
Anlage 66	Premiere: Heilmittel für Krankenhäuser TLfDI startet speziellen Blog zu Datenschutzproblemen im Gesundheitsbereich	680
Anlage 67	TLfDI startet als erster Landesdatenschützer ein Internet-Forum für Krankenhäuser!	681
Anlage 68	Datenschutzrechtliche Kernpunkte für die Trilog-verhandlungen der Datenschutz-Richtlinie im Bereich von Justiz und Inneres	682

Veranstaltungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit 2014

Anlage 69	4. Konferenz für Lehrer, Erzieher und Sonderpädagogische Fachkräfte	694
Anlage 70	Veranstaltung im Staatlichen Gymnasium Neuhaus/Rwg	695
Anlage 71	"Datenschutz in der verwaltungsgerichtlichen Justiz" Thüringer Verwaltungsrichterverein	696
Anlage 72	2. Tandemfortbildungsveranstaltung für Schulsozialarbeiterinnen und Schulleitungsmitglieder“ Thematik: Erfolgreiches Agieren im Rahmen des gesetzlichen Datenschutzes	697
Anlage 73	HWK Erfurt Veranstaltung, Wie kann ich vorsorgen... ..	698
Anlage 74	Gewerkschaft Erziehung und Wissenschaft Landesverband Thüringen (GEW)	699
Anlage 75	Datenschutz für Personalratsmitglieder THÜRINGER MINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND KULTUR (TMBWK)	700
Anlage 76	Datenschutz im Schulbereich und Einzelfälle Datenschutz in der Erwachsenenbildung Landesorganisation	

	der freien Träger in der Erwachsenenbildung e. V., LOFT	701
Anlage 77	Konsequenz bei Verstößen, Regelungen im ThürDSG	702

Veranstaltungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit 2015

Anlage 78	Veranstaltung der Fakultät für Mathematik und Informatik der FSU Jena.....	703
Anlage 79	Evangelisches Ratsgymnasium in Erfurt	704
Anlage 80	1. Datenschutztag Karl-Volkmar-Stoy-Schule Jena	705
Anlage 81	Vortrag am Staatlichen Berufsschulzentrum Kyffhäuser	706
Anlage 82	Fraktionsveranstaltung, Bündnis 90/Die Grünen....	707
Anlage 83	FSU Jena – Institut für Politikwissenschaft	708
Anlage 84	„Grundkenntnisse im Datenschutzrecht“ Thüringer Volkshochschulverband e.V.	709
Anlage 85	Veranstaltung der SPD Jena zur Vorratsdaten- speicherung der Gesetzentwurf der Bundesregierung zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten	710
Anlage 86	E-Mail-Verschlüsselung für GnuPG und Outlook, Kooperationsveranstaltung des ThILLM und des TLfDI.....	711
Anlage 87	„Datenschutz in sozialen Einrichtungen“ PARITÄTISCHE Akademie Thüringen	712
Anlage 88	Fachtagung der Kultusministerkonferenz KMK in Berlin	713
Anlage 89	Fachhochschule Erfurt, Angewandte Informatik	714
	Abkürzungsverzeichnis.....	715
	Sachregister	722

A Öffentlicher Bereich

Vorwort



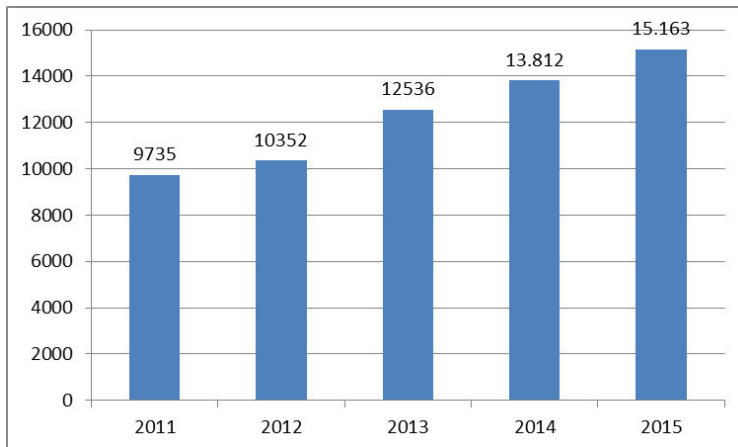
Dr. Lutz Hasse

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

öffentlichen Bereich in zwei gesonderten Bänden veröffentlicht werden.

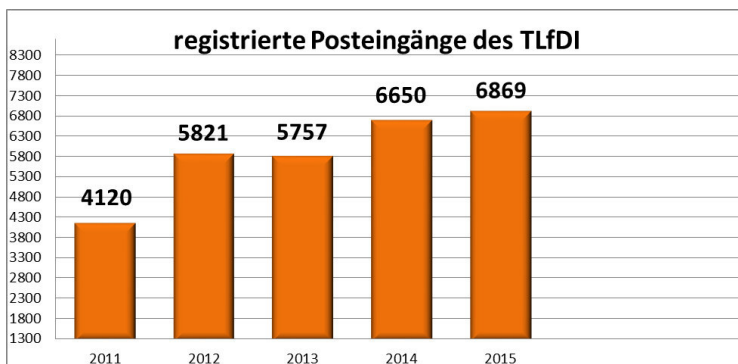
Vorab sei angemerkt, dass sich die Beiträge nahezu ausschließlich auf den Berichtszeitraum beziehen. Wenn es nach dem Ende des Berichtszeitraums eine wesentliche Änderung gegeben hat, gibt es einen entsprechenden Hinweis.

Insgesamt wurden beim TLfDI im Berichtszeitraum 28.975 Dokumente im Dokumentenmanagementsystem erstellt (13.812 im Jahr 2014 und 15.163 im Jahr 2015). Vergleicht man diese Zahlen mit denjenigen der letzten Jahre seit Einführung des Dokumentenmanagementsystems, ist ein kontinuierlicher Anstieg zu verzeichnen.



Diese Zahlen erfassen alle beim TLfDI elektronisch angelegten Dokumente, also Posteingänge und Postausgänge sowie interne Vermerke.

Sieht man sich lediglich die Posteingänge an, ergibt sich ein ähnliches Bild:



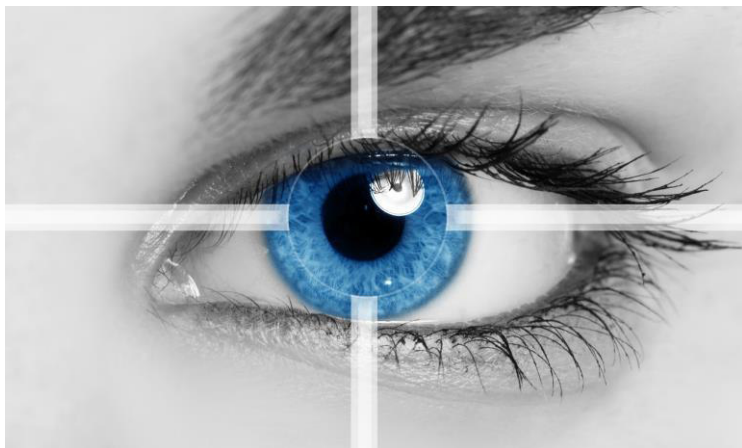
Auch in den Jahren 2014/2015 ist daher die personelle Situation der Behörde nach wie vor äußerst angespannt. Aufgrund der wachsenden Zahl der Eingaben und auch wegen der zunehmenden Komplexität datenschutzrechtlicher Fragestellungen kommt die Behörde immer wieder an ihre Grenzen. Anlassunabhängige Kontrollen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

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



Zur einfacheren Navigierbarkeit wurden die in diesem Tätigkeitsbericht verwendeten Links zusätzlich mit QR-Codes codiert. Die QR-Codes enthalten den Link in gerätelesbarer Form (beispielsweise der QR-Code links: <https://www.tlfdi.de/tlfdi/>). Dadurch kann auf Geräten mit Kamera (z. B. Smartphones oder Tablets) und einer entsprechenden

Software der Link durch das Gerät wieder decodiert werden und „Abschreibfehler“ können vermieden werden. Für Android-Smartphones kann der „Barcode Scanner“ des Entwicklers „Marty Mouse“ in der Version 1.0 empfohlen werden, da hier Open-Source-Software genutzt wird und die App nur minimale Funktionen besitzt. Für iOS ist dem TLfDI keine datenschutzgerechte App bekannt.



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

1 Schwerpunkte im Berichtszeitraum

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

Zu nennen ist auch die Safe-Harbor-Entscheidung des EuGH vom 6. Oktober 2015. Seit dem Tag der Entscheidung wechselten sich Abstimmungen, E-Mails über neueste Entwicklungen und Termine sowie Sondersitzungen der Datenschutzkonferenz im Tagesrhythmus ab. Zu klären war, welche Rechtsgrundlagen Behörden nach dem EuGH-Urteil, das die Safe-Harbor-Entscheidung für nichtig erklärt hatte, alternativ für Datenübermittlungen in die USA nutzen konnten (siehe dazu im Einzelnen Nr. 3.1 sowie Anlage 22).

Seit Ende Februar 2016 ist nunmehr mit "Privacy Shield" das geplante Nachfolgeabkommen zu "Safe Harbor" bekannt. Die Art. 29-Datenschutzgruppe der Europäischen Datenschutzbeauftragten hält aber auch die Privacy-Shield-Regelungen an mehreren Stellen für mit dem europäischen Datenschutzstandard nicht vereinbar.

Der Datenschutz in den Thüringer Kommunen war ebenfalls ein großer Aufgabenschwerpunkt im Berichtszeitraum: Als Klassiker in der Aufgabenstellung für den TLfDI sind hier die Übertragung von Sitzungen des Stadtrates im Internet sowie die Videoüberwachung durch Städte und Gemeinden zu nennen. Aber auch Kuriositäten fanden sich in der Aufgabenliste des TLfDI: Von unrechtmäßig erhobenen personenbezogenen Daten aus einer Unterschriftensammlung, über Anrufe angeblicher Interessenten (mystery calls) bei Hotels und Pensionen im Thüringer Wald bis hin zum Fund einer ausgemusterten Festplatte mit personenbezogenen Daten aus einem kommunalen Betrieb auf einer Müllkippe war alles dabei.

Sehr viele Fälle gab es auch im Bereich des Beschäftigtendatenschutzes. Die fortschreitende Technologisierung der Arbeitswelt ermöglicht es den Dienstherren, auf immer leichterem Weg Mitarbeiter zu überwachen. Im medizinischen Bereich ist die Tendenz zu verzeichnen, dass die verschiedenen Akteure sich zum Informationsaustausch immer stärker vernetzen. Dies betrifft den Bereich der Forschung aber auch die konkrete Behandlung eines Patienten. Hier gilt es, streng darauf zu achten, dass die Datenübertragung sicher ist und die Zugriffsrechte sich an der Erforderlichkeit der Aufgabenerfüllung orientieren.

Die Informationstechnik (IT) hat nun endgültig nicht nur im privaten Sektor, sondern auch im öffentlichen Sektor Einzug gehalten. Kaum ein Lebensbereich ist heutzutage noch ohne IT denkbar. Innerhalb der Cyberkriminalität werden zunehmend zwei Trends sichtbar. Seit Jahren versuchen Hacker private Rechner zu kapern, um Daten auf den Rechnern auszuspionieren, die elektronische Kommunikation

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

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



Datenschutz — © fotodo / Fotolia.com

2 Allgemeine Entwicklungen im Datenschutz

2.1 Überblick

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

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

richtsentscheidungen für den Datenschutz von besonderer Bedeutung gewesen:

Der Deutsche Bundestag hatte am 20. März 2014 auf Antrag aller Fraktionen die Einsetzung eines Untersuchungsausschusses beschlossen (BT Drucks. 18/843), der die Hintergründe und das Ausmaß ausländischer nachrichtendienstlicher Ausspähungen aufklären soll (NSA-Untersuchungsausschuss). Dieser war im Berichtszeitraum noch nicht abgeschlossen, sodass über den Abschluss und die Ergebnisse wohl erst im kommenden Tätigkeitsbericht berichtet werden kann. Der TLfDI hatte bereits in seinem 10. Tätigkeitsbericht (siehe 10. Tätigkeitsbericht, Nummer 2.2 Snowden, NSA, PRISM, Tempora und Antiterrordatei – das Jahr 2013 als „datenschutzrechtlicher Durchlauferhitze“, Seite 26) darauf hingewiesen, dass die Bundesregierung gefordert bleibe, auf politische Lösungen hinzuwirken. Vielleicht bewirken die Empfehlungen des NSA-Untersuchungsausschusses, die es mit Sicherheit nach Beendigung seiner Arbeit geben wird, einen verbesserten Schutz von personenbezogenen Daten gegenüber deutschen und anderen Geheimdiensten. Neben dem wegweisenden Urteil des Europäischen Gerichtshofes (EuGH) zu Safe Harbor dürfen an dieser Stelle auch zwei weitere wichtige Urteile nicht unerwähnt bleiben:

Mit seinem Urteil vom 8. April 2014 (Az.: C-293/12 und C-594/12 [verbundene Rechtssachen]) erklärte der EuGH die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, für ungültig. Der EuGH stellte in seiner Entscheidung fest, dass die Verpflichtung zur Vorratsdatenspeicherung und der Zugriff der zuständigen nationalen Behörden auf diese Daten ein besonders schwerwiegender Eingriff der Richtlinie in die Grundrechte auf die Achtung des Privatlebens und auf Schutz personenbezogener Daten ist. Aus der Gesamtheit der Daten könnten genaue Rückschlüsse auf die Gewohnheiten von Personen, ihre Aufenthaltsorte, ihre ausgeübten Tätigkeiten und auch auf das soziale Umfeld gezogen werden. Der EuGH urteilte, dass der europäische Gesetzgeber beim Erlass der Richtlinie die Grenze der Verhältnismäßigkeit überschritten habe. Die Datenschutzbeauftragten des Bundes und der Länder begrüßten diese Entscheidung des EuGH und wiesen in ihrer Entschließung „Keine Vorratsdatenspeicherung in Europa!“ vom 25. April 2014 (siehe hierzu Anlage 8) darüber hinaus ausdrücklich

darauf hin, dass der Maßstab des EuGH auch für das anlasslose, exzessive Überwachen durch sämtliche Nachrichtendienste gelten müsse.

Nichtsdestotrotz trat am 18. Dezember 2015 in Deutschland das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten in Kraft (Drucksache 18/5088). Quasi „durch die Hintertür“ wurde damit zugleich der neue Straftatbestand der Datenhehlerei eingeführt, § 202d Strafgesetzbuch. Diesem Straftatbestand wird zur Last gelegt, dass er unpräzise formuliert sei und daher eine kritische Berichtrecherche durch Journalisten zumindest behindern kann. Es bleibt daher spannend abzuwarten, ob auch diese Regelungen wieder einmal vom Bundesverfassungsgericht aufgehoben werden.

Mit seiner Entscheidung vom 13. Mai 2014 (Az.: C-131/12 „Google Spain“) urteilte der EuGH, dass ein Suchmaschinenbetreiber (hier: Google Spain) unter bestimmten Voraussetzungen verpflichtet ist, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über eine Person von seiner Ergebnisliste entfernen muss. Der EuGH schuf mit diesem Urteil das „Recht auf Vergessenwerden“, das auch die neue Europäische Datenschutzgrundverordnung (DSGVO) erstmals in Art. 17 regelt. Betroffene Personen können sich nach dem EuGH-Urteil nunmehr direkt an die jeweiligen Suchmaschinenbetreiber wenden und von ihnen verlangen, dass bei der Suche einzelne Links zu ihrem Namen nicht mehr angezeigt werden. Unangetastet lässt das Urteil die Löschung der Inhalte selbst, diese bleiben weiterhin frei zugänglich. Der EuGH entschied, dass der Suchmaschinenbetreiber selbst Daten verarbeite und somit als verantwortliche Daten verarbeitende Stelle zu qualifizieren sei. Da es sich bei Google Spain um eine Tochtergesellschaft von Google Inc. in Spanien handele, sei diese als Niederlassung im Sinne der Europäischen Datenschutzrichtlinie 95/46/EG anzusehen.

Die Datenschutzbeauftragten des Bundes und der Länder sahen in dem Urteil einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Oktober 2014; „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ (siehe dazu Anlage 12). Das Urteil muss nun von den einzelnen Suchmaschinenbetreibern umgesetzt werden.

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

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

2.2 Wann dürfen öffentliche Stellen einen externen Datenschutzbeauftragten haben?

Immer wieder wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit sowohl von öffentlichen Stellen als auch von externen Datenschutzbeauftragten gefragt, ob eine Bestellung eines externen Datenschutzbeauftragten möglich ist, ohne dass dieser Beschäftigter der öffentlichen Stelle ist. Diese Frage beantwortet das Gesetz klar. Nach § 10a Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) haben Daten verarbeitende Stellen, die personenbezogene Daten mithilfe automatisierter Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Aus dieser Formulierung geht hervor, dass der Beauftragte für den Datenschutz Beschäftigter der jeweiligen öffentlichen Stelle sein muss. Eine Ausnahme besteht nach § 10a Abs. 6 ThürDSG für die staatlichen Schulen. Hier kann die Aufsichtsbehörde einen ihrer Beschäftigten zum Beauftragten für den Datenschutz bestellen.

Etwas anderes gilt für juristische Personen oder sonstige Vereinigungen, die nach § 2 Abs. 2 ThürDSG als öffentliche Stellen gelten, wenn sie am Wettbewerb teilnehmen. In diesem Fall sind nach § 26 ThürDSG auf sie die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mit Ausnahme des zweiten Abschnitts des § 38 anwendbar. Dies betrifft beispielsweise öffentliche Schwimmbäder oder Krankenhäuser. Die einschlägige Regelung des § 4f BDSG enthält eine derartige Beschränkung auf eigene Beschäftigte nicht.

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

2.3 Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes (BMG)

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

Darüber hinaus äußerte sich der TLfDI im Rahmen des Anhörungsverfahrens gemäß § 112 Abs. 4 Geschäftsordnung des Thüringer Landtags gegenüber dem zuständigen Ausschuss zum o. g. Thema.

Seit dem 23. September 2015 ist das Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes in Kraft (GVBl. S. 131).

Im Ergebnis wurden die aus datenschutzrechtlicher Sicht erforderlichen Änderungswünsche des TLfDI zum Teil umgesetzt. So wurde der Forderung entsprochen, bei der Datenübermittlung zwischen den Meldebehörden das Übertragungsprotokoll OSCI-Transport und bei der Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften auch das Übertragungsprotokoll OSCI-Transport einzusetzen, wenn die öffentlich-rechtlichen Religionsgesellschaften dem zugestimmt haben. Somit werden die Daten mittels einer Ende-zu-Ende-Verschlüsselung sicher übertragen, sodass kein Unbefugter Kenntnis erlangen kann.

Leider wurden die bestehenden datenschutzrechtlichen Bedenken und Ergänzungswünsche bezüglich § 2 Abs. 1 Nr. 2 ThürAGBMG nicht aufgenommen.

Eine verbindliche Regelung zur Löschung dieser Daten wird weiterhin für dringend erforderlich erachtet. Wenn es bspw. in einem Wahl- bzw. Abstimmungsbezirk nur eine Unterstützerliste gab, kann später immer noch genau recherchiert werden, welcher Bürger eine Unterstützungsunterschrift leistete. Selbst bei zwei Unterstützerlisten kann gerade im ländlichen Gebiet später u. U. noch eine Zuordnung möglich sein.

Mit Wirkung vom 1. November 2015 ist die Thüringer Meldeverordnung (GVBl. 2016, 49) in Kraft getreten, an der der TLfDI seitens des Thüringer Ministeriums für Inneres und Kommunales (TMiK) ebenfalls beteiligt wurde und über die er im Einzelnen im nächsten Tätigkeitsbericht informieren wird.

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

2.4 Datenerfassung beim Waffenregister – verkannt?

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

Datenschutz und die Informationsfreiheit (TLfDI) im 10. Tätigkeitsbericht unter Punkt 2.9. Zudem berichtete der TLfDI über eine Kontrolle in einer Waffenbehörde, bei der Mängel zutage traten.

Infolgedessen kontrollierte der TLfDI 2015 erneut diese sowie eine weitere Waffenbehörde, um den Umgang mit personenbezogenen Daten zu überprüfen. Wie bereits 2013 festgestellt, waren in der betreffenden Waffenbehörde die Unterlagen in Regalen und nicht, wie erforderlich, in verschließbaren Schränken untergebracht.

Auch nach einer entsprechenden Beanstandung im März 2014 wurden die notwendigen Vorkehrungen aus haushaltstechnischen Gründen nicht getroffen.

Sowohl bei der Kontrolle 2015 als auch zum Redaktionsschluss des vorliegenden Tätigkeitsberichtes waren die vorhandenen offenen Regale weiterhin nicht durch zusätzliche Türen geschützt oder durch neue Schränke ausgetauscht worden.

Wegen der weiterhin offen zugänglichen Lagerung von Unterlagen ist deshalb nicht auszuschließen, dass außerhalb der Bürozeiten oder in der Urlaubszeit des zuständigen Sachbearbeiters die in den Unterlagen enthaltenen personenbezogenen Daten von unbefugten Dritten zur Kenntnis genommen werden können.

Dies stellt weiterhin einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Die zwischenzeitlich getroffene organisatorische Festlegung, dass keine Unbefugten ohne Anwesenheit einer berechtigten Person Zugang zu den Büros der Waffenbehörde haben dürfen, mildert diesen festgestellten Verstoß aus Sicht des TLfDI nicht ab.

Dem TLfDI wurde auf Nachfrage mitgeteilt, dass im Haushaltsplan 2016 vom zuständigen Fachamt finanzielle Mittel zur Nachrüstung angemeldet wurden. Sofern der Haushaltsplan 2016 vom Kreistag bestätigt und durch die Aufsichtsbehörde genehmigt wird, würde entsprechend nachgerüstet werden.

Weiterhin wurde im Zuge der Kontrollen in den betreffenden Waffenbehörden bei einer stichprobenartigen Prüfung der Eingabemasken bezüglich des lokalen Waffenregisters festgestellt, dass die Eingabefelder „Erlerner Beruf“ und „derzeit ausgeübter Beruf“ vorhanden waren. Der TLfDI musste dabei feststellen, dass bei einer Anzahl von Datensätzen diese Angaben auch ausgefüllt waren. Auch das papiergebundene Formular „Antrag auf Erteilung einer waffenrechtlichen Erlaubnis“ enthält beide Felder „Erlerner Beruf“ und „derzeit ausgeübter Beruf“. Auf Nachfrage zur Notwendigkeit der

Felder erhielt der TLfDI in beiden Waffenbehörden die Antwort, dass man diese Angaben eigentlich nicht benötige. Regelungen, wann diese Felder auszufüllen sind, seien auch nicht vorhanden.

Gemäß § 6 Waffengesetz (WaffG) ist die persönliche Eignung von Personen zum Besitz von Waffen zu beurteilen. Dies kann aus Sicht des TLfDI grundsätzlich aber unabhängig vom Beruf der zu beurteilenden Person erfolgen. Allerdings gesteht der TLfDI dem Datum „derzeit ausgeübter Beruf“ immerhin eine Indizwirkung zu, wenn besondere Erlaubnistatbestände für bestimmte Personengruppen eine Rolle beim Erteilen der Waffenerlaubnis zu berücksichtigen sind. So kann gemäß WaffG bei Jägern (§ 13), Sachverständigen (§ 18), gefährdeten Personen (§ 19), Waffenherstellern und Waffenhändlern (§§ 21, 26), Bewachungsunternehmen und Bewachungspersonal (§§ 28, 28a) der Beruf tatsächlich als allgemeines Kriterium zur Beurteilung der persönlichen Eignung von Personen zum Besitz von Waffen Verwendung finden.

Eine Erfassung des erlernten und des derzeit ausgeübten Berufes bei allen Antragstellern sieht der TLfDI allerdings nicht für erforderlich an. Deshalb bat er die betroffenen Waffenbehörden um Stellungnahmen bis Ende März 2016, um ggf. landes- oder bundesweit eine einheitliche Lösung anzustreben. Diese sind zwischenzeitlich eingetroffen und werden im kommenden Berichtszeitraum geprüft.

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

2.5 Wissensdurstige Meldebehörde – nach dem neuen Bundesmeldegesetz Durst zulässig

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde eines Hausverwalters, der sich erkundigte, ob folgendes Auskunftersuchen der Meldebehörde zulässig sei: Als ein durch den Wohnungsgeber beauftragter Hausverwalter habe er Daten eines Mieters der Meldebehörde mitteilen müssen.

Als Wohnungsgeber gemäß § 17 des neuen Bundesmeldegesetzes (BMG) kommt grundsätzlich der Wohnungseigentümer, mit dem ein

Mietvertrag geschlossen wird, in Betracht. Es kann sich aber auch um den Hauptmieter handeln, mit dem ein Untermietverhältnis besteht.

Grundsätzlich bestehen verschiedene Mitwirkungsverpflichtungen des Wohnungsgebers oder einer von ihm beauftragten Person im Zusammenhang mit Meldeangelegenheiten nach dem BMG.

Zunächst hat der Wohnungsgeber nach dem BMG den Einzug oder den Auszug der meldepflichtigen Person, also dem Mieter, schriftlich oder elektronisch innerhalb der in § 17 Absatz 1 oder 2 BMG genannten Fristen zu bestätigen (§ 19 Abs. 1 S. 2 BMG). Diese Verpflichtung besteht seit dem 1. November 2015, dem Inkrafttreten des neuen BMG.

Die Auskunftspflicht des Wohnungsgebers gegenüber dem Mieter zur Vorlage bei der Meldebehörde nach § 19 Abs. 1 S. 2 BMG umfasst folgende Angaben:

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

Verweigert der Wohnungsgeber diese Bestätigung, hat der Mieter als meldepflichtige Person dies der Meldebehörde unverzüglich mitzuteilen. Versäumt der Wohnungsgeber das Ausstellen der Bestätigung, sieht das Bundesmeldegesetz dafür Bußgelder von bis zu 1.000 Euro vor. Bis zu 50.000 Euro Bußgeld sind möglich, wenn eine Person nur zum Schein in einer Immobilie angemeldet wird.

Daneben beinhaltet die in § 19 BMG geregelte Mitwirkungspflicht auch die Auskunft des Eigentümers und, wenn er nicht selbst Wohnungsgeber ist, auch vom Wohnungsgeber über die Personen, welche bei ihm wohnen oder gewohnt haben. Diese Auskunftsverpflichtung des Eigentümers oder des Wohnungsgebers ergibt sich aus § 19 Abs. 5 BMG.

Der vom Beschwerdeführer dargelegte Sachverhalt ist der Auskunftsverpflichtung des Wohnungsgebers nach § 19 Abs. 5 BMG zuzuordnen, da sich die Meldebehörde unmittelbar an ihn als vom Wohnungsgeber beauftragte Person gewandt hatte. Der Beschwerdeführer hat keine Tatsachen vorgetragen, die darauf schließen lassen könnten, dass das Auskunftsbegehren der Meldebehörde unzulässig

gewesen sei. Deswegen war vom TLfDI in dieser Angelegenheit nichts weiter zu monieren oder zu beanstanden.

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

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

2.6 Endlich eine Orientierungshilfe zur Videoüberwachung

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

Bereits im letzten Berichtszeitraum war bei allen Aufsichtsbehörden im nicht-öffentlichen Bereich zu beobachten, dass die Videoüberwa-

chung einen immer größeren Stellenwert einnimmt. Dies lag sicherlich auch daran, dass Kameras und Videoüberwachungssysteme zu immer günstigeren Preisen angeboten wurden. Größere Unternehmen haben Filialen in mehreren Bundesländern. Besonders sie waren daran interessiert, dass die datenschutzrechtliche Beurteilung der Videoüberwachung von den Aufsichtsbehörden im Bundesgebiet einheitlich vorgenommen wird. Die Datenschutzkonferenz rief daher eine Ad-hoc-AG Videoüberwachung als Unterarbeitsgruppe des Düsseldorfer Kreises ins Leben. Diese Arbeitsgruppe sollte sich mit speziellen Fragen der Videoüberwachung befassen und dafür sorgen, dass unbestimmte Rechtsbegriffe im Bundesgebiet von Aufsichtsbehörden möglichst einheitlich ausgefüllt werden. Schnell war man sich einig, dass es einer Orientierungshilfe bedarf, um das komplexe Feld der Videoüberwachung datenschutzrechtlich möglichst bundeseinheitlich bewerten zu können. Es gibt im Wesentlichen drei Bestimmungen, nach denen sich die datenschutzrechtliche Beurteilung einer Videoüberwachung richtet:

Dies sind § 6b Bundesdatenschutzgesetz (BDSG) für die Videoüberwachung in öffentlich zugänglichen Bereichen, § 28 BDSG für die Videoüberwachung in öffentlich nicht zugänglichen Bereichen und § 32 BDSG für den Fall, dass Mitarbeiter überwacht werden.

Alle drei Bestimmungen enthalten einige unbestimmte Rechtsbegriffe, die es auszufüllen galt. In mehreren Sitzungen wurde die OH „Videoüberwachung durch nicht-öffentliche Stellen“ erarbeitet und schließlich vom Düsseldorfer Kreis mit Stand vom 19. Februar 2014 beschlossen. Die OH ist auf der Homepage des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) unter https://tlf-di.de/imperia/md/content/datenschutz/orientierungshilfe/oh_v___durch-nicht-__ffentliche-stellen.pdf veröffentlicht.



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

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

Im Berichtszeitraum stellte sich schnell heraus, dass es weitere Sonderprobleme der Videoüberwachung gibt. Die Ad-hoc-AG wurde daher verstetigt und tagt nunmehr regelmäßig. Sie hat für zwei weitere Bereiche potentieller Videoüberwachung Regelungen getroffen. Zum einen wurde die OH „Videoüberwachung in öffentlichen Ver-



kehrsmitteln“ erarbeitet und vom Düsseldorfer Kreis mit Stand vom 16. September 2015 beschlossen, zum anderen wurde ein Zusatz zur OH „Videoüberwachung durch nicht-öffentliche Stellen“ zur Videoüberwachung in Schwimmbädern erarbeitet. Dieser Zusatz ist unter

[https://www.tlfdi.de/imperia/md/content/dat](https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/01_zusatz_zur_oh_v__.pdf)
en-

schutz/orientierungshilfe/01_zusatz_zur_oh_v__.pdf auf der Homepage des TLfDI veröffentlicht. In dem Zusatz werden ergänzend zur OH „Videoüberwachung durch nicht-öffentliche Stellen“ spezielle Probleme, die in Schwimmbädern auftauchen datenschutzrechtlich beurteilt. Bereits in seinem 9. Tätigkeitsbericht zum Datenschutz im öffentlichen Bereich hatte der TLfDI unter Nr. 5.5 über die Schwierigkeiten bei datenschutzrechtlichen Kontrollen in Frei- und Hallenbädern berichtet. Nunmehr liegen auch hier bundeseinheitliche Anforderungen vor und der TLfDI kann bei seinen Prüfungen nun die mit den anderen Aufsichtsbehörden abgestimmten Anforderungen anwenden.

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

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



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

3 Europäischer und Internationaler Datenschutz

3.1 Safe Harbor – Anlegen verboten

Der 6. Oktober 2015 war ein guter Tag für den Datenschutz. Die Luxemburger Richter des Europäischen Gerichtshofes (EuGH) urteilten, dass die Entscheidung der Europäischen Kommission vom 26. Juli 2000 (2000/520/EG) über die Gewährung eines angemessenen Datenschutzniveaus auf der Grundlage des Safe-Harbor-Abkommens (Übersetzung wörtlich: „Sicherer-Hafen-Abkommen“) für Übermittlungen von Daten in die USA keine Gültigkeit mehr besitze (Az.: C-362/14).

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sowie die anderen Datenschutzbeauftragten des Bundes und der Länder hatten bereits nach den Enthüllungen von Edward Snowden im Sommer 2013 immer wieder die Aussetzung der Übermittlung personenbezogener Daten auf der Grundlage des Safe-Harbor-Abkommens gefordert, da nach Ansicht der deutschen Datenschutzbeauftragten das Abkommen keinen ausreichen-

den Schutz vor Eingriffen in das Grundrecht auf informationelle Selbstbestimmung durch die amerikanischen (Sicherheits-)Behörden biete. Die USA verfügten demnach nicht über ein für europäische Standards notwendiges angemessenes Datenschutzniveau. Dies wurde nunmehr durch die Richter des EuGH bestätigt. Als Folge des Urteils wird der TlfdI zunächst die Übermittlung von personenbezogenen Daten, die sich ausschließlich auf das Safe-Harbor-Abkommen stützen, untersagen und gegebenenfalls mit den ihm zur Verfügung stehenden Mitteln ahnden.

Im Lichte des EuGH-Urteils sind aber darüber hinaus auch die Datenübermittlungen in die USA, basierend auf EU-Standardvertragsklauseln oder so genannten verbindlichen Unternehmensregelungen (auf Englisch: Binding Corporate Rules (BCR)) höchst fraglich geworden. In jedem Fall werden die deutschen Datenschutzbehörden keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von BCR oder Datenexportverträgen erteilen. Zu klären ist auch, ob und inwieweit Datenübermittlungen aufgrund einer Einwilligung der Betroffenen vorgenommen werden können.

Der EuGH stellte in seinem Urteil weiter fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten unabhängig von der Entscheidung der Kommission nicht daran gehindert sind, die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen. Schwierig wird es jedoch, die Entscheidungen der Kommission rechtlich anzugreifen, da den Datenschützern bisher kein eigenes Klagerecht zur Verfügung steht. Hier ist – so der EuGH – der Gesetzgeber gefordert, ein entsprechendes Klagerecht gesetzlich zu verankern.

Diese und weitere Punkte wurden auf einer Sondersitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) am 21. Oktober 2015 in einem Positionspapier zusammengetragen (siehe Anlage 68).

Die „Schonfrist“ für Unternehmen, ihre Arbeitsabläufe entsprechend datenschutzkonform anzupassen bzw. neu zu regeln, lief bis zum 31. Januar 2016 und wurde dann noch einmal bis zum 29. Februar 2016 verlängert. Das mittlerweile von der EU-Kommission vorgelegte geplante Privacy-Shield-Abkommen wird aber nicht nur von der Artikel 29-Datenschutzgruppe als dringend nachbesserungswürdig erachtet. Die Kompetenzen und die Unabhängigkeit einer Ombudsperson für datenschutzrechtliche Belange von EU-Bürgerinnen und Bürgern in den USA erscheint dabei

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

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

3.2 Die Datenschutzgrundverordnung: Trilog beendet und alles auf Anfang!

DSGVO – wissen Sie, was sich hinter dieser ominösen Abkürzung versteckt? Nein? Aufklärung ist in jeder Hinsicht dringend geboten: Diese Abkürzung steht für die Datenschutzgrundverordnung – im Amtsdeutsch der Europäischen Union (EU) auch „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung)“ genannt. Das Ausmaß dieser neuen Regelung ist den meisten Bürgern bisher ebenso unbekannt wie vielen Betrieben und Behörden. Dennoch soll die DSGVO im wahrsten Sinne „für alle“ gelten, denn zum ersten Mal vereint sie ein Regelwerk, dass sowohl im öffentlichen Bereich, also für Landes- und Kommunalbehörden, als auch im nicht-öffentlichen Bereich, also für Betriebe, unmittelbare Anwendung findet. Die DSGVO soll die „alte“ Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 ablösen und unmittelbar in allen Mitgliedstaaten der EU gelten.

Rückblende: Die Vorarbeiten für die Entstehung einer DSGVO reichen bis ins Jahr 2012 zurück. Zuerst erarbeitete die Europäische Kommission einen Vorschlag für eine DSGVO (Vorschlag vom 25. Januar 2012 KOM[2012]11 endgültig; 2012/0011 [COD]) es folgte ein Beschluss des Europäischen Parlaments vom 12. März 2014. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) begleitete bereits diese Phase des Entstehungsentwurfs, indem sie in Form von zwei Entschlüssen

zum Gesetzgebungsverfahren Stellung bezog (siehe dazu die Entschlüsse vom 28. März 2014 und 19. März 2015 in der Anlage 5 und 21).

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

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

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

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

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

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

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

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

Als große Herausforderung für alle deutschen Datenschutzbeauftragte, aber auch die übrigen Datenschutzbehörden in der EU ist das völlig neu geschaffene Kohärenzverfahren (Artikel 57 ff. DSGVO) anzusehen. Dieses regelt erstmals, wie sich die zuständigen Datenschutzbehörden untereinander und mit dem Europäischen Datenschutzausschuss zu verständigen haben, wenn zum Beispiel ein großer europäischer Konzern mit Hauptsitz in einem EU-Mitgliedstaat und Niederlassungen in mehreren anderen EU-Mitgliedstaaten verbindliche unternehmensinterne Datenschutzvorschriften zur Anwendung bringen will, die von der federführenden Aufsichtsbehörde nach § 43 DSGVO zu genehmigen sind.

Spannend zu beobachten wird es schließlich sein, inwiefern die deutsche Bundesregierung bis zur Bundestagswahl im Herbst 2017 imstande sein wird, diese Öffnungsklauseln „mit Leben zu füllen“ und insgesamt ein Rahmengesetz zur DSGVO als Nachfolgesetz zum BDSG auf den Weg zu bringen.

In einem solchen Gesetz wird sich sehr wahrscheinlich auch eine Regelung wiederfinden, welche deutsche Datenschutzbehörde die Bundesrepublik Deutschland im neu einzurichtenden Europäischen Datenschutzausschuss vertreten darf.

Am 14. April 2016 hat das Europäische Parlament die DSGVO verabschiedet. Nach anschließender Veröffentlichung der DSGVO im Amtsblatt der EU wird diese sehr wahrscheinlich noch im Mai 2016 in Kraft treten.

Anschließend bleibt allen Anwendern dieses neuen Regelungswerkes eine Übergangsfrist von zwei Jahren, sodass die DSGVO spätestens im Frühjahr 2018 für alle Betroffenen anzuwenden ist. Der TLfDI wird diesen Einführungs- und Anwendungsprozess intensiv begleiten

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

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

3.3 Die JI-Richtlinie – war da was?

Großen Beratungs- und Gesprächsbedarf verursachte im Berichtszeitraum des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Datenschutzgrundverordnung (DSGVO) (siehe dazu Nummer 3.2). Ein unbedeutendes Schattendasein im Vergleich dazu fristete die so genannte JI-Richtlinie – wobei der Buchstabe J für Justiz und der Buchstabe I für Inneres steht. Die korrekte Bezeichnung dieser Richtlinie lautet: „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“.

Das Ziel dieser Richtlinie ist gemäß ihres Artikels 1 Abs. 1 die Aufstellung von „Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt.“

Dass der JI-Richtlinie keine große Beachtung in der Öffentlichkeit geschenkt wurde, lag zum einen daran, dass sie von der Kommission bereits am 25. Januar 2012 sozusagen „im Doppelpack“ mit der DSGVO vorgestellt wurde und ab Herbst 2015 dann auch im Trilog-Verfahren wieder zusammen mit der DSGVO beraten wurde. Deshalb war es auch nicht weiter verwunderlich, dass sowohl der Stand-

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

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

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

verarbeitung für diesen anderen Zweck als erforderlich und verhältnismäßig erachtet.

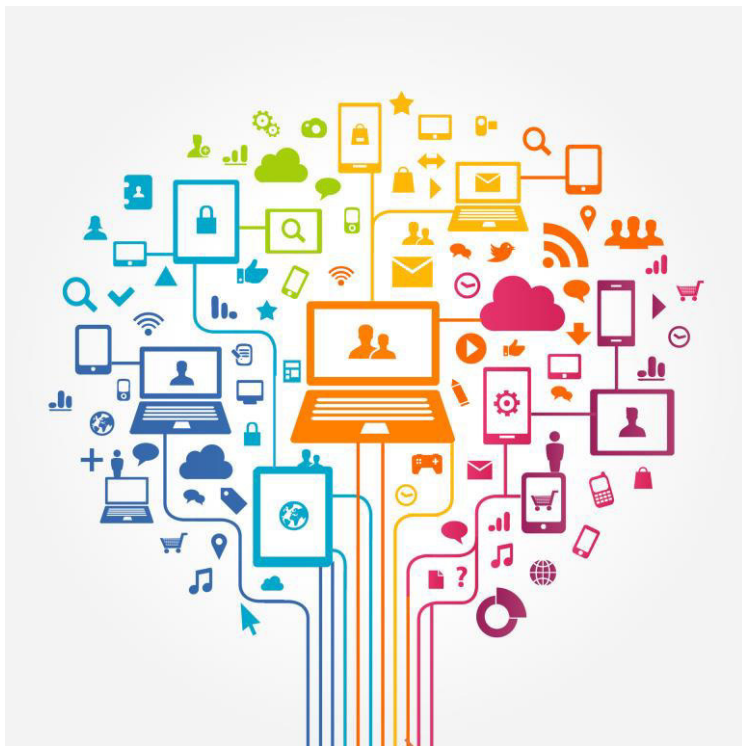
Dieses Beispiel aus Artikel 4 Abs. 2 der JI-Richtlinie offenbart eine ihrer Hauptschwächen: Ihrer Zielsetzung, ein zentrales Regelungswerk für den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit zu schaffen, wird die JI-Richtlinie nicht gerecht. Dies verhindern allein schon die vielen Öffnungsklauseln, die den Mitgliedstaaten eine nationale Regelungsmöglichkeit offerieren.

Eine weitere Regelung, die zu weniger statt zu mehr Rechtsklarheit im Bereich des Datenschutzes führen wird, ist Artikel 59 der JI-Richtlinie: Dieser bestimmt, dass besondere Bestimmungen zum Schutz personenbezogener Daten, die in vor Erlass dieser Richtlinie im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit erlassenen Rechtsakten der Union enthalten sind, von der JI-Richtlinie unberührt bleiben sollen. Das bedeutet: Der speziellere Rechtsakt, der vor der JI-Richtlinie in Kraft getreten ist, verdrängt diese in ihrer Anwendung. Das erhöhte Prüfungsaufkommen in Polizei und Justiz, welches EU-Regelungswerk, das der JI-Richtlinie zeitlich vorausgegangen ist, spezieller als diese ist, darf man sich bereits jetzt konkret ausmalen.

Angesichts dieser fragwürdigen Fortschritte, die die JI-Richtlinie für Polizei und Justiz im Bereich des Datenschutzes bereithält, fragen sich nicht wenige Datenschützer und Rechtsprofessoren, ob das „wirklich Neue“ des Regelungswerkes nicht darin zu sehen ist, was nicht in der Richtlinie zu Papier gebracht worden ist: die Anwendung der Grundrechte aus der Charta der Grundrechte der EU (GR-Charta) auch auf deutsche Straf- und Polizeigesetze gemäß Art. 51 GR-Charta. Denn da die nationalen Gesetze nunmehr auch von der JI-Richtlinie berührt werden, wirken die Grundrechte der GR-Charta auf diese Normen der Mitgliedstaaten ein. Das hätte für die Bundesrepublik Deutschland zur Folge, dass sich künftig nicht mehr nur das Bundesverfassungsgericht und die Verfassungsgerichte der Länder, sondern auch der Europäische Gerichtshof in Luxemburg mit der Frage beschäftigen könnten, ob deutsche Straf- und Polizeigesetze gegen Grundrechte verstoßen.

Mit der Umsetzung dieser Richtlinie in deutsches Recht wird sich beim TLfDI unter anderem eine Polizistin beschäftigen, die seit Ende März 2016 für insgesamt sechs Monate von der Thüringer Landespolizeidirektion abgeordnet worden ist.

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



internet – © Julien Eichinger / Fotolia.com

4 Neue Medien – Rundfunk – Telekommunikation

4.1 Melderegisterdaten für ARD, Günter Jauch und Co.?

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

müsse oder ob sie sich ggf. darauf berufen könne, dass die Datenübermittlung unzulässig sei und die Gebührenforderung deshalb als eine Art Werbung angesehen werden könne. Als „kleiner Bürger“ wolle sie zudem nicht für die Gagen von Herrn Günter Jauch und Co. aufkommen.

Der TLfDI hat die Bürgerin hinsichtlich des Verfahrens der Gebührenbeitreibung mittels Meldeamtsdaten informiert und auf den Beschluss des Obergerichts Lüneburg verwiesen (Az. 4 ME 204/13). Darin hatten die Richter festgestellt, dass der durch den Beitragsservice vorgenommene Abgleich der Melderegisterdaten mit dem beim Beitragsservice vorhandenen Datenbestand auf Grundlage des Rundfunkbeitragsstaatsvertrags erforderlich sei und damit keinen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung darstelle. Gegen diese Rechtsprechung kann auch der TLfDI nichts unternehmen. Im Ergebnis hat der TLfDI die Bürgerin darüber informiert, dass ein Widerspruch gegen diesen Datenabgleich mit dem Beitragsservice (wegen Rundfunk- und Fernsehgebühren) nicht erfolgversprechend ist.

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

4.2 Löschung von Google-Suchergebnissen

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

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

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

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

So hat die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2014 in ihrer Entschließung „Zum Recht

auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen“ auch darauf hingewiesen, dass aufgrund der territorialen Unbeschränktheit des Internets auch der Schutz des Einzelnen universell gelten muss (s. Link

<https://www.tlfdi.de/imperia/md/content/daten->

[schutz/entschliessungen/dsk_google_sucher](https://www.tlfdi.de/imperia/md/content/daten-schutz/entschliessungen/dsk_google_sucher)

[ergebnisse.pdf](https://www.tlfdi.de/imperia/md/content/daten-schutz/entschliessungen/dsk_google_sucher_gesuche.pdf)). Das bedeutet, eine Beschränkung nur auf den Europäischen Raum ist für die Betroffenen derzeit nicht in jedem Fall zielführend.

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



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

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



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

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

4.3 16 Millionen Zugangsdaten geraubt – was nun?

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

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

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

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



Da man sich vor Cyberattacken auf Rechner Dritter (z. B. externe Rechenzentren oder Server in der Cloud), wo auch die eigenen Zugangsdaten gespeichert sind, nicht selbst schützen kann, gilt es, die Auswirkungen von Cyberattacken selbst so gut wie möglich zu minimieren. Deshalb veröffentlichte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) dazu auch eine entsprechende Pressemitteilung:

(https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pressemitteilung_tlfdi_21012014.pdf). In dieser werden erste Maßnahmen vorgestellt, wie man als Betroffener reagieren sollte.

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



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

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

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

4.4 Datenschutz und Medienprivileg

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

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

Gegendarstellungsanspruch. Nach § 11a TPG gelten die Bestimmungen des BDSG, wie oben zu § 41 BDSG ausgeführt, nur eingeschränkt. Das bedeutet auch, dass eine Aufsichtstätigkeit des TLfDI nach § 38 BDSG nicht möglich ist und der TLfDI deshalb nicht im Sinne der Beschwerdeführerin tätig werden konnte. Der TLfDI konnte die Bürgerin lediglich darauf verweisen, dass es ihr unbenommen war, mögliche zivilrechtliche oder presserechtliche Ansprüche gegen die veröffentlichende Stelle prüfen zu lassen. Außerdem konnte sie sich wie jedermann beim Presserat über eine redaktionelle Veröffentlichung in Zeitungen, Zeitschriften und Online-Medien beschweren und presseethisch prüfen lassen.

Unter <https://www.presserat.de/beschwerde/online-beschwerde/> ist ein entsprechendes Beschwerdeformular abgedruckt. Der Deutsche Presserat ist auch unter der Adresse Fritzschestraße 27/28 in 10585 Berlin zu erreichen.



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

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

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

legt worden. Mittels der „Wegeheld“-App würden die Ordnungsämter sodann benachrichtigt werden, um tätig zu werden. Auch ein „Anschwärzen“, so der Zeitungsbericht, über Twitter und Facebook sei möglich.

Der TLfDI nahm diesen Bericht zum Anlass, bei den 26 größeren Thüringer Kommunen nachzufragen, ob deren Ordnungsämter diese „Wegeheld“-App bereits nutzten und gegebenenfalls Daten daraus verarbeitet hätten.

Das Ergebnis der TLfDI-Umfrage war datenschutzrechtlich erfreulich: Keine der 26 angefragten Kommunen hatte bisher Daten von oder im Zusammenhang mit der „Wegeheld“-App verarbeitet. Einigen Kommunen war die besagte App nicht einmal bekannt.

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

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

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

ein Cookie setzt und Informationen an sich weiterleitet. Welche Daten diese Informationen beinhalten, wollte Facebook bisher nicht transparent offenlegen.

Das Unabhängige Datenschutzzentrum Schleswig Holstein (ULD) leitete sogar gegen drei Unternehmen, die Fanpages betreiben, ein Verfahren ein. Dies mag für den normalen Bürger unverständlich wirken. Dennoch muss tatsächlich die Frage rechtlich geklärt werden, ob jemand eine Fanpage einrichten darf, wissentlich, dass seine Besucher von Facebook erfasst/getrackt werden, Daten also an die USA übermittelt werden. Mittlerweile liegt dieser Rechtsstreit beim Bundesverwaltungsgericht und sollte am 17. Dezember 2015 behandelt werden. Das Verfahren wurde am 25. Februar 2016 vom Bundesverwaltungsgericht ausgesetzt, weil dem Gerichtshof der Europäischen Union sechs Rechtsfragen zur Beantwortung vorgelegt wurden. Es scheint unwahrscheinlich, dass hier eine nationale Lösung erfolgt. Kundige Beobachter und Datenschützer vermuten und hoffen sogar, dass hier eine europäische Lösung angestrebt wird, sodass es nicht unwahrscheinlich erscheint, dass der Europäische Gerichtshof sich damit befassen muss, also es an diesen vom Bundesverwaltungsgericht zwecks Klärung weitergeleitet wird.

Unabhängig davon gab es in Thüringen eine Reihe von Anfragen zum Betreiben von Fanpages an den TLfDI von Landes- und Kommunalbehörden. Aus diesem Grund schaltete der TLfDI bereits im Dezember 2014 eine Pressemitteilung zum Sachstand und gab entsprechende Hinweise (siehe dazu die Anlage 44). Zudem ist die Empfehlung, bis zur endgültigen Entscheidung durch das Bundesverwaltungsgericht auch weiterhin vom Betreiben von Fanpages abzusehen.

Außerdem wandte sich der TLfDI im Dezember 2014 sowohl an den Thüringer Landkreistag und an den Thüringer Gemeinde- und Städtebund und empfahl diesen, bis zur endgültigen rechtskräftigen Entscheidung auch weiterhin vom Betreiben von Fanpages abzusehen.

Anfang 2015 lud der TLfDI diesbezüglich auch die obersten Landesbehörden zu einem Gespräch ein. In diesem Gespräch empfahl der TLfDI bei bereits bestehender Fanpage keine Fotos ohne Einwilligung des Betroffenen zu veröffentlichen und die Kommunikationsmöglichkeiten auf ein Minimum zu beschränken. Der TLfDI erkennt die Begehrlichkeiten und die anscheinende Notwendigkeit, in allen sozialen Netzwerken präsent sein zu wollen, um recht viele Bürger ansprechen zu können.

Datenschutzrechtlich gesehen ist es derzeit jedoch empfehlenswerter, bei sozialen Netzwerken, insbesondere bei Facebook, nur eine Startseite zu betreiben und dann auf die eigene Homepage zu verlinken. Dies würde nicht nur einen erheblichen doppelten Aufwand an Öffentlichkeitsarbeit minimieren, sondern auch der notwendigen Datensparsamkeit Rechnung tragen.

Im Ergebnis kann weiterhin nicht ausgeschlossen werden, dass ein Gericht entscheidet, dass keine Fanpage bei Facebook betrieben werden darf, solange Facebook nicht offenlegt, welche Daten tatsächlich von Besuchern der Fanpage erfasst werden.

Unabhängig davon hat der Europäische Gerichtshof (EuGH) mit seinem Urteil vom 6. Oktober 2015 zur Safe-Harbor-Entscheidung der EU-Kommission eine Datenübermittlung von personenbezogenen Daten in die USA für rechtswidrig erklärt (siehe dazu Nr. 3.1.). Im Kontext dieses Urteils sind auch soziale Netzwerke, wie Facebook, und ihre Datenübermittlung neu zu bewerten.

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

4.7 Telemediengesetz (TMG) – zeitgemäß ?

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

§ 15 Abs. 3 TMG regelt, dass der Nutzer nur auf sein Widerspruchsrecht hinzuweisen ist.

Ein weiteres Problem ist, dass mit der fortschreitenden Digitalisierung auch das Bedürfnis nach öffentlichem Zugang im Internet unter Nutzung frei zugänglicher drahtloser Netzwerke (WLANs) besteht. So wurde auch beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage nach der Haftung (Störerhaftung) gestellt und welche Risiken sich damit verbinden. Das Problem dabei ist, dass die „Störerhaftung“ dann eintritt, wenn über ein zur Verfügung gestelltes WLAN eine Rechtsverletzung begangen wurde.

Hintergrund für die unsichere Rechtslage sind § 8 Telemediengesetz (TMG) und verschiedene Urteile des BGHs zur Störerhaftung. Um im Nachhinein die Störerhaftung weitestgehend zu minimieren bzw. gänzlich auszuschließen, bieten viele Anbieter den Internetzugang über WLAN nur mit einem zugewiesenen Account an – oft verbunden mit der Eingabe weiterer Daten. Dies wird z. B. in Hotels, Flughäfen, Zügen, Straßenbahnen, Fernbussen oder auch in Cafés genutzt.

Aufgrund der Störerhaftung sind deshalb „offene“ WLANs, die ohne Anmeldung einen Zugriff auf das Internet ermöglichen, in Deutschland sehr selten anzutreffen.

Auslöser einer Störerhaftung kann bspw. eine Verletzung des Urheberrechts sein, wie beim Filesharing im Video- und Musikbereich.

Gemäß § 8 Telemediengesetz sind von der Haftung als Störer derzeit nur Internet-Provider ausgenommen. Rechtlich ungeregelt ist daher derzeit die Anwendbarkeit des § 8 TMG hinsichtlich der Haftung privater, geschäftsmäßiger und öffentlicher Anbieter.

Dies hat auch die Bundesregierung erkannt und, um die nötige Rechtssicherheit in Haftungsfragen zu verschaffen, am 18. November 2015 einen „Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes“ vorgelegt (BT DS 18/6745).

Der TLfDI empfiehlt daher, das Gesetzgebungsverfahren abzuwarten und wird die Probleme weiter im Blick haben.

Das Telekommunikationsgesetz bedarf hinsichtlich der europäischen Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie) einer Klarstellung.

Auch sollte das Betreiben frei zugänglicher drahtloser Netzwerke (WLANs) rechtsicher geregelt werden. Dabei sollte auch die Sicher-

heit der Netzwerkanbindung dem aktuellen Stand der Technik entsprechen.



Rathaus – © DOC RABE Media / Fotolia.com

5 Kommunales

5.1 Bloßstellung in der Schankwirtschaft – öffentliche Auslegung von Beschwerdeschreiben

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt Kenntnis darüber, dass der Bürgermeister einer Thüringer Gemeinde, einer Mitgliedsgemeinde einer Verwaltungsgemeinschaft (VG), Kopien seines an das Ordnungsamt der VG gerichteten Beschwerdeschreibens mit darin enthaltenen personenbezogenen Daten in der Gaststätte zur Kenntnisnahme für jedermann ausgelegt haben soll.

Der TLfDI stufte diesen Sachverhalt zunächst als einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften, insbesondere gegen § 22 Thüringer Datenschutzgesetz (ThürDSG) (Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs), sowie als einen Bruch des Amtsgeheimnisses ein. Der TLfDI bat die VG aber um eine Stellungnahme zu dem Sachverhalt.

Hierzu teilte die VG u. a. mit, dass der Bürgermeister der Gemeinde sich nicht erklären könne, wie das Beschwerdeschreiben an Dritte weitergegeben worden sei. In diesem Zusammenhang legte die VG dar, dass sie den Bürgermeister auf die unbedingte Einhaltung des

Datenschutzes in seiner Gemeinde und auf den verantwortlichen Umgang mit personenbezogenen Daten hingewiesen habe.

Weiterhin teilte die VG mit, dass die Einhaltung des Datenschutzes in den Mitgliedskommunen und die Verantwortung der Bürgermeister für personenbezogene Daten in einer Versammlung der VG thematisiert würden. Ferner wollte die VG alle nachgeordneten Einrichtungen der Kommunen noch einmal datenschutzrechtlich schulen.

Daraufhin teilte der TLfDI dem Beschwerdeführer mit, dass dem TLfDI keine gesetzlichen Befugnisse zur exakten Klärung des tatsächlichen Sachverhalts, wie sie etwa die Staatsanwaltschaft besitze, zur Verfügung stehen. Beurteilungsprobleme ergaben sich für den TLfDI im konkreten Fall dadurch, dass er Kenntnis von zwei plausiblen, sich jedoch widersprechenden Sachverhalten erhielt und weitere Recherchen keine Aussicht auf Erfolg boten. Insbesondere war für den TLfDI nicht aufklärbar, ob der Bürgermeister das Schreiben des Beschwerdeführers an die VG in der Gaststätte zur Kenntnisnahme für jedermann ausgelegt hatte.

In diesem Falle war es mit den Mitteln, die dem TLfDI nach § 37 Abs. 1 ThürDSG zur Verfügung stehen (Auskunfts- und Frage-recht sowie das Recht auf Akteneinsicht), ausgeschlossen, zweifelsfrei festzustellen, ob sich der beschwerdegegenständliche Datenschutzverstoß so zugetragen hat. Daher konnte der TLfDI die Angelegenheit leider nicht abschließend aufklären.

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

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

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

Ein Jäger hatte sich wegen der Verlängerung seines Bundesjagdscheins in das Landratsamt Saalfeld-Rudolstadt begeben. In der dortigen Unteren Jagdbehörde bemerkte er während des Gesprächs mit einem Mitarbeiter durch die offen stehende Tür des Nebenzimmers Stimmen. Da ein Mithören unberechtigter Dritter nicht auszuschließen gewesen sei, beschwerte er sich daraufhin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Wie das Landratsamt auf Nachfrage des TLfDI mitteilte, hatten sich während des Gesprächs ausschließlich vertretungsberechtigte und damit zuständige Mitarbeiter der Jagdbehörde im Nebenraum aufgehalten. Daher lag eine Übermittlung von personenbezogenen Daten im Ergebnis nicht vor.

Der TLfDI bat das Landratsamt, künftig dafür Sorge zu tragen, dass die Besucher zu Beginn des Gesprächs aufgrund der gebotenen Transparenz über die Möglichkeit des Mithörens der zuständigen Mitarbeiter im Nebenraum mittels geöffneter Tür in Kenntnis gesetzt werden. Ob die Tür geöffnet wird oder bleibt, ist jedoch von der Einwilligung der Besucher abhängig zu machen. Erteilt der Besucher eine Einwilligung, so ist die Tür zum Nebenraum aber auch dann zu schließen, wenn unberechtigte Personen den Nebenraum betreten. Ferner muss der Nebenraum abgeschlossen werden, sobald ihn die dortigen Mitarbeiter verlassen.

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

5.3 Facebook als Informationsquelle für Steuerprüfer

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

Um der Sache aus datenschutzrechtlicher Sicht auf den Grund zu gehen, wandte sich der TLfDI an die Stadtverwaltung Weimar und bat sie um eine Stellungnahme.

Die Stadtverwaltung teilte daraufhin mit, dass weder ein Datenabgleich noch ein Datenaustausch zwischen ihr und Facebook erfolgt sei. Die Teilnehmerzahl konnte die Stadtverwaltung auf der frei zugänglichen Facebookseite der betroffenen Diskothek entnehmen. Die Stadtverwaltung teilte mit, dass eben diese allgemein zugänglichen Informationen im Internet zur steuerrechtlichen Überprüfung verwendet werden können.

Auf der entsprechenden Facebookseite konnte man tatsächlich erkennen, wie viele Personen an dieser Veranstaltung teilgenommen haben. Nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

§ 92 Abgabenordnung (AO), der nach § 15 Abs. 1 Nr. 3a Kommunalabgabengesetz (ThürKAG) Anwendung findet, erlaubt der Finanzbehörde, dass sie sich der Beweismittel bedienen kann, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält. Die Kenntnisnahme der Teilnehmerzahl war hier ein zulässiges Mittel zur Erfüllung der in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgabe. Ein Datenschutzverstoß lag somit selbst für den Fall nicht vor, dass es sich um personenbezogene Daten handelte.

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

5.4 Stadt ist neugierig: Wer wohnt in der Seniorenresidenz?

Der Betreiber einer Seniorenresidenz bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Hilfe. Die zuständige Stadtverwaltung verlangte von ihm, eine Auflistung der Heimbewohner mit Angaben ihrer Zimmergröße in qm neben weiteren mietbezogenen Angaben zu übermitteln. Als Grund wurde die Überprüfung der Alten- und Pflegeheime zur bevorstehenden Änderung des Wohngeldgesetzes angegeben.

Auf Anfrage teilte die Stadtverwaltung zur Erklärung dem TLfDI mit, sie bräuchte die Informationen von den Betreibern von Alten- und Pflegeheimen, um sich auf die Änderung des Wohngeldgesetzes einstellen zu können. Dafür benötige sie unter anderem eine Auflistung der Heimbewohner mit Angabe ihrer Zimmergröße in qm. Diese Angaben dienten dem Abgleich bzw. der Aktualisierung der derzeit in der Behörde vorliegenden Angaben bezüglich dieser Wohngeldempfänger.

Als Rechtsgrundlage stützte man sich auf den Amtsermittlungsgrundsatz nach § 20 Zehntes Buch Sozialgesetzbuch (SGB X). Man bediene sich nur der Beweismittel, die nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts erforderlich seien. Die Auflistung der Heimbewohner mit Angabe ihrer Zimmergröße in qm sei so gemeint gewesen, dass nur die Daten der Heimbewohner, für die zu diesem Zeitpunkt ein Wohngeld bewilligt bzw. beantragt war, abgefragt werden sollten. Dies sei auch dem Pflegeheimbetreiber so vermittelt worden, er wolle dies offenbar nicht verstehen. Aus dem Anschreiben an den Betreiber war die Einschränkung auf die Wohngeldempfänger nicht erkennbar. Die Befugnis zur Amtsermittlung bedeutet nicht, dass grundsätzlich ohne konkreten Anlass und ohne Differenzierung Angaben von Dritten verlangt werden können.

Sollten alle Heimbewohner mit den zur Verfügung stehenden Flächen benannt werden, hätte die Behörde abgleichen können, ob sich darunter Wohngeldempfänger befinden. Dann wären allerdings personenbezogene Daten völlig unbetroffener Personen, nämlich auch derjenigen Personen, die kein Wohngeld beziehen, verlangt worden, wozu keine Befugnis nach dem SGB X bestand.

Das Problem kann aber auch nicht dadurch gelöst werden, dass das Pflegeheim lediglich in Bezug auf Wohngeldbezieher befragt wird. Diese sind dem Heim im Zweifel nicht bekannt. Es hätte seinerseits eine Abfrage bei seinen Bewohnern bedurft, wer von ihnen tatsäch-

lich Wohngeld bezieht oder beantragt hatte. Eigene Ermittlungen des Pflegeheimbetreibers diesbezüglich finden jedoch keine Rechtsgrundlage in den sozialgesetzlichen Vorschriften. Die weitere Möglichkeit, dem Pflegeheimbetreiber eine Liste von Wohngeldbezieher in seinem Pflegeheim zu übermitteln, um die entsprechenden qm-Zahlen beizufügen, scheidet ebenfalls aus. Das wäre gleichzeitig eine Übermittlung von Sozialdaten der Wohngeldbezieher an den Betreiber. Auch hierfür war keinerlei Rechtsgrundlage ersichtlich.

Das angestoßene Verfahren war damit nicht zulässig und widersprach darüber hinaus dem Grundsatz der Erhebung beim Betroffenen. Zulässig gewesen wäre, die Wohngeldbezieher in dem Pflegeheim selbst persönlich anzuschreiben und um Auskünfte zur qm-Zahl der bewohnten Fläche zu bitten. Nach § 67a Abs. 2 SGB X gilt nämlich auch für Sozialdaten der Grundsatz der Datenerhebung beim Betroffenen, sofern keine der dort aufgezählten Gründe vorliegen, die eine Erhebung bei anderen Stellen rechtfertigen. Möglicherweise hätten die Wohngeldbezieher die entsprechenden Angaben bei der Heimleitung erfragen und bestätigen lassen müssen. Allein der geringere Aufwand für die Stadtverwaltung, nur eine Stelle anstatt mehrerer Personen anschreiben zu müssen, rechtfertigt jedoch die zuvor gewählte Vorgehensweise nicht. Die Stadtverwaltung bestätigte, die Hinweise zu den datenschutzrechtlichen Problemen bei der Überprüfung und dem Abgleich der Daten von Wohngeldbeziehern zur Kenntnis genommen zu haben und in der künftigen Arbeit zu berücksichtigen.

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

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

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

einem umfangreichen Fragebogen Auskunft über ihre Lebensbedingungen und den Bedarf an Freizeitangeboten zu geben. Wegen der Ausführlichkeit der Fragen, die erheblich ins Detail gehen und auch die familiäre Situation umfassen, wurde der TLfDI erneut angefragt. Zur Erinnerung: Schülerbefragungen, die nicht verpflichtend sind, bedürfen der schriftlichen Einwilligung der Sorgeberechtigten und der bereits grundrechtsmündigen Schüler. Diese Einwilligung wird nur dann rechtswirksam erteilt, wenn der Einwilligende die Bedeutung und die Tragweite seiner Entscheidung zu überblicken vermag. Die datenschutzrechtliche Einwilligung ist erforderlich, weil aufgrund der detailreichen Abfrage eine Personenbeziehbarkeit des einzelnen Fragebogens, also ein Rückschluss auf den Auskunft erteilenden Schüler, nicht ausgeschlossen ist. Der Ablauf gestaltete sich im Wesentlichen so, dass der Stadt vom Forschungsinstitut ein Angebot zur Durchführung im jeweiligen Jahr unterbreitet wird. Die Stadt holt sodann die Genehmigung des zuständigen Schulamts ein. Die Schulleitungen werden darauf hingewiesen, dass die Eltern zu informieren sind. Das Forschungsinstitut verteilt eine ausreichende Anzahl an Fragebögen mit Rückumschlägen an die Schulen.

Den Schülern stand es frei, an der Befragung teilzunehmen. Sie konnten sich, ohne dass eine schriftliche Einwilligung der Eltern vorlag, die entsprechenden Fragebögen nehmen und ausfüllen. In die mitgelieferten Umschläge verpackt, wurden sie von den Schülern in eine der vom Forschungsinstitut in der jeweiligen Schule aufgestellten Urne eingeworfen. Nur die Mitarbeiter des Forschungsinstituts verfügten über einen Schlüssel zur Öffnung des Behältnisses. Weder die Schule noch die Stadtverwaltung hatte Zugriff auf die einzelnen Fragebögen. Von den Mitarbeitern des Forschungsinstituts, die auf das Datengeheimnis verpflichtet waren, wurden die Umschläge geöffnet und die Angaben in das automatisierte Statistikprogramm eingegeben. Danach wurden die Fragebögen vernichtet.

Da die Mitarbeiter des Forschungsinstituts keine Kenntnis darüber haben, wer von den Schülern aus einer Schule letztendlich die Fragebögen ausgefüllt hat, kann die Anonymität gewährleistet werden. Die statistisch aufbereiteten Daten, die veröffentlicht werden, erlauben nach den Darlegungen des Forschungsinstituts auch dann, wenn nur wenig Schüler einer Schule teilgenommen haben, keinen direkten Rückschluss auf den Einzelnen. Die dem TLfDI gegenüber geäußerten Befürchtungen und Bedenken hinsichtlich der Reanonymi-

sierbarkeit des veröffentlichten Ergebnisses der Forschungsarbeit auf einzelne Schüler konnten damit ausgeräumt werden.

Handlungsbedarf stellte der TLfDI jedoch in zwei Punkten fest:

Offenbar gab es zuletzt Defizite bei der Information der Eltern. Dies könnte darauf zurückzuführen sein, dass aufgrund der alljährlichen Befragung eine „Gewohnheit“ eingetreten ist und dadurch den Informationen nicht mehr das gebotene Gewicht beigemessen wurde. Um dies wiederherzustellen, wurde zugesagt, dass zukünftig jedem Schüler, der an der Befragung teilnehmen kann, eine Einwilligungserklärung mitgegeben wird. Nur wenn eine unterschriebene Einwilligung zurückgegeben wird, können die Fragebögen ausgehändigt werden. Selbstverständlich dürfen die Einwilligungserklärungen nicht mit den Fragebögen zusammengeführt werden, weil damit die Anonymisierung wieder aufgehoben wäre.

Außerdem gab es in den geprüften schriftlichen Unterlagen zur Auftragserteilung der aktuellen Jugendstudie keine zusammenhängende Darstellung des konkreten Ablaufs. Der Ablauf musste verschiedenen Dokumenten, die in dem Zusammenhang erstellt worden waren, entnommen werden. Zukünftig werden jedoch die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Angaben hinsichtlich des Ablaufs in das Angebot des Forschungsinstituts aufgenommen.

Insgesamt haben sich auch bei der aktuellen Studie keine Hinweise darauf ergeben, dass eine Reanonymisierung und damit ein Bezug auf einen einzelnen Schüler aufgrund der Darstellung des Ergebnisses der Jugendstudie möglich ist. Keine der beteiligten Stellen hat Kenntnis darüber, welcher Schüler tatsächlich teilgenommen hat. Weiterhin haben sich keine Hinweise darauf ergeben, dass die dargelegten technischen und organisatorischen Maßnahmen zum Schutz der Angaben der Schüler nicht eingehalten worden wären, obwohl diese nicht zusammenhängend, also als Checkliste, vorlagen.

Zwischenzeitlich hat sich zumindest eine weitere Kommune zur Durchführung von Jugendstudien entschieden, andere Kommunen haben ebenfalls Interesse daran bekundet.

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

5.6 Karnevalswagen als Beweis unrechtmäßiger Datenübermittlung?

Ein ehemaliger Bediensteter einer Gemeinde wandte sich wegen einer Fülle von datenschutzrechtlichen Unzulänglichkeiten in seiner Gemeinde an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Ausgangspunkt war, dass sich ein Gemeinderatsmitglied berufen sah, dem Beschwerdeführer nachzuweisen, dass er sich am Eigentum der Gemeinde vergriff und sich mit der Kamera auf die Lauer legte. Dabei angefertigte Fotos legte das Gemeinderatsmitglied dem Bürgermeister als Dienstherrn vor. Das Beschäftigungsverhältnis zwischen der Gemeinde und dem Bediensteten wurde letztendlich durch Vergleich beendet, Verfehlungen bildeten nicht den Grund hierfür. Leider ist der Vorgang publik geworden, die vermeintlichen Verfehlungen wurden sogar im Karnevalsumzug der Gemeinde dargestellt. Der Beschwerdeführer vermutete nun, dass es ein „abgekartetes Spiel“ war und die Darstellung auf dem Umzugswagen durch die Gemeinde, vertreten durch den Bürgermeister, lanciert worden sei.

Auf Nachfrage erklärte der Bürgermeister, das Gemeinderatsmitglied sei nicht durch ihn oder die Gemeinde mit der Beweiserhebung beauftragt gewesen. Wenn ihm jedoch eine Verfehlung durch Dritte bekannt gegeben wird, müsse er dem nachgehen. Eine Information an Außenstehende oder an die Öffentlichkeit habe es durch die Gemeinde aber zu keinem Zeitpunkt gegeben. Wie das in einer kleinen Gemeinde so sei, könnten durchaus sowohl der Beschwerdeführer als auch seine Familienmitglieder Dritten gegenüber die Angelegenheit angesprochen haben.

Damit stand in diesem Fall Aussage gegen Aussage. Weder aus den Angaben des Beschwerdeführers noch aus den Angaben des Bürgermeisters konnten konkrete Anhaltspunkte für berechtigte Zweifel an der Richtigkeit des Vorbringens des jeweils anderen entnommen werden. Die Prüfmöglichkeit des Sachverhalts durch den TLfDI war in diesem Zusammenhang an ihre Grenzen geraten. Dem TLfDI stehen als Kontrollbehörde für öffentliche Stellen keine besser geeigneten Mittel zur Verfügung, die Angaben des Bürgermeisters weiter zu überprüfen. Dem TLfDI ist es nicht möglich, in Wahrnehmung seiner Kontrollkompetenz im öffentlichen Bereich, etwa wie in einem Strafverfahren, Zeugenvernehmungen und Beschlagnahmen

durchzuführen. Die öffentlichen Stellen des Landes haben zwar die Pflicht, auf alle Fragen des TLfDI im Zusammenhang mit einer Kontrolle wahrheitsgemäß und umfassend zu antworten und Zugang zu Dokumenten zu gewähren (§ 38 Thüringer Datenschutzgesetz [ThürDSG]). Ob sie diesen Pflichten ordnungsgemäß nachkommen, kann der TLfDI leider nicht immer zweifelsfrei überprüfen. Im vorliegenden Fall war daher nicht auszuschließen, dass eine Datenübermittlung durch die Gemeinde an die Öffentlichkeit vorlag, doch bedurfte es zum Nachweis dafür konkreter belastbarer Tatsachen. Solche waren indes nicht vorhanden.

Die weiteren Hinweise des Beschwerdeführers, dass in der Gemeinde keine schriftlichen Festlegungen zur Einhaltung der datenschutzrechtlichen Vorgaben vorhanden waren, griff der TLfDI selbstverständlich auf. Er forderte die Gemeinde auf, Dienstanweisungen und weitere Festlegungen zu den technischen organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten zu treffen bzw. solche schriftlich niederzulegen. Da dies im Regelfall nicht von heute auf morgen bewerkstelligt werden kann, ist dieser Fall beim TLfDI leider noch nicht abgeschlossen.

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

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

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

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

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

5.8 Datenerhebung mittels Mülltonne? – Aufkleber mit personenbezogenen Daten

Bereits in seinem achten Tätigkeitsbericht (Nr. 5.16 – Datenhunger der Abfallwirtschaftsgesellschaft Gotha, S. 56 f.) hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über Datenschutzprobleme bei Kommunalen Abfallentsorgungsunternehmen berichtet.

Im Berichtszeitraum erfuhr der TLfDI nunmehr, dass im Versorgungsgebiet des Abfallwirtschaftsbetriebs des Landkreise Saale-Holzland (AWB) an den Tonnen für Papiermüll Aufkleber angebracht waren, auf denen die Kunden des AWB Straßenname, Hausnummer, Postleitzahl und Ort des Abfalltonnenstandorts anzugeben

hätten. Der TLfDI schaltete sich umgehend ein und forderte den AWB zur Stellungnahme auf.

Der AWB vertrat zunächst die unzutreffende Auffassung, dass es sich bei diesen Daten nicht um personenbezogene, sondern lediglich um anonymisierte Daten handle. Dies veranlasste den TLfDI zu folgender rechtlicher Klarstellung:

Nach § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) sind personenbezogene Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Anonymisieren ist gemäß § 3 Abs. 9 ThürDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Da ein objektiver Dritter ohne größeren Aufwand von den o. g. Daten auf die anschluss- und benutzungspflichtigen natürlichen Personen schließen konnte, handelte es sich bei diesen Daten zweifellos um personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG.

Wie der AWB weiterhin vortrug, sei es fraglich, ob es sich bei den Grundstücksangaben an den Müllbehältern um personenbezogene Daten handle, da sich der Eigentümer des anschlusspflichtigen Grundstückes nur mit größerem Aufwand – hier durch Anfrage beim Amtsgericht / Grundbuchamt – ermitteln lasse.

Hierzu führte der TLfDI aus, dass im Regelfall zwar die Kenntnis der Grundbucheintragung zur Bestimmung des anschluss- und benutzungspflichtigen Eigentümers erforderlich sei. Jedoch sei die Beschaffung des nötigen Zusatzwissens durch eine Anfrage im Grundbuchamt nicht mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft im Sinne von § 3 Abs. 9 ThürDSG verbunden. Diese Beurteilung entspricht der datenschutzrechtlichen Kommentarliteratur. Die Richtlinie 95/46/EG (nachfolgend: Datenschutzrichtlinie) bezieht in die Definition der personenbezogenen Daten (Art. 2 lit. a) „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“ ein und definiert als bestimmbar eine Person, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung einer Kennnummer ...“. Nach Erwägungsgrund 26 der Datenschutzrichtlinie sollen für die Bestimmbarkeit „alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen oder von einem Dritten eingesetzt

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

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

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

Daher stellte der TLfDI im Ergebnis fest, dass der AWB bei der Entsorgung von Papiermüll personenbezogene Daten erhoben hat. Mangels einer geeigneten Rechtsgrundlage im Sinne von § 30 Abs. 2 ThürAbfG handelte es sich hierbei um einen Verstoß gegen datenschutzrechtliche Vorschriften, insbesondere gegen § 4 Abs. 1 ThürDSG, in Form einer unzulässigen Datenerhebung.

Letztendlich erklärte der AWB, dass er die AbfWS umgehend um eine Erlaubnisnorm zur Erhebung der personenbezogenen Daten der Postleitzahl, des Ortes, des Straßennamen und der Hausnummer des betreffenden Grundstückes ergänzen werde. Die Erhebung dieser Daten diene, so der AWB, zum einen dem Dienstleistungsbetrieb der Überwachung und Durchsetzung des Anschluss- und Benutzungszwanges in der Abfallfraktion Papier/Pappe/Kartonagen und zum anderen einer näherungsweisen Überwachung der entsorgten Abfallmenge.

Durch eine solche Ergänzung der AbfWS trägt der AWB der Forderung des § 30 Abs. 2 Satz 2 ThAbfG Rechnung, wonach öffentlich-rechtliche Entsorgungsträger berechtigt sind, die zu ihrer Aufgabenerfüllung erforderlichen personenbezogenen Daten zu erheben.

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

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

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

Der TLfDI teilte der Stadtverwaltung hierzu mit, dass die fachliche Aufsicht und Leitung bzw. Begleitung eines Überprüfungsverfahrens

gemäß Stasi-Unterlagen-Gesetz außerhalb seines Kompetenzbereichs liege. Dies ergibt sich insbesondere aus den Regelungen zu den Aufgaben des TLfDI aus §§ 37 bis 40 ThürDSG und den Rechten des Betroffenen in den §§ 5 und 11 bis 17 Thüringer Datenschutzgesetz (ThürDSG). Der TLfDI empfahl, sich in dieser Angelegenheit ggf. an den Landesbeauftragten des Freistaates Thüringen zur Aufarbeitung der SED-Diktatur zu wenden.

Zugleich wies der TLfDI auf den sorgsamsten Umgang mit den bei der Überprüfung ggf. zu erwartenden hochsensiblen personenbezogenen Daten im Sinne von § 4 Abs. 5 ThürDSG hin. Über den weiteren Fortgang dieses Falls erhielt der TLfDI mangels Zuständigkeit keine weiteren Informationen – was datenschutzrechtlich korrekt ist.

Über die Aufgaben und Zuständigkeiten des TLfDI besteht auf kommunaler Ebene noch deutlicher Informationsbedarf. Für eine Überprüfung von Stadtratsmitgliedern nach dem Stasi-Unterlagen-Gesetz ist der TLfDI nicht zuständig.

Die erforderlichen datenschutzrechtlichen Kenntnisse im Freistaat Thüringen und in seinen Kommunen zu vermitteln, bleibt daher eine Aufgabe des TLfDI, die einen langen Atem erfordert.

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

Im Berichtszeitraum ging dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Vielzahl von Schreiben von Bürgern der Stadt Jena zu, die sich gleichlautend darüber beschwerten, dass mit ihren im Rahmen einer Unterschriftensammlung für ein Moratorium erhobenen und an den Oberbürgermeister übergebenen Daten nach ihrer Meinung nicht datenschutzkonform umgegangen worden sei.

Die Beschwerdeführer informierten den TLfDI darüber, dass Ende des Jahres 2013 ca. 10.000 Unterschriften für ein Moratorium zur Bebauung eines städtischen Platzes an den Oberbürgermeister übergeben worden seien. Die Unterschriften seien von einer Bürgerinitiative freiwillig gesammelt worden. Die Bürgerinnen und Bürger, die ein solches Moratorium unterstützten, hätten sich jeweils mit ihren Nachnamen, ihren Vornamen, ihren Adressen, dem Datum und ihren Unterschriften in der Unterschriftensammlung eingetragen. Nicht zuletzt aufgrund der zahlreichen Unterstützer der Unterschriften-

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

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

Im Ergebnis stellte der TLfDI Folgendes fest:

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

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

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

§ 15 Abs. 1 ThürKO. § 29 Abs. 2 Nr. 1 ThürKO, der nur die laufenden Angelegenheiten des eigenen Wirkungskreises erfasst, die keine grundsätzliche Bedeutung haben, war demzufolge nicht anwendbar. Ferner konnte auch § 34 Abs. 4 Thüringer Meldegesetz (ThürMeldeG) nicht als Rechtsgrundlage für eine Verarbeitung und Nutzung personenbezogener Daten durch die Stadt aus den genannten Unterschriftensammlungen herangezogen werden. Dies ergab sich daraus, dass eine anzustellende Interessenabwägung im konkreten Fall zugunsten des Schutzes des Rechts auf informationelle Selbstbestimmung aller Unterzeichner der Unterschriftensammlung ausfiel, weil die Verarbeitung ihrer personenbezogenen Daten durch den Oberbürgermeister in Form eines Anschreibens an die Gegner der Bebauung des städtischen Platzes hier nicht erforderlich war. Denn der Oberbürgermeister konnte hier ebenso gut mittels einer Abstimmungsbroschüre noch einmal die Vorteile einer Bebauung des Platzes deutlich machen.

Das Speichern oder Nutzen dieser personenbezogenen Daten konnte auch nicht nach § 20 Abs. 2 ThürDSG gerechtfertigt werden, da im vorliegenden Sachverhalt kein Grund ersichtlich war, der eine Zweckänderung für die Nutzung der personenbezogenen Daten rechtfertigte.

Schließlich war im konkreten Fall auch keine Einwilligung der Betroffenen im Sinne von § 4 Abs. 1 Satz 1 ThürDSG in die Verarbeitung und Nutzung der personenbezogenen Daten zu erkennen. Dies ergab sich daraus, dass die Unterzeichner der genannten Unterschriftensammlung an keiner Stelle signalisiert hatten, dass sie mit einer weiteren Korrespondenz gegenüber der Stadt in der Angelegenheit rechneten, geschweige denn einverstanden wären. Auch bei der Übergabe der Unterschriftlisten war eine solche weitere Dialogbereitschaft von keinem Beteiligten signalisiert oder später behauptet worden.

Der TLfDI hat im Ergebnis der datenschutzrechtlichen Kontrolle und Prüfung die somit ohne Rechtsgrundlage erfolgte Verarbeitung und Nutzung von Unterschriften der Unterschriftensammlung für persönliche Anschreiben des Oberbürgermeisters an die Unterschriftenleistenden als datenschutzrechtliche Verletzung gemäß § 39 Abs. 1 ThürDSG beanstandet und die zuständige Aufsichtsbehörde informiert.

Die im Sinne des Datenschutzes rechtswidrige Maßnahme war aber bereits durchgeführt und abgeschlossen, sodass die Behebung dieser

datenschutzrechtlichen Verletzung i. S. d. § 39 Abs. 1 Satz 1 ThürDSG nicht mehr möglich war. Der TLfDI forderte die Stadtverwaltung daher auf, für die Zukunft darauf hinzuwirken, dass vorgenannte datenschutzrechtliche Verstöße verhindert werden.

Abschließend teilte die Stadtverwaltung auf Nachfrage des TLfDI mit, dass jegliche im Zusammenhang mit der Unterschriftensammlung gespeicherten Daten gelöscht worden seien.

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

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

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

Ausweislich der vom Beschwerdeführer vorgelegten Schreiben hatte er sich an das Meldeamt mit der Bitte um Melderegisterauskunft hinsichtlich der jetzigen Anschrift seiner Tochter gewandt. Diesem Auskunftersuchen entsprach das Meldeamt nicht, vielmehr forderte es den Beschwerdeführer zur Begründung eines berechtigten/rechtlichen Interesses an der Auskunft auf.

Die zuständige Meldebehörde informierte den TLfDI auf dessen Bitte dahingehend, dass die Tochter des Beschwerdeführers einen Antrag auf Einrichtung einer Auskunftssperre gemäß § 31 Abs. 7 Thüringer Meldegesetz (ThürMeldeG) gestellt hatte. Als Gründe habe die Tochter große Probleme im Umgang mit dem Beschwerdeführer, ihrem Vater, angegeben. Diese zögen sich bereits über mehrere Jahre hin, die Aggressivität seitens des Vaters habe zugenommen. Es standen Beschimpfungen und Beleidigungen in verbaler und schriftlicher Form im Raum. Dies habe die Tochter mit verschiedenen Schreiben des Beschwerdeführers belegt. Die Tochter habe sich deshalb zu einem Umzug entschlossen. Die Auskunftssperre sei antragsgemäß im Melderegister eingetragen worden. Auf das schriftliche Auskunftersuchen des Beschwerdeführers hin wurde die Tochter gemäß § 31 Abs. 7 Satz 2 ThürMeldeG angehört. In Folge erhielt der Beschwerdeführer eine schriftliche Mitteilung vom Meldeamt, dass es eine Auskunft zu seiner Tochter wegen einer eingetragenen Melderegisterauskunftssperre nicht erteilen könne. Das Meldeamt habe den Beschwerdeführer vielmehr aufgefordert, ggf. sein rechtliches bzw. berechtigtes Interesse an der Auskunft nachzuweisen. Das habe er nicht getan.

Der TLfDI hat den Beschwerdeführer im Ergebnis darüber informiert, dass die Verweigerung der Melderegisterauskunft an ihn wegen der für seine Tochter eingetragenen Melderegisterauskunftssperre und seinem nicht vorgetragenen rechtlichen Interesse an dieser Auskunft nicht nur datenschutzrechtlich unbedenklich, sondern datenschutzrechtlich erforderlich war (§ 31 Abs. 7 Satz 2 ThürMeldeG). Weiter hat der TLfDI dem Beschwerdeführer mitgeteilt, dass eine eingetragene Auskunftssperre nicht zwingend zu einer Verweigerung jedweder Melderegisterauskunft führt. Hat die anfragende Person gegenüber der Meldebehörde ein berechtigtes Interesse an der Erteilung der Meldedaten glaubhaft gemacht – dies ist in der Regel anzunehmen, wenn z. B. der Auskunftssuchende die erbetenen Daten zur Rechtsverfolgung/Rechtsverteidigung benötigt –, gilt die Auskunftssperre ggf. nicht in vollem Umfang. Ob allerdings die Voraus-

setzungen der für die Tochter eingetragenen Melderegisterauskunftssperre im konkreten Fall vorlagen, hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit mangels Zuständigkeit nicht zu prüfen. Diese Aufgabe liegt allein im Kompetenzbereich der zuständigen Meldebehörde. Der TLfDI hat den Beschwerdeführer ergänzend darüber informiert, dass die Ablehnung seines Auskunftersuchens durch die Meldebehörde für ihn einen (belastenden) Verwaltungsakt im Sinne von § 35 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) darstelle und diese Ablehnung seinerseits mit einem Widerspruch gemäß §§ 68 ff. Verwaltungsgerichtsordnung (VwGO) und einer Klage (§ 42 Abs. 1 VwGO) angefochten werden könne.

Schließlich ist auf Folgendes hinzuweisen: Zum 1. November 2015 ist das Bundesmeldegesetz (BMG) in Kraft getreten. Das Meldewesen liegt nunmehr in der ausschließlichen Gesetzgebungskompetenz des Bundes. Die Regelungen zu Auskunftssperren im Melderegister sind aber im Wesentlichen nicht verändert worden (vgl. § 51 BMG).

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

5.12 Aushändigung einer Meldebescheinigung an Nichtberechtigte

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

klären, ob seine Mutter oder ggf. eine dritte Person diese Meldebescheinigung angefordert habe und ob ein berechtigtes Interesse vorgetragen worden sei. Der Beschwerdeführer ging davon aus, dass die Meldebescheinigung entgegen aller Datenschutzbestimmungen an einen Nichtberechtigten ausgehändigt wurde, sodass er den TLfDI um Datenschutz-Hilfe bat.

Der TLfDI wandte sich an die Stadtverwaltung Schmalkalden mit der Bitte um Stellungnahme zur Angelegenheit, insbesondere um Mitteilung der Rechtsgrundlage für die ggf. erfolgte Übermittlung der personenbezogenen Daten des Beschwerdeführers an seine Mutter oder sonstige Dritte.

Der TLfDI teilte dem Beschwerdeführer nach Eingang der Stellungnahme der Stadtverwaltung und datenschutzrechtlicher Prüfung der Angelegenheit mit, dass die Mutter des Beschwerdeführers gegenüber der Meldebehörde ein berechtigtes Interesse an der Erteilung der Meldedaten glaubhaft gemacht habe und ihr die Meldebescheinigung deshalb zur Verfügung gestellt worden sei. Das Vorliegen eines berechtigten Interesses ist in der Regel dann anzunehmen, wenn der Auskunftssuchende die erbetenen Daten zur Rechtsverfolgung/Rechtsverteidigung benötigt. Hier handelt es sich zudem um ein rechtliches Interesse, das als Kriterium insbesondere zur Durchsetzung von Rechtsansprüchen gilt (vgl. dazu Medert/Süßmuth, Melderecht des Bundes und der Länder, Kommentar, Teil I: Bundesrecht, I C Erl. § 21 MRRG, Rz. 31). Das berechtigte Interesse wurde dem TLfDI seitens der Stadtverwaltung Schmalkalden dargelegt. Auskunftssperren im Datensatz des Beschwerdeführers lagen nach Angaben der Stadtverwaltung nicht vor.

Der TLfDI hat den Beschwerdeführer im Ergebnis darüber informiert, dass die in Rede stehende Auskunftserteilung gemäß § 21 Melderechtsrahmengesetz i. V. m. § 31 Abs. 4 Thüringer Meldegesetz datenschutzrechtlich zulässig gewesen ist.

Eine ausführliche datenschutzrechtliche Bewertung der Angelegenheit hat der TLfDI dem Beschwerdeführer bisher nicht zur Verfügung gestellt. Dies geschah aus folgenden Gründen nicht: Die Bewertung der Stadtverwaltung Schmalkalden beinhaltete zum einen sehr sensible Daten zur Person des Beschwerdeführers. Zum anderen hatte sich der Beschwerdeführer ausschließlich per E-Mail an den TLfDI gewandt. Um eine sichere Übermittlung sensibler personenbezogener Daten gewährleisten zu können, bat der TLfDI den Beschwerdeführer um Übersendung seines öffentlichen Schlüssels für

eine verschlüsselte Übersendung der genannten Daten per E-Mail oder um Mitteilung seiner postalischen Anschrift. Leider antwortete der Beschwerdeführer bisher nicht auf diese Bitte des TLfDI.

Zum 1. November 2015 ist das Bundesmeldegesetz (BMG) in Kraft getreten. Das Meldewesen liegt nunmehr in der ausschließlichen Gesetzgebungskompetenz des Bundes. Es ist aber dabei geblieben, dass bei Glaubhaftmachung eines berechtigten Interesses eine erweiterte Melderegisterauskunft erteilt werden darf (§ 45 BMG).

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

5.13 Besonderer Meldeschein: Bayerisches Muster vom TLfDI abgelehnt

Aufgrund einer Bürgeranfrage und im Zuge der Reform des Meldewesens wollte eine Stadt in Thüringen den zur Abrechnung des Kurbeitrages genutzten besonderen Meldeschein für Beherbergungsbetriebe (§ 30 Bundesmeldegesetz (BMG)) neu und vor allem auch datenschutzgerecht gestalten. Die Stadt wandte sich deshalb im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um datenschutzrechtliche Prüfung ihres – nach Angaben der Stadt ursprünglich aus einer bayerischen Gemeinde stammenden – Meldescheinentwurfs.

Gemäß § 30 Abs. 1 BMG haben die Leiter der Beherbergungsstätte besondere Meldescheine bereitzuhalten und darauf hinzuwirken, dass die betroffenen Personen (die Beherbergten) ihrer Meldepflicht nachkommen. Die Meldescheine enthalten vom Grundsatz die in § 30 Abs. 2 BMG aufgeführten Daten. Gemäß § 30 Abs. 3 BMG i. V. m. § 9 Thüringer Kommunalabgabengesetz dürfen Gemeinden durch Satzung zusätzlich zu diesen in § 30 Abs. 2 des BMG genannten Daten weitere für die Erhebung des Kurbeitrags erforderliche Daten auf dem Meldeschein erheben.

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

Zunächst war auf dem vorgelegten Entwurf des Meldescheines das „Geburtsdatum des begleitenden Ehegatten/Lebenspartners“ anzugeben. Gemäß § 29 Abs. 2 BMG sind aber mitreisende Angehörige auf dem Meldeschein nur der Zahl nach anzugeben. Zwar dürfen Gemeinden, wie oben ausgeführt, durch Satzung zusätzlich die für die Erhebung des Kurbeitrags erforderlichen Daten auf dem Meldeschein erheben. Der höchstmögliche Kurbeitrag beträgt aber gemäß der dem TLfDI vorgelegten „Satzung über die Erhebung eines Kurbeitrages“ ab einem Alter von 16 Jahren 2,00 Euro/Aufenthaltstag, sodass die Erhebung des Geburtsdatums „Begleitender Ehegatte/Lebenspartner“ für die Erhebung des Kurbeitrages nicht erforderlich war. Der TLfDI bewertete infolgedessen die Erhebung dieses Datums als datenschutzrechtlich unzulässig.

Auch die Erhebung der Geburtsdaten der mitreisenden Kinder auf dem Meldeschein hat der TLfDI für datenschutzrechtlich unzulässig erachtet. Zwar unterscheidet sich der „Kurbeitrag für Kinder unter 7 Jahren“ gemäß Satzung von dem „Kurbeitrag für Kinder von 7 bis 16 Jahren“. Der TLfDI empfahl deshalb, statt der Geburtsdaten der Kinder die „Anzahl der Kinder unter 7 Jahre“ und „Anzahl der Kinder im Alter von 7–16 Jahre“ zu erheben.

Der TLfDI teilte der Stadt weiter mit, dass mittels Meldeschein in keinem Fall die Personalausweisnummer erhoben werden dürfe. Lediglich bei ausländischen Personen muss auf den Meldescheinen gemäß § 30 Abs. 2 Nr. 8 BMG die Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiere verlangt werden.

Abschließend hat der TLfDI darauf hingewiesen, dass es bei einer Verarbeitung und Nutzung der nach § 30 Abs. 2 BMG erhobenen Daten für eine Beherbergungs- oder Fremdenverkehrsstatistik gemäß § 31 BMG auch bei freiwilligen Auskünften - nach dem Thüringer Statistikgesetz (ThürStatG) der Einrichtung einer Statistikstelle (§ 20 ThürStatG) bedürfe.

Die Stadtverwaltung informierte den TLfDI im Anschluss, dass sie die Beherbergungsbetriebe über die ab 1. November 2015 geltende Rechtslage informiert habe und mittlerweile ein – entsprechend den Hinweisen des TLfDI – datenschutzkonformes Layout der Meldescheinvordrucke erstellt worden sei.

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

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

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

Eine Verwaltungsgemeinschaft (VG) wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat ihn um Rat in folgender Angelegenheit:

Im Bereich Meldewesen der VG war der Hinweis eines Anzeigenden eingegangen, dass ein Bürger sich in einer Wohnung aufhalte, in der er laut Melderegister nicht gemeldet sei. Der zuständige VG-Mitarbeiter habe mit dem Anzeigenden vereinbart, dass bei einer evtl. erforderlichen Anhörung des Betroffenen keine namentliche Benennung des Anzeigenden vorgenommen werde. Nun fordere der Rechtsanwalt des betroffenen Bürgers Akteneinsicht, und es stelle sich die Frage, ob der Bereich Meldewesen auch den Namen des Anzeigenden an den Anwalt übermitteln dürfe. Dies sei in vorliegender Angelegenheit besonders heikel, da hier eine Nachbarschaftsstreitigkeit, eine „Schraube ohne Ende“, vorliege.

Der TLfDI teilte der VG nach Prüfung des Sachverhalts mit, dass er im vorliegenden Fall nicht von einer Übermittlung von Daten, sondern von einem Auskunftsanspruch ausgehe. Auskunft an den Betroffenen (auch an den mandatierten Rechtsanwalt des Bürgers) hat die Meldebehörde auf Antrag nach § 9 Abs. 1 ThürMeldeG zu erteilen. Diese Auskunft erstreckt sich dabei gemäß § 9 Abs. 1 Nr. 1 ThürMeldeG auf alle personenbezogenen Daten und Hinweise des Betroffenen (auch soweit sie sich auf deren Herkunft beziehen), die über ihn im Melderegister, in Akten, Aktensammlungen oder sonstigen Unterlagen der Meldebehörde gespeichert sind. Die Auskunftserteilung unterbleibt, soweit gemäß § 9 Abs. 3 Nr. 3 ThürMeldeG die Daten ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

Der TLfDI informierte die VG ferner über seine Rechtsauffassung, dass die Ablehnung des Auskunftersuchens des Rechtsanwalts im vorliegenden Fall zulässig sei. Denn hier müsse das Interesse des durch den Rechtsanwalt vertretenen Bürgers hinter das schützenswerte Interesse des Hinweisgebers zurücktreten.

Ergänzend wies der TLfDI die VG darauf hin, dass die Meldebehörde gemäß § 10 Abs. 2 ThürMeldeG verpflichtet sei, bei konkreten Anhaltspunkten für die Unrichtigkeit oder Unvollständigkeit des Melderegisters bezüglich namentlich bekannter Einwohner den Sachverhalt von Amts wegen zu ermitteln. Ob Meldedaten unrichtig sind, bestimmt sich dabei aber ausschließlich nach objektiven Kriterien. Nach der einschlägigen Kommentarliteratur (Medert/Süßmuth/Dette-Koch, Kommentar zum Melderecht des Bundes und der Länder, Erl. zu § 4a MRRG, Rn. 15 bis 19) reichen jedenfalls Vermutungen oder bloße Hinweise, dass Daten unrichtig sein könnten, als „konkrete Anhaltspunkte“ für die Unrichtigkeit des Melderegisters nicht aus.

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

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

5.15 Unterschriftensammlung – auch hier gilt der Datenschutz

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

(ThürKO) ein Bürgerentscheid durchzuführen. Die Bürgerinitiative teilte mit, dass das Landratsamt Schmalkalden-Meiningen auf einer Besprechung die Vorgehensweise der Listenübergabe und Stimmentzählung bekannt gegeben habe. Dabei erfuhr die Bürgerinitiative insbesondere von einer beabsichtigten Vervielfältigung und Digitalisierung der Eintragungslisten durch das Landratsamt. Dies hielt die Bürgerinitiative für bedenklich.

Aufgrund der Kurzfristigkeit der Angelegenheit wandte sich der TLfDI umgehend an das Landratsamt Schmalkalden-Meiningen und bat um eine Stellungnahme.

Das Landratsamt teilte daraufhin dem TLfDI mit, dass es die Vervielfältigung und Digitalisierung der Eintragungslisten ausschließlich zum Zweck der Prüfung der Wahlberechtigungen der Unterzeichner durchgeführt habe, um diese dann an das jeweils zuständige Einwohnermeldeamt weiterzuleiten. Mit der Feststellung der Zulässigkeit des Bürgerbegehrens seien sämtliche gespeicherte Daten dort unwiederbringlich gelöscht worden.

Es stellte sich dabei die Frage, was mit den ursprünglichen Eintragungslisten passieren sollte. Nach der Aussage des Landratsamtes sollten die Eintragungslisten entsprechend der gesetzlichen Vorgaben der § 17a Abs. 2 Satz 3 ThürKO, § 49 Kommunalwahlordnung (ThürKWO) aufbewahrt werden. Nur der Leiter des Büros Landratsamt könne auf diese Daten zugreifen.

Der § 49 ThürKWO regelt u. a. die Vernichtung von Wahlunterlagen nach Abschluss eines etwaigen Verfahrens zur Wahlprüfung bzw. zur Anfechtung der Feststellung des Wahlergebnisses, nicht aber die Vernichtung von Unterlagen zu Bürgerbegehren im Sinne von § 17 ThürKO. Nachdem jedoch das Bürgerbegehren das erforderliche Unterstützungsquorum erreicht hatte, beschloss der Kreistag, den Bürgerentscheid durchzuführen. Im Ergebnis war damit der erste Verfahrensschritt des Bürgerbegehrens abgeschlossen, sodass eine weitere Aufbewahrung der Daten zu dem abgeschlossenen Verfahren des Bürgerbegehrens nach Ansicht des TLfDI nicht mehr erforderlich war. Aus diesem Grund fragte der TLfDI erneut beim Landratsamt nach, auf welcher Rechtsgrundlage die fortgesetzte Aufbewahrung der Daten des Bürgerbegehrens beruhe und weshalb dies erforderlich sei. Das Landratsamt war der Auffassung, dass die Eintragungslisten zum Bürgerbegehren einer zweijährigen Bindungsfrist nach § 17 Abs. 8 Satz 3 ThürKO unterlägen. Diese Rechtsauffassung teilte der TLfDI nicht. § 17 Abs. 8 Satz 3 ThürKO bezieht sich ledig-

lich auf Bürgerentscheide und regelt, dass ein Bürgerentscheid unter den dort genannten Voraussetzungen innerhalb von zwei Jahren nur durch einen neuen Bürgerentscheid abgeändert werden kann. Dass ein Bürgerbegehren und ein Bürgerentscheid in datenschutzrechtlicher Hinsicht eigenständig zu betrachten sind, ergibt sich unter anderem mittels Vergleichs mit der Datenschutznorm in § 5 des Thüringer Gesetzes über Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid (ThürBVVG). Danach dürfen personenbezogene Daten, die auf der Grundlage dieses Gesetzes erhoben werden, nur für die Durchführung des jeweiligen Antrags auf Zulassung eines Volksbegehrens oder Volksentscheids verarbeitet oder genutzt werden. Werden sie für das Verfahren nicht mehr benötigt, sind sie unverzüglich zu vernichten.

Der TLfDI vertrat deshalb im Ergebnis die Rechtsauffassung, dass die Eintragungslisten zum Bürgerbegehren mit den darin enthaltenen personenbezogenen Daten nach dem erfolgten Kreistagsbeschluss zur Durchführung des Bürgerentscheides entsprechend § 16 Thüringer Datenschutzgesetz (ThürDSG) zu löschen waren und forderte das Landratsamt Schmalkalden-Meinungen auf, entsprechend zu handeln. Unter Berücksichtigung von § 4 Abs. 1 Satz 2 Thüringer Archivgesetz, der die Archivierung kommunalen Archivguts durch Gemeinden, Landkreise und kommunale Verbände in eigener Verantwortung und Zuständigkeit regelt, ist vom Gesetzgeber hier eine Klarstellung in der ThürKO zu verlangen, dass personenbezogene Daten aus Eintragungslisten von Bürgerbegehren unverzüglich zu löschen sind, sobald sie für das Verfahren zum konkreten Bürgerbegehren nicht mehr benötigt werden.

Daraufhin teilte das Landratsamt dem TLfDI mit, dass sämtliche Unterschriftslisten zum Bürgerbegehren vernichtet wurden. Der TLfDI sah infolgedessen die Angelegenheit als erledigt an.

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

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

5.16 Thüringer Landeswahlordnung – Klappe, die Vierte (Änderung)

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm Anfang des Jahres 2014 Stellung zu einem Entwurf der vierten Änderung der Thüringer Landeswahlordnung (ThürLWO). Der Verordnungsentwurf sollte die notwendigen Folgeänderungen, die sich aus dem Fünften Gesetz zur Änderung des Landeswahlgesetzes vom 22. März 2012 ergeben hatten, vornehmen. Darüber hinaus sollte die Verordnung die zwischenzeitlich erfolgten Änderungen der Bundeswahlordnung aufgreifen, so dass die Landeswahlordnung nach dem Grundsatz der Harmonisierung des Wahlrechts des Bundes und der Länder an die Bundeswahlordnung anzupassen war. Die Änderungen betrafen im Wesentlichen die Abschaffung von Antragsgründen für die Beantragung der Briefwahl, die Anpassung von Begrifflichkeiten sowie die Harmonisierung des Wahlrechts des Bundes und der Länder.

Der TLfDI begrüßte aus datenschutzrechtlicher Sicht, dass nunmehr die Wahlscheine unmittelbar an den Wahlberechtigten übersandt werden sollten. Die Zustimmung des TLfDI fand auch, dass im Wählerverzeichnis gemäß § 19 Abs. 2 des Entwurfes der Vierten Verordnung zur Änderung der Thüringer Landeswahlordnung (ThürLWO-E) während der Auslegungsfrist die Wohnung (Anschrift) für Wahlberechtigte, für die im Wählerverzeichnis eine Auskunftssperre gemäß § 31 Abs. 7 Thüringer Meldegesetz (nunmehr § 51 Bundesmeldegesetz [BMG]) eingetragen ist, von Amts wegen unkenntlich zu machen war. Der TLfDI gab hierzu aber den Hinweis zu prüfen, ob in § 19 ThürLWO-E die Unkenntlichmachung lediglich der Wohnung und nicht zum Beispiel auch des Geburtsdatums von Amts wegen aufgrund des Zweckes des damals geltenden § 31 Abs. 7 Thüringer Meldegesetz (Auskunftssperre bei der Möglichkeit der Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen des Betroffenen oder einer anderen Person) zum Schutz des Betroffenen dienlich wäre. Es blieb jedoch dabei, dass im Wählerverzeichnis während der Auslegungsfrist von Amts wegen zunächst nur die Wohnung (Anschrift) von Wahlberechtigten,

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

In § 19 Abs. 2 Thüringer Landeswahlordnung (ThürLWO) heißt es nunmehr:

„Im Wählerverzeichnis ist während der Auslegungsfrist die Wohnung von Wahlberechtigten, für die im Melderegister eine Auskunftssperre nach § 51 Abs. 1 BMG eingetragen ist, von Amts wegen unkenntlich zu machen. Auf Verlangen des Wahlberechtigten ist in dem Wählerverzeichnis während der Auslegungsfrist das Geburtsdatum unkenntlich zu machen.“

5.17 Leck im Rathaus Nordhausen? – personenbezogene Daten im Netz

Wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) der Presse entnehmen konnte, war eine Liste der Stadtverwaltung Nordhausen zu Geschwindigkeitsmessungen mit personenbezogenen Daten der daran beteiligten Mitarbeiter von privater Seite in das soziale Netzwerk Facebook gestellt worden. Bei einer solchen Veröffentlichung handelt es sich um eine unbefugte Übermittlung personenbezogener Daten.

Daraufhin bat der TLfDI die Stadtverwaltung Nordhausen mitzuteilen, wie es zu diesem Vorfall kommen konnte und welche technisch-organisatorischen Maßnahmen eingeleitet wurden, um künftig ähnliche Vorkommnisse auszuschließen.

Die Stadtverwaltung Nordhausen teilte mit, dass die veröffentlichten Daten aus den bei der Verfolgung von Verkehrsordnungswidrigkeiten an die betreffenden Fahrzeughalter übersandten Fragebögen stammten, da hierin die als Zeuge der Feststellung von Verkehrsordnungswidrigkeiten beteiligten Mitarbeiter der Stadtverwaltung mit Anrede und Nachnamen genannt würden.

Nach Auffassung der Stadtverwaltung Nordhausen gehörte der Versand von Fragebögen an die Fahrzeughalter zum nichtförmlichen Verwarngeld-Vorverfahren. Im Unterschied zum förmlichen Bußgeldverfahren sei hierbei die Übermittlung von personenbezogenen Daten der beteiligten Mitarbeiter nicht erforderlich. Daher beabsichtigte die Stadtverwaltung, in den o. g. Fragebögen künftig anstelle von Anrede und Nachname lediglich Pseudonyme ihrer Mitarbeiter

anzugeben. Das Pseudonymisieren ist gemäß § 3 Abs. 10 ThürDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch Kenzeichen zu dem Zweck, die Bestimmung des Betroffenen ohne Nutzung der Zuordnungsfunktion auszuschließen oder wesentlich zu erschweren.

Diese Vorgehensweise stellt aus Sicht des TLfDI eine geeignete organisatorische Maßnahme dar, um zur Erhöhung des Datenschutzniveaus im öffentlichen Bereich zu gelangen.

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

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

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

Zu dem Vorhaben vertrat der TLfDI folgende Auffassung:

Das Kopplungsverbot nach § 28 Abs. 3b Bundesdatenschutzgesetz (BDSG) verbietet es der verantwortlichen Stelle, den Abschluss eines Vertrags von einer Einwilligung des Betroffenen zur werblichen Datennutzung abhängig zu machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.

Hier wird der Erhalt der Boni unter die Voraussetzung der Einwilligung in die werbliche Nutzung von Kundendaten gestellt, wobei

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

Insoweit unterliegt die vorgesehene Gewährung von Bonusleistungen in Abhängigkeit von einer Einwilligung in die konzernweite Nutzung der Namens- und Adressdaten zur werblichen Ansprache durch die Konzernunternehmen der SWE Gruppe nicht dem Kopplungsverbot im Sinne von § 28 Abs. 3b BDSG. Die vorgelegte schriftliche Einwilligungserklärung entsprach den datenschutzrechtlichen Anforderungen.

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

5.19 Video(attrappen)gaga 1

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

Da der Stadt Erfurt die Rechtslage bei Videoüberwachungen bekannt war, beschränkte sich der TLfDI auf die folgenden Hinweise zum Einsatz von Kameraattrappen:

Kameraattrappen sind so zu beurteilen, als ob unter den gegebenen Umständen eine echte Videoüberwachung durchgeführt würde. Da diese Maßnahme im konkret zu beurteilenden Fall auf einen nicht öffentlich zugänglichen Bereich und auf die Zeiten außerhalb der Arbeitszeit beschränkt war, waren schutzwürdige Interessen der Beschäftigten nicht tangiert. Daher sah der TLfDI den Einsatz einer Kameraattrappe unter den o. g. Voraussetzungen als zulässig an.

Die Maßnahme der Videoüberwachung – so die Aufforderung des TLfDI – sollte aber mittels eines Piktogramms und der Angabe der verantwortlichen Stelle erkennbar gemacht werden. Einen zeitlichen Hinweis über den Einsatz der Videoüberwachung hielt der TLfDI nicht für erforderlich.

Bei der Beteiligung des Personalrates nach § 74 Abs. 2 Nr. 11 Thüringer Personalvertretungsgesetz handelte es sich um eine Frage des Personalvertretungsrechts, nicht des Datenschutzrechts. Aus datenschutzrechtlicher Sicht war der Personalrat aber zumindest darüber in Kenntnis zu setzen, dass keine Videoüberwachung innerhalb der Arbeitszeit stattfindet.

Eine Dokumentation gemäß § 10 Thüringer Datenschutzgesetz (ThürDSG) war nach Auffassung des TLfDI nicht erforderlich. Jedoch sollten beim Verfahrensverzeichnis die erforderlichen Angaben bezüglich der Kameraattrappe dokumentiert werden, um der Auskunftspflicht im Sinne vom § 10 Abs. 3 ThürDSG nachkommen zu können.

Der behördliche Datenschutzbeauftragte war schließlich auch in Fällen des Einsatzes von Kameraattrappen zu beteiligen.

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

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

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

Nach § 3 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) umfasst die Verarbeitung personenbezogener Daten auch deren Löschung, die naturgemäß mit der Entsorgung bzw. Vernichtung von Schriftgut verbunden ist. Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt gemäß § 8 ThürDSG der Auftraggeber für die Einhaltung der Bestimmungen des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung für die jeweils zum Einsatz kommenden technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und erforderlichenfalls alle Unterauftragsverhältnisse schriftlich festzulegen sind. Entsprechendes gilt auch für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen, soweit ein Zugriff auf personenbezogene Daten dabei nicht ausgeschlossen werden kann. In diesem Zusammenhang weist der TLfDI auf den in der Anlage 23 seines 5. Tätigkeitsberichts veröffentlichten Mustervertrag zur Auftragsdatenverarbeitung hin.

Jedoch gibt es keine datenschutzrechtlichen Vorgaben, wonach unternehmensbezogene Zertifikate als Entscheidungskriterium im Sinne eines „K.o.-Kriteriums“ zur Auftragsvergabe heranzuziehen sind, zumal durch ein solches Vorgehen Unternehmen, die nicht zertifiziert wurden, jedoch die geforderte Eignung besitzen, vom Vergabeverfahren ausgeschlossen wären. Ggf. sollten Nachweise zu einem Datenschutzaudit nach § 9a Bundesdatenschutzgesetz (BDSG) als ein Orientierungsmerkmal zur fachlichen Beurteilung der Unternehmen herangezogen werden. Der Auftraggeber sollte sich in jedem Fall von den infrage kommenden Unternehmen Nachweise zur Umsetzung der §§ 4 ff. BDSG vorlegen lassen und sich darüber informieren, ob die potentiellen Auftragnehmer datenschutzrelevante

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

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

5.21 Dürfen personenbezogene Daten von Wahl-Kandidaten ins Internet?

Ein behördlicher Datenschutzbeauftragter beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum über die Veröffentlichung von Geburtsdaten der Kandidaten zur Kommunalwahl im Jahr 2009 auf der Internetseite des Thüringer Landesamts für Statistik (TLS).

Der TLfDI vertrat hierzu die Auffassung, dass eine Veröffentlichung personenbezogener Daten von Kandidaten zur Kommunalwahl im Internet mangels einer geeigneten Rechtsgrundlage nicht zulässig sei. Zu dieser Frage vom TLfDI zur Stellungnahme aufgefordert, teilte das TLS mit, dass es die Geburtsdaten der Kandidaten für die Kommunalwahlen 2014 nicht ins Internet einstellen werde. Diese Zusage wurde eingehalten.

Jedoch stellte der TLfDI im Falle der Landtagswahl 2014 fest, dass das TLS und die Stadt Erfurt die personenbezogenen Daten (Name, Vorname, Geburtsjahr, Wohnanschrift, Beruf) der Bewerber der zugelassenen Landeslisten bzw. Wahlkreisvorschläge auf ihren Internetseiten veröffentlicht hatten. Da auch in diesen Fällen eine ge-

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

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

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

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

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

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

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

5.22 Eine amtliche E-Mail als lehrreiches Eigentor

Das Ordnungsamt einer Stadtverwaltung hatte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum eine Ordnungswidrigkeiten-Anzeige nebst Anlagen mit den darin enthaltenen personenbezogenen Daten per E-Mail in unverschlüsselter Form übersandt.

Aus diesem Anlass wies der TLfDI die verantwortliche Stadtverwaltung darauf hin, dass für die Zulässigkeit einer Datenübermittlung personenbezogener Daten an eine andere öffentliche Stelle die übermittelnde Stelle verantwortlich ist (§ 21 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG)). Nach § 9 i. V. m. § 3 Abs. 3 ThürDSG haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, auf der Grundlage eines Sicherheitskonzeptes die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses

Gesetzes zu gewährleisten. Hierzu zählen gemäß § 9 Abs. 2 Nr. 1 bis 6 ThürDSG die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und die Transparenz. Um diese Ziele auch bei der Datenübermittlung von personenbezogenen Daten über den unsicheren Übertragungsweg per E-Mail zu gewährleisten, ist sicherzustellen, dass Unbefugte durch geeignete Verschlüsselungsverfahren die Daten nicht zur Kenntnis nehmen können. Kann die öffentliche Stelle dies nicht gewährleisten, so hat sie den (sicheren) Postweg zu nutzen.

Im Ergebnis stellte der TLfDI fest, dass eine unverschlüsselte Übermittlung personenbezogener Daten mittels des unsicheren Übertragungsweges per E-Mail gegen datenschutzrechtliche Bestimmungen verstößt und bat, dafür Sorge zu tragen, dass die o. g. Hinweise künftig in der verantwortlichen Stadtverwaltung beachtet werden. Zugleich bat der TLfDI, ihm die Regelungen der Stadtverwaltung zum Umgang mit elektronischer Kommunikation (E-Mail) zu übersenden. Daraufhin teilte die Stadtverwaltung dem TLfDI mit, dass die unverschlüsselte E-Mail aus Versehen übersandt worden sei und sie zukünftig die datenschutzrechtlichen Vorgaben beachte. Der TLfDI stellte fest, dass vorgelegte Regelung der Stadtverwaltung zum Umgang mit elektronischer Kommunikation (E-Mail) den datenschutzrechtlichen Vorgaben entsprach.

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

5.23 Hunger des Landratsamtes Saale-Orla-Kreis auf Grundsteuerdaten

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

das Landratsamt des Saale-Orla-Kreises zur Mietwerterhebung zum Zwecke der Feststellung der Angemessenheitsgrenzen der Kosten der Unterkunft für Leistungsempfänger nach dem SGB II und SGB XII von der Stadtverwaltung Bad Lobenstein die Anzahl der Grundeigentümer, die Adressdaten kleiner Vermieter, bei denen vermutet wurde, dass diese Wohnraum vermieten, sowie die Adressen etwaiger Mietobjekte.

Nach datenschutzrechtlicher Prüfung vertrat der TLfDI im konkreten Fall die Auffassung, dass eine Übermittlung der Anzahl der potentiellen Vermieter keinen datenschutzrechtlichen Bedenken begegnet.

Nach § 31 Abs. 3 Abgabenordnung (AO) dürfen Gemeinden Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung der Grundsteuer bekannt geworden sind, zur Verwaltung anderer Aufgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben verwenden. Sofern nicht schutzwürdige Verhältnisse des Betroffenen überwiegen, dürfen diese Verhältnisse auch den zuständigen Gerichten, Behörden und anderen juristischen Personen des öffentlichen Rechts offenbart werden. Da ein Überwiegen schutzwürdiger Interessen der betroffenen Grundstückseigentümer gegenüber der Aufgabe des Landratsamtes zur Mietwerterhebung zum Zwecke der Feststellung der Angemessenheitsgrenzen der Kosten der Unterkunft für Leistungsempfänger nach dem SGB II und SGB XII nicht ersichtlich war, war eine Übermittlung der Namen und Anschriften von Grundstückseigentümer zu dem o. g. Zweck zulässig.

Anders stellte sich die Rechtslage nach Auffassung des TLfDI für die Übermittlung von Adressen etwaiger Mietobjekte dar:

Mangels einer geeigneten Rechtsgrundlage war eine Übermittlung der Adressen etwaiger Mietobjekte nicht zulässig. § 31 Abs. 3 AO war in diesem Fall nicht anwendbar, da danach nur Name und Anschrift der Grundstückseigentümer mitgeteilt werden dürfen und somit bei der gebotenen restriktiven Auslegung dieser Norm kein Raum für die Übermittlung weiterer Datenarten bestand.

Zur Frage, ob sich öffentliche Stellen privater Dienstleister zur Verarbeitung von Steuerdaten zur Mietwerterhebung, etwa im Wege der Auftragsdatenverarbeitung, bedienen dürfen, vertrat der TLfDI folgende Auffassung:

Der Anwendungsbereich der AO wird nach § 15 Thüringer Kommunalabgabengesetz (ThürKAG) eröffnet. Hier ist geregelt, dass für Kommunalabgaben die Abgabenordnung anzuwenden ist, soweit gesetzlich nichts anderes bestimmt ist. Insbesondere ist damit

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

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

5.24 Mystery-Check im Thüringer Wald

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

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

Der TLfDI hat den festgestellten Sachverhalt wie folgt bewertet:

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

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

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

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

unbedeutend wäre. Die Kenntnis der Daten ist dann erforderlich, wenn die öffentliche Stelle im jeweiligen konkreten Einzelfall ihre Aufgaben nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und außerdem erst aktuell dann und nur in dem Umfang, wie es die Aufgabenerfüllung gerade in Bezug auf die betroffene Person erfordert (Sokol in Simitis, Bundesdatenschutzgesetz, 6. Auflage, § 13, Randnummern 25 und 26).

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

Im konkreten Fall war hier weder eine Rechtsvorschrift im Sinne des § 19 Abs. 2 Nr. 1 ThürDSG ersichtlich, auf die diese Datenerhebung gestützt werden konnte, noch konnte angenommen werden, dass eine Verwaltungsaufgabe einen derartigen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Inhaber und Mitarbeiter der befragten Unternehmen zwingend voraussetzte bzw. erforderlich machte. Da im Ergebnis nicht erkennbar war, dass die Zulässigkeitsvoraussetzungen des § 19 Abs. 2 ThürDSG vorlagen, stellte die Erhebung und Verarbeitung von personenbezogenen Daten mittels des Verfahrens „Mystery-Check“ einen Verstoß gegen datenschutzrechtliche Vorschriften dar.

Aufgrund dieser Bewertung beanstandete der TLfDI die rechtswidrige Erhebung und Verarbeitung personenbezogener Daten von Beherbergungsunternehmen schließlich gegenüber den für die unzulässige Datenerhebung verantwortlichen Mitgliedsgemeinden des KAG gemäß § 39 Abs. 1 Satz 1 ThürDSG. Der TLfDI unterrichtete ferner die für die betroffenen Gemeindeverwaltungen zuständigen Kommunalaufsichten des Ilm-Kreises, der Landkreise Gotha und Schmalkalden-Meinungen sowie der Stadt Suhl von der o. g. Beanstandung. Abschließend wurden dem TLfDI die Protokolle zum Nachweis der erfolgten Löschung der unrechtmäßig erhobenen Daten vorgelegt.

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

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

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

Da insofern ein Verstoß gegen amtsbezogene Geheimhaltungspflichten sowie datenschutzrechtliche Bestimmungen nicht ausgeschlossen werden konnte, konfrontierte der TLfDI die Bürgermeisterin mit dem o. g. Beschwerdegegenstand.

Hierzu teilte die Bürgermeisterin mit, dass sie zwar nach der Versammlung vor dem Verwaltungsgebäude noch einige Minuten mit Gemeinderäten zusammengestanden habe. Dabei habe sie jedoch weder ein amtliches Schreiben verlesen noch personenbezogene Daten im Zusammenhang mit einer Vollstreckungsangelegenheit offenbart.

Der TLfDI wies den Beschwerdeführer in diesem Zusammenhang darauf hin, dass ihm keine vergleichbaren gesetzlichen Befugnisse zur exakten Klärung des realen Sachverhalts, wie etwa einer Staatsanwaltschaft, zur Verfügung stünden. Beurteilungsprobleme ergeben sich für den TLfDI insbesondere dann, wenn zwei plausible, sich jedoch widersprechende Sachverhalte vorgetragen werden und weitere Recherchen keine Aussicht auf Erfolg bieten. Dem TLfDI stehen auch in so einem Fall „nur“ ein Auskunfts- und Fragerecht gegenüber den öffentlichen Stellen und ein Einsichtsrecht in Akten und Dateien gemäß § 38 Abs. 1 Satz 2 Nr. 1 ThürDSG sowie ein Zutrittsrecht zu allen Diensträumen der öffentlichen Stellen gemäß § 38 Abs. 1 Satz 2 Nr. 2 ThürDSG zur Verfügung.

Leider war es auch in diesem Falle mit den Mitteln, die dem TLfDI zu Gebote stehen, ausgeschlossen, zweifelsfrei festzustellen, ob die Bürgermeisterin personenbezogene Daten im Zusammenhang mit einer Vollstreckungsangelegenheit offenbart hat. Da von der Beantwortung dieser Frage jedoch die datenschutzrechtliche Beurteilung der konkreten Angelegenheit entscheidend abhing, war die Angelegenheit für den TLfDI nicht weiter aufklärbar.

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

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

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erlangte über folgenden Beschwerdesachverhalt Kenntnis:

Das Bürgeramt Erfurt habe die Ehefrau des Beschwerdeführers als verantwortliche Fahrerin für eine Geschwindigkeitsüberschreitung ermittelt, da deren Daten samt Lichtbild aus einem vorherigen Verfahren mit demselben Fahrzeug vorgelegen hätten. Der Halter des Fahrzeugs sei der Schwiegervater der Fahrerin.

Der Beschwerdeführer bat den TLfDI deshalb, mitzuteilen, ob und inwieweit die Identität des Fahrers bzw. der Fahrerin mittels Lichtbildabgleich – auch von mit im Haushalt eines Fahrzeughalters lebenden Angehörigen – durch Einsichtnahme in das Personalausweisregister ermittelt werden dürfe.

Wie die Stadtverwaltung Erfurt zunächst auf Anfrage des TLfDI mitteilte, habe aufgrund einer Recherche im EDV-Verfahren SCOWI und dem augenscheinlichen Alter der Fahrerin der Verdacht bestanden, dass sie, die Ehefrau des Beschwerdeführers, auch im aktuellen Verfahren das Kfz gefahren haben könnte. Um dies abzuklären, sei daraufhin ein Passbildabgleich gemäß § 24 Personalausweisgesetz (PAuswG) durchgeführt worden. Von einer Vorortermittlung durch den Außendienst sei gemäß § 24 Abs. 2 Nr. 3 PAuswG abgesehen worden, da der damit verbundene Aufwand gegenüber der Recherche im Personalausweisregister zu hoch sei.

Die Frage, die sich für den TLfDI stellte, war nun, zu prüfen, unter welchen Voraussetzungen ein solcher Lichtbildabgleich in Thüringen zulässig ist. Dabei stieß der TLfDI auf die Nummer 2.3.2 der Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei (VwV VASTvOWi) vom 19. Dezember 2006 (ThürStAnz. 2007, S. 171), der die Modalitäten des Lichtbilderabgleichs mit Passfotos aus dem Personalausweis bzw. Passregister zur Verfolgung von Verkehrsordnungswidrigkeiten regelt. Zur Auslegung dieser Regelung teilte das ehemalige Thüringer Innenministerium (TIM) dem TLfDI im Oktober 2014 u. a. Folgendes mit:

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

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

Im Beschwerdefall hätte somit nur das Lichtbild des Fahrzeughalters bzw. von dessen Ehefrau, nicht jedoch das Lichtbild der Schwiegertochter angefordert werden dürfen.

Aufgrund der o. g. Auslegung der Verwaltungsvorschrift VwV VA-StVOWi bat der TLfDI die Stadtverwaltung, zur Zulässigkeit des Lichtbilderabgleichs mittels des Personalausweisregisters im konkreten Fall sowohl rechtlich als auch tatsächlich Stellung zu nehmen. Die Stadtverwaltung legte sodann dem TLfDI dar, dass es sich aus ihrer Sicht beim Beschwerdeführer um einen von der Eintragung im Fahrzeugregister abweichenden Kfz-Halter im Sinne des Beschlusses des OLG Schleswig-Holstein vom 20. September 2004, 2 Ss 133/04 gehandelt habe. Nach diesem Beschluss sei derjenige als Halter anzusehen, der die Kosten bestreitet und tatsächlich über die Fahrzeugnutzung verfügen könne.

Vom TLfDI zu dieser Sachverhaltsauslegung durch die Stadtverwaltung Erfurt befragt, erklärte der Beschwerdeführer, dass er zwar das Kfz genutzt habe, jedoch sein Vater, der Kfz-Halter, die Kosten für das Fahrzeug tragen würde.

Wie weitere Recherchen des TLfDI ergaben, lagen der Stadtverwaltung Erfurt keine nachvollziehbaren Anhaltspunkte dafür vor, dass es sich beim Beschwerdeführer um einen von der Eintragung im Fahrzeugregister abweichenden Kfz-Halter im Sinne des genannten Beschlusses des OLG Schleswig-Holstein vom 20. September 2004 gehandelt hatte.

Somit erfolgte der Lichtbildabgleich des Blitzerfotos mit der Abbildung der Ehefrau des Beschwerdeführers durch die Stadt Erfurt entgegen der Nummer 2.3.2 der Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei (VwV VASTVOWi) vom 19. Dezember 2006 (Thür. Staatsanzeiger 2007, S. 171).

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

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

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

5.27 Rechtswidrige Datenübermittlung - der geblitzte künftige MP?

Am 17. April 2014 um 9:38 Uhr erfasste die Blitzer-Säule an der Bundesstraße 7 bei Weimar ein zu schnell fahrendes Auto mit dem amtlichen Kennzeichen EF-... . Dieser Sachverhalt, der in Deutschland jeden Tag tausendfach geschieht, wäre für eine Zeitung eigentlich uninteressant. In diesem Fall stand der mutmaßliche Fahrer aber wegen der Landtagswahl 2014 im Rampenlicht der Presse.

Am 6. November 2014 veröffentlichte die Bild-Zeitung in diesem Zusammenhang unter der Überschrift „Wird hier Thüringens neuer Landeschef geblitzt?“ einen Artikel mit Bildern. Auf einem dieser Bilder, einem so genannten Radarbild, soll der Vorsitzende der Fraktion DIE LINKE im Thüringer Landtag, Bodo Ramelow, zu erkennen gewesen sein.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm in der Folge Ermittlungen zum geschilderten Sachverhalt auf, weil der Verdacht im Raum stand, dass das in der Bild-Zeitung veröffentlichte Blitzerfoto aus der Verfahrensakte stammen könnte. Eine solche Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs ist nur unter den engen Voraussetzungen von § 22 ThürDSG zulässig. Deshalb stand hier eine unzulässige Datenübermittlung im Raum.

Im Zuge der Ermittlungen führte der TLfDI Kontrollen bei der Stadtverwaltung Weimar sowie bei der Staatsanwaltschaft Erfurt

durch. Gleichzeitig wurde die Direktorin des Amtsgerichtes Weimar zu diesem Sachverhalt befragt.

Trotz umfangreicher und mehrfacher Untersuchungen konnte der TLfDI im Ergebnis keine verwertbaren Beweise für ein Fehlverhalten der genannten öffentlichen Stellen feststellen, das zur Übermittlung der personenbezogenen Daten des Fahrers – hier also des Fotos – geführt hatte.

Indizien dafür, dass ein(e) infrage kommende(r) MitarbeiterIn der Stadtverwaltung Weimar die entsprechenden Fotos einer dritten Person übermittelt haben könnte, konnte der TLfDI nicht erhärten.

Anlässlich seiner Ermittlungen stellte der TLfDI jedoch fest, dass insgesamt 17 Personen bei der Stadtverwaltung Weimar zugriffsberechtigte Nutzer der dazugehörigen elektronischen Akte waren. Nach § 9 Abs. 2 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) ist zu gewährleisten, dass in jedem Falle nur die befugten Personen personenbezogene Daten in Ordnungswidrigkeitenverfahren zur Kenntnis nehmen können, damit die Vertraulichkeit gewahrt ist. In diesem Zusammenhang empfahl der TLfDI der Stadtverwaltung Weimar dringend, den Kreis der Zugriffsberechtigten, insbesondere zur elektronischen Akte, zu beschränken.

Ebenfalls konnte der TLfDI letztlich nicht aufklären, ob und wie gegebenenfalls Mitarbeiterinnen oder Mitarbeiter der Staatsanwaltschaft Erfurt für die Übermittlung des Lichtbildes verantwortlich waren.

Auch die Nachfrage bei der Direktorin des Amtsgerichtes Weimar hat keine Anhaltspunkte dafür ergeben, dass Bedienstete des Gerichtes das fragliche Foto des Fahrers einem Dritten übermittelt haben könnten.

Letztlich konnte der TLfDI somit nicht belastbar ermitteln, wer das Blitzerfoto an die Bild-Zeitung oder einen Dritten übermittelt hatte.

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

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

5.28 Geblitzt – wer darf Daten auswerten?

Die Stadt Erfurt wandte sich mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob für die stationäre Geschwindigkeitsüberwachung in der Landeshauptstadt Erfurt durch einen externen Auftragnehmer ein Vertragsverhältnis zur Datenverarbeitung im Auftrag nach der Mustervereinbarung gemäß dem 5. Tätigkeitsbericht des TLfDI, Anlage 23, geschlossen werden muss. Für die Beantwortung dieser Frage ist entscheidend, ob es sich um eine Auftragsdatenverarbeitung nach § 8 Thüringer Datenschutzgesetz (ThürDSG) handelt. Das setzt voraus, dass die Stadt Erfurt weiterhin für die Verarbeitung und deren Ergebnisse verantwortlich bleibt und keine umfassende Funktionsübertragung an die externe Firma vorliegt. Eine Funktionsübertragung wäre nur durch oder aufgrund Gesetzes möglich. Da ein solches Gesetz nicht vorliegt, wäre die Datenerhebung durch die externe Firma unzulässig.

Auf Nachfrage des TLfDI teilte die Stadt Erfurt mit, dass im Rahmen der Dienstleistungen des Auftragnehmers die an den Messstationen entstandenen Daten zur amtlichen Kontrollauswertung durch die Behörde aufbereitet werden. Die Datenauswertung und -verarbeitung wird ausschließlich von der Stadt Erfurt vorgenommen. Die Aufarbeitung besteht lediglich darin, dass der Auftragnehmer Bilder in der Totalansicht sowie Bildausschnitte vom Fahrer und Kennzeichen generiert. Es werden Datum und Uhrzeit der Aufnahme und die gemessene Geschwindigkeit des Fahrzeugs und das am Standort geltende Geschwindigkeitslimit dargestellt. Diese Daten werden der Behörde zum Abruf auf einem gesicherten Server des Anbieters bereitgestellt. Die Aufbereitung dient allein dazu, dass die Stadt Erfurt die Bilder einer rechtlichen Prüfung unterziehen kann. Damit bleibt weiterhin die Stadt Erfurt die datenschutzrechtlich verantwortliche Stelle, eine Funktionsübertragung an den Auftragnehmer liegt nicht vor. Es ist daher ein Vertrag zu schließen, der den Anforderungen des § 8 ThürDSG entspricht.

Die Stadt Erfurt legte dem TLfDI den Vertrag zur Auftragsdatenverarbeitung im Anschluss zur Prüfung vor. Der TLfDI stellte nach

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

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

5.29 Personenbeziehbarkeit von Daten zu einem Stadtentwicklungskonzept

Eine Stadtverwaltung bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum um die Bewertung der von ihr vorgesehenen Datenübermittlung an ein privates Planungsbüro im Rahmen der Fortschreibung eines Stadtentwicklungskonzeptes. Konkret begehrte das Planungsbüro unter anderem gebäudedifferenzierte Daten zur Altersstruktur, zur Stellung der Einwohner der Kommune im Erwerbsleben, zur Verkehrsmittelverfügbarkeit, zu Verkehrsmitteln und Verkehrszielen.

Zu diesem Vorhaben äußerte der TLfDI seine datenschutzrechtlichen Bedenken. Diese beruhten insbesondere darauf, dass bei der Erhebung der Verkehrsquellen bzw. -ziele eine adressscharfe Auflistung der Firmen mit konkreten Angaben über die jeweiligen Zufahrten und ihre Lieferanten und Kunden sowie der Anzahl der jeweils Beschäftigten gefordert wurde.

Da sich aus diesen Daten relativ leicht Personenbezüge ableiten ließen, schlug der TLfDI vor, die Einzelangaben nach Straßenabschnitten zusammenzufassen und die Anzahl der Beschäftigten und die Lieferanten und Kunden nicht als konkreten Wert, sondern in Form einer Von-bis-Spanne, zu übermitteln. Die Stadt Suhl hat den Vorschlag des TLfDI berücksichtigt und die o. g. Daten nur in der empfohlenen Form an das Planungsbüro übermittelt.

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

5.30 Rathaus-Videokamera: dieses Mal nicht so gaga!

Ein Bürger setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) anonym über eine Videokamera am Rathaus Geschwenda in Kenntnis, wobei er sich darüber beschwerte, dass kein optischer Hinweis auf den Umstand der Überwachungsmaßnahme existiere.

Nachfolgend bat der TLfDI die Gemeindeverwaltung Geschwenda, zu der Angelegenheit Stellung zu nehmen und insbesondere mitzuteilen, auf welcher Rechtsgrundlage die Videoüberwachung beruhe und zu welchem Zwecke sie erfolge. Weiterhin forderte der TLfDI, ihn über die konkreten technisch-organisatorischen Regelungen zum Betrieb der Videoanlage in Kenntnis zu setzen (unter Berücksichtigung der unter Gliederungspunkt 5.2 ab S. 35 ff. des achten TLfDI-Tätigkeitsberichts aufgelisteten Kriterien zum Betrieb kommunaler Videoanlagen). Dazu forderte der TLfDI die entsprechenden Unterlagen, z. B. in Form einer Dienstanweisung, an.

Die Gemeindeverwaltung Geschwenda antwortete dem TLfDI, dass sie die Videoüberwachung zur Vermeidung von Beschädigungen am Rathaus und der angrenzenden Bushaltestelle installiert habe. Es seien von ihr mehrere Hinweisschilder auf die Videoüberwachung angebracht worden. Da es in den vergangenen Jahren mehrfach zu Randalen im Ort gekommen sei und die Gemeinde die im Rahmen der Dorferneuerung geschaffenen Werte erhalten wolle, sei die Installation einer Videoüberwachung erforderlich gewesen. Die Notwendigkeit des Betreibens der Anlage prüfe die Gemeinde zweimal im Jahr. Die von der Gemeindeverwaltung Geschwenda vorgelegte Dienstanweisung zum Einsatz von Videotechnik entsprach den datenschutzrechtlichen Vorgaben, insbesondere denen des § 25a Thüringer Datenschutzgesetz (ThürDSG). Im Ergebnis hatte der TLfDI daher keine Einwände gegen die geschilderte Videoüberwachung. Dies ergab sich auch daraus, dass der Bürger, der den TLfDI über die Videoüberwachung in Kenntnis gesetzt hatte, selbst keine eigene Beeinträchtigung seiner schutzwürdigen Interessen geltend gemacht

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

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

5.31 Videogaga 2 in Piesau

Ein Beschwerdeführer setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber in Kenntnis, dass am Gemeindeamt Piesau und am Treffpunkt der Gemeindejugend im Bauhof der Gemeinde Piesau je eine Videokamera installiert sei.

Der TLfDI wies die Bürgermeisterin von Piesau in diesem Zusammenhang auf die Regelung des § 25a Thüringer Datenschutzgesetz (ThürDSG) hin und bat sie, zu der Angelegenheit Stellung zu nehmen. Dabei interessierte den TLfDI, auf welcher Rechtsgrundlage die o. g. Videoüberwachungen beruhten und zu welchem Zwecke sie erfolgten. Zugleich forderte der TLfDI die Bürgermeisterin auf, ihn über die konkreten technisch-organisatorischen Regelungen der Gemeinde Piesau zum Betrieb der beiden Videokameras in Kenntnis zu setzen und entsprechende Unterlagen, z. B. in Form einer Dienstanweisung, zu übersenden. Der TLfDI verwies dabei auf die unter Gliederungspunkt 5.2 (Seiten 35 ff.) seines achten Tätigkeitsberichts aufgelisteten Kriterien zum Betrieb kommunaler Videoanlagen.

Daraufhin informierte die Bürgermeisterin den TLfDI darüber, dass beide o. g. Videokameras schon seit längerem defekt und außer Betrieb seien.

Zu diesem neuen Sachverhalt nahm der TLfDI gegenüber der Bürgermeisterin von Piesau wie folgt Stellung:

Auch deaktivierte Kameras können ebenso wie Kameraattrappen bei Passanten bzw. Besuchern den Anschein erwecken, dass ihr Verhalten überwacht werde. Dies könne eine negative Beeinflussung des

Verhaltens von Bürgern zur Folge haben. Somit sei die Angelegenheit gemäß § 25a ThürDSG zu beurteilen.

Im Ergebnis ging der TLfDI von einer datenschutzrechtlichen Unzulässigkeit der Installation der (deaktivierten) Videokameras bzw. Kameraattrappen aus, da Betroffene davon ausgehen konnten, dass sie mit derart platzierten Kameras aufgenommen werden.

Der TLfDI forderte die Bürgermeisterin von Piesau auf, beide Videokameras abzubauen bzw. sie mittels einer Schutzfolie erkennbar zu deaktivieren und ihn über den Vollzug dieser Maßnahmen in Kenntnis zu setzen.

Nachfolgend informierte die Bürgermeisterin von Piesau den TLfDI darüber, dass die defekten Kameras am Gemeindeamt und am Treffpunkt der Gemeindejugend mit einer Schutzfolie abgedeckt worden und damit nicht mehr sichtbar seien.

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

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

Die Stadtverwaltung Jena legte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum Unterlagen zur Software zum vorbeugenden Brandschutz (VoBraWeb) zur Bewertung vor. Die Stadtverwaltung beabsichtigte, der verantwortlichen Softwarefirma einen Auftrag zu erteilen. Jedoch vertrat die Softwarefirma zunächst die Auffassung, dass hierbei ein Vertrag über eine Auftragsdatenverarbeitung im Sinne des § 8 Thüringer Datenschutzgesetz (ThürDSG) nicht abgeschlossen werden müsste.

Der TLfDI stellte nach datenschutzrechtlicher Prüfung fest, dass im o. g. Verfahren personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG, z. B. Name, Adresse und Telefonnummer von Hauseigentümern als Kontaktdaten, verarbeitet und genutzt wurden. Unerheblich war dabei, ob diese Daten anderweitig öffentlich zugänglich waren. Bei dem Verfahren VoBraWeb stellt die Soft-

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

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

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

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

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



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

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

an die Softwarefirma zu erteilen sei, falls das Unternehmen den Abschluss eines solchen Vertrages gemäß § 8 ThürDSG ablehnen sollte.

Letztendlich legte die Stadtverwaltung Jena dem TLfDI einen sowohl von ihr als auch der Softwarefirma unterschriebenen datenschutzkonformen Vertrag zur Auftragsdatenverarbeitung vor.

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

5.33 Offene Unterstützungslisten bei der Kommunalwahl

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die Unterstützungslisten von Kandidaten der Kommunalwahlen, die in der Stadtverwaltung geführt werden, mit den darin enthaltenen personenbezogenen Daten der Unterstützer für diejenigen sichtbar seien, der vorgebe, sich in der betreffenden Unterstützungsliste eintragen zu wollen.

Hierzu teilte der TLfDI mit, dass nach § 14 Abs. 6 Satz 1 und 2 Thüringer Kommunalwahlgesetz Wahlberechtigte, die einen Wahlvorschlag unterstützen wollen, sich in den bei der Gemeinde ausgelegten Unterstützungslisten unter Angabe ihres Vor- und Nachnamens, ihrer Anschrift und ihres Geburtsdatums einzutragen und eine eigenhändige Unterschrift zu leisten haben.

Mit Schreiben vom 24. März 2014 hatte sich das frühere Thüringer Innenministerium (TIM) gegenüber dem Thüringer Landesverwaltungsamt, den Landkreisen, Gemeinden, Verwaltungsgemeinschaften und Wahlleitern zu der o. g. Thematik wie folgt geäußert:

„Der Wahlvorschlag ist vom Tag nach der Einreichung verbunden mit einer Liste zur Leistung von Unterstützungsunterschriften während der üblichen Dienstzeiten der Gemeindeverwaltung zur Unterschriftsleistung auszulegen. Aus Datenschutzgründen ist darauf zu achten, dass die Unterschriftsleistenden nicht die bereits geleisteten Unterschriften einsehen (z. B. durch Abdecken); auch Beauftragte des Wahlvorschlags haben kein Einsichtsrecht.“

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

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

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

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Information, dass die Stadt Jena ein Baulandkataster mit Grundstücken einer bestimmten Mindestgröße, die als potenzielles Bauland in Betracht kamen, erstellt und öffentlich zugänglich gemacht hätte. Bedenklich erschien hierbei die Gestaltung der Widerspruchsmöglichkeit der Grundstückseigentümer. Nach § 200 Abs. 3 Satz 2 und 3 Baugesetzbuch (BauGB) kann die Gemeinde die betreffenden Flächen veröffentlichen, soweit der Grundstückseigentümer nicht widersprochen hat. Die Gemeinde hat danach ferner ihre Absicht zur Veröffentlichung einen Monat vorher öffentlich bekannt zu geben und dabei auf das Widerspruchsrecht der Grundstückseigentümer hinzuweisen.

Die Stadt Jena hatte in ihrem Amtsblatt mitgeteilt, dass sie beabsichtige, frühestens nach Ablauf eines Monats, gerechnet ab der Bekanntgabe ihrer Veröffentlichungsabsicht, auf ihrer Internetseite ein Baulandkataster zu jedermanns Einsicht bereitzuhalten. Die Stadt führte weiter aus, dass im Fall von fristgerechten Widersprüchen die betroffenen Grundstücke aus dem Baulandkataster entfernt würden. Ein zusätzlicher Passus besagte, dass „... *nach Fristablauf eingehende Widersprüche nur insoweit Berücksichtigung finden, als dass eine nachträgliche Streichung der Angaben ohne unverhältnismäßigen Aufwand möglich ist.*“ Eine dem kursiv gekennzeichneten Wort-

laut entsprechende Mitteilung befand sich auch in einem Anschreiben der Stadt Jena an die betroffenen Grundstückseigentümer. Die Stadt teilte erst auf Nachfrage des TLfDI mit, dass sich der o. g. kursiv gekennzeichnete Wortlaut ausschließlich auf nicht-digitale Formen des Baulandkatasters bezöge, wobei Bürger gedruckte Karten mit den Baulandkatasterflächen in der Stadtverwaltung einsehen könnten. Laut der Aussage der Stadt Jena hätte es einen unverhältnismäßigen Aufwand bedeutet, diese Karten nach jedem einzelnen Widerspruch neu zu drucken.

Das Anschreiben der Stadt Jena an die betroffenen Grundstückseigentümer enthielt die Anlage *„Information: Fragen und Antworten“*, das auch als PDF-Dokument auf der Internetseite der Stadt Jena abrufbar war. Darin enthalten war der Hinweis: *„Wurde Ihr Grundstück bereits im Baulandkataster veröffentlicht, so können Sie auch zu einem späteren Zeitpunkt der Veröffentlichung widersprechen. Das in Ihrem Eigentum befindliche Grundstück wird zum nächstmöglichen Zeitpunkt aus der im Internet veröffentlichten Datenerfassung entfernt.“*

Aus dem Wortlaut des Amtsblattes, dass die nach Fristablauf eingehenden Widersprüche nur berücksichtigt würden, wenn deren Umsetzung keinen unverhältnismäßigen Aufwand erfordere, entstand der Eindruck, dass die Stadt Jena nicht alle Widersprüche bearbeiten werde. Zudem enthielt das Amtsblatt keinen Hinweis dazu, dass sich diese genannte Einschränkung nur auf nicht-digitale Formen des Baulandkatasters in Form von gedruckten Karten bezog. Die Formulierung im Amtsblatt, wonach Eigentümer mittels eines unter einer angegebenen Internetadresse abrufbaren Formulars auch nach der Veröffentlichung des Katasters von ihrem Widerspruchsrecht Gebrauch machen könnten, ließ zudem einen Hinweis darüber vermischen, dass auch schriftliche Widersprüche, bei denen das Formular nicht benutzt wurde, jederzeit von der Stadt Jena bearbeitet werden. Zusammenfassend stellte der TLfDI fest, dass die Informationen zum Widerspruchsrecht unvollständig waren, sich teilweise widersprachen und somit für den Bürger irritierend sein konnten. Einzig die *„Information: Fragen und Antworten“* entsprach – für sich genommen – den Vorgaben des § 200 Abs. 3 Satz 2 und 3 BauGB, wonach ein Grundstückseigentümer der Veröffentlichung hinsichtlich der ihn und sein Grundstück betreffenden Angaben jederzeit auch nach Ablauf der Monatsfrist widersprechen kann (Battis/Krautzberger/Löhr, BauGB-Kommentar, 12. Auflage, Anm. 9 zu

§ 200, S. 1512 und inhaltsgleich BauGB-Kommentar, 7. Auflage, W. Schröder, Anm. 8, S. 1958).

Der TLfDI bat die Stadt um Mitteilung, welche Maßnahmen sie zur Herstellung einer umfassenden und widerspruchsfreien Information der Betroffenen zur Wahrnehmung des Widerspruchsrechts zum Baulandkataster beabsichtige. Der TLfDI selbst schlug vor, eine klarstellende Presseerklärung zu veröffentlichen oder ein entsprechendes Anschreiben zu erstellen. Die Stadt Jena folgte dem Hinweis des TLfDI und teilte ihm daher mit, eine entsprechende Pressemitteilung vorzubereiten.

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

5.35 Der mitteilsame Oberbürgermeister – Vorsicht bei Pressemitteilungen

Im Berichtszeitraum erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis über einen Sachverhalt, der im Laufe seiner Kontrollpraxis der letzten Jahre als alles andere als datenschutzrechtlich „gewöhnlich“ zu bezeichnen war.

Ein leitender Beamter der Stadt Nordhausen berichtete dem TLfDI, dass gegen ihn eine Staatsanwaltschaft ein strafrechtliches Ermittlungsverfahren wegen des Vorwurfs des sexuellen Missbrauchs widerstandsunfähiger Personen gemäß § 179 Abs. 5 Strafgesetzbuch geführt habe. Hauptbelastungszeugin sei eine Kollegin des Beamten und zugleich das mutmaßliche Opfer (so genannte Opferzeugin) gewesen. Ende September 2013 habe die zuständige Staatsanwaltschaft dieses Ermittlungsverfahren aber gemäß § 170 Abs. 2 Strafprozessordnung eingestellt. Der Grund dafür war, was die Recherchen des TLfDI bestätigten, dass die Staatsanwaltschaft keine Anhaltspunkte für ein dem beschuldigten Beamten vorgeworfenes Han-

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

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

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



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

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

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

gelangt. Die datenschutzrechtliche Prüfung durch den TLfDI ergab dabei Folgendes:

Bei den Informationen „Geschlechtsverkehr unter Alkoholeinfluss“ handelte es sich zunächst um Einzelangaben über persönliche Verhältnisse von bestimmbaren Personen und damit um personenbezogene Daten im Sinne von § 3 Abs. 1 ThürDSG. Denn sowohl bei der Information „Geschlechtsverkehr“ als auch bei der Information „unter Alkoholeinfluss“ werden geistige Zustände bzw. körperliche Merkmale genannt, die allesamt unter den Begriff der persönlichen Verhältnisse zu subsumieren sind (vgl. Dammann in: Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 3, Rz. 10). Diese persönlichen Verhältnisse waren auch auf den beschuldigten Beamten bzw. die Opferzeugin eindeutig beziehbar.

Indem die Stadtverwaltung Nordhausen die genannten beiden personenbezogenen Daten im unmittelbaren Kontext (Geschlechtsverkehr unter Alkoholeinfluss) in der Pressemitteilung erwähnte und diese per E-Mail an den Presseverteiler versandte, übermittelte sie diese auch im Sinne von § 3 Abs. 3 Nr. 4. a) ThürDSG.

Die Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ durch die Pressemitteilung des Oberbürgermeisters erfolgte auch ohne Rechtsgrundlage. Denn weder war die Datenübermittlung durch § 22 Abs. 1 Nr. 1 ThürDSG noch durch § 22 Abs. 1 Nr. 2 ThürDSG gerechtfertigt.

§ 22 Abs. 1 Nr. 1 ThürDSG schied im vorliegenden Sachverhalt als Ermächtigungsgrundlage aus, weil die Übermittlung des genannten personenbezogenen Datums „unter Alkoholeinfluss“ zur Erfüllung der Aufgaben des Oberbürgermeisters nicht erforderlich gewesen ist. Der Oberbürgermeister berief sich zwar darauf, dass er aus der „Fürsorgepflicht des Dienstherrn“ gehalten war, „unabgewogene(n) Pressemitteilungen“ und dem Eindruck entgegenzuwirken, dass die Opferzeugin „nachweislich gelogen habe“. Selbst wenn der TLfDI aber in dieser Frage unterstellt hätte, dass eine solch weitgehende Fürsorgepflicht des Dienstherrn tatsächlich existierte, so war es gleichwohl nicht erforderlich, dass der Oberbürgermeister quasi zur Wiederherstellung der Glaubwürdigkeit der Opferzeugin das personenbezogene Datum „unter Alkoholkonsum“ mit dem personenbezogenen Datum „Geschlechtsverkehr“ in einen unmittelbaren Kontext stellt und an die Presse übermittelt. Denn nach dem Grundsatz der Erforderlichkeit ist von mehreren geeigneten Maßnahmen diejenige zu wählen, die den einzelnen am wenigsten beeinträchtigt (siehe dazu Maurer,

Allgemeines Verwaltungsrecht, 17. Auflage, § 10, Rz. 17). Dafür hätte es ausgereicht, wenn der Oberbürgermeister allein darauf hingewiesen hätte, dass Aussage gegen Aussage stehe.

Auch § 22 Abs. 1 Nr. 2 ThürDSG konnte im vorliegenden Sachverhalt nicht als Rechtsgrundlage für die Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ herangezogen werden. Denn ein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hatte insbesondere der betroffene Beamte, aber auch die Opferzeugin.

Dieses bestand hier darin, die Öffentlichkeit nicht wissen zu lassen, dass es unter Alkoholeinfluss zwischen beiden zum Geschlechtsverkehr gekommen war. Denn bei dieser Information handelte es sich um ein – höchst persönliches – personenbezogenes Datum. Dieses personenbezogene Datum ist schützenswert im Sinne von § 22 Abs. 1 Nr. 2 ThürDSG, wenn es aus objektiver Sicht unter Zugrundelegung durchschnittlicher Verhältnisse zu Nachteilen für den Betroffenen führen kann (vgl. zur gleich lautenden Regelung in § 16 Abs. 1 Nr. 2 BDSG Dammann in: Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 16, Rz. 21). Welcher Art die drohenden Nachteile dabei sind, etwa wirtschaftlicher, sozialer oder persönlicher Art, ist dabei gleichgültig (vgl. auch insoweit, Dammann in Simitis, a.a.O., § 16, Rz. 22).

Vorliegend war der Nachteil für den betroffenen Beamten vor allem darin zu sehen, dass von ihm aufgrund der Pressemitteilung des Oberbürgermeisters das personenbezogene Datum des „Geschlechtsverkehrs unter Alkoholeinfluss“ in die Öffentlichkeit gelangte. Diese Information konnte seine Integrität, bzw. sein Ansehen beschädigen und damit zu sozialen und persönlichen Nachteilen führen.

Das Gleiche galt hier für die betroffene Opferzeugin. Zusätzlich war bei ihr an dieser Stelle zu berücksichtigen, dass durch Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ an die Presse der mit der Pressemitteilung des Oberbürgermeisters verfolgte Zweck, nämlich den Eindruck zu vermeiden, dass die Opferzeugin „nachweislich gelogen habe“, gerade nicht dienlich war und daher auch insoweit Nachteile persönlicher Art für die Opferzeugin zu befürchten waren.

Diese dargestellten schutzwürdigen Interessen des betroffenen Beamten und der betroffenen Opferzeugin wogen im Ergebnis auch höher als das Interesse der Pressevertreter, Detailkenntnisse über den Sachverhalt zu erfahren, der Gegenstand des strafrechtlichen Ermitt-

lungsverfahrens gegen den betroffenen Beamten war. Denn über die wesentlichen Gründe für die Einstellung des strafrechtlichen Ermittlungsverfahrens hatte der Pressesprecher der zuständigen Staatsanwaltschaft die Medien hinreichend unterrichtet.

Daran änderte auch der Einwand des Oberbürgermeisters nichts, dass sämtliche Presseartikel, die einen „Geschlechtsverkehr unter Alkoholeinfluss“ thematisiert hätten, zeitlich vor der Veröffentlichung der Pressemitteilung des Oberbürgermeisters erschienen seien.

Denn diese behauptete zeitliche Reihenfolge von Medienveröffentlichungen traf nach den Recherchen des TLfDI gerade nicht zu. Die vom Oberbürgermeister veröffentlichte Pressemitteilung war demnach am besagten Tag Ende September 2013 mindestens eineinhalb Stunden vor dem Erscheinen des Artikels im Portal „inSüdthüringen.de“ veröffentlicht worden. Dies konnte der TLfDI dem Oberbürgermeister anhand weiterer Presseveröffentlichungen an diesem Tage belegen.

Schließlich kam auch § 4 Abs. 1 Thüringer Pressegesetz (TPG) hier nicht als Ermächtigungsgrundlage für eine Datenübermittlung infrage. Dies ergab sich bereits aus § 4 Abs. 1 Satz 2 TPG. Danach steht in Thüringen einer Behörde gerade dann kein Ermessen hinsichtlich des presserechtlichen Auskunftsanspruchs zu, soweit Vorschriften über die Geheimhaltung und den Datenschutz entgegenstehen. In den genannten Fällen trifft die Behörde eine Pflicht zur Verschwiegenheit (so Weberling in: Ricker/Weberling, Handbuch des Presserechts, 6. Auflage, 4. Abschnitt, 20. Kapitel, Rz. 3; ebenso Löffler, Presserecht, 5. Auflage, Kommentar, § 4, Rz. 92). Eine solche Pflicht zur Verschwiegenheit traf im vorliegenden Fall auch den Oberbürgermeister, da ihn – wie dargelegt – die Regelungen von § 22 Abs. 1 Nr. 1 und Abs. 1 Nr. 2 ThürDSG an einer Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ an die Presse hinderten.

Aufgrund des Ergebnisses der datenschutzrechtlichen Prüfung beanstandete der TLfDI gemäß § 39 Abs. 1 Satz 1 ThürDSG die rechtswidrige Übermittlung des personenbezogenen Datums „unter Alkoholeinfluss“ in Form der Pressemitteilung des Oberbürgermeisters.

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

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

5.36 Eichsfelder Wurst oder Datenschutz bei Internetumfragen

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



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

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

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

Auswertung ihres Nutzungsverhaltens zur Verfügung stand, konnte der TLfDI auch in diesem Zusammenhang die Erhebung weiterer personenbezogener Daten nicht ausschließen.

Das Betreiben der o. g. Webseite mit Eingabemöglichkeiten stellte zugleich einen Telemediendienst nach dem Telemediengesetz (TMG) dar. Die Anbieter für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien haben deshalb die unter § 5 Abs. 2 Nr. 1 bis 7 TMG angegebenen Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten (Impressumspflicht).

Ferner darf gemäß § 13 Abs. 2 Nr. 1 TMG eine solche Webseite nur betrieben werden, wenn der Nutzer gegenüber dem Webseitebetreiber in die damit verbundene Übertragung personenbezogener Daten bewusst und eindeutig eingewilligt hat. Da die Pflichtangaben gemäß § 5 TMG sowie die Einwilligungsaufforderung in die Datenübermittlung gemäß § 13 Abs. 2 TMG nicht festgestellt werden konnten, war ein Verstoß gegen das TMG in diesem Falle nicht auszuschließen.

Der TLfDI teilte dem Landratsamt Eichsfeld mit, dass im Zusammenhang mit der o. g. Webseite ein Verstoß gegen § 5 und § 13 Abs. 2 TMG seitens des beauftragten Softwareunternehmens nicht ausgeschlossen werden könne. Ferner forderte der TLfDI das Landratsamt auf, zu der Angelegenheit Stellung zu nehmen und den Vertrag zur Datenverarbeitung im Auftrag nach § 8 ThürDSG mit dem Softwareunternehmen vorzulegen, das die Internet-Umfrage durchgeführt hatte.

Daraufhin teilte das Landratsamt Eichsfeld dem TLfDI mit, dass es das Softwareunternehmen nur mit der strategischen Erarbeitung einer Dachmarken- und Standortmarketingkonzeption für das Eichsfeld beauftragt habe. Die Durchführung einer Internetumfrage sei von ihm nicht explizit gefordert worden. Vielmehr sollte es dem Auftragnehmer, hier also der Softwarefirma, überlassen bleiben, auf welche Art und Weise er den Ist-Zustand feststellt.

Entsprechende Nachweise legte das Landratsamt in Form einer Leistungsbeschreibung „Entwicklung einer Markenkonzepion und eines Corporate Designs für die Region Eichsfeld“ und eines nichtförmlichen und nicht näher konkretisierten Schreibens zur Auftragserteilung vor. Ferner, so das Landratsamt, sei mittlerweile die Internetumfrage beendet worden.

Abschließend regte der TLfDI gegenüber dem Landratsamt Eichsfeld an, künftig den Auftragnehmer in verbindlicher Form vorsorg-

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

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

5.37 Hundezensus

Die Stadt Gotha bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Beratung. Sie wollte in Erfahrung bringen, inwieweit es datenschutzrechtlich möglich wäre, dass die Stadt ein Unternehmen beauftragt, das in jedem Haushalt nachfragt, ob in diesem ein Hund gehalten werde. Nicht gemeldete Hunde könnten somit aufgespürt werden. Die Hundesteuersatzung der Stadt sah eine Hundebestandsaufnahme durch ein privates Unternehmen nicht vor.

Der TLfDI teilte der Stadt Gotha hierzu Folgendes mit:

Die Beauftragung eines privaten Unternehmens zwecks Wahrnehmung kommunaler Aufgaben wäre unter anderem dann möglich, wenn eine Rechtsgrundlage dies zuließe. Als solche käme eine kommunale Hundesteuersatzung grundsätzlich in Betracht. Allerdings bedürfte die Hundesteuersatzung in diesem Falle einer besonderen Regelung, wonach Grundstückseigentümer oder Haushaltsvorstände verpflichtet sind, den Mitarbeitern der Stadt bzw. den Mitarbeitern eines beauftragten Unternehmens, auf deren Nachfrage über die von ihnen gehaltenen Hunde und deren Halter wahrheitsgemäß Auskunft zu erteilen.

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

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

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

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum den Hinweis, dass die elektronische Anzeigetafel im Bürgerservice der Stadt Jena die Namen von Bürgern sichtbar anzeige. Die Namen könnten somit auch von den anderen Wartenden wahrgenommen werden.

Der TLfDI bat die Stadt Jena um Mitteilung, ob die Bürger wissen, dass ihre Namen auf der elektronischen Anzeigetafel angezeigt werden. Die Stadt Jena teilte daraufhin mit, dass die elektronische Anzeigetafel nur die Namen der Bürger anzeige, die elektronisch einen Termin vereinbart hätten. Bei der Buchung eines Online-Termins werde der Nutzer mit folgendem Satz auf die Verfahrensweise beim Aufruf über die Anzeigetafel informiert:

„Tragen Sie zur Bestätigung Ihren Familiennamen (Achtung: Dieser wird später am Bildschirm der Aufrufanlage des Bürgerservice angezeigt) [...] ein.“

Welchen Namen der Nutzer schlussendlich eingebe, bleibe ihm, dem Bürger, selbst überlassen. So sei es nach Aussage der Stadt auch schon vorgekommen, dass die Bürger ihre Namen selbst gestalteten, sodass auf der Anzeigetafel unter anderem Fantasienamen wie Biene Maja oder Captain Chaos erschienen seien.

Da es somit nicht erforderlich war, den Familiennamen (wie jedoch oben im Text gefordert) anzugeben, riet der TLfDI der Stadt, dies in ihrem Hinweistext aufzunehmen. Zusätzlich sollte der Hinweis aufgenommen werden, wie lange der Name sichtbar ist. Der Text sollte nach Empfehlung des TLfDI wie folgt lauten:

„Tragen Sie zur Bestätigung einen Namen ein (Achtung: Dieser wird später am Bildschirm der Aufrufanlage des Bürgerservice angezeigt. Die Anzeigedauer des von Ihnen eingegeben Namens erstreckt sich bis zum Aufruf des viertnächsten Kunden.“

Da zum Ende des Berichtszeitraumes der Sachverhalt noch nicht abgeschlossen war, wird der TLfDI im kommenden Tätigkeitsbericht erneut über diesen kuriosen Fall berichten.

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

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

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

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

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

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

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

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

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

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

Im Berichtszeitraum hatte es der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mit einem Fall zu tun, bei dem es um eine Akteneinsicht nach § 13 Thüringer Datenschutzgesetz (ThürDSG) gegenüber dem Landratsamt Altenburger Land ging. Nach § 13 Abs. 1 Satz 3 ThürDSG schließt das Recht auf Auskunft das Recht auf Einsicht in die betreffenden Akten und Dateien ein. Das Landratsamt Altenburger Land verweigerte hier die Einsicht unter Hinweis auf das Vorliegen von Versagungsgründen im Sinne des § 13 Abs. 5 ThürDSG. Gemäß § 13 Abs. 7 ThürDSG muss in einem solchem Fall dem TLfDI Auskunft erteilt werden, soweit nicht das zuständige Landesministerium im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde.

Dem anwaltlich vertretenen Beschwerdeführer waren Versagungsgründe jedoch nicht ersichtlich, sodass er weiterhin auf die Akteneinsicht nach § 13 ThürDSG bestand. Er bat den TLfDI, das Verfahren nach § 13 Abs. 7 ThürDSG durchzuführen. Dazu fuhr der TLfDI zum Landratsamt Altenburger Land und schaute sich die entsprechende Akte an. Der TLfDI stellte dabei fest, dass die verweigerte Akteneinsicht durch das Altenburger Land aufgrund von Auskunftsverweigerungsgründen i. S. d. § 13 Abs. 5 ThürDSG aus datenschutzrechtlicher Sicht nicht zu beanstanden war. Allerdings darf dann in einem solchen Fall gemäß § 11 Abs. 3 Satz 1 ThürDSG die Mitteilung des TLfDI an den Betroffenen bzw. hier an den bevollmächtigten Rechtsanwalt zu den Erkenntnissen aus der Akteneinsicht des TLfDI keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zugestimmt hat. Eine Zustimmung erfolgte in diesem Fall nicht. Somit teilte der TLfDI dem Rechtsanwalt mit, dass

nach dem erfolgten Ortstermin des TLfDI sowie dessen datenschutzrechtlicher Prüfung die Verweigerung der Akteneinsicht auf Grundlage der gesetzlichen Regelung des § 13 Abs. 5 ThürDSG erfolgte und aus datenschutzrechtlicher Sicht nicht zu beanstanden war.

Da in diesem Fall ein verwaltungsrechtliches Klageverfahren in Arbeit war, wies der TLfDI darauf hin, dass hier das zuständige Verwaltungsgericht über die Freigabe der Akten zu entscheiden habe.

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

5.41 Kommunale Eigenbetriebe: BDSG oder ThürDSG?

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

ge zu entscheiden, ob für den KommunalSERVICE Jena (KSJ), einem Eigenbetrieb der Stadt Jena, das Bundesdatenschutzgesetz (BDSG) oder das Thüringer Datenschutzgesetz (ThürDSG) anzuwenden ist.

Nach datenschutzrechtlicher Prüfung der Angelegenheit gelangte der TLfDI zu folgender Auffassung:

Für den KSJ ist allein das ThürDSG und nicht das BDSG anwendbar. Dies ergibt sich daraus, dass der KSJ als Eigenbetrieb im Sinne von § 76 Abs. 1 Thüringer Kommunalordnung (ThürKO) keine eigene Rechtspersönlichkeit besitzt (Rücker/Dieter/Schmidt, ThürKO, Kommentar, Band II, § 76, Nr. 1), sondern er unmittelbar von der Gemeinde abhängig ist.

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

Die o. g. Argumente führten zu dem Ergebnis, dass für den KSJ als Eigenbetrieb im Sinne von § 76 ThürKO ausschließlich das ThürDSG anzuwenden ist. Daraus folgte weiterhin, dass gemäß § 10a ThürDSG ein Mitarbeiter der Stadt Jena bzw. des KSJ als Datenschutzbeauftragter zu bestellen ist.

Die Stadtverwaltung Jena ist dieser Forderung des TLfDI zunächst nicht gefolgt, einen Mitarbeiter bzw. eine Mitarbeiterin der Stadt Jena bzw. des KSJ als Datenschutzbeauftragten zu bestellen. Vielmehr sollte weiterhin das Auftragsverhältnis zwischen dem KSJ und dessen externem Datenschutzbeauftragten beibehalten werden.

Im Ergebnis stellte der TLfDI fest, dass ein für den KSJ zuständiger bzw. mitzuständiger Datenschutzbeauftragter gemäß § 10a ThürDSG entgegen der Forderung des TLfDI nicht bestellt wurde und beanstandete daher gemäß § 39 Abs. 1 Satz 1 ThürDSG die rechtswidrige Nichtbestellung eines internen Datenschutzbeauftragten für den Eigenbetrieb der Stadt Jena KSJ. Zugleich forderte der TLfDI die Stadt Jena auf, gemäß § 10a ThürDSG einen Mitarbeiter der Stadt Jena bzw. des KSJ als Datenschutzbeauftragten des KSJ zu bestellen und dies durch die Vorlage der Bestellungsurkunde nachzuweisen.

Daraufhin teilte der Oberbürgermeister der Stadt Jena dem TLfDI mit, dass nunmehr die Datenschutzbeauftragte der Stadtverwaltung Jena gemäß § 10a ThürDSG auch für alle Eigenbetriebe der Stadt Jena, einschließlich des KSJ, zuständig und der bisherige externe Datenschutzbeauftragte des KSJ von seiner Funktion entbunden worden sei. Damit war die Stadt Jena den Forderungen des TLfDI vollumfänglich nachgekommen.

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

5.42 Global Positioning System (GPS) für Kommunalbedienstete

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

Der TLfDI teilte mit, dass zunächst zu prüfen ist, welche konkreten Daten für den festgelegten Zweck erforderlich sind (§ 19 Abs. 1 Thüringer Datenschutzgesetz – ThürDSG). Dabei ist zu berücksichtigen, dass die erfassten Daten, soweit sie auf den jeweiligen Fahrer bezogen werden können, personenbezogene Daten im Sinne des § 3 Abs. 1 ThürDSG darstellen. GPS-Systeme ermöglichen die Erfassung einer Vielzahl von Einzeldaten. Für die Tourenplanung und die Organisation der Fahrzeugflotte war aus Sicht des TLfDI lediglich eine Positionserfassung der Fahrzeuge erforderlich. Die auf diese Art und Weise erhobenen Daten dürfen auch nur so lange gespeichert werden, wie sie zur Aufgabenerfüllung erforderlich sind. Für die dargelegten Zwecke war eine Speicherung für einen längeren Zeitraum nicht erforderlich, vielmehr war ein aktueller Zugriff ausreichend. Eine Speicherung über den Tag hinaus wäre nicht zu rechtfertigen gewesen.

Im Zusammenhang mit der Erbringung der Leistungen für den Winterdienst können beim Einsatz von GPS über die Positionsdaten hinaus weitere Vorgänge erfasst werden. Hierzu zählen beispielsweise die Nutzung des Schneepflugs und die Menge des ausgestreuten Salzes. Für die Beantwortung von Beschwerden von Anwohnern oder Anfragen der Polizei im Zusammenhang mit Verkehrsunfällen können zum Nachweis der Leistungserbringung die Daten für einen festzulegenden kurzen Zeitraum gespeichert werden.

Da aber immer ein Bezug zu den Fahrern hergestellt werden kann, ist im Hinblick auf die betroffenen Beschäftigten zu beachten, dass eine Leistungs- und Verhaltenskontrolle mittels Auswertung der Positionsdaten nach § 33 Abs. 4 ThürDSG nicht zulässig ist.

In der erforderlichen Dienstvereinbarung oder Dienstanweisung müsste aus Gründen der Transparenz für die betroffenen Fahrer und Mitarbeiter zwingend festgelegt werden, welche konkreten Daten erfasst werden und für welchen Zeitraum diese von wem unter welchen Voraussetzungen und zu welchem Zweck ausgewertet werden können.

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

5.43 Weitergabe einer Telefonnummer zur Verfolgung einer Ordnungswidrigkeit

Die Polizeiinspektion Eichsfeld übersandte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) einen dienstlichen Vermerk zu einer Anzeige über die Herausgabe einer privaten Telefonnummer durch die Wohnungsverwaltung der Verwaltungsgemeinschaft Niederorschel an das zuständige Ordnungsamt.

Hintergrund der Angelegenheit war ein seit längerem dauernder Streit über die Nutzung eines Anwohnerparkplatzes, den der Beschwerdeführer von der Wohnungsverwaltung gemietet hatte. Anlass der polizeilichen Anzeige des Beschwerdeführers war ein Anruf des Ordnungsamtes beim Beschwerdeführer zu o. g. Angelegenheit, wobei das Ordnungsamt mitteilte, die Telefonnummer des Beschwerdeführers von der Wohnungsverwaltung erfahren zu haben.

Nach Auffassung des Beschwerdeführers sei die Übermittlung seiner Telefonnummer nicht zulässig, da er in deren Herausgabe nicht einwilligt habe und sie auch nicht in öffentlichen Verzeichnissen eingesehen bzw. recherchiert werden könne.

Der TLfDI forderte die Wohnungsverwaltung zur Stellungnahme in der Angelegenheit auf. Die Wohnungsverwaltung teilte dem TLfDI mit, dass die Telefonnummer des Beschwerdeführers auf Anfrage des Ordnungsamts zum Zwecke der Verfolgung einer Ordnungswidrigkeit wegen nicht vorschriftsgemäßer Nutzung eines Parkplatzes übermittelt worden sei, um mit dem Beschwerdeführer Kontakt aufnehmen zu können.

Nach Auffassung des TLfDI handelt es sich hierbei um eine Datenübermittlung innerhalb des öffentlichen Bereichs, deren Zulässigkeit nach § 21 i. V. m. § 20 Thüringer Datenschutzgesetz (ThürDSG) zu beurteilen ist. Gemäß § 21 Abs. 1 ThürDSG ist eine solche Übermittlung zulässig, wenn sie 1. zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Dritten erforderlich ist – dies konnte im vorliegenden Fall für das Ordnungsamt bejaht werden – und 2. die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden. Nach § 20 Abs. 2 Nr. 7 ThürDSG ist das Speichern, Verändern oder Nutzen für andere Zwecke unter anderem zulässig, wenn es zur Verfolgung von Ordnungswidrigkeiten erforderlich ist. Im vorliegenden Fall forderte das Ordnungsamt gerade die Adresse

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

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

5.44 Fotosafari im Schlafzimmer oder eine mitteilsame Waffenbehörde

Ein Betroffener setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum über eine mutmaßlich unzulässige Weitergabe personenbezogener Daten durch einen Mitarbeiter der Waffenbehörde eines Landratsamtes in Kenntnis.

Zur „Vorgeschichte“ der Angelegenheit teilte der Betroffene mit, dass er Jäger und Inhaber eines Jagdscheins sowie einer Waffenbesitzkarte sei und daher legal Schusswaffen und Munition besitzen dürfe. Infolge einer anonymen Strafanzeige wegen eines Verstoßes gegen das Waffengesetz sei ein Strafverfahren gegen ihn eröffnet worden. Im Rahmen dieses Strafverfahrens hätten die Waffenbehörde eines Landkreises und die ermittelnden Polizeibeamten eine Hausdurchsuchung bei ihm als Betroffenen durchgeführt und dabei Fotos der Wohnung einschließlich seines Schlafzimmers gefertigt und Waffen und Munition beschlagnahmt. Nachfolgend habe das zuständige Amtsgericht diese Hausdurchsuchung für rechtswidrig erklärt, die Beschlagnahme der aufgefundenen Schusswaffen und Munition aufgehoben und das Strafverfahren gegen den Betroffenen eingestellt.

Später habe ein Mitarbeiter der Waffenbehörde dem Leiter des Hegerings (einer Organisationseinheit der Jägerschaft), dem auch der Betroffene angehört, Einzelheiten zur Hausdurchsuchung mitgeteilt und angeboten, die dabei gefertigten Fotos der Wohnung des Betroffenen zu zeigen. Da der Zustand der Wohnung schlampig gewesen sei, könne der Hegering ggf. Disziplinarmaßnahmen gegen den

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

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

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

Der TLfDI kontrolliert u. a. die Einhaltung datenschutzrechtlicher Bestimmungen bei öffentlichen Stellen Thüringens und beanstandet die dort festgestellten datenschutzrechtlichen Verstöße. Der TLfDI ist hingegen nicht die zuständige Behörde zur Verfolgung und Ahndung von datenschutzrechtlichen Ordnungswidrigkeiten im öffentlichen Bereich. Zuständig ist nach § 36 Abs. 2 des Gesetzes über Ordnungswidrigkeiten (OWiG) in Verbindung mit § 8 der Thüringer Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Innenministeriums diejenige Behörde, der der Vollzug derjenigen Rechtsvorschrift obliegt, gegen die sich der Verstoß richtet.

Sofern eine Straftat im Sinne von § 43 Abs. 3 ThürDSG vorliegt, kann eine solche Tat auf Antrag verfolgt werden; antragsberechtigt sind der Betroffene und der TLfDI. Insofern besteht für den TLfDI die Möglichkeit, einen entsprechenden Antrag bei der zuständigen Staatsanwaltschaft zu stellen.

Der Betroffene bat den TLfDI, die Angelegenheit zur strafrechtlichen Verfolgung an die zuständige Staatsanwaltschaft abzugeben und Strafantrag gegen die jeweils handelnden Behördenmitarbeiter zu stellen. Dies sah auch der TLfDI aus folgenden Gründen als sachdienlich an:

Es bestand der Anfangsverdacht, dass die rechtswidrige Bekanntgabe des Akteninhalts an eine verfahrensfremde Privatperson, insbesonde-

re die Gewährung der Einsichtnahme in Fotos der Wohnung mit dem Wohn- und Schlafzimmer (die einen besonders geschützten Persönlichkeitsbereich zeigten), einzig zu dem Zweck erfolgte, den Betroffenen in der Öffentlichkeit herabzuwürdigen und verächtlich zu machen. Deshalb war nach Auffassung des TLfDI insoweit auch der Straftatbestand des § 43 Abs. 3 ThürDSG erfüllt, denn die Handlung des Mitarbeiters der Waffenbehörde erfolgte, um den Betroffenen zu schädigen.

Nachfolgend stellte der TLfDI einen Strafantrag gegen Unbekannt gemäß § 43 Abs. 3 Satz 2 und Satz 3 ThürDSG wegen Verstoßes gegen das Thüringer Datenschutzgesetz. Daraufhin bestätigte die zuständige Staatsanwaltschaft gegenüber dem TLfDI den Eingang seines Strafantrages. Das strafrechtliche Ermittlungsverfahren wurde bislang noch nicht abgeschlossen. Der TLfDI wird daher nach Abschluss der strafrechtlichen Ermittlungen diesen Fall im nächsten Tätigkeitsbericht wieder aufgreifen.

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

5.45 Individuelle Hilfeplanung: Datenverarbeitung nur bei datenschutzgerechter Einwilligungserklärung

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

(TLfDI) das im Internet verfügbare Formular einer eingehenden datenschutzrechtlichen Prüfung.

Zur Erhebung waren auf diesem Formblatt neben Angaben zu den „im Moment“ vorhandenen Hilfen und Gegebenheiten eine Vielzahl von Wünschen und Vorstellungen des Betroffenen zur zukünftig angestrebten Wohn- und Lebensform einzutragen, die vom Sozialamt aus fachlicher Sicht ergänzt werden konnten. Mit der Unterschrift des Betroffenen und ggf. seines Betreuers am Ende des Formulars sollten die Information über die Datenverarbeitung im Merkblatt bestätigt und gleichzeitig auch alle beteiligten Mitarbeiter der betreffenden Stadtverwaltung von der Schweigepflicht entbunden werden.

Diese Form des Antrags entsprach nicht den gesetzlichen Anforderungen an den Datenschutz. Nach dem Wortlaut von § 67b SGB X ist der Betroffene, sofern die Einwilligung bei ihm eingeholt wird, auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung und der Hinweis bedürfen der Schriftform. Soll die Einwilligung, wie hier, zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie im äußeren Erscheinungsbild der Erklärung hervorzuheben. Für die Wirksamkeit der datenschutzrechtlichen Einwilligungserklärung ist es erforderlich, dass die Sozialdaten genau festgelegt werden, auf die sich die Verarbeitung oder Nutzung bezieht. Weiterhin müssen die Stellen festgelegt werden, die zur Verarbeitung oder Nutzung berechtigt sein sollen. Auch der Verarbeitungs- und Nutzungszweck ist hinreichend festzulegen. Von der Erteilung der Einwilligung nach § 67b Abs. 1 SGB X ist die Schweigepflichtentbindung zu unterscheiden, die eine Strafbarkeit der beteiligten Personen nach § 203 Strafgesetzbuch verhindert, sofern es sich dabei um Berufsgeheimnisträger handelt. Diese Einwilligung bedarf grundsätzlich keiner bestimmten Form. Die Schweigepflichtentbindung kann zwar grundsätzlich mit der datenschutzrechtlichen Einwilligungserklärung verbunden werden, stellt aber selbst keine Befugnis zur Datenverarbeitung dar.

Der TLfDI forderte das Sozialamt auf, die datenschutzrechtliche Einwilligungserklärung nach einem Text abgeben zu lassen, der den Inhalt des Merkblatts zumindest im Wesentlichen wiedergibt. Daraufhin wurden das Merkblatt und das veröffentlichte Formular überarbeitet. Mit der am Ende des Formblatts vorgesehenen Unter-

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

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

5.46 Beschlüsse von Stadtratssitzungen können grundsätzlich im Netz veröffentlicht werden!

Ein Beschwerdeführer setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber in Kenntnis, dass der Inhalt des öffentlichen Teils einer Sitzung des Stadtrates Eisenach samt einer Vorschlagsliste für Schöffen einschließlich der Namen und Anschriften der Betroffenen ins Internet gestellt worden sei.

Der TLfDI bat daraufhin die Stadtverwaltung Eisenach, mitzuteilen, auf welcher Rechtsgrundlage diese Übermittlung personenbezogener Daten beruhte und zu welchem Zwecke sie erfolgte.

Nachfolgend teilte die Stadtverwaltung Eisenach dem TLfDI mit, dass sie im Jahr 2009 ein Ratsinformationssystem eingeführt habe, worüber die Beschlüsse des Stadtrates interessierten Bürgern auf der städtischen Internetseite zur Verfügung gestellt würden. Dabei achte die Stadt Eisenach darauf, dass keine personenbezogenen Daten im Internet veröffentlicht würden.

Die Stadtratsbeschlüsse, die vor 2009 gefasst worden seien, seien ebenfalls im Internet zu finden gewesen. Dabei sei versehentlich auch der Beschluss zur Schöffenwahl mit Namen und Anschriften der vorgeschlagenen Schöffen unter den öffentlichen Bekanntmachungen der Beschlüsse eingestellt worden. Unmittelbar nach Eingang des Schreibens des TLfDI habe die Stadtverwaltung die Be-

schlüsse aus den Jahren vor 2009 von der städtischen Internetseite genommen.

Hiervon hat sich der TLfDI überzeugt und deshalb die Beschwerde als erledigt angesehen.

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

5.47 Keine Telefonauskünfte an Unbekannte!

Ein Betroffener beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass das Wahlbüro des Landratsamtes Nordhausen Daten zu seiner Person an einen Dritten übermittelt hätte.

Zunächst habe der Betroffene per E-Mail das Wahlbüro beim Landratsamt Nordhausen zum Zwecke seiner Kandidatur für die Bundestagswahl angeschrieben. Daraufhin habe ein Mitarbeiter des Wahlbüros mit einem Dritten telefonisch über die persönlichen Daten des Betroffenen aus dessen E-Mail gesprochen und gebeten, dem Betroffenen auszurichten, dass er das Wahlbüro anrufen möchte. Der Betroffene gab an, dass die Telefonnummer des Dritten nicht von ihm preisgegeben worden sei und daher aus einer anderen Quelle stammen müsste.

Der TLfDI forderte das Landratsamt auf, zu den Beschwerdepunkten Stellung zu nehmen und mitzuteilen, zu welchen Zwecken eine dritte Person in einer Angelegenheit des Betroffenen telefonisch kontaktiert und dieser Person personenbezogene Daten des Betroffenen mitgeteilt wurden sowie auf welchen Rechtsgrundlagen dieses Handeln beruhte.

Das Landratsamt Nordhausen setzte den TLfDI daraufhin darüber in Kenntnis, dass das Wahlbüro offene Fragen zur E-Mail des Betroffenen, mit der er sich als Kandidat für die Bundestagswahl beworben hatte, schnellstmöglich klären wollte. Hierzu sei anhand der Anschrift aus der o. g. E-Mail per Internet ein Telefonanschluss mit dem Nachnamen des Betroffenen recherchiert worden. Daraufhin habe das Wahlbüro unter dieser Telefonnummer eine Frau, bei der es

sich nach deren eigenen Angaben um die Großmutter des Betroffenen gehandelt habe, angerufen. Hierbei seien Fragen zu Angaben des Betroffenen, die dieser im Zusammenhang mit seiner Wahlkandidatur gemacht habe, erörtert worden. Abschließend habe das Wahlbüro gebeten, dem Betroffenen auszurichten, er möge das Wahlbüro anrufen. Nachfolgend habe das Wahlbüro eine E-Mail an den Betroffenen mit der Bitte um Rückruf gesandt.

Das Landratsamt teilte die Auffassung des TLfDI, dass die telefonische Mitteilung von personenbezogenen Daten gegenüber Dritten mangels Rechtsgrundlage einen datenschutzrechtlichen Verstoß darstellte.

Aufgrund der verbindlichen Zusage des Landratsamtes Nordhausen, künftig dafür Sorge zu tragen, dass derartige Fehler nicht wiederholt werden, sah der TLfDI die Angelegenheit als erledigt an. Der TLfDI wies das Landratsamt jedoch abschließend darauf hin, dass die Übermittlung personenbezogener Daten nicht über das unsichere Übertragungsmedium einer unverschlüsselten E-Mail erfolgen dürfe.

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

5.48 Keine Umfrage ohne Datenschutzhinweis

Ein Bürger setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Bedarfsermittlung zur Nutzung von Digital Subscriber Line- (DSL) bzw. Breitbandversorgung zum Zweck der Internetversorgung in der Stadt Bad Frankenhausen in Kenntnis und bat um Prüfung des verwendeten Fragebogens.

Der TLfDI stellte zunächst fest, dass der verwendete Fragebogen, der neben dem Namen und der Anschrift des Inhabers des Internet-

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

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

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

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



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

online.de/ unter den Menüpunkten „Service“, „Download“, „Anträge und Formulare“ zum Download bereit stünde. Der Tlfdi überzeugte sich von der Datenschutzkonformität des überarbeiteten Musterfragebogens.

Da dem von der Stadtverwaltung Bad Frankenhausen verwendeten Fragebogen möglicherweise eine ältere Version ohne die erforderlichen Hinweise zum Datenschutz zugrunde lag, forderte der Tlfdi die Stadt Bad Frankenhausen auf, den Fragebogen entsprechend seiner o. g. Hinweise zu überarbeiten bzw. auf den aktuellen Musterfragebogen des Breitbandkompetenzzentrums Thüringen zurückzugreifen und die bisher verwendeten Fragebögen durch die überarbeitete Fassung zu ersetzen.

Nachfolgend teilte die Stadtverwaltung Bad Frankenhausen dem Tlfdi mit, dass sie die Bedarfsermittlung vorzeitig beendet und alle ausgelegten Fragebögen eingesammelt sowie den Fragebogen von der Internetseite der Stadt Bad Frankenhausen entfernt habe.

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

5.49 Offene Briefe vom Finanzamt

Ein Beschwerdeführer teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (Tlfdi) im Berichtszeitraum mit, dass ein Schreiben des Finanzamtes Pößneck unverschlossen an ihn zugestellt worden sei.

Das Finanzamt Pößneck bestätigte gegenüber dem Tlfdi diesen Sachverhalt und bestätigte, dass die Klebevorrichtung bzw. -technik

in der Poststelle des Amtes versagt habe. Zugleich sicherte das Finanzamt zu, alles zu unternehmen, damit sich ein solches Vorkommnis nicht wiederhole und entschuldigte sich gegenüber dem Beschwerdeführer. Nach Prüfung der Angelegenheit sah der TLfDI deshalb von einer datenschutzrechtlichen Beanstandung des Vorkommnisses nach § 39 Thüringer Datenschutzgesetz (ThürDSG) ab. Wenige Wochen später erreichte den TLfDI allerdings ein weiteres Schreiben desselben Beschwerdeführers, der über ein zweites unverschlossenes Schreiben des Finanzamtes Pößneck informierte. So sei dem Beschwerdeführer eine Lohnsteuerbescheinigung, aus der das Einkommen als „Nichtselbstständiger“ erkennbar gewesen sei, ebenfalls unverschlossen übersandt worden.

Da es aus datenschutzrechtlicher Sicht somit ein grundlegendes Problem bei der Postzustellung durch das Finanzamt zu geben schien, bat der TLfDI das Finanzamt um erneute und eingehende Stellungnahme zum Sachverhalt. Vorsorglich wies der TLfDI das Finanzamt auf seine Unterstützungs- und Auskunftspflicht gemäß § 38 ThürDSG hin und teilte mit, dass, falls der Sachverhalt nicht vollends aufgeklärt werden könne und die datenschutzrechtlichen Verstöße im Finanzamt weiterhin andauerten, sich der TLfDI es vorbehalte, das Finanzamt einer datenschutzrechtlichen Kontrolle gemäß § 37 ThürDSG zu unterziehen.

Daraufhin teilte das Finanzamt dem TLfDI mit, dass durch Lagerdauer, Lagerort oder den Transport der Briefsendungen die selbstklebende Eigenschaft der selbstklebenden Briefumschläge nachgelassen haben und somit ein technisches Versagen nicht ausgeschlossen werden könnte. Jedoch habe das Finanzamt die Angelegenheit nicht restlos aufklären können, unter anderem weil der Beschwerdeführer nicht bereit gewesen sei, die mutmaßlich mangelhaften Briefumschläge dem Finanzamt vorzulegen. Jedoch habe das Finanzamt seine Bediensteten angewiesen, die betroffenen Briefumschläge nicht mehr zu verwenden und die Kuverts mittels Klebestreifen bzw. Klebestift selbst und sicher zu verschließen. Auch sagte das Finanzamt zu, künftig bei der Beschaffung sorgfältiger auf die Qualität der Kuverts zu achten und die Ausgangspost regelmäßig zu kontrollieren.

Da die vom Finanzamt getroffenen Maßnahmen eine datenschutzkonforme Zustellung seiner Post erwarten ließen und dem TLfDI ferner keine weiteren unverschlossenen Briefe des Finanzamts be-

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

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

5.50 Grabstelleninhaber wider Willen

Wie der Presse zu entnehmen war, hatte das Garten- und Friedhofsamt Erfurt einen Bürger aus Neu-Ulm als Nutzungsberechtigten einer Grabstelle angeschrieben. Später stellte sich jedoch heraus, dass der Betroffene kein Grab in Erfurt nutzte.

Daher bat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Stadtverwaltung Erfurt, zu der Angelegenheit Stellung zu nehmen und insbesondere konkret mitzuteilen, wie es zu dieser Verwechslung bzw. Fehlnutzung personenbezogener Daten kommen konnte und auf welche Weise, ggf. durch Änderung der Arbeitsabläufe, dies künftig in ähnlichen Fällen ausgeschlossen werden könnte.

Die Stadtverwaltung Erfurt setzte den TLfDI sodann darüber in Kenntnis, dass in diesem Falle die Altdaten nicht korrekt abgeglichen worden seien. Zwar sei eine Person gleichen Namens festgestellt worden, die ehemals in Erfurt gewohnt habe und danach nach Neu-Ulm verzogen sei. Aber deren Erfurter „Altadresse“ habe nicht der im Friedhofs-Informationen-Management vorgehaltenen Adresse entsprochen; jedoch sei dem zuständigen Mitarbeiter des Friedhofsamtes diese Nichtübereinstimmung nicht aufgefallen.

Die Stadtverwaltung sagte zu, die betreffenden Mitarbeiter nochmals ausdrücklich darauf hinzuweisen, bei der Prüfung darauf zu achten, dass die der Stadtverwaltung vorliegenden Altdaten vollständig mit den Einwohnermeldedaten übereinstimmen müssten, ehe eine vermeintlich neue Adresse genutzt werde. Zusätzlich prüfe zukünftig ein weiterer Mitarbeiter die Ergebnisse der Recherche.

Des Weiteren würde bei Neuerfassungen von Adressen im Friedhofs-Informationen-Management seit geraumer Zeit das Geburtsdatum miterfasst, um künftige Nachforschungen sicherer zu machen. Da die Mitarbeiter entsprechend sensibilisiert worden seien, könne eine derartige Verwechslung künftig ausgeschlossen werden. Auch

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

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

5.51 Zulässigkeit des Verfahrens E-POSTBUSINESS-BOX

Ein Landratsamt bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um die datenschutzrechtliche Beurteilung des Einsatzes des E-POSTBUSINESS-BOX-Verfahrens und legte den Entwurf eines Vertrages zur Datenverarbeitung im Auftrag zwischen dem Landratsamt (Auftraggeber) und einem Postdienstleister (Auftragnehmer) vor. Konkret war vorgesehen, dass die Poststelle des Landratsamtes mittels des Verfahrens E-POSTBUSINESS-BOX Massendrucksaachen ohne Unterschriftserfordernis, wie z. B. für Schreiben zu Hortgebühren, bearbeitet.

Bei dem Verfahren wird die Ausgangspost nicht direkt gedruckt, sondern über eine „E-POSTBUSINESS-BOX“, die der Auftragnehmer dem Auftraggeber zur Verfügung stellt, versendet.

Dabei kann zwischen elektronischer Zustellung und physischer Zustellung gewählt werden. An die Adressaten, die eine elektronische Zustellung ermöglicht haben, also schon eine E-Postbriefadresse besitzen und diese öffentlich gemacht haben, wird das Dokument elektronisch übermittelt, andernfalls ausgedruckt, kuvertiert und auf dem herkömmlichen Postweg (E-Postbrief) übermittelt.

Der TLfDI teilte dem Landratsamt mit, dass er dieses Verfahren wie auch das Verfahren De-Mail aus datenschutzrechtlicher Sicht grundsätzlich als kritisch ansieht, da nicht ausgeschlossen werden kann, dass der Inhalt der Schreiben dem Auftragnehmer zur Kenntnis gelangt.

Analog der Nutzung von De-Mail, gilt auch hier, dass bei Verfahren, in denen personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, verarbeitet werden, zusätzlich eine Ende-zu-Ende-Verschlüsselung einzusetzen ist.

Sofern die Behörde Hortgebührenbescheide versenden würde, könnte daraus die Adresse und die Höhe des zu leistenden Hortbeitrags erfasst werden. Hieraus ließen sich Rückschlüsse auf die Einkommenssituation des betroffenen Haushalts ziehen.

Bei dem vorgelegten Entwurf des Vertrages zur Datenverarbeitung im Auftrag handelte es sich zudem um einen Standardvertrag nach § 11 Bundesdatenschutzgesetz, der zwar den inhaltlichen Vorgaben des § 8 Thüringer Datenschutzgesetz (ThürDSG) entspricht, jedoch keine ausdrückliche Bezugnahme auf das ThürDSG beinhaltet. Sind auf den Auftragnehmer die Bestimmungen des ThürDSG nicht anwendbar, ist der Auftraggeber gemäß § 8 Abs. 6 Satz 1 ThürDSG verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen des ThürDSG befolgt. Insofern forderte der TLfDI gegenüber dem Landratsamt, in die Ausgestaltung des Vertrages mindestens noch eine Regelung aufzunehmen, wonach § 8 ThürDSG auf das Auftragsdatenverarbeitungsverhältnis anzuwenden ist.

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

5.52 Wie viel Arbeitszeit braucht der Datenschutzbeauftragte?

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

und aufrechtzuerhalten. Das Anliegen war, diesen prozentualen Anteil der Arbeitszeit für den internen Datenschutz auch weiterhin zu erhalten, um nicht nur die aktuellen dringlichen Aufgaben zu erledigen, sondern auch frühzeitige Informationen erarbeiten und Schulungen für die Mitarbeiter der Stadtverwaltung anbieten zu können.

Der Oberbürgermeister, dem der Datenschutzbeauftragte nach § 10a ThürDSG direkt zu unterstellen ist, beauftragte nun den Fachdienst Personal und Organisation, um feststellen zu lassen, wieviele Arbeitszeiteile für die Aufgabe Datenschutz benötigt würden. Dieser Fachdienst entwarf einen umfangreichen Fragebogen, in dem sich der Datenschutzbeauftragte für die Reihenfolge der Bearbeitung, den langen Zeitraum etc. rechtfertigen und seine jeweilige Tätigkeit genau auflisten sollte. Darüber hinaus sollte er zunächst für mehrere Wochen aufschreiben, womit er sich den ganzen Tag beschäftige (Kennzahl, Fallzahl, Sachverhalt, Abfolge der Tätigkeiten, Beginn, voraussichtliche Fertigstellung und Bearbeitungsdauer etc.).

Zu dem Ansinnen des Oberbürgermeisters führte der TLfDI aus, dass es der öffentlichen Verwaltung grundsätzlich zusteht, Organisationsuntersuchungen durchzuführen, um daraus Erkenntnisse für Organisationsfestlegungen zu treffen. Die Aufforderung zur Protokollierung der Tätigkeit des Datenschutzbeauftragten für den Zeitraum von mehreren Wochen stieß aus Sicht des TLfDI jedoch auf erhebliche Bedenken in Bezug auf die Stellung des Datenschutzbeauftragten nach § 10a ThürDSG.

Abgesehen davon, dass der Datenschutzbeauftragte nach § 10a Abs. 2a und Abs. 5 ThürDSG eine besondere Verschwiegenheitsverpflichtung hat und deshalb Sachverhalte umfangreich zu anonymisieren sind, damit keine Rückschlüsse auf die betroffenen Personen auch innerhalb der Stadtverwaltung ermöglicht werden, hat der Gesetzgeber dem Datenschutzbeauftragten eine besondere Stellung zugeschrieben. Er ist gemäß § 10a Abs. 2 ThürDSG in dieser Funktion dem Leiter der Daten verarbeitenden Stelle unmittelbar zu unterstellen und hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken. In dieser Eigenschaft als Datenschutzbeauftragter ist er nicht weisungsgebunden.

Diese Weisungsfreiheit in der fachlichen Aufgabenerfüllung bedeutet allerdings nicht, dass die verantwortliche Stelle im Rahmen ihrer Dienstaufsicht nicht befugt wäre, sich zu vergewissern, ob der Beauftragte ordnungsgemäß seiner Aufgabe nachkommt (so auch Simi-

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

Offenbar war der Oberbürgermeister einsichtig, denn der Datenschutzbeauftragte machte von dem Angebot des TLfDI, erforderlichenfalls zu intervenieren, keinen Gebrauch.

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

5.53 Dürfen Stadtratsmitglieder die Gehälter der kommunalen Bediensteten überprüfen?

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

tung im Zusammenhang mit der Rechnungsprüfung und auch zur Möglichkeit der Auskünfte aus bzw. der Einsicht in die Personalakten für Stadträte. Der TLfDI hat hierzu Folgendes ausgeführt:

Die Verarbeitung personenbezogener Daten ist nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) nur dann zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Das Thüringer Datenschutzgesetz ist jedoch nach § 2 Abs. 3 ThürDSG subsidiär, wenn eine so genannte bereichsspezifische Regelung vorliegt. Die Thüringer Kommunalordnung (ThürKO) als Spezialgesetz enthält jedoch keine Erlaubnisnorm zur Verarbeitung von Mitarbeiterdaten durch den Stadtrat. Insoweit ist zunächst auf § 33 ThürDSG zurückzugreifen. Danach sind für das Verarbeiten oder Nutzen von personenbezogenen Daten über Angestellte, Arbeiter und Auszubildende in einer öffentlichen Stelle die dienstrechtlichen Vorschriften (§§ 79 bis 87 des Thüringer Beamtengesetzes (ThürBG)) anzuwenden. Für (Kommunal-) Beamte gelten diese Vorschriften unmittelbar. Hier gilt der Grundsatz des § 80 Abs. 1 ThürBG, nach dem Zugang zu Personaldaten nur Beschäftigte (nicht Stadtratsmitglieder) haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist.

Nach § 80 Abs. 2 Satz 2 ThürBG haben Zugang ferner die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse nur auf diesem Weg und nicht durch Auskunft aus der Personalakte gewinnen können. Für andere Personen, also für Stadtratsmitglieder als Dritte, besteht keine Vorlage- oder Auskunftsmöglichkeit. Den Mitgliedern des Stadtrats und den Ausschüssen stehen jedoch nach der Rechtsprechung (VG Meiningen, Urteil vom 20. September 2011 – 2 K 303/10 Me- und Thüringer Obergerverwaltungsgericht, Urteil vom 14. November 2013 – 3 KO 900/11-, juris) allgemeine Informationsrechte nach § 24 Abs. 1 ThürKO zu. Nach § 29 Abs. 3 ThürKO ist der Bürgermeister oberste Dienstbehörde der Beamten der Gemeinde und Dienstvorgesetzter der Gemeindebediensteten. Für die in § 29 Abs. 3 Satz 3 Nr. 1 und 2 ThürKO genannten Personalentscheidungen (Ernennung, Abordnung, Versetzung, Versetzung in den Ruhestand und Entlassung der Beamten des gehobenen und höheren Dienstes sowie Einstellung, Höhergruppierung und Entlassung von Angestellten mit vergleichbarer Vergütung) bedarf es der Zustimmung

mung des Gemeinderats oder des zuständigen Ausschusses. Die Gewährung von Zulagen ist hier nicht konkret genannt. Insoweit hat der Bürgermeister in Wahrnehmung seiner Fürsorgepflicht für die betroffenen Beschäftigten mit Zulagen zunächst die Personalakten-
daten vor unbefugter Einsicht zu schützen.

Eine Befugnis zur Offenbarung der Personalaktendaten gegenüber Stadträten besteht jedoch dann, wenn das allgemeine Informationsrecht auch personenbezogene Daten von Bediensteten umfassen muss, weil sonst die Kontrollfunktion der Stadträte nicht ausgeübt werden könnte. In einem solchen Fall ist das Kontrollrecht mit den schützenswerten Interessen der betroffenen Bediensteten abzuwägen. Im Rahmen dessen ist zu prüfen, ob zur Ausübung der Kontrollrechte durch die Stadtratsmitglieder oder den Ausschuss anonymisierte Angaben ausreichen. Sollte dies nicht der Fall sein, ist abzustufen, ob eine personenbezogene Auskunft für die Aufgabenerfüllung ausreicht, was in den meisten Fällen zutreffend sein sollte. Sollte im Einzelfall die Einsicht in Personalaktendaten begehrt werden, ist dies nach Auffassung des TLfDI auf die für die Aufgabenerfüllung zwingend erforderlichen Angaben zu beschränken.

Aber auch im Falle der Auskunft über personenbezogene Daten sind flankierende Maßnahmen zum Schutz des informationellen Selbstbestimmungsrechts der Betroffenen zu treffen. Die personenbezogenen Daten dürfen daher nur in nicht-öffentlicher Sitzung (vgl. Thüringer Obergerverwaltungsgericht, Urteil vom 14. November 2013 – 3 KO 900/11) unter Hinweis auf die Zweckbindung zur konkreten Aufgabenerfüllung zur Kenntnis gegeben und seitens der Empfänger nicht für andere Zwecke genutzt werden (siehe dazu Nr. 5.40).

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

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

Im Mai 2015 startete die Landesbeauftragte für den Datenschutz in Niedersachsen eine Umfrage unter den deutschen Datenschutzbehörden, um zu klären, ob bzw. in welchen Bundesländern Bild- und Tonaufzeichnungen von öffentlichen Stadtratssitzungen mit dem Ziel der Veröffentlichung üblich bzw. gesetzlich geregelt sind. Die gesammelten Erkenntnisse sollten dann in einer allgemeinen Übersicht zusammengefasst werden.

Bereits in dem Tätigkeitsbericht 2011/2012 hatte der niedersächsische Datenschutzbeauftragte sich zu der Thematik eindeutig positioniert und hauptsächlich auf mangelnde gesetzliche Grundlagen hingewiesen, um im Ergebnis eine generelle Aufzeichnung oder einen Live-Stream abzulehnen. Dazu griff sie auch die Argumentation des Bundesverwaltungsgerichts (vgl. Urteil vom 3. August 1990, Aktenzeichen 7 C 14/90) auf, wonach zu befürchten sei, dass sich weniger wortgewandte Sitzungsteilnehmer zu sehr exponiert fühlen, als dass sie im Bewusstsein einer Aufzeichnung oder Live-Übertragung überhaupt noch frei und ungehemmt an der Sitzung teilnehmen und an der Beschlussfassung mitwirken könnten.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) teilte seiner niedersächsischen Kollegin mit, dass es in Thüringen derzeit keine Rechtsgrundlage in der Thüringer Kommunalordnung (ThürKO) für solche Aufzeichnungen oder Übertragungen gibt und verwies auf seinen eigenen Tätigkeitsbericht 2012/2013, in dem er ab Seite 95 ff. zur Live-Übertragung von Sitzungen eines Stadtrates Stellung bezogen hatte. Dort hatte der TLfDI auch die „Erfurter Lösung“ vorgestellt, die sich übrigens bis heute bewährt hat. Der TLfDI ist gespannt zu erfahren, wie die übrigen Datenschutzbeauftragten der Länder dieses Modell beurteilen.

Nach § 40 Abs. 1 Thüringer Kommunalordnung (ThürKO) sind Sitzungen des Gemeinderats grundsätzlich öffentlich durchzuführen. Dieses Gebot ist jedoch schon dann gewahrt, wenn ein ausreichend großer Sitzungsraum für den Normalbürger zumutbar erreichbar ist, zu dem jedermann im Rahmen des hierfür zur Verfügung stehenden Platzes in der Reihenfolge des Eintreffens freien Zugang hat. Daher besteht keine Berechtigung für eine Übertragung des Sitzungsverlaufs mit elektronischen Medien. Folglich können aus § 40 Abs. 1

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

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

chend angepasst. Der TLfDI wird daher zu gegebener Zeit erneut seine Vorschläge zu dieser wichtigen Thematik an die Fraktionen des Landtags übermitteln.

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

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

5.55 Verarbeitung von Einkommensdaten zur Festsetzung von Hortgebühren

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

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

5.56 Datenübermittlung im Verwaltungsverfahren

Im Berichtszeitraum hatte sich ein Ehepaar als Beschwerdeführer mit folgendem Sachverhalt an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt:

Sie hätten eine Dienstleisterfirma wegen zahlreicher illegaler Handlungen beim Landratsamt Schmalkalden-Meiningen angezeigt. Dabei hätten sie das Landratsamt gebeten, ihre personenbezogenen Daten nicht weiterzugeben. Daraufhin habe das Landratsamt den Beschwerdeführern erklärt, nur dann tätig werden zu können, wenn es ihre personenbezogenen Daten dem Angezeigten, also der Dienstleisterfirma, mitteilen könnte.

Der TLfDI bat das Landratsamt Schmalkalden-Meiningen um eine Stellungnahme zum oben genannten Tatbestand und forderte es auf, die Rechtsgrundlage zu nennen, die ein Tätigwerden des Landratsamtes zwingend von der Benennung personenbezogener Daten der Beschwerdeführer abhängig macht.

Außerdem fragte der TLfDI nach, warum eine Übermittlung personenbezogener Daten der Beschwerdeführer im konkreten Fall erforderlich sei.

Das Landratsamt Schmalkalden-Meiningen erklärte dem TLfDI daraufhin, dass es in seiner Anordnung an die Dienstleisterfirma (als Störer) – die aufgrund der Anzeige der Beschwerdeführer erfolgte – keine Zeugen benannt habe; dies werde sich aber in einem zu erwartenden Widerspruchsverfahren zur erfolgreichen Widerspruchsbe gründung nicht vermeiden lassen.

Als Rechtsgrundlage für die Benennung von Zeugen verwies die Behörde auf § 26 Abs. 1 Nummer 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG), der das Beweismittel der Vernehmung von Zeugen regelt. Danach ist es den Behörden im Verwaltungsverfahren in den Grenzen ihres pflichtgemäßen Ermessens überlassen, Beweise zu erheben.

Eine Mitwirkungspflicht der Beteiligten besteht dabei grundsätzlich nicht. Eine Einvernahme von Zeugen geschieht freiwillig und kann –

von wenigen Ausnahmen abgesehen – nicht von der Behörde erzwungen werden.

Vorliegend war eine Mitwirkungshandlung insoweit erforderlich, weil ohne die Anzeige der Beschwerdeführer das in Rede stehende Verfahren gar nicht in Gang gesetzt worden wäre.

Von diesem Mitwirken der Beschwerdeführer in dieser Angelegenheit zu unterscheiden ist die Bekanntgabe ihrer Namen gegenüber dem Adressaten des Bescheides.

Dazu bestimmt § 39 ThürVwVfG – Begründung des Verwaltungsaktes – Folgendes:

„Ein schriftlicher oder elektronischer sowie ein schriftlich oder elektronisch bestätigter Verwaltungsakt ist mit einer Begründung zu versehen. In der Begründung sind die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen, die die Behörde zu ihrer Entscheidung bewogen haben. Die Begründung von Ermessensentscheidungen soll auch die Gesichtspunkte erkennen lassen, von denen die Behörde bei der Ausübung ihres Ermessens ausgegangen ist.“

Die Mitteilung des Namens von Anzeigenerstatter ist dort nicht vorgesehen und damit datenschutzrechtlich grundsätzlich unzulässig. In einem weiteren Schreiben bat der TLfDI das Landratsamt deswegen, nochmals zu prüfen, ob eine namentliche Nennung der Beschwerdeführer im weiteren Verfahren erforderlich sei und ob ein anderes, gleichwertig geeignetes Beweismittel im Sinne des § 26 ThürVwVfG in Betracht käme.

Das Landratsamt Schmalkalden-Meiningen erklärte daraufhin dem TLfDI, dass die Beschwerdeführer sich damit einverstanden erklärt hätten, als Zeugen zur Verfügung zu stehen. Das Landratsamt hatte aber von der Möglichkeit, die Beschwerdeführer als Zeugen einzusetzen, wie dargelegt, keinen Gebrauch gemacht. Das wies das Landratsamt gegenüber dem TLfDI auch nach, indem es seine bisherige Korrespondenz in der Angelegenheit offenlegte.

In der Regel überwiegt das Interesse des Anzeigenerstatters, anonym zu bleiben, das Interesse des Bescheidadressaten auf Nennung dessen Namens, sodass grundsätzlich – wie oben ausgeführt – die Übermittlung des Namens im Bescheid ohne dessen Einverständnis unzulässig ist.

Im Ergebnis konnte der TLfDI nicht feststellen, dass das Landratsamt Schmalkalden-Meiningen personenbezogene Daten der Beschwerdeführer rechtswidrig verarbeitet hatte. Die Beschwerde war daher unbegründet.

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

5.57 Pfändung nur bei Kenntnis der Bankverbindung zulässig!

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag im Berichtszeitraum eine Beschwerde vor, die folgenden Sachverhalt umfasste:

Gegen den Beschwerdeführer sei eine Pfändungs- und Einziehungsverfügung der Stadtverwaltung Eisfeld ergangen. Die Stadtverwaltung habe ihm einen entsprechenden Bescheid über eine Kontopfändung bei der VR-Bank Südthüringen zugestellt. Der Beschwerdeführer habe im Gegensatz zu seiner Ehefrau jedoch gar kein Konto bei der VR-Bank Südthüringen unterhalten. Der von diesem Verwaltungshandeln betroffene Beschwerdeführer begehrte von der Stadtverwaltung Eisfeld Auskunft, woher ihre Kenntnis über das vermeintliche Konto des Beschwerdeführers bei der VR-Bank Südthüringen stamme. Diese Auskunft sei dem Beschwerdeführer mehrfach telefonisch von der Stadt Eisfeld verweigert worden.

Der TLfDI bat die Stadtverwaltung Eisfeld um eine Stellungnahme zu der geschilderten Sach- und Rechtslage. Insbesondere interessierte ihn, aufgrund welcher Rechtsgrundlage die Stadtverwaltung Eisfeld die VR-Bank über die geplante Kontopfändung beim Beschwerdeführer in Kenntnis gesetzt habe und inwieweit diese Mitteilung für ihr Handeln in dieser Angelegenheit erforderlich gewesen sei.

Darüber hinaus wollte der TLfDI wissen, ob die Stadt Eisfeld dem Beschwerdeführer die Auskunft darüber verweigert habe, woher sie die Kenntnis über ein angebliches Konto des Beschwerdeführers bei der VR-Bank erlangt habe.

Der Vorwurf des Beschwerdeführers, ihm sei die Auskunft darüber verweigert worden, hat sich nach den Recherchen des TLfDI nicht bestätigt. Denn die Stadt Eisfeld hatte gegenüber dem Beschwerde-

führer schriftlich Auskunft erteilt, woher ihr Wissen um das vermutliche Konto des Beschwerdeführers stammte.

Zum Beweis dafür überließ die Stadtverwaltung dem TLfDI ein Schreiben, das sie seinerzeit an den Beschwerdeführer übersandt hatte. Darin hatte die Stadt Eisfeld dem Beschwerdeführer unter anderem mitgeteilt, dass das Auskunftersuchen gegenüber der VR-Bank Südthüringen lediglich auf Erfahrungswerten beruhe, da dieses Institut erfahrungsgemäß in der Region häufig als Bank in Erscheinung träte. Eine unzulässige Verwendung personenbezogener Daten seitens der Stadtverwaltung Eisfeld wäre damit aber nicht verbunden gewesen.

Die Stadtverwaltung Eisfeld konnte jedoch keine Rechtsgrundlage für die von ihr gegenüber der Bank begehrte Übermittlung von Daten des Beschwerdeführers benennen.

Die Erfahrung, dass dieses Institut in dieser Region oft als Hausbank auftritt, rechtfertigt es nicht, ohne Rechtsgrundlage – nur aufgrund dieser Erkenntnis – „ins Blaue“ hinein das Kreditinstitut über eine geplante Kontopfändung eines ihrer Kunden in Kenntnis zu setzen. „Verwaltungserfahrungen“ legitimieren keine Anfrage einer Behörde nach personenbezogenen Kontodaten bei einer nichtöffentlichen Stelle.

Im Ergebnis handelte es sich vorliegend um einen Verstoß gegen § 22 Thüringer Datenschutzgesetz (ThürDSG). Die Übermittlung personenbezogener Daten an eine nicht-öffentliche Stelle – eine solche Stelle stellt die VR-Bank Südthüringen dar – ist nur zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (§ 4 Abs. 1 ThürDSG). Eine Regelung oder Einwilligung des Beschwerdeführers, die die Behörde ermächtigt, der VR-Bank Südthüringen personenbezogene Daten des Beschwerdeführers zu übermitteln, lag mithin nicht vor.

Der TLfDI hat die Stadtverwaltung Eisfeld über seine Bewertung der Sach- und Rechtslage in Kenntnis gesetzt und sie aufgefordert, künftig den Belangen des Datenschutzes in gleichgelagerten Fällen Rechnung zu tragen. Beispielsweise könne der Schuldner unter Fristsetzung zukünftig zunächst aufgefordert werden, seine Bankverbindung zum Zwecke der Kontenpfändung der Stadtverwaltung bekanntzugeben; hiermit verbunden sein könnte der Hinweis, dass andernfalls eine Pfändung durch den Gerichtsvollzieher erfolgen wird.

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

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

5.58 Facebook weckt behördliche Überwachungsfantasien

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

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

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

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

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

Zu 1. (Vorbereitung von Erlaubnis- bzw. Auflagenbescheiden nach § 42 OBG):

§ 42 OBG regelt die Veranstaltung von Vergnügungen. Nach § 42 Abs. 1 OBG hat, wer eine öffentliche Vergnügung veranstalten will, der zuständigen Stelle Art, Ort, und Zeit der Veranstaltung sowie die Zahl der zuzulassenden Teilnehmer spätestens eine Woche zuvor schriftlich anzuzeigen. § 42 Abs. 3 OBG regelt Veranstaltungen öffentlicher Vergnügungen, die einer Erlaubnis bedürfen und die Zuständigkeit der Erteilung einer solchen Erlaubnis. Ein Veranstalter, der nach § 42 Abs. 1 OBG der Stadtverwaltung die o. g. Pflichtangaben gemeldet hat, bedarf keiner Erlaubnis. Einer Erlaubnis bedarf es lediglich in Fällen des § 42 Abs. 3 OBG, z. B. wenn es sich um eine motorsportliche Veranstaltung handelt.

Da eine Stadtverwaltung durch die Anzeigeverpflichtung in ausreichendem Maße über Veranstaltungen in Kenntnis gesetzt wird, bestand aus der Sicht des TLfDI im konkreten Fall keine Notwendigkeit für eine zusätzliche Datenerhebung mittels einer Recherche in sozialen Netzwerken durch Mitarbeiter der Stadtverwaltung Arnstadt. Zu berücksichtigen war dabei auch die Möglichkeit, dass weitere personenbezogene Daten, ggf. auch von Dritten, die in keinem Zusammenhang mit der ordnungsbehördlichen Tätigkeit stehen, quasi als „Beifang“ hätten erhoben werden können. Im Ergebnis waren deshalb die beabsichtigten präventiven und kontrollierenden Facebook-Recherchen zu öffentlichen Vergnügungen nicht von § 19 Abs. 2 ThürDSG in Verbindung mit § 42 OBG gedeckt. Anderweitige Rechtsgrundlagen, die eine derartige Datenerhebung erlaubt hätten, waren für den TLfDI nicht ersichtlich.

Zu 2. (Erlangung relevanter Hintergrundinformationen zu sozialen Gruppen und Initiativen):

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

Zu 3. (Umsetzung / Ergreifung von Maßnahmen nach der Thüringer Prostitutionsverordnung):

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

Zu 4. (als „usw.“ bezeichnete weitere Aufgaben):

Das ThürDSG verbietet grundsätzlich jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten, es sei denn, sie ist ausdrücklich gesetzlich erlaubt (Grundsatz des Verbots mit Erlaubnisvorbehalt, vgl. § 4 Abs. 1 ThürDSG).

Daraus ergab sich für den vorliegenden Fall, dass die offene Formulierung „usw.“ Raum ließ für weitere, nicht näher bezeichnete und damit ggf. unerlaubte Erhebungszwecke. Im Ergebnis genügte die Formulierung „usw.“ nicht den datenschutzrechtlichen Anforderungen.

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

das Ordnungsamt recherchieren sollte, öffentlich zugänglichen Quellen im Sinne von § 20 Abs. 2 ThürDSG entstammten. Kann auch ein nicht angemeldeter Nutzer bei Facebook personenbezogene Daten einsehen, so handelt es sich um öffentlich zugängliche Quellen. Hat ein Betroffener bei der Einrichtung einer Facebook-Seite seine Daten öffentlich zugänglich gemacht, ist nicht von einem schutzwürdigen Interesse an der Nicht-Nutzung dieser personenbezogenen Daten auszugehen.

Vom Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder wurde im Februar 2011 erörtert, welche Daten in sozialen Netzwerken als allgemein zugängliche Daten angesehen werden können. Im Ergebnis wurde übereinstimmend festgestellt, dass diejenigen Daten, die über allgemeine Suchmaschinen erschlossen werden können, allgemein zugängliche Daten sind.

Die Erhebung allgemein zugänglicher Daten aus sozialen Netzwerken durch Strafverfolgungs- und Gefahrenabwehrbehörden stellt zumindest dann einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, wenn dies zielgerichtet zu einer bestimmten oder bestimmbaren Person erfolgt. Als Rechtsgrundlage hierfür reichen in der Regel die Generalklauseln (§§ 161, 163 StPO, polizeiliche Generalklauseln) aus. §§ 161, 163 StPO finden gemäß § 46 Abs. 1 OWiG auch bei der Verfolgung von Ordnungswidrigkeiten Anwendung.

Zur Aufgabenerfüllung darf eine öffentliche Stelle jedoch grundsätzlich nicht selbst als privater Nutzer mit einem „Fake-Account“ in Facebook recherchieren und personenbezogene Daten erheben. Dies würde nicht zuletzt einen Verstoß gegen die Nutzungsbedingungen von Facebook darstellen. So fordert Facebook z. B. in seinen Nutzungsbedingungen Nr. 5 Pkt. 7 folgendes Verhalten:

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

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

Facebook installiert eine Reihe von Cookies, d. h. in einem solchen Falle auch auf den Dienst-PCs! Da Facebook seine tatsächliche Funktionalität derzeit noch nicht datenschutzrechtlich befriedigend transparent dargestellt hat, kann nicht ausgeschlossen werden, dass sämtliche besuchte Internet-Seiten und auch auf dem PC vorhandene Adressbücher mit den darin enthaltenen Kontaktadressen unbeteiligter Dritter heimlich durch Facebook erfasst werden. Dies stellt eine unzulässige Datenübermittlung dar.

Im Ergebnis riet der TLfDI dringend von der beabsichtigten Facebook-Nutzung ab. Die Stadt Arnstadt trug den Bedenken des TLfDI Rechnung und gab das Vorhaben auf.

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

5.59 Durch und durch Datenschutz

Im Berichtszeitraum erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis von möglichen datenschutzrechtlichen Verstößen der Stadt Nordhausen. Es stand der Verdacht im Raum, dass verschiedene Dokumente, die einen Personenbezug zu einem Beschwerdeführer aufwiesen, unrechtmäßig an Dritte weitergegeben bzw. veröffentlicht wurden.

Zur Sachverhaltsaufklärung wandte sich der TLfDI an den Oberbürgermeister der Stadtverwaltung Nordhausen und bat im Rahmen seiner Kontrollkompetenz nach § 37 Abs. 1 i. V. m. § 38 Abs. 1 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) um eine Stellungnahme zu diesen Vorwürfen. Eine Antwort des Oberbürgermeisters blieb aus. Trotz nochmaliger Erinnerung seitens des TLfDI blieben die Fragen unbeantwortet. Der von der Stadt Nordhausen zwischenzeitlich beauftragte Rechtsanwalt teilte dann in einem Schreiben unter anderem mit, dass eine Stellungnahme derzeit nicht erfolgen würde. Diese Weigerung stellte einen Verstoß gegen die Pflicht der Stadtverwaltung Nordhausen dar, den TLfDI gemäß § 38 Abs. 1 Nr. 1 ThürDSG in der Erfüllung seiner Aufgaben zu unterstützen. Der TLfDI beanstandete gemäß § 39 Abs. 1 S. 1 ThürDSG förmlich diesen Datenschutzverstoß und unterrichtete hiervon das Landratsamt Nordhausen

als Kommunalaufsichtsbehörde und das Thüringer Innenministerium gemäß § 39 Abs. 1 Satz 2 ThürDSG.

Kurz darauf führte der TLfDI eine datenschutzrechtliche Kontrolle bei der Stadtverwaltung Nordhausen durch. Dabei stellte der TLfDI fest, dass seit dem Ausscheiden des vorherigen behördlichen Datenschutzbeauftragten (bDSB) aus dem Dienst die Stadt Nordhausen von Ende Oktober 2012 bis Mitte des Jahres 2014 über keinen rechtswirksam bestellten behördlichen Datenschutzbeauftragten nach § 10a ThürDSG verfügte. Weiterhin hatte die Stadt Nordhausen in einem Disziplinarverfahren einen Rechtsanwalt als externen Ermittlungsführer beauftragt und diesem sensible personenbezogene Daten übermittelt. Die Beauftragung eines Rechtsanwalts als externen Ermittlungsführer seitens der Stadt Nordhausen in einem Disziplinarverfahren stellte eine unzulässige Datenübermittlung an einen unberechtigten Dritten dar, die nicht durch § 22 ThürDSG gerechtfertigt war. Insbesondere kann § 28 Thüringer Disziplingesetz (ThürDG) in Verbindung mit § 21 Abs. 1 Nr. 1 und § 20 Abs. 2 Nr. 1 ThürDSG in diesem Fall nicht zur Rechtfertigung einer Datenübermittlung herangezogen werden. Bereits aus dem Wortlaut von § 28 Satz 2 ThürDG, aber auch nach Auffassung der Literatur, ergibt sich, dass Ermittlungsführer nur eine innerhalb des öffentlichen Dienstes stehende Person sein kann. Denn nur eine solche Person kann nach dem Wortlaut dieser Vorschrift als „Ermittlungsführer“ für die Dauer seiner Aufgabe „im Hauptamt entlastet“ werden. Für einen Rechtsanwalt als Ermittlungsführer – wie im vorliegenden Fall – läuft § 28 Satz 2 ThürDG gerade ins Leere.

Der TLfDI stellte weiter fest, dass in einer öffentlichen Sitzung des Hauptausschusses der Stadt Nordhausen der Oberbürgermeister Angaben über die Eröffnung eines Disziplinarverfahrens gemacht hatte. Diese Übermittlung der bis dahin nicht medienbekannten personenbezogenen Daten stellte einen Verstoß gegen § 40 Abs. 1 Thüringer Kommunalordnung (ThürKO) dar, da Personalangelegenheiten als Teil des vertraulich zu behandelnden persönlichen Bereichs des Einzelnen nicht Gegenstand einer öffentlichen Sitzung sein dürfen (siehe dazu Rücker/Dieter/Schmidt, ThürKO, Kommentar, § 40, Nr. 2.4, Seite 6).

Diese Verstöße beanstandete der TLfDI förmlich gemäß § 39 Abs. 1 S. 1 ThürDSG und unterrichtete hiervon das Landratsamt – Kommunalaufsicht – und das Thüringer Innenministerium gemäß § 39 Abs. 1 S. 2 ThürDSG.

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

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

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

Im Berichtszeitraum hatte, laut einem Bericht des MDR, einer seiner Mitarbeiter zwei Festplatten auf einem Werkstoffhof in Gera gefunden. Der MDR informierte daraufhin in Erfurt den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), da auf den gefundenen Festplatten zum Teil brisante Arbeitnehmerdaten seien. Der MDR, die Bild-Zeitung und zahlreiche andere Medien berichteten dann über den „Datenskandal bei den Kraftwerken Gera“.

Der TLfDI erhielt Zugang zu Kopien der aufgefundenen Festplatten und überprüfte diese auf das Vorhandensein personenbezogener Daten. Seine Prüfung ergab, dass es sich bei den aufgefundenen Festplatten um solche von zwei Mitarbeitern der Kraftwerke Gera GmbH handelte und dass neben dienstlichen Berichten, Bestellungen und Anweisungen auch Gehalts-, Gesundheits- und Urlaubsdaten auf den Festplatten vorhanden waren.

Zudem konnte man aus noch vorhandenen Browsercaches u. a. die Hobbies/Interessen des jeweiligen Mitarbeiters sowie dessen dienstliches Aufgabengebiet einschätzen.

Der TLfDI bat daraufhin die Kraftwerke Gera GmbH unter anderem um die Übersendung des datenschutzrechtlichen Sicherheitskonzepts und der Dienstanweisungen, aus denen sich ergibt, inwieweit Mitarbeiter/-innen der Kraftwerke Gera GmbH vor Aussonderung ihrer Dienst-PCs angehalten sind, personenbezogene Daten auf den Dienst-PCs zu löschen.

Die Kraftwerke Gera GmbH teilte mit, dass sie nicht über eigenes IT-Personal verfüge, sondern in den Konzernverband der Stadtwerke Gera AG eingebunden sei, wobei die Stadtwerke mit der IT-

Betreuung und der Entsorgung jeglicher Hardware beauftragt worden seien. Zudem verwies die Kraftwerke Gera GmbH auf Geschäftsanweisungen zum Umgang mit Daten, in denen auch die Löschung und Vernichtung von Daten vorgesehen sei.

Im Rahmen der weiteren Prüfung informierte die Kraftwerke Gera GmbH den TLfDI, dass es ihr gelungen sei, betriebsintern aufzuklären, wer für den Vorfall der datenschutzwidrigen Entsorgung der Festplatten auf dem Werkstoffhof verantwortlich sei. Es handelte sich dabei um einen Mitarbeiter der Kraftwerke Gera GmbH, der beide Festplatten widerrechtlich und wissentlich mit nach Hause genommen, sie dort weitergenutzt und anschließend nach längerer Lagerung über den Elektroschrott entsorgt hatte. Die Kraftwerke Gera GmbH fügte quasi als Beweis für die Glaubhaftigkeit dieses Sachverhalts auch ein Schreiben an, in dem der Mitarbeiter seine Verfehlungen einräumte.

Unabhängig davon steht aus datenschutzrechtlicher Sicht fest, dass die Kraftwerke Gera GmbH als verantwortliche Stelle gemäß § 9 BDSG die technischen und organisatorischen Maßnahmen zu treffen hat, die erforderlich sind, um die Ausführung datenschutzrechtlicher Bestimmungen zu gewährleisten. Dies ergibt sich aus § 2 Abs. 2 ThürDSG, da es sich bei der Kraftwerke Gera GmbH um eine öffentliche Stelle handelt, die am wirtschaftlichen Wettbewerb teilnimmt und auf die nach § 26 ThürDSG nur die Bestimmungen des 5. Abschnitts des ThürDSG (ausgenommen § 34 Abs. 2 ThürDSG) anzuwenden sind. Im Übrigen gelten für sie die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mit Ausnahme des 2. Abschnitts und des § 38 BDSG.

Die von der Kraftwerke Gera GmbH getroffenen technischen und organisatorischen Maßnahmen waren deshalb verbesserungsbedürftig, um künftig solche Fallkonstellationen wie hier geschildert zu verhindern, bzw. weitestgehend auszuschließen. Da die Kraftwerke Gera GmbH aber selbst nicht nur tatkräftig an der lückenlosen Aufklärung dieses Falles mitwirkte, sondern konstruktiv auch die entsprechenden datenschutzrechtlichen Lehren aus diesem Fall zog, sagte sie zu, ihr Sicherheitskonzept dergestalt zu verbessern, dass konkrete Handlungsanweisungen für den sicheren Umgang (insbesondere die Löschung und die Vernichtung) von personenbezogenen Daten aufgenommen werden sollten. Diese und weitere Verbesserungen in ihren technischen und organisatorischen Maßnahmen hat

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

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



Personal Personalakte – © Wolfilser / Fotolia.com

6 Personaldaten

6.1 Datenleck bei Betriebsratswahl

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

Die Wahl war letztendlich vom Gericht als nichtig erklärt worden, wobei man festgestellt hatte, dass ein Mitglied des Wahlvorstands

regelwidrig Wahlvorschläge entgegengenommen und kurzerhand für unzulässig erklärt hatte.

Der TLfDI konnte wegen der Dringlichkeit der Angelegenheit zunächst nur eine vorläufige Einschätzung vornehmen. Wahlunterlagen enthalten personenbezogenen Daten und dienen dazu, den Nachweis der ordnungsgemäßen Durchführung zu erbringen. Zum Zweck der Wahlanfechtung kann Einblick genommen werden. Auch Unterstützungsunterschriften können zum Zweck der Einschätzung der Wirksamkeit überprüft werden, selbst wenn der Wahlvorstand ursprünglich irrtümlich gegenüber den unterzeichneten Unterstützern die Versicherung abgegeben hatte, dass die Unternehmensleitung davon nichts erfahre.

Der Betriebsrat bat den TLfDI, datenschutzrechtliche Maßnahmen einzuleiten. Der Eigenbetrieb war privatrechtlich organisiert, unterlag jedoch aufgrund der Beteiligung des Landkreises dem Thüringer Datenschutzgesetz (ThürDSG), § 1 Abs. 2 Satz 1 ThürDSG. Ein Betriebsrat ist der Stelle zuzuordnen, auch wenn er die gesonderte Aufgabe hat, die Beschäftigteninteressen gegenüber der Unternehmensleitung zu vertreten. Nach der Aufgabenwahrnehmung des Eigenbetriebs war er als Wettbewerbsunternehmen einzuordnen, sodass nach § 26 ThürDSG nur der Fünfte Abschnitt des ThürDSG anzuwenden war, im Übrigen die Bestimmungen des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts und des § 38. Daher war zu prüfen, ob ein Ordnungswidrigkeitenverfahren gegen ein Mitglied des Wahlvorstands eingeleitet werden konnte, das nach Auffassung der Beschwerdeführer der Unternehmensleitung bewusst die Unterlagen unzulässigerweise zugespielt hatte. Da aber bereits ein entsprechender Strafantrag bei der zuständigen Staatsanwaltschaft gestellt war, ist zunächst der Ausgang des Strafverfahrens abzuwarten. Unter Umständen kann danach ein Ordnungswidrigkeitenverfahren eingeleitet werden, wenn ersteres Verfahren eingestellt werden sollte.

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

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

6.2 Darf der behördeninterne Datenschutzbeauftragte den Personalrat kontrollieren?

Ein Mitglied eines Personalrats bei einer Thüringer Behörde wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob der behördliche Datenschutzbeauftragte der Dienststelle denn befugt sei, den Personalrat zu überprüfen. Die geschilderte Situation gestaltete sich so, dass der Personalrat keinen eigenen Raum für die Personalratsarbeit zur Verfügung hatte. Den Vorsitzenden und den Stellvertreter hatte man einfach in einem Büroraum untergebracht, wo jeder zur Hälfte seiner jeweiligen Arbeitszeit sowohl Personalratsarbeit als auch behördliche Verwaltungstätigkeit verrichten sollte. Ein verschließbarer Schrank stand zur Verfügung, in dem die Unterlagen, die zur Personalratsarbeit benötigt werden, eingeschlossen werden konnten, um unbefugte Kenntnis während der „normalen Dienstzeiten“ mit Publikumsverkehr zu verhindern. Auch erhielt der Personalrat eine Sekretärin, die mit einem nicht unwesentlichen Teil ihrer Arbeitszeit, aber auch einem Fachdienst- und Amtsleiter zur Verfügung zu stehen hatte. Die Arbeit für den Personalrat erledigte sie auf einem Notebook, das sie zum Schutz vor unbefugter Einsicht jeweils zuklappen konnte, wenn ihr jemand über die Schulter schauen konnte oder wollte.

Datenschutzrechtlich ist der Personalrat einer Dienststelle als Teil dieser Dienststelle zu bewerten. Die Pflicht zur Sicherstellung der Einhaltung der datenschutzrechtlichen Vorschriften trifft jedoch die verantwortliche Stelle nach § 34 Thüringer Datenschutzgesetz (ThürDSG), also die Dienststelle. Auch beim Personalrat müssen die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten, die im Rahmen seiner Aufgabenerfüllung verarbeitet werden, getroffen sein. Werden Mängel festgestellt, ist die Dienststelle aufgerufen, geeignete Maßnahmen zu treffen, damit die Mängel behoben werden. Hierfür sind dem Personalrat von der Dienststelle auch die Mittel zur Verfügung zu stellen, damit die datenschutzrechtlichen Vorschriften eingehalten werden können.

Unter den in der betroffenen Dienststelle herrschenden Umständen fällt es nicht leicht, die an den Personalrat von den Beschäftigten herangetragenen Anliegen vertraulich zu behandeln und die erforderlichen Maßnahmen zum Schutz personenbezogener Daten der Beschäftigten (oftmals Personalaktdaten), die im Rahmen der Mitbestimmung dem Personalrat von der Dienststelle übermittelt werden müssen, einzuhalten.

Nun hatte der Dienststellenleiter den behördlichen Datenschutzbeauftragten (bDSB) mit einer datenschutzrechtlichen Überprüfung des Personalrats beauftragt und der Personalrat vermutete dahinter keine guten Absichten. Etwas Würze bekam die Sache dadurch, weil es sich beim behördlichen Datenschutzbeauftragten um den ehemaligen Personalratsvorsitzenden handelte, der möglicherweise Freude oder Genugtuung über aufgespürte Fehler seiner Nachfolger haben konnte.

Hierzu hat der TLfDI Folgendes ausgeführt: Die Zuständigkeit und die Befugnisse des Beauftragten für den Datenschutz sind in § 10a ThürDSG festgelegt. Zwar hat das Bundesarbeitsgericht (BAG) in seinem Beschluss vom 11. November 1997 entschieden, dass eine Kontrollbefugnis des betrieblichen Datenschutzbeauftragten für Betriebsräte nicht besteht. Gleichzeitig hat es allerdings dargelegt, dass das Bundesverwaltungsgericht die Frage der Kontrollbefugnis des betrieblichen Datenschutzbeauftragten in Bezug auf die Personalverwaltung im öffentlichen Dienst ausdrücklich offen gelassen hat (BAG, Beschluss vom 11. November 1997, Az.: 1 ABR 21/97, Rn. 31).

Nach § 10a Abs. 2 ThürDSG hat der Beauftragte für den Datenschutz die Aufgabe, die Daten verarbeitende Stelle bei den Ausführungen der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken. Dies gilt grundsätzlich auch für den Personalrat, der als Teil der Dienststelle, die für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist, hiervon nicht grundsätzlich ausgenommen ist. Auch das Thüringer Personalvertretungsgesetz enthält keine Ausnahmeregelung. Eine Ausnahme besteht aber im Hinblick auf personenbezogene Daten in oder aus Personalakten, die nur mit Einwilligung der Betroffenen durch den Beauftragten für den Datenschutz einsehbar sind (§ 10a Abs. 4 Satz 1 ThürDSG). Zudem besteht ein besonderes Amtsgeheimnis der Personalratsmitglieder hinsichtlich der personenbezogenen Daten, die ihnen in ihrer Aufgabenwahrnehmung

bekannt geworden sind. Soweit also Personalaktendaten und einem besonderen Amtsgeheimnis unterliegende personenbezogene Daten beim Personalrat vorhanden sind, dürfen diese vom Beauftragten für den Datenschutz in seiner Aufgabenwahrnehmung nicht ohne Einwilligung des einzelnen Betroffenen eingesehen werden.

Im Falle einer Prüfung durch den behördlichen Datenschutzbeauftragten ist darüber hinaus auch die Sensibilität der Personalratstätigkeit zu beachten. Mitarbeiter dürfen sich vertrauensvoll an den Personalrat wenden, ohne dass die Dienststellenleitung davon über eine Kontrolle des Datenschutzbeauftragten Kenntnis erhalten könnte. Andererseits kann eine Prüfung durch den behördlichen Datenschutzbeauftragten in partnerschaftlicher Zusammenarbeit mit dem Personalrat auch Missstände, wie sie im vorliegenden Fall vorlagen, z. B. die ungeeigneten Räumlichkeiten, Mängel bei der Möglichkeit für Mitarbeiter, sich ungehindert an den Personalrat wenden zu können, ohne dass dies anderen Personen als den berechtigten Personalratsmitgliedern zur Kenntnis gelangt, aufzeigen und dazu beitragen, datenschutzgerechte Lösungen zu finden.

Der TLfDI beschränkte sich bis jetzt auf beratende Unterstützung, behält sich aber eine Kontrolle vor Ort vor.

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

6.3 Zeitungsnotiz zur „krankheitsbedingten“ Schließung eines Amtes

Eine Stadtverwaltung aus dem Saaleholzlandkreis (SHK) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Bewertung folgenden Sachverhalts:

Die Stadtverwaltung hatte in der Regionalzeitung über eine „krankheitsbedingte“ Schließung ihres Ordnungsamtes informiert.

Die Sorge und Frage der Stadt an den TLfDI war nun, ob aufgrund einer solchen Zeitungsnotiz außenstehende Dritte mit einer gewissen Wahrscheinlichkeit auf die Krankheit einer bestimmten Mitarbeiterin der Stadtverwaltung schließen könnten.

Diese Frage konnte der TLfDI nicht „pauschal“ beantworten. Vielmehr kommt es auf die Umstände des Einzelfalls an. Insbesondere spielen die Anzahl der Mitarbeiter des betreffenden Amtes sowie die Bekanntheit des Amtsleiters bei den Bürgern eine Rolle, die naturgemäß in einer Kleinstadt höher sein wird als in einer Großstadt mit einer eher anonym agierenden Verwaltung.

In dieser Stadtverwaltung bestand das Ordnungsamt aus zwei Mitarbeiterinnen. Insofern entspricht es der Lebenserfahrung, dass Dritte unter Berücksichtigung der für eine Kleinstadt typischen Zusatzinformationen, wie z. B. Mitteilungen von gemeinsamen Bekannten und zufällige Beobachtungen der Betroffenen innerhalb ihrer sonstigen Arbeitszeit bei nicht-dienstlichen Tätigkeiten, mit einer relativ hohen Wahrscheinlichkeit auf eine Krankheit der Betroffenen schließen könnten.

Aufgrund der Mitarbeiterzahl im Ordnungsamt im konkreten Fall handelte es sich bei der betreffenden Veröffentlichung – der „krankheitsbedingten“ Schließung – um eine unerlaubte Übermittlung einer Einzelangabe zu einer bestimmbar Person im Sinne des § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) an Stellen außerhalb des öffentlichen Bereichs (§ 22 ThürDSG). Vorstellbar wäre eine solche Veröffentlichung ggf. nur dann, wenn die Betroffene darin eingewilligt hat. Selbstverständlich bezieht sich die o. g. Bewertung auch auf die Übermittlung solcher personenbezogenen bzw. -beziehbarer Daten zu erkrankten Mitarbeitern der Stadtverwaltung innerhalb öffentlicher Sitzungen des Stadtrates und auf Informationen der Stadtverwaltung gegenüber Bürgern mittels Internet und E-Mail.

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

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

6.4 Mitarbeiter: Bitte lächeln!

Der Beauftragte für den Datenschutz einer Thüringer Kommune bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung zu dem Vorhaben, Bilder von Beschäftigten in eigenen Prospekten, Flyern oder der Tageszeitung zu veröffentlichen. Ohne weitere Hintergrundinformationen, beispielsweise zu welchem Zweck welche konkreten Bilder von Beschäftigten veröffentlicht werden sollen, hat der TLfDI im Rahmen seiner Beratungsaufgabe nach § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hierzu allgemein ausgeführt:

Fotografien von Mitarbeitern der Stadtverwaltung sind personenbezogene Daten von Beschäftigten, die gemäß § 33 Abs. 1 ThürDSG nach den dienstrechtlichen Vorschriften der §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) verarbeitet werden dürfen. Bei der Verwendung von Fotografien von Mitarbeitern handelt es sich regelmäßig nicht um eine Aufgabe der Personalverwaltung und -bewirtschaftung, sodass dies nur mit Einwilligung der Betroffenen geschehen kann. Es muss jedoch zur Einholung einer Einwilligung

vorab geprüft werden, dass eine Erforderlichkeit zur Aufgabenerfüllung vorliegt. Eine öffentliche Stelle wie die Stadtverwaltung muss daher auch bei der Veröffentlichung von Mitarbeiterbildern an die Erforderlichkeit zur Aufgabenerfüllung anknüpfen.

Handelt es sich um Bilder des Bürgermeisters oder der Beigeordneten, die in Wahrnehmung von öffentlichen Veranstaltungen und Terminen entstanden sind, bedarf es aufgrund deren Stellung sozusagen als Personen der Zeitgeschichte keiner Einwilligung zur Veröffentlichung von Bildern.

Die Einwilligungserklärung zum Abdruck in Druckerzeugnissen (stadteigenen Prospekten und Flyern) ist an die formellen Voraussetzungen des § 4 Abs. 3 ThürDSG gebunden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist. Die Beschäftigten müssen auf den Zweck und den Umfang der beabsichtigten Veröffentlichung hingewiesen werden. Weiterhin muss die Einwilligung auf Freiwilligkeit beruhen. Sollte die Stadtverwaltung Aufnahmen von Mitarbeitern an die Tageszeitung zur Veröffentlichung geben, gilt dies ebenso. Sofern daran gedacht wird, dass die Prospekte und Flyer auch im Internet veröffentlicht werden, ist § 23 ThürDSG zu beachten. Bei der Veröffentlichung von Daten im Internet handelt es sich um eine Übermittlung personenbezogener Daten an öffentliche und nicht-öffentliche Stellen außerhalb des Geltungsbereiches des Grundgesetzes. Eine solche Übermittlung ist nur unter den Voraussetzungen des § 23 ThürDSG zulässig. Da nicht ausgeschlossen werden kann, dass bei einer weltweiten Veröffentlichung die Daten auch in Staaten übermittelt werden, in denen kein angemessenes Datenschutzniveau gewährleistet ist, müssen die Voraussetzungen des § 23 Abs. 2 ThürDSG gegeben sein. Von diesen Voraussetzungen kommt allenfalls die Nr. 1 in Betracht, nach der eine zweifelsfreie Einwilligung des Betroffenen vorliegen muss.

Die Einwilligung ist nach § 4 Abs. 2 ThürDSG die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seinen personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen. Sofern der Betroffene, dessen Daten veröffentlicht werden, in einem Arbeitsverhältnis mit der Daten übermittelnden Stelle steht, bestehen bereits große Zweifel an der Freiwilligkeit der Einwilligung. Freiwilligkeit ist nur dann gegeben, wenn für die Mitarbeiter keinerlei Druck besteht und im Falle einer Ablehnung auch keine Nachteile entstehen. Diesen Grundsatz

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

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

6.5 Bewerberunterlagen: Einsicht für alle Personalratsmitglieder?

Der Personalratsvorsitzende in einem Landratsamt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, ob denn nur der Personalratsvorsitzende oder auch andere Personalratsmitglieder Einsicht in Bewerberunterlagen nehmen dürften. Hintergrund war folgender:

Dem Personalrat steht bei Einstellungen gemäß § 68 Abs. 2 Satz 4 Thüringer Personalvertretungsgesetz (ThürPersVG) das Recht zur Einsichtnahme in die Bewerbungsunterlagen aller Mitbewerber zu, um Benachteiligungen jeglicher Art auszuschließen. Dementsprechend ist die Dienststelle zur Vorlage der Bewerbungsunterlagen an den Personalrat verpflichtet. Die Dienststelle wollte das Einsichtsrecht mit Hinweis auf den besonderen Schutz von Bewerberdaten auf den Personalratsvorsitzenden beschränken.

Im Rahmen der Aufgabenverteilung unter den Personalratsmitgliedern wurde aber die Zuständigkeit der einzelnen Mitglieder auf verschiedene Ämter aufgegliedert. Das jeweils zuständige Mitglied nimmt folglich auch an den Bewerbergesprächen teil. Wenn die Einsicht in die entsprechenden Bewerberunterlagen auf den Personalratsvorsitzenden beschränkt bliebe, wäre das für das entsprechen-

de Bewerbungsverfahren zuständige Personalratsmitglied auf die Weitergabe der entsprechenden Informationen vom Vorsitzenden angewiesen.

Zur Beantwortung der Frage führte der TLfDI aus, dass aus den datenschutzrechtlichen Grundsätzen die Dienststellenleitung verpflichtet ist, nur die für eine Personalmaßnahme erforderlichen personenbezogenen Daten dem Personalrat zugänglich zu machen. Bei der Einstellung eines Bewerbers sind die Unterlagen des Bewerbers sowie seiner Mitbewerber für die Entscheidung des Personalrats erforderlich. Auch wenn Bewerberdaten eine besondere Sensibilität zukommt, muss dem Personalrat zur Gewährleistung seiner Handlungsfähigkeit Kenntnis der erforderlichen Daten gewährt werden. Aufgrund der Sensibilität der personenbezogenen Daten der Bewerber ist es hingegen nicht erforderlich, dem gesamten Personalrat, also allen seinen Mitgliedern, den Zugang zu den personenbezogenen Daten zu gewähren. Wird jedoch, wie vorliegend geschildert, im Rahmen der Aufgabenverteilung unter den Personalratsmitgliedern die Zuständigkeit der einzelnen Personalratsmitglieder auf verschiedene Ämter aufgegliedert, müssen für das jeweils zuständige Personalratsmitglied, das an den Bewerbungsgesprächen teilnimmt, auch die für die Aufgabenwahrnehmung erforderlichen personenbezogenen Daten der Bewerber zugänglich sein.

Aus datenschutzrechtlicher Sicht sah der TLfDI daher keine Gründe, diesem zuständigen Personalratsmitglied die Einsicht in die zu seiner Aufgabe erforderlichen entsprechenden Bewerbungsunterlagen zu verweigern und diese nur dem Personalratsvorsitzenden zu gewähren, der das Mitglied entsprechend informieren müsste. Soweit aber dem zuständigen Personalratsmitglied die Daten zugänglich gemacht werden, ist darüber hinaus eine Vorlage an den Personalratsvorsitzenden oder andere Mitglieder des Personalrats grundsätzlich nicht mehr erforderlich.

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

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

Eine Mitarbeiterin einer Stadtverwaltung teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Folgendes mit: Der Leiter eines städtischen Amtes habe ein Schreiben des Haupt- und Personalamtes mit sensiblen Daten zu ihrer Person aus einem Verfahren zur Vermeidung und Bekämpfung von Mobbing anderen Mitarbeitern der Stadtverwaltung über das Intranet zur Kenntnis gegeben. Eine Einwilligung der Mitarbeiterin der Stadtverwaltung zu dieser Datenübermittlung lag natürlich nicht vor.

Der TLfDI stellte schnell fest, dass die interne Veröffentlichung sensibler personenbezogener Daten aus einem Verfahren zur Dienstvereinbarung Mobbing an nicht am Verfahren beteiligte Personen im konkreten Fall unzulässig erfolgte und dies einen erheblichen Verstoß gegen datenschutzrechtliche Vorschriften darstellte. Daher hat der TLfDI die datenschutzrechtlichen Mängel in Form einer nach § 21 Thüringer Datenschutzgesetz (ThürDSG) unzulässigen Übermittlung personenbezogener Daten gemäß § 39 Abs. 1 Satz 1 ThürDSG beanstandet. Der TLfDI forderte die Stadtverwaltung auf, dafür Sorge zu tragen, dass künftig in ähnlichen Fällen die Datenübermittlung auf den Kreis der Berechtigten beschränkt wird. Die betroffene Stadtverwaltung hat zu der Angelegenheit ein Ordnungswidrigkeitenverfahren eingeleitet.

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

6.7 Mitarbeiter im GPS-Dauer-Fokus

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

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

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

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

Durch GPS erhobene Standortdaten oder Bewegungsprofile von Fahrzeugen sind personenbeziehbar und damit personenbezogene Daten, wenn sie einem konkreten Fahrer zugeordnet worden sind. Damit verbunden ist, dass der jeweilige Beschäftigte einer Leistungs- und Verhaltenskontrolle unterzogen werden kann, die nach § 33 Abs. 4 Thüringer Datenschutzgesetz (ThürDSG) unzulässig ist. Nach § 19 Abs. 2 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Zu dem angegebenen Zweck der Standortlokalisierung zur Koordinierung der täglichen Einsätze ist eine Erforderlichkeit zur Erfassung der Position während der Fahrt gegeben. Eine Erforderlichkeit zur Erfassung z. B. der gefahrenen Geschwindigkeit ist nicht ersichtlich und damit unzulässig.

Nach § 20 Abs. 1 ThürDSG ist die Speicherung der Daten zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Zur Feststellung der Position für Einsatzzwecke ist eine aktuelle Positionsbestimmung ausreichend. Hierfür bedarf es keiner über das Tagesende hinaus andauernden Speicherung. Aus der Feststellung der Fahrzeugposition im Fall eines Diebstahls ist eine Echtzeitfeststellung ausreichend. Die Speicherung der Fahrzeugdaten für 90 Tage war daher nicht begründbar und mangels Erforderlichkeit unzulässig. Der TLfDI forderte daher, dass mangels Rechtsgrundlage die Geschwindigkeitserfassung zu deaktivieren ist und die gespeicherten Daten zu löschen sind.

Die im Nachgang erarbeitete Dienstanweisung enthält nunmehr eine Auflistung der erfassten Daten, konkrete Festlegungen zur Zweckbindung und der Zugriffs- und Nutzungsrechte. Die Nutzung der erfassten Fahrzeugdaten zur Verhaltens- und Leistungskontrolle der Fahrzeugführer ist ausgeschlossen. Die Dauer der Speicherung wurde auf 72 Stunden verkürzt. Diese Speicherdauer kann ausnahmsweise damit begründet werden, dass unter Umständen ein zulässiger Zugriff am Montag auf den vorhergehenden Freitag erforderlich sein kann.

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

6.8 Übermittlungsbefugnis des Amtsarztes – keine Generalvollmacht!

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

und 4 Thüringer Beamten-gesetz (ThürBG). Danach teilt der Arzt der zuständigen Behörde die tragenden Feststellungen und Gründe des Ergebnisses der ärztlichen Untersuchung mit, soweit deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist. Ferner berichtet er über die infrage kommenden Maßnahmen zur Wiederherstellung der Dienstfähigkeit und die Möglichkeit einer anderen Verwendung. Als technische und organisatorische Maßnahmen zum Schutz dieser sensiblen Angaben ist weiterhin gesetzlich bestimmt, dass die Mitteilung des Arztes über die Untersuchungsergebnisse in einem gesonderten, verschlossenen und versiegelten Umschlag zu übersenden ist. Sie ist verschlossen zur Personalakte des Beamten zu nehmen. Weiterhin dürfen die an die Behörde übermittelten Daten nur für die im Einzelfall konkret zu treffende Entscheidung verarbeitet oder genutzt werden. Somit ist auch eine besondere Zweckbindung festgeschrieben.

Die Transparenz für die Betroffenen wurde ebenfalls berücksichtigt. Nach § 33 Abs. 2 ThürBG ist der Beamte zu Beginn der Untersuchung oder der Beobachtung auf deren Zweck und die Übermittlungsbefugnis an die Behörde hinzuweisen. Der Arzt übermittelt dem Beamten oder, soweit dem ärztliche Gründe entgegenstehen, dessen Bevollmächtigten eine Kopie der an die Behörde erteilten Auskünfte.

Eine in diesem Sinne betroffene Person wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), nachdem sie vom Amtsarzt keine Auskunft dazu erhielt, was denn nun an die personalverwaltende Dienststelle als Ergebnis einer Untersuchung gesandt worden war. Nachdem sie sich an ihre Personalverwaltung gewandt und Einsicht in die Unterlagen genommen hatte, fiel sie aus allen Wolken. Es waren alle erdenklichen Diagnosen aufgeführt, ob sie nun mit der Dienstfähigkeit in Verbindung standen oder nicht. Weiterhin machte die betroffene Person geltend, sie habe eine Schweigepflichtentbindungserklärung in pauschaler Form vorgelegt erhalten, die sie bereits vor der Untersuchung unterschreiben sollte, obwohl weder die zu entbindenden Ärzte noch der konkrete Zweck darin erkennbar waren.

Nachdem der TLfDI gegenüber dem Amtsarzt die Rechtslage dargelegt hatte, sagte dieser unverzüglich zu, zukünftig nur noch die für die Kenntnis der Behörde für die von ihr zu treffende Entscheidung erforderlichen Angaben zu übermitteln. Weiterhin werde zukünftig

beachtet, dass auch die begutachteten Beamten einen Anspruch auf eine Kopie der an die Behörde erteilten Auskünfte haben. Die formulärmäßige Entbindung von der Schweigepflicht für behandelnde andere Ärzte wurde überarbeitet und konkretisiert, sodass zukünftig wirksame Schweigepflichtentbindungen erteilt werden können.

Aufgrund der prompten Zusage zur Behebung der erheblichen datenschutzrechtlichen Verstöße hat der TLfDI unter Anwendung des § 39 Abs. 3 ThürDSG zunächst von einer Beanstandung nach § 39 Abs. 1 ThürDSG abgesehen. Nachdem sich aber die Beschwerdeführerin nach Ablauf einer angemessenen Frist wieder meldete, weil sie auf ihre Anfragen und Bemühungen immer noch keine Kopie des „neuen“, den gesetzlichen Anforderungen entsprechenden Gutachtens erhalten habe, musste der TLfDI davon ausgehen, dass die Zusagen (noch) nicht umgesetzt wurden. Daher sprach er eine Beanstandung nach § 39 Abs. ThürDSG in Verbindung mit § 33 Abs. 3 und 5 ThürBG mit Fristsetzung zur Behebung der datenschutzrechtlichen Mängel aus.

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

6.9 GPS: nicht vom richtigen Weg abkommen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Information, dass die Stadtwerke Schmölln GmbH ihre Fahrzeuge mit Möglichkeiten zu einer Global Positioning System (kurz GPS)-Überwachung und damit zu einer weitgehenden Verhaltens- und Leistungskontrolle der jeweiligen Fahrer ausgestattet hätten.

Der TLfDI nahm sich dieses Falles an und forderte die Stadtwerke zu einer Stellungnahme auf. Aus dieser ging hervor, dass eine Auswertung des GPS-Systems zu Kontrollzwecken erfolge, wenn der Verdacht bestehe, dass Fahrzeuge zu betriebsfremden, nicht genehmigten Fahrten benutzt werden oder wenn der Verdacht einer Straftat vorliege. Eine Rechtsgrundlage für die Überprüfung der Protokolldaten (u.a. die Fahrzeit und Fahrtstrecke und eingesetzter Fahrer) des eingesetzten GPS-Systems in diesem Zusammenhang war nicht ersichtlich. Aufgrund der fehlenden Rechtsgrundlage lag somit eine

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

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

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

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

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

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

6.10 Bewerbungen per E-Mail

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

Der TLfDI nahm dies zum Anlass, die obersten Landesbehörden auf die nachfolgenden datenschutzrechtlichen Aspekte hinzuweisen und

bat darum, auch die nachgeordneten Bereiche hierüber zu informieren und bei zukünftigen Ausschreibungen zu beachten:

Kommt es aufgrund einer Bewerbung zu einer Beschäftigung, werden die von Bewerbern mit der Bewerbung eingereichten personenbezogenen Daten Bestandteil der Personalakten, für die die dienstrechtlichen Vorschriften der §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) gelten, die besondere Schutzvorschriften und Zugangsregelungen enthalten. Diese Bestimmungen finden gemäß § 33 Thüringer Datenschutzgesetz (ThürDSG) für Angestellte, Arbeiter und Auszubildende im öffentlichen Dienst entsprechend Anwendung. Den von den Bewerbern zum Zweck der Eingehung eines Dienstverhältnisses eingereichten personenbezogenen Daten kommt somit ein besonderer Schutzbedarf zu. Zugang zu diesen Daten dürfen nur damit betraute Personen haben (vgl. § 80 Abs. 1 ThürBG). Ein allgemeiner Zugang zu Bewerberdaten ist daher in den Behörden auszuschließen.

Sollen von öffentlichen Stellen Bewerbungen per E-Mail zugelassen werden, sind besondere technische und organisatorische Maßnahmen zu treffen, die unbefugte Kenntnis der Bewerbungsunterlagen ausschließen. Für den unversehrten Zugang der personenbezogenen Daten muss daher eine Verschlüsselung und Entschlüsselung möglich sein.

Weiterhin kann nicht das allgemeine Postfach eines Hauses genutzt werden, da die allgemeine Poststelle und Registratur mangels konkreter Aufgabenerfüllung zu diesen personenbezogenen Daten der Bewerber keinen Zugang/Zugriff haben darf.

Wie im Nachgang festzustellen war, wurden die Ausführungen bei daraufhin folgenden Stellenausschreibungen berücksichtigt. Die meisten Ressorts verfügen offenbar nicht über die erforderlichen Vorrichtungen zur Sicherstellung gegen unbefugte Kenntnisnahme, denn es findet sich nunmehr meistens der Zusatz, dass E-Mail-Bewerbungen aus datenschutzrechtlichen Gründen nicht erwünscht sind.

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

6.11 Elektronische Personalakte

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

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

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

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

http://www.moderneverwaltung.sachsen.de/download/Handreichung_rechtssichere_Aufbewahrung_V1_2009.11.16.pdf



Weiterhin ist die Problematik der Urkundenqualität von elektronischen Dokumenten in diesem Zusammenhang noch nicht konkret geklärt. Daher ist es angeraten, Unterlagen mit Urkundenqualität auch noch in Papierform zu führen (so genannte Hybridakte). Kann zu einzelnen Unterlagen eine gesonderte Löschung aufgrund Fristablaufs im automatisierten Verfahren

nicht vorgenommen werden, sind diese Dokumente ebenfalls besser in Papierform zu führen. Dies betrifft Krankmeldungen, Arbeitszeitdaten, Urlaubsgewährung, aber auch für Betroffene ungünstige Beschwerden und Behauptungen (§§ 86, 87 ThürBG). Näheres, auch zur teilweisen oder vollständig automatisiert geführten Personalakte, sollte in einer novellierten Personalaktenführungsrichtlinie geregelt werden.

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

6.12 Fingerabdruckscanner zur Arbeitszeiterfassung?

Vereinzelte wenden sich Beschäftigte und Betriebsräte Hilfe suchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil in ihrem Betrieb im Zuge der fortschreitenden Technisierung ein Fingerabdruckscanner zur Arbeitszeiterfassung eingeführt werden soll. Mit solchen Geräten zur Erfassung von Fingerabdrücken sind bisweilen ungute Vorstellungen und Befürchtungen verbunden, da man mit der Abgabe von Fingerabdrücken oftmals polizeiliche Maßnahmen vor Augen hat. Fingerabdrücke müssen doch meist nur Verbrecher abgeben ...

Zur datenschutzrechtlichen Problematik des Einsatzes eines Fingerabdruckscanners bei der Arbeitszeiterfassung verweist der TLfDI auf die „Hinweise zur biometrischen Datenerfassung am Arbeitsplatz“, die auf seiner Homepage unter Themen – Beschäftigtendatenschutz verfügbar sind. Folgendes ist zu beachten:

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

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

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

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

6.13 Fragebögen zur Mitarbeiterbefragung

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

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

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

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

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

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

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

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

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

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

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

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

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

Der TLfDI, der nebenbei aufgrund der geäußerten Befürchtungen der Beschwerdeführerin wegen dienstlicher Nachteile darauf hinwies, dass nach § 11 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) niemand benachteiligt oder gemäßregelt werden dürfe, weil er von seinem Recht, sich an den TLfDI zu wenden, Gebrauch gemacht hat, fragte beim Amtsleiter nach. Der angesprochene Amtsleiter erläuterte, er wolle unbedingt vermeiden, dass private Auseinandersetzungen ins Amt getragen und am Arbeitsplatz – eventuell unter Einbeziehung von Arbeitskollegen – zum Nachteil der Arbeitsleistung und des Amtsfriedens ausgefochten werden. Es sei richtig, er habe als Leiter des Amtes – persönlich – E-Mails eines Beschäftigten erhalten. Den Inhalt, der keinen dienstlichen Bezug aufwies, habe er zur Entscheidung zum weiteren Vorgehen mit dem örtlichen Personalrat, der Leiterin der Personalverwaltung und dem Datenschutzbeauftragten vertraulich erörtert. Zu diesem Zweck habe er die E-Mails ausgedruckt und in seinem elektronischen Postfach gelöscht. Weil aber die ihm unaufgefordert zugesandten und von ihm unerwünschten E-Mails auch besonders zu schützende personenbezogene Daten des Absenders enthielten, könne er sie der Beschwerdeführerin nicht zugänglich machen, weil sonst das datenschutzrechtliche Interesse des Absenders massiv verletzt wäre.

Der TLfDI legte gegenüber dem Amtsleiter dar, dass die Erörterung des Inhalts mit den genannten Funktionsträgern zur weiteren Vorgehensweise keinen grundsätzlichen datenschutzrechtlichen Bedenken begegnete. Die Äußerungen des Absenders waren zwar gegenüber dem Amtsleiter persönlich, aber dennoch in dessen Eigenschaft als Leiter der Behörde getätigt worden und somit der öffentlichen Stelle zuordenbar. Durch die dienstliche Erörterung mit den genannten Funktionsträgern kam den E-Mails auch eine dienstliche Behandlung zu, auch wenn letztendlich ein dienstlicher Bezug des Inhalts verneint worden war. Damit unterlagen die die Beschwerdeführerin betreffenden personenbezogenen Daten der Auskunftspflicht nach § 13 ThürDSG bzw. § 33 ThürDSG i. V. m. § 85 Abs. 4 Thüringer Beamtengesetz. Die personenbezogenen Daten, die der Absender dem Amtsleiter gegenüber von sich selbst offenbart hatte, konnten – wie richtig erkannt wurde – als Daten Dritter grundsätzlich nicht beauskunftet werden; insoweit kommt eine Schwärzung der Daten Dritter in Betracht.

Auch die weitere Aufbewahrung der E-Mails in Papierform war ein Problem. Sie stellte nämlich weiterhin eine Verarbeitung personen-

bezogener Daten dar (§ 3 Abs. 3 Nr. 2 ThürDSG). Da ein dienstlicher Bezug verneint worden war, waren die personenbezogenen Daten, die mit den E-Mails zur Kenntnis gelangten, für die (weitere) Aufgabenerfüllung der Stelle nicht erforderlich. Mangels des Vorliegens der Zulässigkeitsvoraussetzungen dürfen die Daten auch nicht weiter verarbeitet werden. Die E-Mails waren deshalb nach § 16 Abs. 1 Nr. 1 ThürDSG auch in Papierform zu löschen. Jedoch musste die Löschung unterbleiben, solange dem Auskunftsbegehren der Beschwerdeführerin noch nicht nachgekommen wurde.

Der Amtsleiter tut sich aber offenbar immer noch schwer, der Beschwerdeführerin eine entsprechende Auskunft zu geben und hat die E-Mail-Ausdrucke zur weiteren Prüfung, wie weit der Auskunftsanspruch gehe, erst mal dem TLfDI übersandt. Die Prüfung hierzu ist noch nicht abgeschlossen.

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

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

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

Zur Sachverhaltsaufklärung wandte sich der TLfDI im Rahmen seiner Kontrollbefugnis gemäß § 37 Thüringer Datenschutzgesetz

(ThürDSG) umgehend an die LEG. Von dieser erhielt er die Auskunft, dass die Übermittlung auf ein Ersuchen der LPI Erfurt erfolgt sei, und die betroffenen Mitarbeiter zudem per E-Mail über den Vorgang informiert worden wären.

Daraufhin richtete der TLfDI seine Kontrolltätigkeit nunmehr auf die LPI aus und erhielt von ihr eine umfassende Stellungnahme. Darin führte die LPI aus, dass nicht nur die Bundeskanzlerin, sondern auch weitere Veranstaltungsgäste von Seiten des Bundeskriminalamtes (BKA) als gefährdete Schutzpersonen eingestuft seien. Bei der Teilnahme solcher Personen gelten grundsätzlich die höchste Gefährdungsstufe sowie die Veranlassung weitreichender Schutzmaßnahmen. Diese Maßnahmen sollten gewährleisten, dass mögliche Störungen, Angriffe, Sabotageakte und Anschlagsfälle auf Personen und relevante Gebäude verhindert werden.

Aufgrund der baulichen Gegebenheiten – die Tiefgarage befindet sich unter dem Hotel, in dem die Kanzlerin und weitere Veranstaltungsgäste übernachteten – wurde die Tiefgarage als relevantes Gebäude betrachtet und musste daher entsprechend abgesichert werden. Die polizeiliche Absicherung umfasste das Identifizieren potenzieller Gefährder und das frühzeitige Erkennen etwaiger Straftäter. Hierbei beurteilt die Polizei unter Berücksichtigung von Lagefeldern wie Raum, Zeit, Bedrohung, Gefahren, Politik, Staatsschutz usw. die polizeiliche Lage und trifft zur Gefahrenminimierung sowohl vor als auch während der Veranstaltung die erforderlichen Maßnahmen. Dazu gehört der Personen- und Objektschutz in allen denkbaren Facetten, aber auch das Prüfen und Organisieren von Zu- und Abfahrtsmöglichkeiten und Einlasskontrollen. In diese polizeilichen Maßnahmen war das Überprüfen und Sichern der Räume des Aufenthalts gefährdeter Personen sowie von Personen, die ggf. mit gefährdeten Personen in Kontakt treten und sich in ihrer unmittelbaren Umgebung aufhalten konnten, einzuordnen.

§ 31 Abs. 1 Polizeiaufgabengesetz (PAG) regelt als die spezielle Rechtsgrundlage die Grundsätze der Datenerhebung durch die Polizei und schreibt vor, dass die Datenerhebung durch Gesetz oder besondere Rechtsvorschriften zugelassen sein muss.

Die Polizei ist nach § 14 Abs. 1 Nr. 3 Thüringer Polizeiaufgabengesetz (PAG) dazu ermächtigt, die Identität einer Person festzustellen, wenn diese sich unter anderem in oder in unmittelbarer Nähe von einem besonders gefährdeten Objekt aufhält. Die Datenerhebung hat gemäß § 31 Abs. 2 Satz 1 PAG grundsätzlich beim Betroffenen

selbst zu erfolgen. Im vorliegenden Fall wurde die Datenerhebung aber über die LEG betrieben. Eine Datenerhebung bei Behörden, öffentlichen Stellen oder bei Dritten ist jedoch gemäß § 31 Abs. 2 Satz 2 PAG ausnahmsweise zulässig, wenn die Datenerhebung beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder die Erfüllung der polizeilichen Aufgaben gefährdet würde. Diese Voraussetzungen waren hier im konkreten Fall gegeben: Zum einen hätte bei einer Direkterhebung die Polizei jeden einzelnen Mitarbeiter der LEG / Tiefgaragennutzer überprüfen müssen, was ein unverhältnismäßiger Aufwand gewesen wäre, und zum anderen geschah die Datenerhebung auch offen im Sinne von § 14 Abs. 3 PAG. Die betroffenen LEG-Mitarbeiter wurden ja, wie bereits erwähnt, per E-Mail über die Datenerhebung in Kenntnis gesetzt.

Durch den Abgleich der Kennzeichen und Nachnamen der üblichen Tiefgaragennutzer konnte zudem eine Vollsperrung der Tiefgarage vermieden werden. Da eine Vollsperrung die berechtigten Nutzer sowohl in ihrer Handlungsfreiheit als auch in ihren Nutzungsrechten an den gemieteten Stellplätzen maximal eingeschränkt hätte, war die Beschränkung auf eine Berechtigungskontrolle eindeutig das mildere, aber gleichwohl effektive Mittel, um den Sicherungszweck hier zu erreichen.

Im Ergebnis konnte durch diese permanente polizeiliche Kontrolle der Tiefgaragenzufahrt im Interesse der Berechtigten und zur Entlastung der Bürger eine Vollsperrung des näheren Umfeldes vermieden werden.

Die erhobenen Daten waren zur Sicherung der Veranstaltung und der daran teilnehmenden Personen auch erforderlich. Die Aufnahme von Personalien ist polizeirechtlich eines der mildesten Mittel zur Gefahrenabwehr. Es schränkt die Betroffenen kaum fühlbar in ihren Grundrechten und in ihrer allgemeinen Handlungsfreiheit ein, ermöglicht aber auch eine effektive Abwehr oder Verhinderung rechtswidrigen Handelns.

Ein milderer, gleich geeignetes Mittel stand somit zur polizeilichen Aufgabenerfüllung nicht zur Verfügung, um eine Übersicht allgemein Zutritts-/zufahrtsberechtigter LEG-Mitarbeiter zu erhalten.

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

garage, sodass die dargestellten rechtlichen Ausführungen für sie entsprechend galten.

Ein Verstoß gegen Bestimmungen des Datenschutzes, insbesondere des PAG, lag hier somit nicht vor.

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

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

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

In dem Verfahren „Interamt“ konnte beim Einstellen einer Stellenausschreibung auch die Art der Bewerbung (in Papierform, per E-Mail oder unter Nutzung der Stellenplattform „Interamt.de“) festgelegt werden.

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



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

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

Nach den übersandten Unterlagen werden die Daten der Bewerber nach Abschluss des Verfahrens gelöscht, was regelmäßig zum 30. August eines jeden Jahres der Fall ist. Vor diesem Termin können Bewerbungen gelöscht werden, falls die erforderlichen Voraussetzungen für die Ausbildung von einem Bewerber nicht erbracht werden.

Aufgrund dieser Ausführungen der TLFD sah der TLfDI keine weiteren Bedenken gegen die vertraglich vereinbarte Auftragsdatenverarbeitung.

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

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

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

Für die datenschutzrechtliche Beurteilung der Weitergabe der vertraulichen E-Mail durch den Bürgermeister an die Angestellte ist der

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

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

Uckel/Hauth/Hoffmann/Noll, Kommunalrecht in Thüringen, Rechtsammlung, § 22 ThürKO, Nr. 8, S. 10).

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

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

6.18 Geheime Personalakten?

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

sonalunterlagen geführt wurden und darüber hinaus aus seiner Sicht wesentliche Unterlagen in der Personalakte fehlten.

Der TLfDI führte daraufhin in der Beschäftigungsbehörde eine datenschutzrechtliche Kontrolle gemäß § 37 Thüringer Datenschutzgesetz (ThürDSG) durch und ließ sich sämtliche Personalunterlagen und Sachvorgänge, die personenbezogene Daten des Betroffenen als Beschäftigten enthielten, zur Einsicht vorlegen. Die Kontrolle wurde nicht vorher angekündigt, um jeglichen Manipulationsverdacht zu vermeiden. Der Überraschungseffekt einer unangekündigten Kontrolle hat den Vorteil, dass der Sachverhalt seitens der kontrollierten Stelle nicht vorbereitet werden kann. Der Stand der Aktenführung spiegelt dann im Regelfall das wider, was Beschwerdeführer vorgefunden hatten. Gleichzeitig besteht aber andererseits für die Kontrolle der Nachteil, dass auskunftsfähige Ansprechpartner eventuell nicht zur Verfügung stehen oder zwischenzeitliche Ereignisse die Verfügbarkeit der Unterlagen beeinträchtigen konnten. Bei dieser Kontrolle lagen aber keine derartigen Schwierigkeiten vor. Die Personalakte nebst eventueller Sachvorgänge war ausweislich der Anforderung durch das für die Rechtsstreitigkeiten zuständige Gericht abgefordert worden. Von den Unterlagen waren Kopien gefertigt worden, die dem TLfDI anstandslos vorgelegt wurden. Dabei stellte der TLfDI verschiedene Mängel hinsichtlich der Personalaktenführung fest.

Nach § 33 Abs. 1 ThürDSG gelten die §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) für das Verarbeiten oder Nutzen personenbezogener Daten über im öffentlichen Dienst beschäftigte Personen, die nicht verbeamtet sind, entsprechend, es sei denn besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor. Danach ist für jede Beamtin und jeden Beamten eine Personalakte zu führen. Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktenakten). Die Personalakte ist vertraulich zu behandeln. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein, wobei landesrechtlich hierzu Ausnahmen vorgesehen werden können.

Ergänzend zu den dienstrechtlichen Vorschriften kann die Personalaktenführungsrichtlinie (ThürStAnz 1998, S. 1812 ff.) sinngemäß herangezogen werden, auch wenn diese aufgrund der zum

1. Januar 2015 in Kraft getretenen Änderung der beamtenrechtlichen Vorschriften zu überarbeiten ist.

Neben der Personalakte können auch Sachvorgänge zu Bediensteten geführt werden, sofern die zugrundeliegenden Sachverhalte sachlich zu trennen sind. Dies betrifft insbesondere Vorgänge, die im Rahmen der Aufsicht oder zur Rechnungsprüfung angelegt werden, Prüfungs-, Sicherheits- und Kindergeldakten sowie Daten über ärztliche und psychologische Untersuchungen und Tests mit Ausnahme ihrer Ergebnisse (§ 81 Abs. 1 Satz 2 ThürBG). Prozessakten und Vorgänge zu Widerspruchsverfahren zählen ebenso zu derartigen Sachakten. Nach deren Abschluss ist zu prüfen, ob das Ergebnis unmittelbar Auswirkungen auf das Dienstverhältnis hat und damit zur Personalakte zu nehmen ist.

Zuoberst war in der Akte ein amtsärztliches Gutachten offen eingelegt. In der Akte befanden sich noch weitere ärztliche Gutachten. Auch wenn zum Zweck der Personalverwaltung eine Kopie der dem Gericht vorgelegten Personalakte gefertigt wird, ist mit amtsärztlichen Gutachten ebenso zu verfahren, als ob sie im Original vorhanden wären, sie sind nämlich in verschlossenen Umschlägen zur Personalakte zu nehmen. Darüber hinaus dürfen nur die Ergebnisse der Eignungsuntersuchung und dabei festgestellte Risikofaktoren zur Personalakte gelangen, nicht aber umfängliche Gutachten mit der ganzen Familiengeschichte (Daten Dritter) und sämtlichen festgestellten Diagnosen und erhobenen Gesundheitsdaten. Selbst wenn der Beschäftigte selbst ärztliche Gutachten zur Personalakte gibt, weil er damit möglicherweise einen Nachweis führen will, muss die personalverwaltende Stelle derartige Unterlagen mit zu vielen Gesundheitsdaten zurückweisen. In der Akte fanden sich weiterhin verschiedene Dokumente, deren Erforderlichkeit für die Aufgabenerfüllung nicht oder nicht auf den ersten Blick erkennbar war. Erschwerend kam hinzu, dass die Personalakte von einer anderen personalführenden Stelle des Landes übernommen worden war und man sich scheute, Unterlagen, die definitiv für die Aufgabenerfüllung der neuen personalführenden Stelle nicht (z. B. Unterlagen, die mit der Bewerbung eingereicht wurden, wie Exmatrikulationsbescheinigung oder Kündigungsschreiben an einen früheren privaten Arbeitgeber) oder nicht mehr (alter Personalbogen mit Angaben zu den Eltern) erforderlich waren, zu entfernen. Also hatte man lediglich, wie von der Personalaktenführungsrichtlinie vorgeschrieben, ein Trennblatt eingelegt und etwas ungeordnet aktuelle Unterlagen dahinter gehef-

tet. Jedenfalls war die Personalakte anhand der vom TLfDI gegebenen Hinweise nach Rückgabe durch das Gericht zu überarbeiten.

Wie es dazu kam, dass der Beschwerdeführer weitere geheime Dokumente vermutete, war schnell geklärt. Das Gericht hatte nämlich nicht nur die Personalakte, sondern auch andere Vorgänge mit Beschäftigtendaten des Betroffenen abgefordert. Diese Unterlagen wurden nicht geheim geführt, denn auch in diese Akten oder Vorgänge hat ein Betroffener nach § 84 Abs. 4 ThürBG grundsätzlich ein Einsichtsrecht. Es gab einen Vorgang, der Unterlagen mit Notizen und Bemerkungen der unmittelbaren Vorgesetzten über den Beschwerdeführer enthielt. Diese Unterlagen waren über den nächsthöheren Vorgesetzten der Personalverwaltung zugeleitet worden, weil sich der Beschwerdeführer nicht nur mit der Personalverwaltung, sondern auch mit seinen Vorgesetzten und Kollegen kontrovers auseinandersetzte. Die Vorgesetzten sahen daher die Erforderlichkeit, sich über das dienstliche Verhalten und die Leistung des Beschwerdeführers Notizen zu machen, um sich abzusichern und gegebenenfalls rechtfertigen zu können.

Hierzu hat der TLfDI ausgeführt, dass grundsätzlich keine datenschutzrechtlichen Bedenken bestehen, soweit Dienstvorgesetzte sich zum Zweck der Beurteilung Notizen anfertigen und verschiedene Vorgänge als Gedankenstütze aufbewahren, um diese in die Beurteilung einzubeziehen. Für andere Zwecke dürfen die Notizen jedoch nicht genutzt werden. Eine Abbildung der Leistung und des Verhaltens des betreffenden Bediensteten entbehrt nach Erstellung einer Beurteilung der weiteren Erforderlichkeit zur Aufbewahrung. Somit sind die zum Zweck der Erstellung einer Beurteilung angefertigten Unterlagen zu löschen. Von Dienstvorgesetzten dürfen auch keine Kopien von Unterlagen, die sich auch in der Personalakte befinden, abgeheftet werden, weil dies eine unzulässige Führung einer Personalnebenakte darstellen würde. Werden Vermerke für die Personalverwaltung zum Zweck anstehender Personalmaßnahmen oder wegen anhängiger Rechtsstreitigkeiten gefertigt, können in einer Handakte hiervon grundsätzlich Entwürfe für einen kurzen Zeitraum aufbewahrt werden. Es ist jedoch darauf zu achten, dass sich daraus beim Dienstvorgesetzten kein Personalvorgang entwickelt, der das gesamte dienstliche Verhalten des Betroffenen dokumentiert. Die Führung eines solchen Vorgangs wäre nicht erforderlich und damit unzulässig.

Dem nächsthöheren Dienstvorgesetzten dürfen Dokumente und Schreiben über Bedienstete nur dann zugeleitet werden, wenn hierzu eine gesonderte Aufgabenstellung besteht. Werden Schreiben lediglich zur Personalverwaltung weitergeleitet, besteht keine Erforderlichkeit, dass die nächsthöheren Dienstvorgesetzten diese ebenfalls in Kopie aufbewahren.

Der TLfDI hat die Personalaktenführung nach § 39 ThürDSG beanstandet und die Dienststelle aufgefordert, nach Rückgabe der Unterlagen durch das Gericht die Personalakte anhand der gegebenen Hinweise zu überarbeiten. Dies hat die Stelle zugesagt. Zu gegebener Zeit wird der TLfDI dies überprüfen.

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

6.19 Lehrerdaten für die Schuljahresanalyse

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

seine entsprechende Anfrage an die Schulleitung keine zufriedenstellende Antwort erhalten.

Der TLfDI fragte bei der für die Fachschule zuständigen Landesanstalt nach, welchem Zweck die Datenerhebung diene, welche Maßnahmen zum Schutz der personenbezogenen Daten der Lehrer gegen unbefugte Kenntnis getroffen worden waren und ob geprüft worden sei, ob eine anonymisierte Erhebung ausreiche. Gleichzeitig äußerte er erhebliche Bedenken insbesondere gegen die Angabe der Krankheitstage.

Die Landesanstalt teilte mit, die Schuljahresanalyse werde von der Schulaufsicht nach den §§ 2 und 3 Thüringer Schulaufsichtsgesetz (ThürSchulAG) abgefragt. Hintergrund sei, auf diese Weise den sonstigen Einsatz der Lehrkräfte im laufenden Schuljahr planen zu können. Da es um den Einsatz einzelner konkreter Lehrpersonen gehe, sei eine Erhebung in anonymisierter Form nicht zielführend. Die Daten würden von jedem Lehrer abgefragt, von der Schulleitung zusammengefasst und danach an die obere Schulaufsicht weitergeleitet. Unbefugte hätten so keine Chance, von den Daten Kenntnis zu nehmen. Auf die Abfrage von Krankheits- und Urlaubstagen durch die Schulaufsicht werde aber zukünftig verzichtet, da diese Daten ohnehin von der Fachschule als personalführende Stelle erfasst würden.

Nach der Darlegung waren die so genannten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten gegen unbefugte Kenntnis nach § 9 Thüringer Datenschutzgesetz (ThürDSG) getroffen. Nicht erklärbar war jedoch, dass dem TLfDI von einem Betroffenen die ausgefüllte Liste aller Lehrer zugeleitet worden war, der nach den Einlassungen der Schulaufsicht diese Liste nicht hätte haben dürfen. Eine Befugnis eines Fachlehrers, die personenbezogenen Daten anderer Fachlehrer zur Kenntnis zu nehmen, besteht nämlich nicht. Weiterhin erhielt der TLfDI den Hinweis, ein Verzeichnisse nach § 10 ThürDSG für eine entsprechende automatisierte Datei läge nicht vor. Dabei machte die vorliegende ausgefüllte Liste eindeutig den Eindruck, dass es sich um eine automatisierte Verarbeitung der personenbezogenen Daten der Fachlehrer handelte. Der TLfDI bat die Landesanstalt daher unter Einbeziehung des behördlichen Datenschutzbeauftragten (bDSB) zu prüfen, ob eine automatisierte Datei nach § 3 Abs. 2 und 7 ThürDSG vorliege, die gemäß § 34 Abs. 2 ThürDSG hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung (auch in Papierform) der vorher-

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

Der TLfDI wird die Angelegenheit selbstverständlich weiterhin begleiten.

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

6.20 Anmeldepflicht für Prostituierte?

Im Berichtszeitraum übersandte eine Nichtregierungsorganisation (NGO) dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um Stellungnahme den Referentenentwurf des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) für ein Gesetz zur Regulierung des Prostitutionsgewerbes sowie zum Schutz von in der Prostitution tätigen Personen.

Ziel dieses Entwurfes ist es, die Selbstbestimmung der in der Prostitution Tätigen zu schützen, ihre Arbeitsbedingungen zu verbessern und Menschenhandel zu bekämpfen. Dies soll unter anderem auch durch Meldepflichten der Betreiber von Bordellen und Prostituierten geschehen. Dabei werden auch besonders geschützte Daten im Sinne

von § 4 Abs. 5 Satz 1 Thüringer Datenschutzgesetz (ThürDSG), nämlich mit der Tatsache, dass jemand als Prostituierte oder als Prostituerter arbeitet, über das Sexualleben erhoben, verarbeitet und genutzt. Nach § 3 Abs. 1 des Entwurfs muss sich bei der zuständigen Behörde persönlich anmelden, wer eine Tätigkeit als Prostituierte oder als Prostituerter ausüben will. Damit liegt bei der jeweils zuständigen Behörde eine Liste der Personen vor, die in ihrem Bereich der Prostitution nachgehen. Der TLfDI stellte fest, dass mit dieser Tatsache oft auch eine Stigmatisierung der betroffenen Personen verbunden sein könnte und es daher nicht ausgeschlossen sei, dass sich viele betroffene Personen nicht anmelden würden, aus Angst, dass die Tatsache, dass sie der Prostitution nachgehen, bekannt wird. Zwar dürften die erhobenen Daten nach § 35 Abs. 4 Satz 1 des Gesetzesentwurfs nicht an nicht-öffentliche Stellen weitergegeben werden, allerdings besteht nach § 35 Abs. 5 des Entwurfs eine Übermittlungsbefugnis an öffentliche Stellen unter den dort genannten Voraussetzungen. Insbesondere die Möglichkeit der Übermittlung, soweit die Kenntnis der Daten zur Abwehr einer gegenwärtigen Gefahr für die öffentliche Sicherheit erforderlich ist, § 35 Abs. 5 Satz 1 Nr. 2, erscheint für den TLfDI sehr weitgehend. Nicht jede Gefahr für die öffentliche Sicherheit rechtfertigt die Übermittlung derart sensibler personenbezogener Daten.

Nach Artikel 8 der Richtlinie 95/46 EG (EG-Datenschutzrichtlinie) ist die Verarbeitung personenbezogener Daten über das Sexualleben grundsätzlich untersagt. Ausnahmen sind nach Artikel 8 Abs. 4 EG-Datenschutzrichtlinie aus Gründen eines wichtigen öffentlichen Interesses möglich. Ob ein derartiges wichtiges öffentliches Interesse die Meldepflicht von Prostituierten rechtfertigt, daran bestehen hier für den TLfDI erhebliche Zweifel. Über den Ausgang des Gesetzgebungsverfahrens wird der TLfDI im nächsten Tätigkeitsbericht informieren.

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



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

7 Polizei

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

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Februar 2014 Post vom Zentralrat Deutscher Sinti und Roma, der auf folgenden Sachverhalt aufmerksam machte:

Der Einheitsaktenplan des Freistaats Thüringen erfasse in der Rubrik „212 Unterbringung, Besondere Personengruppen, Gefährliche Tiere“ unter dem Aktenplanschlüssel „2124 Landfahrer“ auch die Minderheit der Sinti und Roma rechtswidrig. Dieser Aktenplanschlüssel stehe ferner zwischen den weiteren Aktenplanschlüsseln „2123 Obdachlose“ und „2125 Dirnen, Bordelle“ (Prostitution). Der Zentralrat Deutscher Sinti und Roma bat den TLfDI deshalb, diese Angelegenheit zu prüfen und für die Beseitigung bzw. Löschung der diskriminierenden Akten und Dateien Sorge zu tragen.

Der TLfDI wandte sich deshalb an das damalige Thüringer Innenministerium (TIM) und wollte wissen, auf welcher Rechtsgrundlage

eine Verarbeitung von personenbezogenen Daten welcher Personen/Angehöriger nationaler Minderheiten unter dem Aktenplanschlüssel „2124 Landfahrer“ erfolge und inwieweit dies erforderlich sei.

Das TIM veranlasste daraufhin eine Prüfung in seinem Haus und im „nachgeordneten Polizeibereich“. Diese ergab, so das TIM, dass unter dem Aktenplanschlüssel „2124 Landfahrer“ keine Akten erfasst worden seien, die eine rechtswidrige Sondererfassung von Sinti und Roma beinhaltet hätten. Ferner teilte das TIM dem TLfDI mit, dass der Begriff „Landfahrer“ aus dem Einheitsaktenplan des Freistaates Thüringen gelöscht würde und die Behörden, die mit diesem Aktenplan arbeiteten, entsprechend informiert würden.

Der TLfDI war mit dieser Nachricht aus dem TIM noch nicht ganz zufrieden: Nicht beantwortet war nämlich die Frage, ob es in der Vergangenheit zu einer rechtmäßigen Sondererfassung von Sinti und Roma, die auf einer konkreten Rechtsgrundlage erfolgte, gekommen war. Die entsprechende Nachfrage des TLfDI beim TIM ergab dazu Folgendes:

Das TIM habe – nach eigener Auskunft – unter dem Aktenplanschlüssel „2124 Landfahrer“ bisher lediglich zwei Akten geführt. Diese Akten hätten aber keinen inhaltlichen Bezug zu Sinti und Roma aufgewiesen, sodass sie nunmehr dem korrekten Aktenplanschlüssel „2121 Unterbringungsrecht“ zugewiesen worden seien. Ferner teilte das TIM dem TLfDI mit, dass die Löschung des besagten Aktenplanschlüssels „2124 Landfahrer“ am 25. März 2014 erfolgt sei und der geänderte Einheitsaktenplan im Intranet unter <http://www.thueringen.de/mam/th3/tim/aktenplan.pdf> abgerufen werden könne. Der TLfDI teilte dieses, nicht nur datenschutzrechtlich erfreuliche Ergebnis seiner Prüfung dem Zentralrat der Sinti und Roma mit.



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

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

7.2 Interessenkollisionen beim Polizeiarztlichen Dienst

Von der Landesärztekammer Thüringen erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) den Hinweis auf datenschutzrechtliche Probleme beim PÄD (= polizeiärztlicher Dienst) der Thüringer Polizei.

Die Polizeiarzte haben verschiedene Funktionen und Bereiche abzudecken. Zum einen ist dies die Sicherstellung der arbeitsmedizinischen Betreuung auf der Grundlage des Arbeitssicherheitsgesetzes (ASiG) in allen Behörden, Einrichtungen und Dienststellen der Thüringer Polizei. Weiterhin müssen Untersuchungen bezüglich Fragen der gesundheitlichen Eignung bei allgemeinen personalrechtlichen Entscheidungen durchgeführt werden. Darüber hinaus besteht die Aufgabe, die ärztliche Versorgung und medizinische Betreuung der heilfürsorgeberechtigten Polizeivollzugsbeamten nach den Heilfürsorgebestimmungen wahrzunehmen. Hinzu kommt die Sicherstellung der medizinischen Betreuung und der psychologischen Beratung und Betreuung im Rahmen von Einsätzen, Übungen und Ausbildungsmaßnahmen. Dabei unterscheiden sich die Aufgaben teilweise wesentlich in Zweckrichtung und Interessenssphäre.

Problematisch wird diese Aufgabenvielfalt dann, wenn mehrere dieser Bereiche von einem einzelnen Arzt wahrgenommen werden. Wird der Polizeiarzt im Rahmen der Heilfürsorge oder Arbeitsmedizin tätig, unterliegt er auch gegenüber dem Dienstherrn der ärztlichen Schweigepflicht. Für allgemeine beamtenrechtliche Entscheidungen dürfen diese Daten daher nur mit ausdrücklicher Einwilligung des Betroffenen weiterverarbeitet werden, es sei denn, es liegt eine gesetzliche Offenbarungsbefugnis oder Offenbarungspflicht vor. Muss derselbe Polizeiarzt aber auch Untersuchungen für personalrechtliche Entscheidungen durchführen, besteht die Gefahr einer Interessenskollision und einer möglichen bewussten oder unbewussten Beeinflussung von Personalentscheidungen durch die Kenntnis von heilfürsorge- bzw. arbeitsmedizinischen Daten.

Um dies zu vermeiden, bedarf es einer notwendigen räumlichen, organisatorischen und gegebenenfalls auch personellen Trennung für die Gewährleistung der Einhaltung der ärztlichen Schweigepflicht.

Insbesondere müssen die Bereiche der Heilfürsorge und der Betriebsmedizin von der amtsärztlichen Begutachtung getrennt sein.

Auf Anfrage zu diesen Interessenskonflikten hat das Thüringer Ministerium für Inneres und Kommunales (TMIK) zunächst mitgeteilt, bislang seien die mit betriebsärztlichen Aufgaben befassten Mediziner im polizeiärztlichen Dienst auch mit Amts- und anderen polizeiärztlichen Aufgaben betraut. Es sei beabsichtigt, künftig die Trennung von betriebs- und amtsärztlichen Aufgaben vorzusehen. Der bereits bestellte sowie ein noch zu bestellender Betriebsmediziner der Thüringer Polizei würden danach ausschließlich die Aufgaben nach § 3 des Gesetzes über Betriebsärzte, Sicherheit und andere Fachrichtungen für Arbeitssicherheit (ASiG) wahrnehmen.

Dies war aber noch keine umfassende Lösung zu dem dargestellten Interessenkonflikt. Auf Nachhaken hat das TMIK ergänzend erläutert, dass die für den polizeiärztlichen Dienst verbleibenden Bereiche der Behandlung von Anwärtern im Rahmen der Heilfürsorge und der Durchführung von Untersuchungen zur Unterstützung personalrechtlicher Entscheidungen aufgrund der vorhandenen Personalkapazitäten nicht strikt und vollständig getrennt werden könnten. Die Einstellung weiterer Ärzte sei aufgrund der haushaltsrechtlichen Vorgaben nicht zu realisieren. Die beiden Bereiche seien jedoch rechtlich, funktional und organisatorisch getrennt. Der Bereich der Heilfürsorge sei vor allem in Meiningen angesiedelt. Die beamtenrechtlichen Untersuchungen würden in der Regel durch den Leiter des polizeiärztlichen Dienstes durchgeführt, weil er grundsätzlich keine Behandlung im Rahmen der Heilfürsorge wahrnehme. Sollte ausnahmsweise ein Arzt, der einen Beamten bereits im Rahmen der Heilfürsorge betreut hat, mit der Durchführung der beamtenrechtlichen Untersuchung betraut werden, so behalte sich der Leiter des PÄD bei dem Verdacht dessen möglicher Beeinflussung aus der Zeit der Heilfürsorge die eigene Bearbeitung der Vorgänge jederzeit vor. Damit wurde das Problem bis auf wenige Einzelfälle gelöst.

Inzwischen hat der TLfDI allerdings erfahren, dass man als zweiten Betriebsmediziner nicht etwa einen zusätzlichen Arzt eingestellt, sondern einen bereits im polizeiärztlichen Dienst tätigen Arzt bestellt hatte. Auf diese Weise ergibt sich zwar eine Entspannung des betriebsmedizinischen Dienstes, die übrigen Aufgaben konzentrieren sich aber auf eine Person weniger. Ob damit den Festlegungen nachgekommen werden kann, wird vom TLfDI weiterhin überprüft.

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

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

Das ehemalige Thüringer Innenministerium (nunmehr Thüringer Ministerium für Inneres und Kommunales) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum, eine datenschutzrechtliche Einschätzung gemäß § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hinsichtlich der Vorlage von Personalakten im Rahmen des Untersuchungsausschusses (UA 5/1) des Thüringer Landtags „Rechtsterrorismus und Behördenhandeln“ abzugeben.

Nach einem dem UA 5/1 vorliegenden Beweisantrag sollten dem Ausschuss alle in einem bestimmten Zeitraum zur Personalakte genommenen Vorgänge, insbesondere Stellenbeschreibungen, Versetzungen, einschließlich Gesuche, Anordnungen, zeitweilige Sonderaufgaben, dienstliche Äußerungen, dienstliche Weisungen, Disziplinarmaßnahmen, Beurteilungen, Beförderungsempfehlungen und -anträge sowie Fehlzeiten von Bediensteten zweier Ermittlungsgruppen vorgelegt werden und es sollte schriftlich darüber Auskunft erteilt werden, welche der zuvor beschriebenen Akten, Aktenbestandteile und Dokumente sowie darin enthaltenen Daten seit 1995 vernichtet bzw. gelöscht und welche Akten, Aktenbestandteile und Dokumente im Original bzw. in Kopie an dritte Stellen abgegeben wurden.

Nach § 14 Abs. 1 Thüringer Untersuchungsausschussgesetz (UAG) ist unter anderem die Landesregierung verpflichtet, die vom Untersuchungsausschuss angeforderten Akten vorzulegen und Auskünfte zu geben.

Der TLfDI stellte, wie zuvor bereits schon am Anfang der Jahre 2012 und 2013 fest, dass nach § 14 Abs. 3 UAG die Verpflichtung zur Vorlage nicht besteht, wenn insbesondere nach § 14 Abs. 3 Nr. 3 UAG in Grundrechte eingegriffen würde. Die Berufung auf die Gründe in § 14 Abs. 3 Nr. 3 UAG ist jedoch ausgeschlossen, soweit der unantastbare Bereich privater Lebensgestaltung nicht betroffen

und der Grundsatz der Verhältnismäßigkeit beachtet ist (§ 14 Abs. 3 Satz 2, 2. Alt. UAG). Im Hinblick auf die in dem Beweisbeschluss angeforderten Personalakten musste der TLfDI grundsätzlich davon ausgehen, dass diese personenbezogene Daten enthielten.

Unter Berücksichtigung der Rechtsprechung, insbesondere des Beschlusses des Bundesverfassungsgerichts (Beschluss BVerfG 2 BvE 3/07, zitiert nach juris, Rz. 113) muss bei einem Ersuchen auf Aktenvorlage nicht bereits feststehen, dass die Unterlagen auch tatsächlich entscheidungserhebliches Material oder entsprechende Beweismittel enthalten. Es reicht bereits aus, wenn die Unterlagen Hinweise geben könnten.

Die Landesregierung legt – soweit sie Ausschlussgründe annimmt – dem Untersuchungsausschuss nach § 14 Abs. 4 UAG die Gründe einer Verweigerung in nicht-öffentlicher, gegebenenfalls vertraulicher Sitzung dar. Hält der Untersuchungsausschuss die Voraussetzungen der Verweigerung nicht für gegeben, kann er mit der Mehrheit seiner Mitglieder beschließen, den Verfassungsgerichtshof anrufen. Der Verfassungsgerichtshof entscheidet nach Maßgabe des Gesetzes über den Thüringer Verfassungsgerichtshof (ThürVerfGHG) darüber, ob die Verweigerung begründet ist; erklärt er die Verweigerung für unbegründet, darf sie nicht aufrechterhalten werden.

Im Falle einer Vorlageverweigerung des Thüringer Innenministeriums hinsichtlich der Personalunterlagen, die ersichtlich für die Aufgabenerfüllung des Untersuchungsausschusses nicht erforderlich sind, war für den konkreten Fall in der Abwägung der Grundsatz der Verhältnismäßigkeit einzubeziehen. So war hier nicht auszuschließen, dass beispielsweise personenbezogene Daten Dritter in den hier gegenständlichen Personalakten hätten enthalten sein können, die keinen Bezug zum Untersuchungsgegenstand hatten. Die Abwägung zwischen der verfassungsrechtlichen Stellung des Untersuchungsausschusses und dem Eingriff in das Grundrecht auf informationelle Selbstbestimmung eines in der Regel völlig unbeteiligten Dritten musste dabei nach der Auffassung des TLfDI grundsätzlich zugunsten des betroffenen Dritten ausfallen. Im Rahmen der Abwägung zwischen dem Aufklärungsinteresse des Untersuchungsausschusses und den berechtigten und grundrechtlichen geschützten Interessen der betroffenen Personen war jedoch beispielsweise auch die Möglichkeit einer partiellen Schwärzung von personenbezogenen Daten in Betracht zu ziehen.

Der Untersuchungsausschuss erhebt gemäß § 13 UAG die durch den Untersuchungsauftrag gebotenen Beweise aufgrund von Beweisbeschlüssen. In den Beweisbeschlüssen müssen die Tatsachen, über die Beweis erhoben werden soll, und die Beweismittel bezeichnet werden.

Die Landesregierung und die Behörden des Landes sowie die Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen, sind gemäß § 14 UAG verpflichtet, die von dem Untersuchungsausschuss angeforderten Akten vorzulegen und Auskünfte zu geben, Zutritt zu den von ihnen verwalteten öffentlichen Einrichtungen zu gewähren sowie die erforderlichen Aussagegenehmigungen zu erteilen. Die Verpflichtung besteht gemäß § 14 Abs. 3 UAG grundsätzlich nicht, wenn durch deren Erfüllung interne Beratungen und Entscheidungen offenbart würden, die zum unausforscharen Kernbereich der exekutiven Eigenverantwortung gehören, dem Wohle des Landes, des Bundes oder eines anderen deutschen Landes Nachteile bereitet würden oder in Grundrechte eingegriffen würde. Dies ist im Einzelfall zu prüfen.

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

Ein Beschwerdeführer wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und schilderte im Rahmen eines persönlichen Gespräches, dass eine dritte Person ihn auf seine vermeintlichen Vorstrafen ansprach. Verwundert über die Herkunft dieser Informationen, bat der Beschwerdeführer den TLfDI um Hilfe.

Der TLfDI wandte sich sogleich an die Landespolizeidirektion in Erfurt und bat zur Aufklärung dieses Sachverhaltes um eine Stellungnahme. Zur Prüfung des Sachverhaltes war es wichtig, zu wissen, ob die Polizei die personenbezogenen Daten zu dem Beschwerdeführer abfragte, wann dies geschah und auf welcher Rechtsgrundlage eine mögliche Datenabfrage erfolgte.

In ihrer Stellungnahme teilte die Landespolizeidirektion mit, dass aufgrund einer durch das Thüringer Landeskriminalamt durchgeführten Protokollrecherche ein Angehöriger der Thüringer Polizei tatsächlich im IT-System INPOL unberechtigt – also ohne dienstlichen Auftrag – eine Abfrage zu dem Namen des Beschwerdeführers getä-

tigt hatte. Welche konkreten Erkenntnisse der Angehörige der Thüringer Polizei im Rahmen dieser Abfrage erlangte, war jedoch nicht mehr nachvollziehbar, da die Aussonderungsprüffrist (Homepage TLfDI: Leitfaden über die Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut) für die personenbezogenen Daten des Beschwerdeführers bereits abgelaufen war. Damit waren sämtliche personenbezogene Daten des Beschwerdeführers im INPOL-System gelöscht.

Grundsätzlich ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift (beispielsweise das Polizeiaufgabengesetz oder die Strafprozessordnung) sie erlauben oder der Betroffene einwilligt. Da in diesem Sachverhalt für die Abfrage kein dienstlicher Auftrag zugrunde lag, erfolgte diese rechtsgrundlos und damit unberechtigt.

Diese datenschutzrechtliche Verletzung hat der TLfDI gemäß § 39 Abs.1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet. Ein Ermittlungsverfahren gegen den Angehörigen der Thüringer Polizei leitete die Landespolizeidirektion ein.

Der TLfDI wies die Landespolizeidirektion darauf hin, dass seitens der zuständigen Stellen darauf zu achten ist, dass entsprechende Abfragen nur im gesetzlich erforderlichen und tatsächlich benötigten Maß vorzunehmen sind. Zur Umsetzung dieser Maßnahmen teilte die Landespolizeidirektion mit, dass die Angehörigen der Thüringer Polizei halbjährlich darüber belehrt würden. Zudem sei die Dienstweisung zur Einhaltung datenschutzrechtlicher Bestimmungen in der Landespolizeidirektion bei der jährlichen Belehrung Gegenstand. Unabhängig davon sensibilisiere und belehre der behördliche Datenschutzbeauftragte die Mitarbeiter nochmals schriftlich hinsichtlich der Unzulässigkeit unbefugter Datenabfragen.

Der TLfDI begrüßt diese Maßnahmen und hofft auf eine strikte Einhaltung.

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

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

7.5 Rasterfahndungen in Thüringen – nicht ohne TLfDI

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

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

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

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

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

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

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er seine schutzwürdigen Belange bei der Verarbeitung und Nutzung seiner personenbezogenen Daten in einem gegen ihn geführten strafrechtlichen Ermittlungsverfahren beeinträchtigt sah.

Hintergrund war, dass die Polizei zu dem Betroffenen eine SARS-Abfrage durchgeführt hatte. Die Rechtmäßigkeit dieser Maßnahme zweifelte der Beschwerdeführer an.

Das SYBORG Auskunfts- und Recherche-System – kurz SARS – ist ein automatisiertes Verfahren, um zum Zweck der Gefahrenabwehr und im Zuge der Verfolgung von Straftaten Informationen über den Inhaber einer Rufnummer ermitteln zu können.

Rechtsgrundlagen für eine SARS-Abfrage sind die §§ 161, 163 Strafprozessordnung (StPO) – Ermittlungsgeneralklau-

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

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

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

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

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

7.7 Verwechslung beim Strafbefehl

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und informierte darüber, dass er einen Strafbefehl erhalten habe, in dem er einer Straftat beschuldigt wurde. Der Strafbefehl enthielt zudem die Angabe eines Geburtsdatums sowie eines Geburtsortes, welche jedoch nicht der Person des Beschwerdeführers zugeordnet werden konnten. Offensichtlich handelte es sich hier um eine Verwechslung. Der Beschwerdeführer legte gegen diesen Strafbefehl Einspruch ein.

Der TLfDI fragte beim zuständigen Gericht nach, wie es dazu kommen konnte, dass es den Strafbefehl nicht an den eigentlichen Beschuldigten, sondern an eine andere Person – den Beschwerdeführer – übermittelte, woher die Daten des Beschwerdeführers stammten und ob die personenbezogenen Daten des Beschwerdeführers zwischenzeitlich gelöscht wurden. Das zuständige Gericht konnte diese Fragen nicht abschließend beantworten und verwies den TLfDI an die Staatsanwaltschaft zur weiteren Sachverhaltsaufklärung.

Auf Nachfrage des TLfDI teilte die Staatsanwaltschaft mit, dass sie aus der Ermittlungsakte nicht mehr nachvollziehen konnte, wie die bis zum Abschluss des Ermittlungsverfahrens korrekt erfassten Daten geändert wurden. Nachdem die Staatsanwaltschaft den Fehler infolge des Einspruchs des Beschwerdeführers bemerkt hatte, nahm sie den Strafbefehl zurück. Dies teilte die Staatsanwaltschaft dem Beschwerdeführer auch mit. Gleichzeitig bot das zuständige Gericht dem Beschwerdeführer Hilfe bei der Beseitigung von Nachteilen an, die durch das fehlerhaft gegen ihn geführte Strafbefehlsverfahren möglicherweise entstanden waren.

Darüber hinaus konnte der TLfDI erreichen, dass die personenbezogenen Daten des Beschwerdeführers sowohl aus der Vorgangsbearbeitungsdatei des Gerichtes als auch in dem Datenverarbeitungssystem der Staatsanwaltschaft gelöscht wurden.

Da es sich bei diesem Fall um ein Versehen handelte und die zuständigen Stellen die personenbezogenen Daten des Beschwerdeführers gelöscht hatten, sah der TLfDI von einer Beanstandung ab.

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

7.8 Bei rechtmäßiger Wohnungsdurchsuchung kann auch der TLfDI nicht mehr helfen

Im Berichtszeitraum wandte sich eine Beschwerdeführerin an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um dessen Hilfe.

Sie teilte mit, dass eine Hausdurchsuchung bei ihr stattgefunden hätte und die Beamten dabei diverse Gegenstände (Computer, Handy) beschlagnahmt hätten. Sie sah sich in ihrem Grundrecht auf informationelle Selbstbestimmung verletzt.

Daraufhin fragte der TLfDI bei der zuständigen Staatsanwaltschaft nach, auf welcher Rechtsgrundlage die Durchsuchung und die Beschlagnahme bei der Beschwerdeführerin stattgefunden hätten. Zudem nahm der TLfDI Einsicht in die staatsanwaltschaftliche Ermittlungsakte. Darin befand sich ein richterlicher Durchsuchungs- und Beschlagnahmebeschluss. Liegt ein solcher richterlicher Durchsuchungs- und Beschlagnahmebeschluss vor, ist er für die Strafverfolgungsbehörden in seiner Umgrenzungsfunktion maßgeblich. Er konkretisiert die Durchsuchungs- und Beschlagnahmennormen der §§ 94, 98, 102, 105 Strafprozessordnung (StPO). Anhaltspunkte

dafür, dass die Polizeibeamten während der Durchführung der Durchsuchung außerhalb dieses Beschlusses handelten, ergaben sich aus der Ermittlungsakte nicht. Ein datenschutzrechtlicher Verstoß lag somit auch nicht vor.

Eine Überprüfung des richterlichen Beschlusses (d. h., ob dieser inhaltlich so hätte erlassen werden dürfen) war mangels Zuständigkeit des TLfDI nicht möglich. Nach § 2 Abs. 6 Thüringer Datenschutzgesetz gilt der Fünfte Abschnitt (u. a. die Kontrolle [§ 37], die Unterstützungspflicht [§ 38] und die Beanstandung [§ 39]) für Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Der richterliche Durchsuchungs- und Beschlagnahmebeschluss stellte indes keine Verwaltungsangelegenheit dar, sondern war im Rahmen der richterlichen Unabhängigkeit erlassen worden.

Für die Beschwerdeführerin bestand die Möglichkeit, Beschwerde gegen den Beschluss des Amtsgerichts einzulegen.

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

7.9 Datenabfrage oder keine Datenabfrage – das ist hier die Frage

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

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

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

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

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

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

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

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

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

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

Im vorliegenden Sachverhalt setzten die Verantwortlichen des BZ Meiningen die Betroffenen erst am Ende der Veranstaltung und nur aufgrund der ausdrücklichen Nachfrage eines Bediensteten, ob diese Veranstaltung aufgezeichnet werde, in Kenntnis über die Videoaufnahmen. Der vom BZ Meiningen vertretenen Ansicht, dass von einem Einverständnis der Betroffenen ausgegangen werden könnte, da nach dem Hinweis des Bediensteten die Betroffenen keine Einwände gegen die Aufzeichnungen erhoben hatten, konnte sich der TLfDI aus den oben genannten Gründen nicht anschließen.

Das Aufzeichnen der Dienstversammlung mittels zweier Videokameras ohne Rechtsgrundlage und ohne die Einwilligung der Betroffenen verstieß gegen § 4 Abs. 1, 2 und 3 ThürDSG. Der TLfDI beanstandete dies gemäß § 39 Abs. 1 ThürDSG.

Im Nachgang teilte das BZ Meiningen mit, dass es als erste Konsequenz aus der Beanstandung die Deckenkamera umgehend außer Betrieb gesetzt habe. Des Weiteren drehten die Verantwortlichen des BZ Meiningen das Objektiv der Kamera in Richtung Raumdecke, sodass eine Aufnahme der Bühne bzw. des Plenums nicht mehr erfolgen konnte. Sofern die Notwendigkeit einer Nutzung der Bild- und Tontechnik in Form von Aufzeichnungen von Veranstaltungen in diesem Hörsaal besteht, will das BZ Meiningen künftig im Vorfeld von allen Beteiligten eine entsprechende Einwilligungserklärung im Sinne des § 4 Abs. 2, 3 ThürDSG einholen. Zudem wird das BZ Meiningen eine geplante Aufzeichnung zukünftig ausdrücklich kommunizieren. Der TLfDI begrüßte diese Maßnahmen.

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

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

Ein Beschwerdeführer, der sich bereits im Jahr 2012 an den TLfDI gewandt und um die Prüfung der Zulässigkeit der Speicherung seiner Daten gebeten hatte (siehe hierzu 10. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Punkt 7.8) rief Anfang des Jahres 2015 erneut den TLfDI an und bat darum, die nach seiner Auffassung rechtswidrigen Einträge in den polizeilichen Datenbanken zu löschen.

Der TLfDI prüfte den Fall und musste dem Beschwerdeführer jedoch mitteilen, dass sich die Rechtslage hinsichtlich der Speicherung seiner Daten seit dem Jahr 2012 nicht geändert hatte. Das Prüfergebnis, das der TLfDI dem Beschwerdeführer Ende 2012 mitgeteilt hatte, hatte noch immer Bestand. Insofern konnte der TLfDI aus datenschutzrechtlicher Sicht keine Löschung seiner Daten fordern, da ihre Speicherung noch immer rechtmäßig war.

Gemäß § 40 Abs. 2 Satz 1 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (PAG) in Verbindung mit § 2 Abs. 1 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) beträgt die Prüffrist zur Löschung der Daten bei Erwachsenen und Jugendlichen fünf Jahre. Dabei beginnt diese Aussonderungsprüffrist gemäß § 40 Abs. 2 Satz 4 PAG i. V. m. § 5 ThürPolPrüffristVO grundsätzlich mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat. Sofern sich die laufenden Verfahren beim Beschwerdeführer erledigen und er nicht erneut polizeilich in Erscheinung tritt, werden die Daten des Beschwerdeführers aus dem Jahr 2012 mit Ablauf der Aussonderungsprüffrist im Jahr 2017 aus dem polizeilichen Informationssystem gelöscht.

Die Nachfrage an den Beschwerdeführer, ob gegebenenfalls neue Sachverhalte vorlägen, welche einen anderen Fristablauf zur Folge hätten, blieb ergebnislos. Der TLfDI sah damit den Fall als erledigt an.

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

Aus datenschutzrechtlicher Sicht ist diese Lösung unbefriedigend (siehe hierzu auch den 10. Tätigkeitsbericht des TLfDI unter Punkt 7.8).

Weitere Ausführungen finden sich im Leitfaden des TLfDI zu den Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut, der auf der Homepage des TLfDI (<https://www.tlfdi.de/tlfdi/>) unter dem Menüpunkt Themen / Orientierungshilfe abrufbar ist.



7.12 Mysteriöses Auftauchen personenbezogener Daten – War die Polizei involviert?

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie sich in ihrem Recht auf informationelle Selbstbestimmung verletzt sah.

Sie hegte den Verdacht, dass ein(e) Mitarbeiter(in) einer bestimmten Polizeidienststelle ihre derzeitige Wohnanschrift unerlaubt abgefragt und gegebenenfalls an eine dritte Person weitergegeben habe.

Daraufhin bat der TLfDI das Thüringer Landeskriminalamt um Mitteilung, ob jemand in der konkret benannten Polizeidienststelle in den durch die Meldebehörden zur Verfügung gestellten Daten eine Abfrage zu der Beschwerdeführerin getätigt habe. Das Thüringer Landeskriminalamt prüfte diese Protokolldatei auf Abfragen zu dem Namen der Beschwerdeführerin. Das Auswertungsergebnis ergab jedoch, dass kein Mitarbeiter der in Verdacht geratenen Polizeidienststelle eine solche Abfrage durchgeführt hatte. Eine nähere Zuordnung einer konkreten Abfrage zu der Beschwerdeführerin selbst war anhand der Protokolldatei nicht möglich. Da die Beschwerdeführerin gleichzeitig Strafanzeige erstattet hatte, liefen parallel auch die Ermittlungen der Staatsanwaltschaft. Ein Ermitt-

lungsverfahren wurde jedoch nach § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt, ein weiteres war bei Erstellung dieses Tätigkeitsberichtes noch nicht abgeschlossen.

Die Beschwerdeführerin wollte den Ausgang des zweiten Strafverfahrens abwarten und bat den TLfDI deshalb, in ihrem Fall vorerst nicht weiter tätig zu werden.

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

7.13 Abgefragt – Abfrage von Meldedaten durch die Polizei

Im Berichtszeitraum rief ein Beschwerdeführer den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an und berichtete, dass ein Angehöriger der Thüringer Polizei im Rahmen einer Zeugenvernehmung angegeben habe, die Wohnanschrift des Beschwerdeführers recherchiert zu haben.

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

Um den Sachverhalt jedoch abschließend datenschutzrechtlich zu würdigen, nahm der TLfDI zusätzlich Akteneinsicht bei der Staats-

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

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

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

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

Frage, ob die von Polizeibeamten eingenommenen Verwarngelder als Leistungskriterium bzw. als Leistungskontrolle für diese verwendet würden.

Der TLfDI wandte sich an das damalige Thüringer Innenministerium und bat um eine Stellungnahme zu den Fragen, ob dieses Vorgehen für eine Leistungskontrolle genutzt werde, aus welchem Grund und auf welcher Rechtsgrundlage die Namen der Polizeibeamten notiert würden und wer Zugriff auf diese Daten habe.

Das TIM antwortete unter Beteiligung der Landespolizeidirektion (LPD) und teilte Folgendes mit:

Aufgrund eines Erlasses des TIM vom 21. Februar 2008 über die Beschaffung und Verwaltung der Verwarnungsgeldblöcke sowie die Abrechnung der Verwarngelder würden im Rahmen der Dienst- und Fachaufsicht regelmäßige Kontrollen dieser Blöcke sowie der Abrechnung der Verwarngelder von den Vorgesetzten durchgeführt und nachgewiesen. Die Dienststellenleiter bzw. Leiter der Organisationseinheiten seien dabei verpflichtet, in regelmäßigen Abständen die Geldannahmestelle/Zahlstelle (GASt/ZSt) und deren Nachweisunterlagen zu kontrollieren.

Zu diesen Nachweisunterlagen der GASt/ZSt gehöre auch die Verwaltung und Abrechnung der Verwarnungsgeldblöcke, worüber ein Bestandsnachweis geführt werde. Hierbei führe die GASt/ZSt den Empfang, die Ausgabe, die Vereinnahmung und Weitergabe der Verwarnungsblöcke personenbezogen und listenmäßig auf.

Nach festgelegten Grundsätzen empfangen der Bedienstete gegen Unterschrift auf dieser Bestandsübersicht einen Block, arbeite mit diesem und rechne jeweils vierzehntägig (in Ausnahmen auch monatlich oder nach Erreichen einer bestimmten eingenommen Geldsumme) mit der zuständigen Zahlstelle gegen Quittierung ab. Der Betrag werde in der Anschreibliste für Einnahmen der GASt/ZSt erfasst. Sobald der Block vollständig verbraucht oder eine Abgabe aus anderen Gründen (z. B. Versetzung) erforderlich sei, sei bei der GASt/ZSt abzurechnen, bei der er empfangen wurde.

Zugriff auf diese Daten hätten, so das TIM, die jeweiligen Verwalter der Geldannahmestelle und deren Stellvertreter sowie der Dienststellenleiter und dessen Stellvertreter sowie durch den Dienststellenleiter bzw. die LPD mit der Prüfung beauftragte Beamte.

Das TIM betonte, es bestehe keine Weisungslage, weder seitens des TIM noch der LPD, wonach die eingenommenen Verwarngelder als Leistungskriterium verwendet werden dürften.

Dies wäre nach Ansicht des TLfDI auch unzulässig. Der TLfDI verwies hierzu auf den damals geltenden § 89 Abs. 4 Thüringer Beamtenengesetz (ThürBG), der für Polizisten als Beamte des Freistaates Thüringen gilt. Die Regelung des § 89 Abs. 4 ThürBG (alt) findet sich nach der Novellierung des ThürBG im August 2014 nunmehr in § 79 ThürBG wieder. Danach darf der Dienstherr nur dann personenbezogene Daten über Beamte erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

An diesen Vorgaben gemessen, hielt der TLfDI eine Leistungskontrolle anhand der Quantität der eingenommenen Verwarngelder nicht für erforderlich und damit für unzulässig.

Eine Beanstandung gemäß § 39 Abs. 1 ThürDSG war vom TLfDI im Ergebnis jedoch nicht auszusprechen, da er keine Indizien dafür erkennen konnte, dass die Polizei eingenommene Verwarngelder tatsächlich als Leistungskriterium verwendete.

Sachdienliche Hinweise nimmt der TLfDI aber gern entgegen.

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

7.15 DNA-Datei und Datenschutz

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

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

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

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

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

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

7.16 Zentrum für Überwachung

Auf dem Gebiet der polizeilichen Überwachung der Telekommunikation wollen die Länder Berlin, Brandenburg, Sachsen-Anhalt, der Freistaat Sachsen und der Freistaat Thüringen ein Gemeinsames Kompetenz- und Dienstleistungszentrum (GKDZ) errichten. Dessen Wirkbetrieb soll ab dem Jahr 2018 aufgenommen werden. Das GKDZ soll als Anstalt des öffentlichen Rechts auf der Grundlage eines Staatsvertrags errichtet werden. Da in dem GKDZ höchstwahrscheinlich viele sensible personenbezogene Daten aus fünf Bundesländern verarbeitet werden sollen, sind hohe Anforderungen an den Datenschutz und die Datensicherheit zu stellen.

Da aber neben einem Staatsvertragsentwurf weitere konkrete Konzepte für die tatsächliche Ausgestaltung des GKDZ dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bisher nicht vorliegen bzw. überhaupt noch nicht erstellt wurden, kann der TLfDI eine weitergehende datenschutzrechtliche Beurteilung des GKDZ derzeit noch nicht vornehmen.

Zu dem Entwurf des Staatsvertrages zwischen den teilnehmenden Ländern nahm der TLfDI Stellung und wies unter anderem darauf hin, dass der Aufgabenumfang des GKDZ im Staatsvertrag konkret festzulegen sei, dass die jeweiligen Polizeibehörden in dem GKDZ nur auf ihre eigene Datensätze Zugriff haben dürften und dass die bei einer Telekommunikationsüberwachung erhobenen Daten nach dem jeweiligen Stand der Technik entsprechend zu verarbeiten seien. Der TLfDI wies – gerade im Lichte des ergangenen Urteils des EuGH vom 6. Oktober 2015 C-262/14 (Safe Harbor) – nochmals darauf hin,

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

Der TLfDI wird das Projekt datenschutzrechtlich intensiv betreuen.

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

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

Im Berichtszeitraum testeten mehrere Bundesländer in Pilotprojekten den Einsatz von „Body-Cams“ bei der Polizei. Eine „Body-Cam“ ist eine kleine Videokamera, die der Polizei dazu dienen soll, im Rahmen ihrer Einsätze das Einsatzgeschehen direkt aufzeichnen und somit später auswerten zu können.

Zum möglichen Einsatz von „Body-Cams“ in Thüringen stellte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beim damaligen Thüringer Innenministerium (TIM) die Anfrage, ob ein solches Pilotprojekt auch in Thüringen Anwendung finde. In seiner kurzen Antwort teilte das TIM dem TLfDI mit, dass derzeit weder „Body-Cams“ im Einsatz noch zukünftig geplant seien.

Parallel dazu diskutierten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von „Body-Cams“. Im Ergebnis sind die Datenschützer grundsätzlich der Auffassung, dass für den Einsatz von „Body-Cams“ eine Rechtsgrundlage erforderlich sei. In dieser sollten die Voraussetzungen für den Einsatz und auch für die weitere Verarbeitung (z. B. die Auswertung und Löschung der Daten) geregelt werden.

Der TLfDI hat Verständnis für die Argumente aus den Reihen der Polizeigewerkschaften, dass „Body-Cams“ auch bei Thüringer Polizei zum Einsatz kommen sollen. Ein Einsatz solcher „Body-Cams“ zum Schutz der Polizeibeamten bei Personen- oder Fahrzeugkontrollen an öffentlich zugänglichen Orten ist bereits jetzt nach § 33 Abs. 6 Satz 1 Polizeiaufgabengesetz (PAG) möglich.

Sofern der Einsatz der „Body-Cams“ über den Eigensicherungszweck der Polizisten hinausginge, wäre der Zweck der Aufzeichnung hinreichend klar im PAG zu regeln. Dabei wären in jedem Fall auch beschäftigendatenschutzrechtliche Fragen zu erörtern und zu klären.

7.18 Polizist verkauft Privat-PC mit Dienst-Daten

Wer heutzutage einen gebrauchten Personal Computer (PC) in einem Elektrofachgeschäft kauft, sollte nicht nur mit äußerlichen „Gebrauchsspuren“ des PCs rechnen. Er kann leider auch nicht selten auch noch einige personenbezogene Daten vom Vorbesitzer des PCs finden. So erging es auch einem Inhaber eines Mediaunternehmens. Dieser hatte sich bei einem Elektrofachgeschäft einen gebrauchten PC gekauft. Erstaunlich war nicht nur der günstige Preis. Auch die Daten, die auf dem PC zu finden waren, überraschten ihn so sehr, dass er seinen „Fund“ dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) meldete. Auf dem PC befanden sich tatsächlich über 1.000 Dateien, die einen polizeirelevanten Hintergrund hatten.

Daraufhin hakte der TLfDI bei der Landespolizeidirektion (LPD) nach, welche Regelungen dort für den Umgang mit dienstlichen Dateien auf privaten PCs gälten. Die LPD teilte daraufhin mit, dass es sich bei dem Vorbesitzer des PCs um einen Polizeibeamten einer Polizeiinspektion handelte, der sich jedoch schon seit einigen Jahren im Ruhestand befände. Es gäbe bei der Polizei keine dienstliche Regelung, die erlaube, dass das Speichern von dienstlichen Dateien auf privaten PCs zulässig sei; auch die Möglichkeit der Telearbeit bestünde nicht. Vielmehr verwies die LPD auf die Dienstanweisung Nr. 1/2008 für den Umgang mit IT-Systemen, nach der es jedem Anwender und Polizisten untersagt ist, dienstliche Software bzw. dienstliche Dateien auf privater Hardware zu nutzen. Bei der Versetzung eines Polizeibeamten in den Ruhestand erfolge ferner eine Belehrung, unter anderem zur Treue- und Verschwiegenheitspflicht, zur Herausgabe amtlicher Unterlagen sowie zu den Folgen der

Nichterfüllung (z. B. disziplinarrechtliche Ahndung, vermögensrechtliche Haftung).

Das dafür verwendete Formblatt „Erklärung bei Versetzung in den Ruhestand“ hielt einer datenschutzrechtlichen Prüfung durch den TLfDI nicht stand: Er monierte die veralteten Rechtsnormen, auf die in dem Formblatt verwiesen wurde und regte an, dass Beamte bei Ausscheiden aus dem Polizeidienst künftig auch erklären müssten, nicht im Besitz von Dateien über dienstliche Vorgänge zu sein.

Der TLfDI informierte daraufhin das damalige Thüringer Innenministerium (TIM) als übergeordnete Stelle über diesen Vorfall. Er bat darum, dass nochmals alle Polizeibeamten über den Umgang von dienstlichen Daten belehrt würden und regte die Prüfung der Einleitung disziplinarischer Maßnahmen an.

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

7.19 Fallbearbeitungssystem der Polizei – auch hier gilt Datensparsamkeit

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

nisch recherchierbar vorgehalten werden, bis das Hauptverfahren abgeschlossen ist.

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

Vorgänge, die seit einem Jahr nicht mehr bearbeitet werden, sind aus Sicht des TLfDI (bestenfalls automatisch) auf inaktiv zu setzen. Ist ein Vorgang auf inaktiv gesetzt worden, sollte eine weitere Bearbei-

tung nicht mehr möglich sein und die verantwortliche Stelle hat die Erforderlichkeit einer weiteren Speicherung zu überprüfen.

Schließlich ist auch die gesetzliche Auskunftspflicht gemäß § 47 Polizeiaufgabengesetz (PAG) zu beachten, wonach der Betroffene auch Auskunft zu den in diesem System gespeicherten Daten zu seiner Person erhält.

Der TLfDI wird im Rahmen einer Nachkontrolle das Fallbearbeitungssystem auf seine Vereinbarkeit mit dem Datenschutzrecht überprüfen. Darüber wird der TLfDI im kommenden Tätigkeitsbericht informieren.

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

7.20 Beglaubigte Personalausweiskopien – zukünftig nicht mehr nötig

Nach § 47 Abs. 1 Satz 1 Polizeiaufgabengesetz (PAG) erteilt die Polizei dem Betroffenen auf Antrag grundsätzlich über die zu seiner Person gespeicherten Daten Auskunft.

Im Rahmen der Antragsstellung verlangte die Thüringer Polizei bisher immer eine beglaubigte Personalausweiskopie des Betroffenen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sah im Gegensatz dazu die Anforderung einer einfachen Ausweiskopie als ausreichend an. Unberührt hiervon bleibt die persönliche Identifizierung des Antragstellers auf der Polizeidienststelle. Die Anforderung einer beglaubigten Ausweiskopie ist für die Erreichung des Zwecks der Vermeidung einer Auskunftserteilung an einen unberechtigten Dritten ungeeignet. Eine beglaubigte Kopie bzgl. des Identitätsnachweises besitzt gegenüber einer einfachen Kopie keinen Mehrwert, da sie letztlich nur bestätigt, dass die Kopie mit dem Original übereinstimmt. Eine beglaubigte Personalausweiskopie an sich stellt somit nicht sicher, dass tatsächlich keine unberechtigte Person Kenntnis vom Inhalt des Aus-

kunftsersuchens erlangt. Diese Gefahr einer falschen Versendung könnte unter Umständen lediglich mithilfe eines Einschreibens (mit Rückschein) minimiert werden.

Dem Auskunftersuchen des Bürgers mit der Forderung nach einer beglaubigten Ausweiskopie werden nach Ansicht des TLfDI zu hohe Hürden auferlegt, die den Antrag, eine Auskunftserteilung von der Polizei als öffentliche Stelle zu erhalten, deutlich erschweren.

Vom TLfDI dazu um Stellungnahme gebeten, teilte das Thüringer Ministerium für Inneres und Kommunales (TMIK) mit, dass es erwäge, dieser Auffassung des TLfDI zu folgen, sodass eine beglaubigte Ausweiskopie für die Antragstellung grundsätzlich nicht mehr erforderlich wäre. Eine solche beglaubigte Kopie könnte dann nur noch in Ausnahmefällen von der Polizei gefordert werden, z. B. wenn ein Manipulationsverdacht an der Kopie bestünde.

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

7.21 Polizeiliche Erfassung von Ausweisdaten per Smartphone-Foto?

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

Da es sich bei den Polizeibeamten um Bedienstete der Bundespolizei gehandelt haben soll und für diese Bundesbehörde die Bundesbeauf-

trage für den Datenschutz und die Informationsfreiheit (BfDI) sachlich zuständig ist, gab der TLfDI die weitere datenschutzrechtliche Prüfung an die BfDI ab.

Gleichzeitig nahm der TLfDI diese Bürgeranfrage aber zum Anlass, zu ermitteln, ob die Thüringer Polizei Smartphones zur bildlichen Erfassung von Ausweisdokumenten heranzieht.

Die Rückmeldung der Thüringer Landespolizeidirektion ergab zunächst, dass die Nutzung privater Mobiltelefone bei ihren Bediensteten im Dienst untersagt sei.

Im Hinblick auf die dienstlich bereitgestellten Mobiltelefone sei eine Sperrung von Einzelfunktionen –wie beispielsweise die Kamerafunktion – nicht möglich. Deswegen sei die Möglichkeit, mit dienstlich zur Verfügung gestellten Geräten Ausweisdokumente bildlich zu erfassen, theoretisch nicht ausgeschlossen.

Aus Sicht der Landespolizeidirektion sei das Fotografieren von Ausweisdaten zur polizeilichen Aufgabenerfüllung jedoch weder erforderlich noch verhältnismäßig.

Die der Landespolizeidirektion nachgeordneten Behörden seien angewiesen, deren Bedienstete in dieser Frage hinreichend zu sensibilisieren und die Benutzung von Mobiltelefonen für das Fotografieren von Ausweisdaten zu untersagen.

Im Rahmen der Identitätsfeststellung sei es im Aufgabenkreis der Thüringer Polizei unzulässig, dass Polizeibeamte Ausweisdokumente von Bürgern bildlich erfassen.

Es genügt, wenn der Betroffene dem Polizeibeamten zur Feststellung der Identität seine Ausweispapiere zur Prüfung aushändigt (§ 14 Abs. 2 Satz 2 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei). Das Erheben und das Verwenden personenbezogener Daten aus einem Personalausweis ist mit dem aktuellen Personalausweisgesetz (PAuswG) abschließend gesetzlich geregelt (§§ 14 ff. PAuswG). Bei einer Identifizierung anwesender Personen aus polizeierkennungsdienstlichen Gründen ist eine Kopie nicht erforderlich und damit unzulässig. Einige Gesetze und Verordnungen hingegen sehen eine ausdrückliche Ermächtigung zum Kopieren des Ausweises vor. Für Banken gilt beispielsweise § 8 Abs. 1 Satz 3 Geldwäschegesetz, und für Telekommunikationsanbieter (z. B. beim Handvertrag) § 95 Abs. 4 Satz 2 TKG.

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

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

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

7.22 Kennzeichenerfassung auf Hotelparkplatz

Ein Hotelbetreiber wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass auf seinem Hotelparkplatz in regelmäßigen Abständen von der Polizei die Kennzeichen der parkenden Autos aufgenommen würden. Da ihm mündlich keine Auskunft zum Zweck der Datenerhebung gegeben worden sei, bat er beim TLfDI um Klärung dieses für ihn seltsam anmutenden Sachverhalts.

Der TLfDI fragte dazu bei der zuständigen Landespolizeiinspektion (LPI) an, auf welcher Rechtsgrundlage und zu welchem Zweck die Datenerhebung stattgefunden habe. Ausführlich nahm die Landespolizeiinspektion Stellung in dieser Angelegenheit und teilte dem TLfDI mit, das besagte Hotel sei bei der Polizei dafür bekannt, dass dort seit Jahren rechtsextremistische Veranstaltungen stattfänden und es wiederholt zur Verübung von Straftaten gekommen sei. Die Datenerhebung in Form der Erfassung von Kfz-Kennzeichen stütze die LPI auf § 33 Abs. 1 und 3 Polizeiaufgabengesetz (PAG): Danach kann die Polizei personenbezogene Daten auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder Aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Gem. § 33 Abs. 3 Satz 1 PAG darf die Datenerhebung auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

Nachfragenswert war für den TLfDI jedoch, ob und wie die LPI im Rahmen ihrer Verhältnismäßigkeitsprüfung zur polizeilichen Datenerhebung berücksichtigte, dass nicht sämtliche auf dem Parkplatz befindlichen Fahrzeuge rein vorsorglich überprüft werden mussten, da der Parkplatz auch von anderen Hotelgästen genutzt wird/wurde, von denen eine Gefahr für die öffentliche Sicherheit und Ordnung grundsätzlich nicht angenommen werden kann bzw. konnte.

Die LPI wies nachfolgend darauf hin, dass sie im Rahmen der Prüfung der Angemessenheit die Interessen der polizeilichen Aufgabenerfüllung (Präventivwirkung im Hinblick auf politisch motivierte Straftaten) und das Recht auf informationelle Selbstbestimmung Unbeteiligter (Kennzeichen- bzw. Halterprüfung auf rechtsextremistischen Bezug) abgewogen habe. Dabei sei die LPI zu dem Ergebnis gelangt, dass im Zusammenhang mit der Datenerhebung von Kfz-Kennzeichen der Eingriff in das Recht auf informationelle Selbstbestimmung Unbeteiligter geringer zu bewerten sei, gerade weil ein milderes Mittel als die Datenerhebung in Form der Kennzeichenerfassung vorliegend nicht erkennbar war.

Gegen diese rechtliche Begründung hatte der TLfDI keine Einwände.

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

7.23 Polizei vs. Polizei – Verfahren bei Dienstaufsichtsbeschwerden

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

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

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

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

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

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

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

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

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



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

8 Verfassungsschutz

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

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

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

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

8.2 Kontrolle der Antiterrordatei

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

vollständig zu protokollieren sind (BVerfG Urteil vom 24. April 2013 -1 BvR 1215/07-, Rn. 214f. siehe juris). Dabei muss nach der Aussage des Bundesverfassungsgerichts „durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält“ (BVerfG a.a.O., Rn. 215).

Die Kontrollen der ATD beim Thüringer Landeskriminalamt (TLKA) ergaben bisher keine datenschutzrechtlichen Verstöße, zumal der Datei dort in der Praxis eine eher geringe Bedeutung beigemessen wird. So gab es zum Beispiel keine Suchanfragen in der ATD, die das TLKA im Kontrollzeitraum vorgenommen hätte. In Umsetzung des Urteils des Bundesverfassungsgerichts vom 24. April 2013 wurden auch alle Kontaktpersonen aus der ATD gelöscht. Weitere Nachfragen zu einzelnen Objektkategorien konnten vom TLKA beantwortete werden.

Auch beim Amt für Verfassungsschutz kontrollierte der TLfDI im Berichtszeitraum den Einsatz der ATD und die Protokollierung getätigter Abfragen. Hinweise auf eine rechtswidrige Datenerhebung oder -verarbeitung stellte der TLfDI dabei nicht fest.

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



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

9 Finanzwesen

9.1 Auf Bewährtes vertrauen – keine Geburtsdaten in Kontendaten nutzen

Der Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder diskutierte im Berichtszeitraum Überlegungen eines Finanzministeriums eines anderen Bundeslandes, künftig Zahlungen und Forderungen nicht mehr anhand des Kassenzeichens zu führen, sondern den Betroffenen anhand der Geburtsdaten zuzuordnen, also letztendlich Personenkonten zu führen. Nur so könne eine eindeutige Zuordnung der Personen gewährleistet werden, von denen keine gültigen Adressen vorliegen würden, weil z. B. jemand mehrmals umgezogen sei.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ist der Auffassung, dass das Erheben der Geburtsdaten zu o. g. Zwecken datenschutzrechtlich nicht zulässig ist, da Daten gespeichert werden, die nur in ganz bestimmten Fällen erforderlich sein können, um bei der Forderungseintreibung Personenverwechslungen zu vermeiden.

Der TLfDI bat daraufhin das Thüringer Finanzministerium (TFM) mitzuteilen, wie die Thüringer Finanzverwaltung derzeit Zahlungen und Forderungen den betroffenen Personen zuordnet und ob eine Umstellung zu Personenkonten erfolgen solle.

Das TFM teilte dem TLfDI mit, dass im Mittelbewirtschaftungsverfahren „HAMASYS“ (=Haushaltsmanagementsystem) die Zuordnung der Zahlungen und Forderungen über das jeweilige Kassenzeichen erfolge. Die Speicherung der Geburtsdaten sei mit Eingabe der Grunddaten nicht vorgesehen. Hier würden lediglich die Adressdaten und die Bankverbindung erfasst.

Die Finanzkassen der Finanzämter ordneten Steuerzahlungen anhand des angegebenen Verwendungszwecks der Überweisung zu. Hier sei das Zuordnungskriterium die Steuernummer, nicht jedoch das Kassenzeichen. Eine maschinelle Zuordnung von Zahlungen zugunsten des Steuerkontos sei nur möglich, wenn Zahlungen zugunsten bestimmter Bankverbindungen geleistet würden und der Steuerpflichtige den korrekten Verwendungszweck, die Kundenreferenznummer, die auf dem Zahlschein enthalten ist, die Steuernummer und ggf. weitere Kriterien angebe. Könne eine maschinelle Zuordnung nicht erfolgen, sei die Einzahlung personell durch den Buchhalter anzuweisen.

Abschließend teilte das TFM mit, dass es nicht vorhabe, das bisherige Zuordnungsverfahren zu ändern.

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

9.2 Neugier auf Kontodaten von Kollegen

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Berichtszeitraum eine Neuregelung zum Zugriff auf Mitarbeiterkontendaten innerhalb einer Sparkasse zu bewerten.

Danach war beabsichtigt, den Mitarbeitern das Recht zu geben, auf Antrag und unter Hinzuziehung des internen Datenschutzbeauftrag-

ten und eines Personalratsmitglieds prüfen zu lassen, ob intern ggf. unberechtigt auf die Kontodaten von Kollegen zugegriffen wurde. Sofern ein unberechtigter Zugriff festgestellt würde, sollte der betroffene Mitarbeiter jedoch nicht den Namen des Kollegen, der zugegriffen hat, erfahren.

Hierzu teilte der TLfDI mit, dass die Mitarbeiter einer Sparkasse ausschließlich im Rahmen ihrer dienstlichen Tätigkeit auf die Kontodaten der Kunden zugreifen dürfen. Eine darüber hinausgehende Nutzung der EDV-Systeme ist nicht erlaubt. Sämtliche Zugriffe auf Kundendaten werden 180 Tage protokolliert. Diese Regelung gilt auch für die Konten eigener Mitarbeiter, d. h. „ein Blick auf das Konto des Kollegen“ ist nur aus dienstlichen Gründen erlaubt.

Der TLfDI sah die Neuregelung zur Kontrolle unberechtigter Zugriffe grundsätzlich als zulässig an. Eine andere Bewertung ergibt sich aus der Sicht des TLfDI dann, wenn grundsätzlich vorgesehen ist, den Namen des Kollegen, der unberechtigt auf ein Konto zugegriffen hat, dem Betroffenen zu offenbaren. Jedoch sind ausnahmsweise Fallkonstellationen denkbar, in denen dem betroffenen Kontoinhaber mitgeteilt werden kann, wer unberechtigt auf sein Konto zugegriffen hat. Hat der Kontoinhaber beispielsweise einen Schaden erlitten, muss er auch die Möglichkeit haben, gegen den Verursacher vorgehen zu können.

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

9.3 Wenn der Bankautomat spricht

Eine Anfrage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) thematisierte Datenschutzaspekte bei der Einführung behindertenspezifischer Identifizierungsmethoden für barrierefreie Bankautomaten.

Im Rahmen der Erarbeitung eines deutschlandweiten Branchenstandards für barrierefreie Bankautomaten sollten unter Mitwirkung des Bundeskompetenzzentrums Barrierefreiheit, der Behindertenverbän-

de und der Deutschen Kreditwirtschaft zusätzliche Identifizierungsmethoden entwickelt werden, die behindertenspezifische Gegebenheiten berücksichtigen. Konkret war beabsichtigt, z. B. auf EC-, VISA- oder Mastercard-Karten personenbezogene Daten zu Menschen mit Behinderungen aufzunehmen. Aufgrund dieser Daten sollten dann am künftigen barrierefreien Bankautomaten bestimmte Voreinstellungen aktiviert werden. Konkret handelte es sich dabei z. B. um Kennzeichen für Blinde und Menschen ohne Hand (Ohnhänder). Sind diese Kennzeichen aktiviert und werden vom Kartenleser erkannt, muss eine Sprachausgabe gewährleistet sein bzw. durch spezifische Technikgestaltung die Entnahme des Geldes aus dem Ausgabeschacht auch für Ohnhänder problemlos möglich sein. Der TLfDI regte in diesem Zusammenhang an, eine Liste mit solchen spezifischen Daten, die auf der Karte hinterlegt werden können, zu erstellen. Vor der erstmaligen Nutzung sollte der Betroffene jedoch die Möglichkeit erhalten, eine oder mehrere dieser (Listen-) Daten nach einer individuellen Beantragung von der Bank freischalten zu lassen.

Da die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 BDSG), sollte die Beantragung solcher Kennzeichen mit einer datenschutzrechtlichen Einwilligung im Sinne von § 4a BDSG verbunden sein. Nach § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 4a Abs. 3 BDSG. Personenbezogene Daten nach § 3 Abs. 9 BDSG sind auch Angaben über die Gesundheit des Betroffenen, im konkreten Fall also auch die Daten zu Behinderungen.

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

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

9.4 Videoüberwachung in Sparkassen –kein Videogaga

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte im Berichtszeitraum aufgrund einer Beschwerde die Videoüberwachung einer Zweigstelle der Sparkasse Mittelthüringen. Konkret war zu klären, wie lange die Bildaufnahmen der Überwachungskamera in den Geldautomaten aufbewahrt werden dürfen und ob die Videoüberwachung des Servicepoints zulässig war.

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

darauf zugreifen durfte. Schriftliche Regelungen zum Umgang mit den Videoaufnahmen lagen nicht vor.

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

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

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

9.5 Datenschutz im Falle einer Gesamtrechtsnachfolge

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Bekanntgabe seiner steuerlichen Daten aus einem Einkommenssteuerbescheid an die Miterben seines verstorbenen Ehepartners. Konkret hatte das Finanzamt den Antrag des Beschwerdeführers, seine Einkünfte auf dem gemeinsamen Einkommenssteuerbescheid der Ehepartner für Zwecke der Bekanntgabe an Miterben seines Ehepartners unkenntlich zu machen, abgelehnt. Durch die Schwärzung wollte der Beschwerdeführer die Weitergabe seiner Einkünfte an die Miterben verhindern.

Das Finanzamt teilte dem TLfDI zu der Beschwerde mit, dass der Beschwerdeführer und die übrigen Erben des Verstorbenen für die Leistungen aus dem Steuerschuldverhältnis Gesamtschuldner nach § 44 Abgabenordnung (AO) seien. In den Fällen einer Erbfolge nach § 1922 Abs. 1 Bürgerliches Gesetzbuch (BGB) liege eine Gesamtrechtsnachfolge im Sinne von § 45 AO vor. Forderungen und Schulden gingen kraft Gesetzes auf die Rechtsnachfolger über. Es sei grundsätzlich ein zusammengefasster Bescheid zu erlassen, der an die Gesamtrechtsnachfolger als Gesamtschuldner zu richten und jedem von ihnen bekannt zu geben sei (Pkt. 2.12.3 Anwendungserlass zur AO zu § 122 AO). Es bestehe aber die Möglichkeit, einen Verwaltungsakt an einen Beteiligten mit Wirkung für die anderen Beteiligten bekanntzugeben, soweit alle Beteiligten damit einverstanden seien; die Beteiligten könnten aber auch nachträglich eine Abschrift des Verwaltungsakts verlangen (§ 122 Abs. 6 AO). Eine solche Einverständniserklärung aller Beteiligten lag dem Finanzamt jedoch nicht vor. Somit sei nach der Festsetzung der Einkommens-

teuer der Einkommensteuerbescheid den einzelnen Beteiligten bekannt zu geben (§ 122 AO).

Im Ergebnis stellte der TLfDI fest, dass in diesem Falle die einschlägigen Vorschriften des Steuerrechts eingehalten wurden und kein datenschutzrechtlicher Verstoß vorlag. Eine Bekanntgabe des Steuerbescheides ist dafür erforderlich, dass alle Beteiligten die Zusammensetzung bzw. das Zustandekommen des resultierenden Steuerbetrags nachvollziehen und damit ihre Rechte im Steuerverfahren wahren können.

Die Komplexität datenschutzrechtlicher Sachverhalte zeigt sich insbesondere dann, wenn spezialgesetzliche Vorschriften, in diesem Falle steuerrechtliche Normen, beurteilungsrelevant sind.

In obiger Beschwerdeangelegenheit überwog das Informationsinteresse der Gesamtschuldner zur Wahrung ihrer Rechte aus dem Erbfall das Recht eines Miterben an der Geheimhaltung seines steuerrelevanten Einkommens.

9.6 Besondere Leistungskontrolle in der Thüringer Landesfinanzdirektion

Mehrere Betroffene wiesen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darauf hin, dass in der Thüringer Landesfinanzdirektion (LFD) für einzelne Beamte und Arbeitnehmer die tatsächliche Zahl der Erledigungen erhoben und Zielvorgaben gegenübergestellt und in Listen für den einzelnen Beschäftigten zusammengefasst würden. In einer Dienstversammlung sei sinngemäß verkündet worden, dass „konkrete Maßnahmen zur Sicherstellung des politischen Abarbeitungsziels anlaufen werden“. In den erwähnten Listen sollten von dem jeweiligen Beschäftigten die erledigten Fälle ab dem 1. Februar 2014 alle 14 Tage selbstständig eingetragen werden. Konkrete Bestimmungen, vor allem dazu, wie mit den Listen weiter verfahren werde und zu welchem konkreten Zweck sie genutzt würden, lägen nicht vor. Die Betroffenen befürchteten eine vollständige Leistungs- und Verhaltenskontrolle.

Auf Nachfrage des TLfDI erläuterte die LFD, der Sachverhalt betreffe zwei zum Jahresbeginn 2012 eingegliederte Referate mit derzeit noch etwa 100 Beschäftigten. Bis 2016 sei ein Stellenabbau wegen Erledigung und damit künftigen Wegfalls der Aufgaben auf

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

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

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

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

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

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

Im Januar 2014 legte das Thüringer Finanzministerium (TFM) dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) den Entwurf eines Dritten Gesetzes zur Änderung des Thüringer Gesetzes zur Regelung des Kirchensteuerwesens zur Stellungnahme vor.

Nach datenschutzrechtlicher Prüfung des Gesetzentwurfs teilte der TLfDI dem TFM mit, dass aufgrund der Übereinstimmung der Neuregelung des § 8a Abs. 4 Thüringer Kirchensteuergesetz (Thür-KiStG) mit den entsprechenden bundesgesetzlichen Regelungen in § 51a Abs. 2c Einkommensteuergesetz (EStG) die beabsichtigte Gesetzesänderung keinen datenschutzrechtlichen Bedenken begegne. Zugleich regte der TLfDI jedoch an, die im Gesetzentwurf vorgesehene Regelung zu streichen, wonach die Kirchensteuerdaten für andere Zwecke nur dann verwendet werden dürften, soweit der Kirchensteuerpflichtige zustimmt oder dies gesetzlich zugelassen ist. Diese Anregung zielte darauf ab, die Nutzung der sensiblen personenbezogenen Daten zur Zugehörigkeit bzw. Nichtzugehörigkeit der betroffenen Steuerpflichtigen zu einer Religionsgemeinschaft ausschließlich auf den Kirchensteuerabzug zu beschränken.

Bereits bei der Diskussion zur Neuregelung des Einkommensteuergesetzes zur Abführung der Kirchensteuer hatten es die

Datenschutzbeauftragten des Bundes und der Länder als problematisch angesehen, dass das o. g. personenbezogene Datum gegenüber den zum Kirchensteuerabzug verpflichteten Banken und Kreditinstituten zu offenbaren ist. Einen geeigneten Bewertungsmaßstab stellt in diesem Zusammenhang § 28 Abs. 2 Bundesdatenschutzgesetz dar. Danach ist eine zweckändernde Nutzung personenbezogener Daten nur unter den dort genannten engen, im konkreten Falle der Kirchensteuerdaten wohl nicht vorliegenden Voraussetzungen zulässig.

Mit der Neuregelung des Thüringer Kirchensteuergesetzes hätte sich nach Auffassung des TLfDI daher die Gelegenheit geboten, datenschutzrechtlichen Belangen hinsichtlich einer Nutzungsbeschränkung der zum Zwecke der Durchführung des Kirchensteuerabzugs erlangten personenbezogenen Daten seitens der Kirchensteuerabzugsverpflichteten Rechnung zu tragen und keine Begehrlichkeiten zu diesen Daten zu wecken.

Letztendlich ist das TFM der Anregung des TLfDI, die besagte Regelung zur Nutzung von Kirchensteuerdaten für andere Zwecke aus dem Gesetzentwurf zu streichen, nicht gefolgt. Das TFM hielt den Vorschlag des TLfDI für nicht geboten und verwies dabei unter anderem auf § 51a Abs. 2c Satz 9 EStG: Danach darf der Kirchensteuerabzugsverpflichtete die von ihm für die Durchführung des Kirchensteuerabzugs erhobenen Daten ausschließlich für diesen Zweck verwenden.

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



paragraph_regen – © fotomek/ Fotolia.com

10 Justiz

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

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

Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit

und beschwerte sich darüber, dass der Direktor eines Thüringer Gerichts in einem Zeitungsartikel Ende Januar 2015 Angaben über ein Verfahren gemacht habe, welches nach Auffassung des Beschwerdeführers noch gar nicht rechtskräftig hätte sein können. Zudem habe der Direktor seiner Ansicht nach nicht die Befugnis gehabt, gegenüber der Presse nicht-öffentliche Verfahren zu erörtern. Der TLfDI prüfte den Zeitungsartikel, konnte aber keinen Verstoß gegen datenschutzrechtliche Vorschriften feststellen. Zwar enthielt der Zeitungsartikel Angaben über Verfahren bei dem betreffenden Gericht. Aus diesen Angaben konnte aber aus datenschutzrechtlicher Sicht nicht auf eine konkrete Person geschlossen werden.

In seiner Beschwerde teilte der Beschwerdeführer zudem Folgendes mit: Er wisse, dass Mitarbeiter des Gerichts regelmäßig Gerichtsakten und sonstige Unterlagen mit nach Hause nehmen würden, um dort Heimarbeit zu erledigen, die sie während ihrer regulären Arbeitszeit nicht schaffen würden. Der TLfDI ging auch diesem Hinweis nach, und bat im Rahmen der Zuständigkeit des TLfDI gemäß § 2 Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) das betroffene Gericht um eine Stellungnahme. Aus dieser Stellungnahme ergab sich, dass eine Heimarbeit von Mitarbeitern/innen, die mit der Wahrnehmung von Verwaltungsangelegenheiten betraut sind, nicht durchgeführt wurde. Aus diesem Grund gab es bei dem entsprechenden Gericht bislang auch noch nicht die Notwendigkeit, den datenschutzkonformen Umgang mit Verwaltungsakten bei Heimarbeit zu regeln. Ein Datenschutzverstoß lag demnach nicht vor. Die Kontrollkompetenz des TLfDI für Gerichte bewegt sich dabei im Rahmen des § 2 Abs. 6 ThürDSG und beschränkt sich nur auf deren Verwaltungsangelegenheiten. Das betreffende Gericht bat darum, Hinweise zu geben, falls dem TLfDI Kenntnisse für Datenschutzverstöße vorlägen, die sich auf den Bereich der Rechtssprechungstätigkeit bezögen, um diesen dann in eigener Zuständigkeit nachzugehen.

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

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

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

Im Berichtszeitraum bat das Thüringer Landesverwaltungsamt (TLVwA) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine datenschutzrechtliche Beratung nach § 40 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) hinsichtlich einer möglichen Errichtung einer Videoüberwachungsanlage bei einer Außenstelle der Landesaufnahmeeinrichtung für Flüchtlinge. Als Alternative, so das TLVwA, käme auch die Umzäunung der Gebäude in Betracht.

Die datenschutzrechtliche Zulässigkeit einer Videoüberwachung richtet sich bei öffentlichen Stellen nach § 25a Thüringer Datenschutzgesetz (ThürDSG).

Gemäß § 25a Abs. 1 ThürDSG ist eine Videoüberwachung (Videoüberwachung oder -aufzeichnung) zulässig, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen öffentlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Unter diesen Voraussetzungen kann eine Videoüberwachung im Gegensatz zu einem Zaun durchaus zulässig sein. Die Erforderlichkeit einer Videoüberwachung ist dann gegeben, wenn das festgelegte Ziel mit der Videoüberwachung tatsächlich erreicht werden kann und dafür kein anderes, gleich wirksames, aber das Recht des Betroffenen weniger beeinträchtigendes Mittel zur Verfügung steht (vgl. für das BDSG: Scholz in Simitis, BDSG Kommentar, § 6b, Rz. 86).

In dem vorgelegten Konzeptentwurf zur Videoüberwachung führte das TLVwA auf, dass eine mögliche Gefährdung durch Personen erfolgen könne, die aufgrund ihrer politischen Einstellung Straftaten gegenüber Personen im Gebäude oder gegen das Gebäude der Au-

ßenstelle der Landesaufnahmestelle für Flüchtlinge zu verüben versuchen würden. Das Gefährdungsrisiko bewertete das TLVwA aufgrund der kontrovers geführten öffentlichen Diskussionen in der Asylthematik als mittel bis hoch. Als Zweck der Videoüberwachung nannte das TLVwA in dem Konzept den Schutz von Leben und Gesundheit der Bewohner der Einrichtung, der Mitarbeiter des Freistaats Thüringen, der Mitarbeiter beteiligter Behörden, von zuständigen Verbänden, Firmen und ehrenamtlichen Helfern, die Gewährleistung der Unversehrtheit und der technischen Funktionstätigkeit der bereitgestellten Einrichtungen sowie der Gebäude, die Abschreckung von möglichen Straftaten und die Möglichkeit zur schnellen Intervention durch die Sicherheitsbehörden.

Der TLfDI wies darauf hin, dass auch der Einsatz milderer Mittel in Betracht zu ziehen sei, wie z. B. die Aufstockung des Sicherheitspersonals, eine bessere Beleuchtung der nicht einsehbaren Bereiche, eine sichere Schließanlage oder ggfs. die Umzäunung des Gebäudes. Eine weitere Prüfung des TLfDI erübrigte sich, da er im Laufe des weiteren Verfahrens erfuhr, dass die datenschutzkonforme Lösung der Umzäunung der Gebäude gewählt wurde.

Die Zulässigkeit einer Videoüberwachung aus datenschutzrechtlicher Sicht beurteilt sich bei öffentlichen Stellen nach § 25a Thüringer Datenschutzgesetz (ThürDSG).

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

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

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

war, dass manchen Mitarbeitern der Fahrerlaubnisbehörde bei einer Mitteilung der Strafverfolgungsbehörden nach Nr. 45 (Fahrerlaubnissachen) der Anordnung über Mitteilung in Strafsachen (MiStra) in einzelnen Fällen bekannt sei, dass es sich bei den Personen um Bedienstete des öffentlichen Dienstes handeln würde. Es stand deshalb die Frage im Raum, ob die Mitarbeiter der Fahrerlaubnisbehörde die mitteilende Strafverfolgungsbehörde darüber in Kenntnis setzen dürfen, dass es sich bei den betroffenen Personen um Bedienstete des öffentlichen Dienstes handelt und dass sie deren Dienststelle benennen und auf Nr. 15 und Nr. 16 MiStra hinweisen. Die Nr. 15 und Nr. 16 MiStra regeln, welche Daten in Strafsachen gegen eine Person in einem Beamten- oder Richterverhältnis bzw. gegen Personen in einem Arbeitnehmer- oder sonstigen Beschäftigungsverhältnis im öffentlichen Dienst durch die Staatsanwaltschaft oder das Gericht zu übermitteln sind.

Der TLfDI teilte dem Landratsamt mit, dass die MiStra in ihrem Anwendungsbereich grundsätzlich für die Übermittlung personenbezogener Daten von Amts wegen durch Gerichte und Staatsanwaltschaften an öffentliche Stellen für andere Zwecke als die des Strafverfahrens (für die die Daten erhoben worden sind) gilt (§ 12 ff. Einführungsgesetz zum Gerichtsverfassungsgesetz [EGGVG], Nr. 1, Nr. 4 MiStra). Damit ist es eben nicht Aufgabe der Fahrerlaubnisbehörde, Mitteilungen nach Nr. 15 und Nr. 16 MiStra an die Staatsanwaltschaft zu machen. Eine Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nach § 21 Thüringer Datenschutzgesetz (ThürDSG) zudem nur dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten liegenden Aufgabe erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden. Die Fahrerlaubnisbehörde ist jedoch nicht als Strafverfolgungsbehörde tätig und damit auch nicht zuständig für die Verfolgung etwaiger Straftaten. Auch scheint eine Übermittlung an Dritte (hier: die Staatsanwaltschaft) für die Erfüllung ihrer Aufgaben nicht erforderlich zu sein, da die Staatsanwaltschaft eigenständige Ermittlungen durchführt. Eine Datenübermittlung schied in diesem Fall folglich aus. Dies teilte der TLfDI dem Landratsamt mit.

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

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

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

Ein Beschwerdeführer wandte sich im Berichtszeitraum an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und bat um eine datenschutzrechtliche Prüfung. Hintergrund war, dass der Beschwerdeführer vor ca. einem Jahr unter Angabe seiner privaten Daten bei einer Thüringer Polizeiinspektion Anzeige gegen Unbekannt wegen Sachbeschädigung erstattet hatte. Nun habe er einen Bescheid der Staatsanwaltschaft Erfurt erhalten mit der Mitteilung, dass die Ermittlungen ergebnislos verlaufen seien. Die Staatsanwaltschaft habe daher das Verfahren eingestellt. Diesen Brief habe die Staatsanwaltschaft aber nicht an die Privatadresse des Beschwerdeführers, die er bei der Anzeigeerstattung angegeben hatte, sondern an seine Dienststelle versandt. Der Brief enthielt zudem keinen zusätzlichen Vermerk wie „persönlich“ oder „vertraulich“.

Der TLfDI wandte sich an die Staatsanwaltschaft Erfurt und bat sie um eine Stellungnahme.

Aus dieser ging hervor, dass der Beschwerdeführer bereits vor fast drei Jahren zunächst in seiner dienstlichen Funktion Strafanzeige wegen Sachbeschädigung erstattet hatte. Dabei übernahm die Staatsanwaltschaft die dienstlichen Daten in der Strafanzeige und erfasste sie elektronisch. Das Ermittlungsverfahren wurde eingestellt. Zwei Jahre später erstattete der Beschwerdeführer – nun als Privatperson – erneut eine Anzeige wegen Sachbeschädigung. In diesem Ermittlungsverfahren nahm die Staatsanwaltschaft dieses Mal die Privatschrift des Beschwerdeführers auf. Auch dieses Verfahren wurde später eingestellt. Den Einstellungsbescheid übersandte die Staats-

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

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

10.5 Gesetzentwurf zur Aufbewahrung von Notariatsunterlagen – nicht ohne Datenschutz

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

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

Für kritikwürdig erachtete der TLfDI dabei folgende Punkte:

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

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

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

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

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

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

lich ausgeschlossen sind – muss der Rahmen dazu im Gesetz geregelt sein und nicht in einer Rechtsverordnung (Artikel 80 Grundgesetz (GG)).

Nach dem Gesetzentwurf besteht zudem keine Pflicht des Notars oder mehrerer Notare, die sich zur gemeinsamen Berufsausübung verbunden oder gemeinsame Geschäftsräume haben, zur Bestellung eines Datenschutzbeauftragten.

Aus datenschutzrechtlicher Sicht begegnet diese geregelte „Befreiung“ der Notare von der Pflicht, einen behördlichen Datenschutzbeauftragten (bDSB) zu bestellen, erheblichen Bedenken. § 10a Abs. 1 Satz 4 ThürDSG legt fest, dass u. a. Notare einen Beauftragten einzusetzen haben, wenn mindestens fünf Personen bei der automatisierten Verarbeitung oder Nutzung personenbezogener Daten beschäftigt werden.

Der Datenschutzbeauftragte ist nicht nur für das elektronische Urkundenarchiv, sondern auch etwa für die Mitarbeiterdaten und andere, nicht originär der Notarstätigkeit zuzuordnende Verfahren (Webseite, Internetzugang, Telefonanlage etc.) zuständig.

Der Gesetzentwurf sah zudem eine Änderung des § 92 Bundesnotarordnung (BNotO) vor, was aus datenschutzrechtlicher Sicht absolut inakzeptabel wäre. Diese Änderung bezweckte ausweislich der Gesetzesbegründung, die Notare von der Kontrolle durch die Landesbeauftragten für den Datenschutz vollständig auszunehmen. Die Datenschutzkontrolle soll danach in jeder Hinsicht – also auch im Hinblick auf den Datenschutz – nur noch („ausschließlich“) durch die in § 92 BNotO genannten Stellen der Justizverwaltung durchgeführt werden. Die dafür genannten Gründe überzeugen – jedenfalls für die in Thüringen geltende Rechtslage – nicht. Notare sind eindeutig und voll umfänglich dem Geltungsbereich des ThürDSG unterworfen (vgl. § 2 Abs. 1 ThürDSG), da sie als Beliehene zu Trägern eines öffentlichen Amtes bestellt werden. Damit unterfallen die Notare in Thüringen auch der Prüfungskompetenz des TLfDI nach § 37 Abs. 1 ThürDSG. Eine differenzierte Behandlung öffentlicher Stellen erscheint nicht sinnvoll und wäre den Betroffenen auch kaum vermittelbar. Im Übrigen erscheint es auch sehr fraglich, ob die beabsichtigte Datenschutzaufsicht ausschließlich durch die in § 92 BNotO genannten Stellen der Justizverwaltung mit den Vorgaben des Art. 28 Abs. 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (EG-Datenschutzrichtlinie) im Einklang steht, wonach die mit der Überwachung des Datenschutzes beauftragte

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

Ob die datenschutzrechtlichen Bedenken und Hinweise im Rahmen des weiteren Gesetzgebungsverfahrens berücksichtigt werden, behält der TLfDI im Auge.

Kurz und knapp zusammengefasst:

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

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

Bereits im 10. Tätigkeitsbericht informierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über eine Kontrolle einer Thüringer Justizvollzugsanstalt (JVA).

Dabei stellte der TLfDI fest, dass sich unter anderem an den Haftraumtüren unterschiedliche personenbezogene Daten der Gefangenen, wie der Vorname, der Nachname, spezielle Gesundheitsdaten (z. B. Diabetiker), die Religionszugehörigkeit (z. B. Moslem), die speziellen Essgewohnheiten (z. B. muslimische Kost) und der Hin-

weis auf die Arbeitsstätte in der Justizvollzugsanstalt befanden. Dies sah der TLfDI im Hinblick auf die Gesundheitsdaten und die Religionszugehörigkeit kritisch. Auch folgte die JVA dem Rat des TLfDI und verzichtete nunmehr auf die Angabe von Gesundheitsdaten und der Religionszugehörigkeit an den Haftraumtüren.

Weiterhin veranlasste die JVA, dass keine Krankenakten oder personenbezogene Daten von Gefangenen in unverschlossenen Schränken oder sichtbar und frei zugänglich im medizinischen Bereich lagerten. Darüber hinaus befindet sich in der Vollzugsgeschäftsstelle der JVA ein Ausleihblatt für Archivakten, aus dem ersichtlich ist, wer wann und aus welchem Grund Einsicht in die Gefangenenpersonalakte genommen hat.

Das zwischenzeitlich in Kraft getretene Thüringer Justizvollzugsgesetzbuch (ThürJVollzGB) vom 27. Februar 2014 regelt in § 139 ThürJVollzGB nunmehr auch den Umgang von Gefangenenakten nach deren Entlassung oder einer Verlegung. Danach sind diese Daten spätestens nach Ablauf von zwei Jahren seit der Entlassung oder der Verlegung der Gefangenen in eine andere Anstalt zu kennzeichnen. Ihre weitere Verarbeitung oder Nutzung ist einzuschränken (Sperrung). Die Daten sind nach Ablauf der Frist nur noch ausgewählten Bediensteten zugänglich zu machen. Einzelheiten regelt der Anstaltsleiter. Hiervon können bis zum Ablauf der Aufbewahrungsfrist nach § 140 ThürJVollzGB die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum der Gefangenen ausgenommen werden, soweit dies für das Auffinden der Gefangenenpersonalakte erforderlich ist.

Bei der Aufbewahrung von Akten und Dateien mit nach § 139 ThürJVollzGB gesperrten Daten darf gemäß § 140 ThürJVollzGB für Gefangenenpersonalakten, Gesundheitsakten, Therapieakten, psychologische und pädagogische Testunterlagen und Krankenblätter sowie für Gefangenenbücher eine Frist von drei Jahren nicht überschritten werden.

Als wichtigste datenschutzrechtliche Neuregelung betrachtet der TLfDI die Ausgestaltung der Überwachung der Telefonate der Gefangenen.

Dazu vertrat der TLfDI bereits im 10. Tätigkeitsbericht (Nr. 10.1: Datenschutz hinter Gittern – auch in einer Justizvollzugsanstalt gilt das Grundrecht auf informationelle Selbstbestimmung, S. 183 ff.) die Auffassung, dass das informationelle Selbstbestimmungsrecht des Gefangenen und seines Gesprächspartners es erfordern, beide vor

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

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

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

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

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

Das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) (ehemals Thüringer Justizministerium) folgte schließlich der Rechtsauffassung des TLfDI. Das TMMJV wies die Justizvollzugsanstalten des Freistaates Thüringen an, den Ansagetext der Gefangenentelefonanlagen entsprechend anzupassen, sodass zukünftig nur noch dann ein Hinweis auf eine Überwachung erfolgt, wenn die JVA das Telefongespräch tatsächlich mithört.

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

10.7 Übermittlungssperre für Staatsanwaltschaft

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Beschwerde eines Bürgers aus Nordrhein-Westfalen, der folgenden Sachverhalt schilderte:

Der Bürger habe Ende des Jahres 2014 per E-Mail eine Strafanzeige gegen den Inhaber einer Firma wegen Betruges gestellt. Da sich aber der Sitz dieser Firma, der Wohnort des beschuldigten Firmeninhabers und damit der Tatort in Jena befänden, habe die bisher zuständige Staatsanwaltschaft aus Nordrhein-Westfalen das geführte Ermittlungsverfahren an die Staatsanwaltschaft Gera abgegeben. Die Staatsanwaltschaft Gera gab sodann im Rahmen der Registrierung des zugrunde liegenden Ermittlungsverfahrens im Fachverfahren websta (das einem speziellen elektronischen Aktenführungssystem nahekommt) die Wohnortadresse und nicht die Postfachadresse des Bürgers und Anzeigenerstatters ein. Grund hierfür war – nach dem späteren glaubhaften Vorbringen der Staatsanwaltschaft Gera gegenüber dem TLfDI –, dass die vom Bürger aus Nordrhein-Westfalen per E-Mail erstattete Strafanzeige ausgedruckt und in der Akte zum Teil verdeckt war. Infolgedessen nahm bei der Staatsanwaltschaft niemand zur Kenntnis, dass der Anzeigenerstatter am Ende seiner E-Mail-Strafanzeige auf die für seine Privatanschrift bestehende Auskunftssperre hinwies. Auch die Bitte des Anzeigenerstatters, dass seine Privatanschrift nicht in die Ermittlungsakte aufgenommen werden sollte, beachtete bei der Staatsanwaltschaft Gera niemand. Schließlich erkannte die Staatsanwaltschaft Gera nicht, dass der Anzeigenerstatter ganz unten links in seiner E-Mail-Strafanzeige seine Postfachadresse in Nordrhein-Westfalen angegeben hatte.

Dieser Lapsus der Staatsanwaltschaft Gera fiel dem Bürger und Anzeigenerstatter aber dann auf, als er im Winter 2015 Post von der Staatsanwaltschaft Gera an seine Privatanschrift erhielt und ihm mitgeteilt wurde, dass das strafrechtliche Ermittlungsverfahren eingestellt worden sei. Da der Bürger und Anzeigenerstatter in Sorge war, dass seine Privatanschrift aus der Akte der Staatsanwaltschaft Gera an Dritte übermittelt worden sein könnte, bat er den TLfDI um Hilfe. Dieser prüfte den Fall und kam zu folgenden Ergebnissen:

Die bei der Staatsanwaltschaft (StA) Gera im Programm websta gespeicherte Wohnortadresse des Bürgers und Anzeigenerstatters war nach § 16 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz (ThürDSG)

zu löschen, weil die Kenntnis der Wohnortadresse zur Erfüllung der Aufgaben der StA Gera nicht (mehr) erforderlich war. Dies ergab sich zum einen aus der Tatsache, dass der StA Gera – nach eigenem Bekunden – von vornherein auch die Postfachadresse des Bürgers und Anzeigenerstatters bekannt gewesen sei. Folglich war es demnach auch nicht erforderlich, dass die StA Gera die Wohnortadresse des Bürgers und Anzeigenerstatters ins Programm websta übernahm. Zum anderen war die im Programm websta gespeicherte Wohnortadresse für die StA Gera nicht mehr erforderlich, weil das bei ihr geführte Ermittlungsverfahren laut Mitteilung der StA Gera an den TLfDI im Winter 2015 eingestellt worden war.

Schließlich war dabei auch die melderechtliche Auskunftssperre zugunsten des Bürgers und Anzeigenerstatters im Sinne von § 34 Abs. 6 Meldegesetz NRW zu berücksichtigen.

Ferner war die Wohnortadresse des Bürgers und Anzeigenerstatters gemäß § 16 Abs. 2 Satz 2 ThürDSG in Verbindung mit § 15 Abs. 1 ThürDSG auch in den Akten der Staatsanwaltschaft Gera zum zugrunde liegenden Ermittlungsverfahren zu sperren. Dies ergab sich daraus, dass die Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaft und der Justizvollzugsbehörden (Aufbewahrungsbestimmungen – AufbewBest – hier Anlage zu Nr. 2 der AufbewBest, laufende Nummer 621 b) bei einer Einstellung eines Ermittlungsverfahrens aus sonstigen Gründen eine Aufbewahrungsfrist für die staatsanwaltliche Ermittlungsakte von fünf Jahren vorsehen. Damit konnten die personenbezogenen Daten – hier in Gestalt der Wohnortadresse des Bürgers und Anzeigenerstatters – in der Ermittlungsakte der StA Gera zwar nicht sofort gelöscht, sehr wohl aber gemäß § 15 Abs. 1 ThürDSG gesperrt werden.

Der TLfDI forderte die Staatsanwaltschaft Gera daher auf, die Wohnortadresse des Bürgers und Anzeigenerstatters als personenbezogenes Datum im Programm websta gemäß § 16 Abs. 1 Nr. 2 ThürDSG zu löschen und die Wohnortadresse als personenbezogenes Datum in der Ermittlungsakte der Staatsanwaltschaft Gera (Az. 390 Js 165/15) gemäß § 16 Abs. 2 Satz 2 in Verbindung mit § 15 Abs. 1 ThürDSG zu sperren.

Ferner mahnte der TLfDI dringend an, den Inhalt von Strafanzeigen, insbesondere darin enthaltene Hinweise auf melderechtliche Übermittlungssperren, künftig effektiver zu beachten und zu berücksichtigen und Strafanzeigen in Papierform dergestalt abzuheften, dass ihr

Inhalt für den Bearbeiter leicht und jederzeit sichtbar zur Kenntnis genommen werden kann.

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

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

10.8 Anforderung von Ausländerakten zur Anerkennung ausländischer Entscheidungen in Ehesachen

Im Berichtszeitraum hat der Arbeitskreis „Justiz“ der Landesbeauftragten für den Datenschutz die Praxis der Anforderung von Ausländerakten bei Verfahren zur Anerkennung ausländischer Entscheidungen in Ehesachen thematisiert. Die Beiziehung von Ausländerakten in Familiensachen in diesem Zusammenhang geschieht unterschiedlich.

In einem Bundesland werden die Ausländerakten in Familiensachen in diesen Angelegenheiten grundsätzlich beigezogen, in anderen Bundesländern stellt dies die Ausnahme dar.

Nach § 107 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) sind die Justizverwaltungen der Länder für die Anerkennung ausländischer Entscheidungen in Ehesachen zuständig. Das Beiziehen von Ausländerakten betrifft häufig Fälle, in denen ein in Deutschland lebender Ausländer eine neue Ehe (ggf. mit einer/einem Deutschen) eingehen möchte und dafür die verbindliche Bestätigung benötigt,

dass eine frühere Ehe im Ausland inzwischen rechtskräftig geschieden wurde. Die Anerkennung erfolgt auf Antrag.

In Anerkennungsverfahren fordert die zuständige Justizbehörde des Bundeslandes – das zur Nachfrage Anlass gegeben hatte – von der Ausländerbehörde regelmäßig die Ausländerakte der antragstellenden Person an, ggf. auch die des Ex-Ehepartners. Dieser Akte entnimmt die Justizbehörde Angaben für den Antrag oder auch die Bestätigung, dass die von der antragstellenden Person in dem Antragsformular gemachten Angaben zutreffen.

Die Übersendung der gesamten Ausländerakte führt allerdings zur Übermittlung nicht erforderlicher, zum Teil sehr sensibler Daten an eine dritte Stelle.

In Thüringen ist der Präsident des Oberlandesgerichts für die Entscheidungen über Anträge zur Anerkennung ausländischer Entscheidungen in Ehesachen zuständig. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erkundigte sich beim damaligen Thüringer Justizministerium (TJM), wie die Thüringer Familiengerichte die Beiziehung der genannten Ausländerakten handhaben. Nach Auskunft des TJM würden in Thüringen bei Anerkennungsverfahren nach § 107 FamFG Ausländerakten nicht regelmäßig, sondern nur aus besonderem Anlass beigezogen. Dies geschehe insbesondere dann, wenn Zweifel an der Identität des Betroffenen oder an den Angaben zum Familienstand bestünden und daher eine Überprüfung geboten erscheine. Der familienrechtliche Sachverhalt sei von Amts wegen aufzuklären. Das ergibt sich aus § 26 FamFG. Gemäß § 29 FamFG erhebt das Gericht die erforderlichen Beweise in geeigneter Form. Dazu zählt, so das TJM, auch die Einholung amtlicher Auskünfte von Behörden sowie die Einsichtnahme in jede Art von Urkunden, insbesondere auch die Einsicht in Behördenakten. Aus besonderem Anlass könne somit auch die Ausländerakte in das Verfahren einbezogen werden.

Aus Sicht des TLfDI stieß die Thüringer Praxis – die Beiziehung der ausländischen Akte in Anerkennungsverfahren nach § 107 lediglich in begründeten Ausnahmefällen – auf keine Bedenken.

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

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

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

Das Thüringer Ministerium für Migration, Justiz und Verbraucherschutz (TMMJV) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit TLfDI im Berichtszeitraum um eine Stellungnahme hinsichtlich des Zugangs des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT) zu Gefangenendaten. Das CPT besucht Hafteinrichtungen und prüft, wie die Gefangenen dort behandelt werden.

Eine Einsichtnahme des CPT in die Gefangenenpersonalakte und/oder Krankenakte bzw. eine Übermittlung der Daten an den CPT wäre nur zulässig, wenn eine Rechtsgrundlage die Datenverarbeitung erlauben würde oder eine Einwilligung der Betroffenen vorläge (§ 4 Abs. 1 Thüringer Datenschutzgesetz [ThürDSG]).

Art. 8 Abs. 2 d der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe stellte nach der Ansicht des TLfDI keine taugliche Rechtsgrundlage für eine Einsichtnahme der Mitglieder des CPT in die Gefangenenpersonal- und/oder die Gesundheitsakte dar.

Art 8 Abs. 2 d der Europäischen Konvention zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung von Strafe bestimmt, dass die Vertragspartei – also auch die Bundesrepublik Deutschland, die der Konvention beigetreten ist – dem CPT alle sonstigen zur Verfügung stehenden Auskünfte, die der CPT zur Erfüllung seiner Aufgabe benötigt, zu gewähren hat. Bei der Beschaffung solcher Auskünfte beachtet der CPT die innerstaatlichen Rechtsvorschriften einschließlich des Standesrechts. In dem „Erläuternden Bericht“ wird dazu ausgeführt, dass der CPT seinerseits verpflichtet ist, die geltenden Regeln der nationalen Rechtsvorschriften und des Standesrechts (insbesondere Regeln bezüglich des Datenschutzes und des Arztgeheimnisses) zu berücksichtigen, wenn er eine Vertragspartei um Auskünfte ersucht. Nach der Auffassung des TLfDI hat die Konvention ausdrücklich einen Vorbehalt in Bezug auf nationale Datenschutzbestimmungen vorgesehen. Eine spezialge-

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

§ 119 ThürJVollzGB bestimmt jedoch, dass das Thüringer Datenschutzgesetz (ThürDSG) Anwendung findet, soweit in diesem Gesetz nichts Abweichendes geregelt ist. Das ThürDSG differenziert dabei zwischen der Datenverarbeitung (hier: Datenübermittlung) personenbezogener Daten und besonderen Arten von personenbezogenen Daten. Eine Übermittlung personenbezogener Daten käme gegebenenfalls unter den Voraussetzungen des § 23 Abs. 1 ThürDSG bzw. bei besonders geschützten Daten wie Gesundheitsdaten unter den Voraussetzungen in § 4 Abs. 5 Nr. 1 bis 8 ThürDSG in Betracht. Aufgrund der Kurzfristigkeit des anstehenden Besuchs des CPT in Thüringer Justizvollzugsanstalten kam im vorliegenden Fall die Erteilung der Einwilligung der betroffenen Gefangenen (§ 4 Abs. 2,3, 5 Nr. 2 ThürDSG) für die Einsichtnahme in ihre Gefangenakte durch das CPT als eine datenschutzkonforme Lösung in Betracht. Die Einwilligung hat den Vorgaben des § 4 Abs. 3 ThürDSG zu entsprechen. Danach ist der Betroffene auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen (informierte Einwilligung). Der Betroffene ist auch darauf hinzuweisen, dass er seine Einwilligung jederzeit widerrufen kann. Die Einwilligung bedarf grundsätzlich der Schriftform. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die Einwilligung ist nur dann wirksam, wenn der Betroffene die Bedeutung und die Tragweite seiner Entscheidung zu überblicken vermag. Für besonders geschützte Daten (z. B. Gesundheitsdaten) gilt, dass die Einwilligung sich ausdrücklich auf diese Daten beziehen muss (§ 4 Abs. 5 Nr. 2 ThürDSG). Das TMMJV folgte der Einwilligungslösung, sieht aber – wie der TLfDI – die Schaffung einer eigenständigen Rechtsgrundlage für die Akteneinsicht durch Mitglieder des CPT als sachdienlich an.

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

10.10 Neufassung des Thüringer Maßregelvollzugsgesetzes

Seit Anfang 2002 war der Maßregelvollzug in Thüringen infolge Beleihung auf private Träger übertragen. Eine Neuregelung wurde notwendig, weil das Bundesverfassungsgericht (BVerfG) in seiner Entscheidung BVerfGE 130,76 Vorgaben für eine Privatisierung des Maßregelvollzugs aufgestellt hatte. Außerdem hatte das BVerfG in seinen Entscheidungen aus dem Jahr 2011 und 2013 (BVerfGE 128, 282; 129 269) festgelegt, dass die medizinische Zwangsbehandlung eines im Maßregelvollzug untergebrachten Patienten besonderer materiell-rechtlicher und verfahrensrechtlicher Voraussetzungen bedarf. Im Gesetz mussten daher vor allem die Regelungen zur Beleihung von psychiatrischen Kliniken in privater Hand angepasst werden, damit diese die hoheitliche Aufgabe des Maßregelvollzugs und zur medizinischen Zwangsbehandlung wahrnehmen können. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gab zu dem vom damaligen Thüringer Ministerium für Soziales, Familien und Gesundheit (TMSFG) übersandten Gesetzentwurf eine Stellungnahme ab und machte zahlreiche Änderungsvorschläge, von denen hier nur die wichtigsten dargestellt werden:

Nach der damals vorgesehenen Regelung zum Besuchsrecht konnte ein Besuch davon abhängig gemacht werden, dass sich der Besucher durchsuchen lässt, wenn Anhaltspunkte dafür bestanden, dass die Sicherheit der Einrichtung gefährdet wird. Bei der Durchsuchung eines Besuchers werden dessen personenbezogene Daten erhoben. Die Durchsuchung stellt damit einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Besucher dar. Dabei können Informationen zutage treten, die der höchstpersönlichen Lebenssphäre des Besuchers zuzuordnen sind. Ein derartiger Eingriff kann daher

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

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

Es sollte möglich sein, den Schriftwechsel eines Patienten sowie den Paketverkehr zu überwachen und Schreiben und Pakete anzuhalten, soweit es zur Verhinderung von Nachteilen für den Patienten, zur Sicherung des Zwecks zur Unterbringung, für die Sicherheit der Einrichtung oder zur Verhinderung einer Gefährdung bedeutender Rechtsgüter Dritter erforderlich war. Auch die Überwachung und ggf. die Anhaltung des Schriftverkehrs ist ein sehr starker Grundrechtseingriff, der nur gerechtfertigt sein kann, wenn er aus den angeführten Gründen unerlässlich ist. Der TLfDI regte daher an, auch hier eine zwingende Erforderlichkeit als Voraussetzung aufzustellen. Nach einer Regelung konnten zur Verhinderung des Suchtmittelmissbrauchs der Patienten Kontrollen durchgeführt werden. Nicht dargelegt war, welcher Art diese Kontrollen sein sollten und unter welchen konkreten Voraussetzungen sie durchgeführt werden dürfen. Für Regelungen, die eine Ermächtigung zu Grundrechtseingriffen enthalten, gilt das Gebot der Normenklarheit und -bestimmtheit. Diesem widersprach die sehr allgemein gehaltene Formulierung.

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

schutzgesetz, § 3 Abs. 1 Thüringer Datenschutzgesetz, § 67 Abs. 1 Satz 1 Sozialgesetzbuch Zehntes Buch).

Da beabsichtigt war, besondere Arten von personenbezogenen Daten einem besonderen Schutz zu unterwerfen, sollten diese nach Auffassung des TLfDI als besondere Arten von personenbezogenen Daten im Gesetz näher definiert werden.

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

Die angeregten Änderungen wurden größtenteils übernommen. Im parlamentarischen Verfahren wurde der TLfDI nochmals zur Stellungnahme aufgefordert. Er wies darauf hin, dass eine Kontrolle von Besuchern auch zur Verhinderung des Suchtmittelmissbrauchs zum einen unverhältnismäßig sein dürfte und zum anderen auch der Re-

gelung widerspricht, nach der bei konkreten Anhaltspunkten dafür, dass ein Besucher selbst berauscht ist oder Drogen oder Rauschmittel in die Vollzugseinrichtung hineinbringen will, der Besuch davon abhängig gemacht werden kann, dass der Besucher sich geeigneten Maßnahmen zur Entkräftung des Verdachts unterwirft.

Da die Anregung des TLfDI nicht übernommen wurde, stellte der TLfDI nochmals die Forderung, dass bei Kontrollen zur Verhinderung des Suchtmittelmissbrauchs darzulegen ist, welcher Art diese Kontrollen sind und unter welchen konkreten Umständen sie durchgeführt werden dürfen. Diese Forderung wurde im parlamentarischen Verfahren leider nicht aufgegriffen.

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

10.11 Den Wächtern auf der Spur

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

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

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

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

Das damalige Thüringer Justizministerium (TJM) gab dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im November 2014 die Gelegenheit zur Stellungnahme im Anhörungsverfahren zur ersten Änderung der Thüringer Verordnung zur Regelung der allgemeinen Beeidigung von Dolmetschern und der Ermächtigung von Übersetzern (DolmV TH).

Obgleich der Änderungsentwurf lediglich das Datum des Außerkrafttretens aufhob, nutzte der TLfDI die „Gunst der Stunde“ zur inhaltlichen Stellungnahme zur DolmV TH. Denn diese besaß in § 2 Abs. 2 DolmV TH folgenden Wortlaut:

„(2) Abweichend von Absatz 1 Satz 3 bedarf es für die Veröffentlichung der Daten der bei Inkrafttreten dieser Verordnung bereits allgemein beeidigten Dolmetscher und ermächtigten Übersetzer im Internet keiner Einwilligung. Die Betroffenen werden spätestens sechs Wochen vor der Einstellung ihrer Daten ins Internet schriftlich informiert und können einer vollständigen oder teilweisen Veröffentlichung ihrer Angaben im Internet innerhalb von vier Wochen wider-

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

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



Weiterhin ergibt sich daraus im Umkehrschluss, dass nach Ablauf der Übergangszeit und Einrichtung einer länderübergreifenden Dolmetscher- und Übersetzerdatenbank (<http://www.justiz-dolmetscher.de/>) für alle beeidigten Dolmetscher und ermächtigten Übersetzer eine Einwilligung erforderlich ist, um ihre personenbezogenen Daten im

Internet zu veröffentlichen. Denn zu beachten ist, dass die Veröffentlichung eines Verzeichnisses über beeidigte Dolmetscher und ermächtige Übersetzer nach § 22 ThürAGGVG im Internet stets auch eine Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes darstellt, deren Zulässigkeit nach § 23 Thüringer Datenschutzgesetz (ThürDSG) zu beurteilen ist. Demzufolge verlangt § 23 Abs. 2 Nr. 1 ThürDSG für eine Übermittlung personenbezogener Daten in Drittstaaten, in denen kein angemessenes Datenschutzniveau im Sinne von § 23 Abs. 1 ThürDSG gewährleistet ist, die zweifelsfreie Einwilligung des Betroffenen.

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

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

netzöffentlichen Verzeichnis nicht einwilligten oder ihr widersprachen.

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

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



Family doctor woman. — © Kurhan / Fotolia.com

11 Arbeit, Gesundheits- und Sozialdatenschutz, Frauen und Familien

11.1 Logo arbeitsuchend? Jobcenter verwenden kein spezielles Logo

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

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

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

11.2 Originalunterlagen für das Jobcenter?

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

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

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



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

11.3 Datensucht im Jobcenter

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

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

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

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

leitet werden könne. Die enthaltenen Angaben würden in der Regel mit den Leistungsberechtigten im persönlichen Gespräch geklärt. Manchmal würden die Bögen zur Vorbereitung für die Betroffenen auch vorab per Post zugesandt. Jedenfalls seien sensible Angaben zu Gesundheit, Finanzen, Süchten und Strafen freiwillig. Fehlende oder falsche Angaben hierzu hätten keine Konsequenzen, nur der Beratungsansatz könne dann nicht optimal sein. Alles diene dem Ziel einer schnellen Arbeitsmarktintegration.

Die Frage nach der Selbstständigkeit konnte vom Jobcenter damit begründet werden, dass dann ein bestimmter Fallmanager zuständig ist. Auch das daraus erzielte Einkommen war für die weitere Beratung begründbar.

Die Frage nach dem Führerschein habe den Hintergrund, dass dann von einer besseren Mobilität insbesondere im ländlich geprägten Bereich ausgegangen werden könne. Ein fehlender Führerschein sei ein Vermittlungshemmnis, das – sofern er nicht entzogen wurde – schnell beseitigt werden könnte. Aufgrund der Hinweise des TLfDI hat das Jobcenter dann aber doch die Frage nach dem Führerschein-entzug aus dem Fragebogen entfernt.

Suchtprobleme und auch größere finanzielle Probleme, so legte das Jobcenter dar, stünden in der Regel einer Arbeitsaufnahme entgegen und müssten vorrangig behandelt werden. Zielgerichtet beraten könne man aber nur, wenn das Problem benannt und bekannt sei. Gesundheitliche Einschränkungen hätten Einfluss auf die Zumutbarkeit der Aufnahme einer bestimmten Arbeit. Es würde Geld und Zeit ersparen, wenn der Betroffene hier freiwillig Angaben machte und entsprechende Belege vorlegte. Ansonsten müsste der Amtsarzt eingeschaltet werden.

Das Jobcenter hat den Profilingbogen entsprechend den Forderungen und Hinweisen des TLfDI überarbeitet. Insbesondere wurde deutlich gemacht, welche Angaben für welchen Zweck nur freiwillig zu machen und welche Angaben Pflicht sind. Der Fragebogen enthält daher immer noch eine Fülle von Fragen, die mit Sternchen gekennzeichnet und daher nur freiwillig zu machen sind. Genaue Angaben zu gesundheitlichen Einschränkungen sind nicht mehr vorgesehen; ebenso können keine „sonstigen Hinweise“ oder Angaben zur familiären Situation mehr gemacht werden. Ob jemand Suchtprobleme hat, kann er freiwillig angegeben, um ein Beratungsangebot zu erhalten. Das sollte reiflich abgewogen werden.

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

11.4 Datenabgleich durch Jobcenter

Ein Betroffener beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über ein kommunales Jobcenter einer kreisfreien Stadt. Dieses hatte ihn nämlich zur Mitwirkung nach § 60 Abs. 1 Sozialgesetzbuch (SGB) Erstes Buch (I) aufgefordert, seinen Arbeitslosengeld I-Bezug von der Agentur für Arbeit mitzuteilen. Dies konnte er sich nicht erklären, weil er zwar einen Antrag auf Grundsicherung nach Sozialgesetzbuch (SGB) Zweites Buch (II) beim Jobcenter gestellt hatte, aber keine ALG I-Leistungen von der Agentur für Arbeit des Landkreises bezog. Da ihm bekannt war, dass das Jobcenter regelmäßig zu Beginn eines jeden Quartals einen automatisierten Datenabgleich gemäß § 52 SGB II zum Zweck der Überprüfung seitens der Bundesagentur für Arbeit durchführt, ob und in welcher Höhe jemand Leistungen der Agentur als Träger der Arbeitsförderung nach dem SGB erhält, schlussfolgerte der Beschwerdeführer, das Jobcenter habe Daten über ihn erhoben und gespeichert, die es weder erheben noch speichern durfte.

Das vom TLfDI zur Stellungnahme aufgeforderte Jobcenter teilte mit, es habe mit der Agentur für Arbeit weder Daten ausgetauscht noch abgeglichen. Bei der laufenden Bearbeitung sei aufgefallen, dass der Beschwerdeführer möglicherweise einen Anspruch auf Arbeitslosengeld I erworben haben könnte, weil er Bundesfreiwilligendienst geleistet und dabei Einkommen erzielt hatte. Daher sei der Beschwerdeführer mit einem Schreiben aufgefordert worden, seinen Leistungsbescheid über die Bewilligung des Arbeitslosengeldes I vorzulegen. Da er aber nun Leistungen nach SGB II erhielt, habe das Jobcenter pflichtgemäß mit einem weiteren Schreiben an die Agentur für Arbeit auch gleich einen Erstattungsanspruch eingereicht. Schließlich dürfe ein Betroffener nicht gleichzeitig beide Leistungen beziehen. Auf beide Schreiben habe das Jobcenter allerdings keine Antwort erhalten. Diese Darlegung war plausibel und das Vorgehen

wurde, gestützt auf die angegebenen Rechtsgrundlagen, als datenschutzrechtlich zulässig angesehen.

Der TLfDI stellte fest, dass das vom Jobcenter an den Betroffenen gerichtete Schreiben zumindest missverständlich war. Dem Leser wurde nicht deutlich, dass lediglich der Sachverhalt, nämlich ob der Betroffene die bezeichneten Leistungen erhält, überprüft werden sollte. Vielmehr wurde in dem Schreiben ohne konkrete Hinweise bereits davon ausgegangen, dass die Leistungen erbracht werden, die durch den geforderten Bescheid nachzuweisen sind.

Offenbar hatte man einfach ein Formularschreiben genutzt, dessen Inhalt und Intention nicht auf den Sachverhalt passte. Der TLfDI wies das Jobcenter darauf hin, dass, wenn auf ein Formularschreiben zurückgegriffen werden soll, vor seiner Verwendung jeweils zu prüfen ist, ob der Inhalt auf den konkreten Fall zutrifft. Sind Sachverhalte ungeklärt, bedarf es einer Erläuterung für die Betroffenen. Diese Maßnahmen sind einfachste Mittel, um in Zukunft derartige Beschwerden zu vermeiden. Der Vorgang ist noch nicht abgeschlossen.

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

11.5 Immer wieder Kontoauszüge für das Jobcenter

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

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

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

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

und Ähnliches durch eigene Texte ersetzen. Mit derartigen Grundlagen könne man keine gesetzlich vorgeschriebene Prüfung durchführen. Im Übrigen verfähre man genau, wie von der oben zitierten Rechtsprechung verlangt.

Nach der Darlegung des Jobcenters und ergänzend aus der Durchsicht der umfangreichen Unterlagen, die die Beschwerdeführerin dem TLfDI zugeleitet hatte, konnten keine Hinweise auf die Verletzung datenschutzrechtlicher Vorschriften festgestellt werden.

Eine Übersendung von Originalunterlagen der Beschwerdeführerin in unverschlossenem Umschlag schloss das Jobcenter aus und verwies auf die Praxis, dass ein Versand immer in verschlossenem Umschlag erfolge. Damit stand wieder einmal Einlassung gegen Einlassung. Mangels weiterer konkreter Anhaltspunkte konnte nicht festgestellt werden, dass im Fall der Beschwerdeführerin vom üblichen Postversand abgewichen worden war. Der TLfDI konnte daher der Beschwerdeführerin nicht behilflich sein, was er ihr auch mitteilte.

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

11.6 Vorsicht bei der Akteneinsicht

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

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

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

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

tendmachung oder Verteidigung rechtlicher Interessen auch die Möglichkeit einer zumindest teilweisen Schwärzung von in Akten befindlichen personenbezogenen Informationen vor der Einsichtnahme zu prüfen.

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

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

11.7 E-Health-Gesetz des Bundes

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

Der Begriff eHealth bedeutet „elektronische Gesundheit“ und umfasst die aktive Nutzung der Gesundheitskarte (siehe dazu Nummer

15.8) und die Telematik im Gesundheitsbereich, also generell die Nutzung von Informationstechnik innerhalb des Gesundheitswesens. Hinsichtlich eHealth liegt derzeit beim Bundestag ein Gesetzesentwurf „Gesetz für sichere digitale Kommunikation und Anwendung im Gesundheitsbereich“ vor (E-Health-Gesetz). So soll per Gesetz die medizinische Versorgung durch moderne Informations- und Kommunikationstechnologien verbessert werden. Ziel dabei ist es unter anderem, die Einführung der elektronischen Gesundheitskarte einschließlich ihrer nutzbringenden Anwendungen zu unterstützen und die Telematik und die Interoperabilität der informationstechnischen Systeme im Gesundheitswesen zu verbessern. Unter Interoperabilität versteht man, dass Geräte oder Anwendungen (Software) so gestaltet, also so standardisiert werden, dass sie mit anderen Geräten oder Systemen zusammenarbeiten können. Auch der Patienten-Nutzen würde sich dadurch erhöhen, da eine zielgenauere und schnellere Behandlung möglich wäre und auch gefährliche Wechselwirkungen, z. B. durch das Erfassen von verordneten Medikamenten, verringert werden könnte.

Aus datenschutzrechtlicher Sicht gibt es allerdings zurzeit noch Bedenken.

Deshalb erachtete die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder es im März 2015 für notwendig, in einer entsprechenden Entschließung Nachbesserungen zum Gesetzesentwurf zu fordern (siehe dazu Anlage 26). So mahnte sie insbesondere an, die Vertraulichkeit der Daten und Transparenz der Datenverarbeitung zu regeln. Da die Betroffenen selbst über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte entscheiden können, bedarf es eben der Transparenz, welche Daten durch wen verarbeitet werden können. Außerdem muss zu jeder Zeit die gebotene Vertraulichkeit der Daten gewährleistet sein. Auch im Hinblick darauf, dass insbesondere durch immer modernere Informationstechnik die Einschaltung externer Dienstleister durch Berufsgeheimnisträger nicht ausbleiben wird, bedarf es neben der technischen Sicherstellung der Vertraulichkeit weiterer Regelungen. Um nicht in die Gefahr eines Verstoßes gegen die Schweigepflicht (§ 203 StGB) zu kommen, gilt es, klare Rahmenbedingungen zu schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger überhaupt externe Dienstleister einschalten dürfen.

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

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

Gehören Sie auch zu den gesundheitsbewussten Menschen, die täglich Ihre Armbänder, Brustbänder oder eine entsprechende moderne Uhr bei sich tragen, damit diese Geräte Ihre Fitness überprüfen? Zählen Sie täglich elektronisch Ihre Schritte und Ihren Kalorienverbrauch per App (App = Applikationssoftware)? Schlafen Sie nachts mit einem eingeschalteten Smartphone neben sich, damit eine App Ihren Nachtschlaf überwacht?

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

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

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

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

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

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

möglicherweise auch in einem Drittstaat erfolgen. Ob in diesem Drittstaat ein angemessenes Datenschutzniveau herrscht, ist ungewiss.

Datenschutzrechtliche Bedenken sieht der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch im Hinblick auf eine mögliche Übermittlung der teilweise sensiblen personenbezogenen Daten – ob nun gewollt oder ungewollt – zum Beispiel an den Arbeitgeber, an die Versicherung oder an einen sonstigen Dritten.

Auch an die technischen und organisatorischen Maßnahmen für den Einsatz solcher Apps sind hohe Anforderungen zu stellen. Es muss aus datenschutzrechtlicher Sicht sichergestellt werden, dass die mitunter sehr sensiblen Daten nicht in die Hände unberechtigter Dritter gelangen und sie für Zwecke, zu denen der Betroffene nicht zugestimmt hat, verwendet werden. Dem Zweckbindungsgrundsatz ist in diesem Sinne eine hohe Bedeutung zuzumessen.

Schließlich gilt es zu bedenken, dass in Zeiten von „Big Data“ die Möglichkeit besteht, Datensätze durch die Verwendung von Algorithmen in Verbindung zu setzen und zu analysieren. Die aufbereiteten analysierten Informationen können unter Umständen für einen Dritten sehr wertvoll sein, nicht stets aber auch für den Betroffenen.

Im Berichtszeitraum beschäftigte sich auch der Europaausschuss des Thüringer Landtages mit dem Thema „Grünbuch der Kommission über Mobile-Health-Dienste („mHealth“)“ und lud hierzu den TLfDI ein, um dieses Thema zu erörtern. Dabei wies der TLfDI unter anderem darauf hin, dass der Nutzer grundsätzlich das Recht habe, die Nutzung dieser Dienste abzulehnen bzw. einen Anspruch auf Löschung seiner erfassten Daten habe, wenn er die Dienste nutze.

Weiterhin wies der TLfDI darauf hin, dass die Nutzung von Cloud-Computing Services (= Speichern von Daten jenseits des eigenen Personalcomputers, z. B. in entfernten Rechenzentren) zur Verarbeitung von Gesundheitsdaten datenschutzrechtlich problematisch sei und eine cloud-basierte Verarbeitung nur dann erfolgen könne, wenn sie über die Cloud sicher sei und die Zugriffsrechte eindeutig festgelegt seien und eine Datenübertragung verschlüsselt erfolge. Vor Akzeptanz der Allgemeinen Geschäftsbedingungen, in der eine datenschutzrechtliche Einwilligung erblickt werden kann, ist also Vorsicht mehr als geboten!

Eine Nachfrage des TLfDI beim Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMA SGFF) ergab, dass

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

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

11.9 Maßregelvollzug: Besuch nur mit Drogenscreening?

Von einer Abgeordneten im Thüringer Landtag erfolgte der Hinweis auf Probleme bei der Besucherkontrolle in Einrichtungen des Thüringer Maßregelvollzugs. Dort würden nämlich Besuche davon abhängig gemacht, dass Besucherinnen und Besucher Urin- und Speichelproben zur Untersuchung auf Drogenkonsum abgeben.

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

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

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

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

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

Grundlage des § 17 Abs. 2 ThürMRVG rechtswidrig war, hat der TLfDI gefordert, dass die Daten gelöscht werden.

Das TMASGFF hat die Einstellung von Drogenscreenings auf der genannten, nicht ausreichenden Rechtsgrundlage und die Löschung der bisher erhobenen Daten zugesagt. Es wurde mitgeteilt, dass der Aktenbestand sukzessive nach so genannten Besucherlisten durchsucht wird, auf denen die Ergebnisse der Untersuchungen vermerkt sind, um diese zu vernichten.

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

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

Die Kassenärztliche Vereinigung Thüringen hat die ambulante vertragsärztliche Versorgung in Thüringen sicherzustellen, allgemein bekannt als der Kassenärztliche Notfalldienst. Die Sicherstellung umfasst vor allem die ambulante Versorgung zu den sprechstundenfreien Zeiten (Notdienst). Die Versorgung der nicht-gefähigen Patienten im ärztlichen Notdienst wird durch Fahrdienste sichergestellt, welche dann direkt zum Patienten fahren.

Die Fahrten und der getätigte medizinische Einsatz müssen durch den diensthabenden Arzt und dessen Assistenzpersonal dokumentiert werden. Um diese Protokollierung teilweise zu automatisieren und zumindest zu digitalisieren, setzt die Kassenärztliche Vereinigung Thüringen seit 2015 ein System ein, mit dem die durchgeführten Fahrten und die ärztlichen Einsätze zentral digital erfasst werden können. So werden bspw. auch personenbezogene Daten des Hilfesuchenden wie der Name, die Versicherungsnummer und durchgeführte Untersuchungen (ohne Diagnosen) erfasst. Diese Erfassung erfolgt entweder über Tablet oder PC mittels https oder optional über eine entsprechende mobile App (für Android).

Da diese Daten einem besonderen Schutz unterliegen, wandte sich die Kassenärztliche Vereinigung Thüringen zuvor an den TLfDI. So ist nun über ein Rollen- und Berechtigungskonzept geregelt, was z. B. ein „Administrator“, ein „Auswerter“ oder ein „Erfasser“ alles an Daten erfassen, sehen und verändern darf. Außerdem wurden die technischen Sicherheitsmaßnahmen der beteiligten Systemkomponenten bewertet.

Besonderes Augenmerk fiel der mobilen App zu, da bei dieser auf einem tragbaren Endgerät, wie z. B. einem Tablet oder Smartphone, die Daten für einen vorgegebenen Zeitrahmen gespeichert werden. Hier war insbesondere die Gefahr zu beachten, dass bei Verlust des Gerätes auch unberechtigte Dritte an persönliche Daten von Patienten gelangen könnten. Daher wurde mit den Entwicklern der App gemeinsam die Datensicherheit auf dem Gerät diskutiert. Neben der Notwendigkeit der Anmeldung bei Dateneingabe wurde noch eine zusätzliche Authentifizierungsstufe bei lesendem Zugriff auf die gespeicherten Daten hinzugefügt. Auch die verschlüsselte Übertragung sowie die verschlüsselte Datenspeicherung und die Datenlöschung bei der Nutzung der App waren ein Datenschutzthema. Zusätzlich dürfen nur dienstliche Tablets und Smartphones genutzt werden, um diese aus Sicherheitsgründen zentral administrieren zu können und nur dienstlich notwendige Apps für den Einsatz zuzulassen. Damit wird auch die Vermischung von dienstlichen und privaten Daten unterbunden.

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

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

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

Erstattung stellen. Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) lag die Beschwerde eines Beihilfeberechtigten vor, der sich darüber beschwerte, dass die Beihilfestelle forderte, die Ärzte sollten in den Rezepten die ärztliche Diagnose angeben. Als Grund hierfür wurde genannt, dass anderenfalls die medizinische Notwendigkeit der Medikation nicht geprüft werden könne.

Die Angabe der Diagnose im Rezept stellt eine Übermittlung von personenbezogenen Daten an Dritte, beispielsweise den Apotheker, dar. Hierbei handelt es sich um Gesundheitsdaten, die nach dem Gesetz einem besonderen Schutz unterliegen, § 4 Abs. 5 Thüringer Datenschutzgesetz. Die Angabe ist datenschutzrechtlich unzulässig. § 2 Abs. 1 der Verordnung über die Verschreibung von Arzneimitteln legt fest, welche Angaben in einer Verschreibung zwingend enthalten sein müssen. Die Diagnose ist hier nicht genannt. Vielmehr ist davon auszugehen, dass der Arzt sich wegen Verletzung des Berufsgeheimnisses strafbar macht (§ 203 Strafgesetzbuch), wenn er die Diagnose auf dem Rezept vermerkt.

Nach § 7 Abs. 1 Satz 1 der Thüringer Beihilfeverordnung wird Beihilfe nur gewährt, wenn die Aufwendung medizinisch notwendig war. Es kann daher im Einzelfall erforderlich sein, die medizinische Notwendigkeit einer Verschreibung überprüfen zu müssen. Dies kann aber nicht regelmäßig erfolgen, sondern es ist davon auszugehen, dass bei einer ärztlichen Verschreibung grundsätzlich eine medizinische Notwendigkeit besteht. In Zweifelsfällen kann aber der Nachweis der medizinischen Notwendigkeit gefordert werden. Dies ist beispielsweise durch eine ärztliche Bescheinigung möglich. Die Beihilfestelle hat keinen Einfluss darauf, ob ein Arzt bei der Ausstellung eines Rezeptes die Angabe der Diagnose, die der ärztlichen Verordnung zugrunde liegt, mit auf dem Rezept vermerkt. Die Beihilfestelle hat aufgrund des Einschreitens des TLfDI den Erläuterungstext im Beihilfebescheid dahingehend geändert, dass nunmehr nicht der Vermerk der Diagnose auf dem Rezept, sondern die Vorlage von Unterlagen gefordert werden kann.

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

11.12 Privatadressen von Ärzten: Herausgabe durch Krankenhaus?

Die Landesärztekammer Thüringen wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie von einer Klinik die Privatadressen von Ärzten aus Datenschutzgründen nicht erhielt. Hintergrund war folgender:

Mitglied der Landesärztekammer Thüringen wird ein Arzt nach § 2 Abs. 1 Thüringer Heilberufegesetz (ThürHeilBG), sobald er in Thüringen eine ärztliche Tätigkeit aufnimmt, oder, wenn er keine ärztliche Tätigkeit ausübt, er seinen gewöhnlichen Aufenthalt hier hat. Dies gilt auch für Ärzte, welche als Honorarärzte an wechselnden Einsatzorten im ganzen Bundesgebiet tätig werden, oder für solche, die in einem anderen Bundesland ihre Haupttätigkeit ausüben und regelmäßig nebenberuflich in Thüringen arbeiten. In letzter Zeit häuften sich die Fälle von Ärzten, welche honorarärztlich kurzfristig (zwischen wenigen Tagen und mehreren Monaten), oft auch mehrmals in Kliniken oder anderen Einrichtungen in Thüringen ärztlich tätig werden und sich nicht bei der Kammer anmelden. Nach § 2 Abs. 2 ThürHeilBG sind die Ärzte verpflichtet, sich binnen eines Monats, bei vorübergehender Ausübung der Tätigkeit innerhalb von fünf Tagen nach Aufnahme der Tätigkeit, bei der Landesärztekammer anzumelden. Kammerangehörige, die dieser Verpflichtung nicht nachkommen, können nach § 11 ThürHeilBG mit einem Ordnungsgeld von bis zu 5.000 Euro belegt werden. Die Verhängung dieses Ordnungsgeldes ist dem Pflichtigen vorher schriftlich anzukündigen, was nur möglich ist, wenn seine Privatanschrift bekannt ist.

Nach § 19 Thüringer Datenschutzgesetz (ThürDSG) ist die Erhebung der notwendigen Daten durch die Landesärztekammer Thüringen zunächst bei dem Betroffenen zu veranlassen, Grundsatz der Datenerhebung beim Betroffenen. Möglich ist es auch, sich eines so genannten Adressmittlungsverfahrens zu bedienen, bei dem derjenige, der in Kenntnis der Adresse der Person ist, an die das Schreiben gerichtet werden soll, gebeten wird, das Schreiben an den Adressaten weiterzuleiten. Dieses Verfahren wurde bereits durchgeführt und führte nicht in allen Fällen zum Erfolg.

Nach § 19 Abs. 2 Satz 1 Nr. 2 bzw. 3 ThürDSG dürfen die Daten ohne die Mitwirkung des Betroffenen erhoben werden, wenn die zu erfüllende Aufgabe (hier die Registrierung und Berufsaufsicht) ihrer Art nach die Erhebung bei anderen Personen oder Stellen erforder-

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

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

11.13 Rücksendung von Arztrechnungen und Rezepten an eine andere Beihilfeberechtigte

Eine Thüringer Beamtin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil sie die von ihr der Beihilfestelle zur Abrechnung eingereichten Arztrechnungen und Rezepte mit einem Fax-Aufdruck einer Thüringer Polizeidienststelle zurückerhielt. Sie bat um Prüfung, weshalb ihre sensiblen Patientendaten denn bei der Polizei gelandet waren, denn sie war weder im Polizeidienst noch konnte sie sich erklären, weshalb die Beihilfestelle die Polizei eingeschaltet haben sollte.

Auf Nachfrage des TLfDI erklärte die Beihilfestelle, ihre Mitarbeiter seien sich sehr darüber bewusst, dass sämtliche Angelegenheiten, die der Beihilfestelle im Zusammenhang mit der Bearbeitung von Beihilfeanträgen bekannt werden, einem besonderen Schutz unterlägen.

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

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

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

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

Aus einem Zeitungsartikel erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass eine Klinik beabsichtige, eines ihrer Krankenhäuser zu schließen. Bei der Schließung eines Krankenhauses stellt sich immer die Frage, was mit den Patientendaten passieren soll. Dies betrifft sowohl die Patientenakten aus Papier als auch die Patientendaten, die elektronisch gespeichert sind sowie die Informationstechnik des Krankenhauses selbst. Der TLfDI wandte sich an die verantwortliche Klinik und teilte dieser mit, dass sie als verantwortliche Stelle nach § 57 Abs. 10 Thüringer Krankenhausgesetz die technischen und organisatorischen Maßnahmen zu treffen habe, die erforderlich und angemessen sind, um die Beachtung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Hierzu gehören die Einhaltung der Löschfristen und auch die Gewährleistung der Patientenrechte auf Auskunftserteilung nach dem Thüringer Krankenhausgesetz.

Die Klinik übersandte dem TLfDI ihre Archivordnung, die auch für die Akten des zu schließenden Krankenhauses zur Anwendung kommen sollte. Nach datenschutzrechtlicher Prüfung stellte der TLfDI fest, dass die dort enthaltenen Regelungen etwas zu allgemein gefasst waren. Es war nicht ganz eindeutig geregelt, in welchen Fällen und unter welchen Voraussetzungen Krankenhausakten an Dritte herausgegeben werden dürfen. Der TLfDI forderte, sicherzustellen, dass Arztpraxen Patientenakten nur dann erhalten dürfen, wenn eine Schweigepflichtsentbindung des Patienten vorliegt und an Forschungseinrichtungen prinzipiell nur anonymisierte Daten herausgegeben sind. Es existierten zudem keine klaren Regelungen zur Vernichtung von Patientenakten, in denen festgeschrieben wird, wer diese Akten wann vernichtet, durch wen dies protokolliert wird und welche Geräte zum Einsatz kommen. Weiterhin entsprach die Archivordnung nicht der geltenden Gesetzeslage im Hinblick auf das im Jahr 2013 in Kraft gesetzte Patientenrechtegesetz, das neue Regelungen im Bürgerlichen Gesetzbuch (BGB) trifft. Nach § 630g BGB ist dem Patienten auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist dabei zu begründen. Diese Voraussetzungen erfüllte

die Archivordnung nicht, da die Einsichtnahme pauschal verweigert wurde, wenn es um subjektive Wertungen, persönliche Bemerkungen oder Eindrücke des Arztes ging.

Weiterhin teilte die Klinik mit, dass bezüglich der Patientenakten des geschlossenen Krankenhauses im Klinikgebäude ein separater Archivraum genutzt würde. Die Einlagerung der Akten sei notwendig, da die Daten weiter aufbewahrt werden müssen, weil die Aufbewahrungsfristen noch nicht abgelaufen sind. Dokumente, die entsorgt werden durften, wurden nach Angaben der Ansprechpartner im Rahmen einer Auftragsdatenverarbeitung datenschutzgerecht vernichtet.

Die Archivordnung legte aber nicht fest, wie die Patientenakten der verschiedenen Kliniken jeweils getrennt aufbewahrt und vor dem Zugriff Unberechtigter geschützt werden sollten. Die Klinik wurde daher gebeten, die Archivordnung in allen durch den TLfDI kritisierten Punkten zu überarbeiten.

Die Klinik nahm daraufhin die notwendigen Änderungen ihrer Archivordnung vor und übermittelte sie erneut dem TLfDI zur Prüfung. Damit wurde dem größten Teil der Forderung des TLfDI nachgegeben. Einige unklare Punkte, wie beispielsweise die Frage, was mit den Personalakten der damals angestellten Mitarbeiter nach Auflösung des Krankenhauses passiert, konnten im weiteren Schriftverkehr geklärt werden.

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

11.15 Darf der Hausarzt alles wissen?

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

Nachbehandlung zu seinem Hausarzt gegangen sei, habe der schon alle seine Behandlungsdaten auf dem Bildschirm gehabt. Der Betroffene bat den TLfDI, den Sachverhalt zu überprüfen.

Da das Universitätsklinikum Jena als Krankenhaus mit anderen, auch privaten Krankenhäusern im Wettbewerb steht, gilt nach § 26 Thüringer Datenschutzgesetz grundsätzlich das Bundesdatenschutzgesetz (BDSG). Der TLfDI wies gegenüber dem Universitätsklinikum Jena darauf hin, dass ein solcher Austausch von besonderen Arten von personenbezogenen Daten, § 3 Abs. 9 BDSG, nur mit einer wirksamen Einwilligung des Betroffenen und unter Beachtung der nach § 9 BDSG erforderlichen Maßnahmen zulässig sei. Deshalb wurde erfragt, ob es schriftliche Festlegungen zu dem Verfahren gebe, in denen geregelt ist, ob und auf welche Weise die Einwilligung der betroffenen Patienten eingeholt werde, auf welche Weise genau die Datenübermittlung erfolge, welche Patientendaten auf welche Weise an welchem Ort für welche Zeit gespeichert würden und welche Personen unter welchen Voraussetzungen Zugriff auf diese Daten haben.

Die Klinik teilte mit, dass seit 2011 ein Zuweiserportal für niedergelassene Ärzte eingesetzt werde. Derzeit nutzen dieses Portal ausschließlich niedergelassene Ärzte der Fachrichtungen Urologie und Gynäkologie. Im Rahmen des Aufnahmeprozesses wird der Patient über die Möglichkeit der Nutzung dieses Portals aufgeklärt, wenn der angegebene niedergelassene Arzt an dem Verfahren teilnimmt. Der Patient hat dann die Wahl zu entscheiden, ob die Datenübermittlung an seinen Hausarzt beziehungsweise seinen weiterbehandelnden Arzt klassisch mit Papierversand oder über das Zuweiserportal erfolgen soll. Bei der Nutzung des Zuweiserportals erhält der Patient ein zusätzliches Informationsblatt zur Erläuterung des Verfahrens. Erst nach erfolgter schriftlicher Einwilligung erfolgt die Übermittlung an den (Haus-) Arzt.

Ob der Beschwerdeführer im vorliegenden Fall eine solche Einwilligung erteilt hatte, konnte vom TLfDI nicht geprüft werden, weil dieser Patient gegenüber dem TLfDI anonym bleiben wollte. Da der TLfDI der Sache aber grundsätzliche Bedeutung beimaß, wurden die technischen und organisatorischen Maßnahmen, die in Bezug auf das Projekt seitens des Klinikums nach § 9 BDSG getroffen wurden, vor Ort geprüft. Im Ergebnis wurde festgestellt, dass das Verfahren datenschutzkonform durchgeführt wurde. Für die Übermittlung ist eine rechtswirksame Einwilligung der Patienten Bedingung. Die wirksa-

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

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

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

Im Rahmen einer Vorortkontrolle bei einem Arzt brachte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in Erfahrung, dass viele Ärzte in Thüringen ihre Patientenakten, die der gesetzlichen Aufbewahrungsfrist nicht mehr unterliegen, an die Kassenärztliche Vereinigung (KV) Thüringen zur Vernichtung weitergeben. Hierzu wurde die KV Thüringen um Abgabe einer Stellungnahme gebeten. Die KV Thüringen teilte mit, dass es sich um einen Service der KV handele, der allen knapp 4.000 Mitgliedern in Thüringen angeboten werde. Der Ablauf stellte sich dabei wie folgt dar:

Die Praxen vereinbaren mit der KV Thüringen einen Abholtermin, an dem ein datenschutzbelehrter Fahrer die Unterlagen in einem verschlossenen Behälter von der Praxis übernimmt. Die vollen Behälter werden dann bei der KV Thüringen zwischengelagert, in Behälter umgepackt, die von dem privaten Vernichtungsunternehmen zur Verfügung gestellt wurden. In diesen Behältern holt das Unternehmen die Akten dann in einem verschlossenen LKW ab und führt sie der weiteren Vernichtung zu. Das Verfahren wird dadurch protokolliert, dass die jeweiligen Behälter nummeriert werden und die Menge der übernommenen Behälter vom jeweiligen Fahrer quittiert wird.

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

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

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

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

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

Unter der Prämisse, dass die Überlassung von Patientenakten an ein Archiv im Sinne des ThürArchivG stets auch die Übermittlung per-

sonenbezogener Daten beinhaltet, beantwortete der TLfDI die beiden Fragen des UKJ wie folgt:

Patientenunterlagen des UKJ stellten nach Auffassung des TLfDI keine archivwürdigen Unterlagen gemäß § 2 Abs. 1 ThürArchivG dar. Dies ergab sich für den TLfDI aus folgenden Überlegungen:

§ 2 Abs. 1 ThürArchivG bestimmt, dass öffentliches Archivgut alle archivwürdigen Unterlagen der in § 3 Abs. 1 und § 4 Abs. 1 genannten öffentlichen Stellen sind, die zur dauernden Aufbewahrung von einem öffentlichen Archiv übernommen werden. Gem. § 3 Abs. 1 Satz 1 ThürArchivG werden als öffentliches Archivgut des Landes alle archivwürdigen Unterlagen bestimmt, die [...] bei sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts entstanden sind und von den thüringischen Staatsarchiven nach Maßgabe dieses Gesetzes archiviert werden.

Diese Voraussetzungen des § 3 Abs. 1 Satz 1 ThürArchivG erfüllte das UKJ im zu beurteilenden Sachverhalt gerade nicht. Das UKJ ist zwar gemäß § 91 Abs. 1 Satz 1 Thüringer Hochschulgesetz (ThürHG) eine rechtsfähige Teilkörperschaft der Friedrich-Schiller-Universität Jena. Ferner untersteht das UKJ gemäß § 91 Abs. 4 1. Halbsatz ThürHG der Rechtsaufsicht des Landes.

Allerdings scheiterte eine Subsumtion des UKJ unter den § 3 Abs. 1 Satz 1 ThürArchivG daran, dass seine Unterlagen nicht nach Maßgabe dieses Gesetzes – dem ThürArchivG – zu archivieren sind. Dies ergab sich für den TLfDI daraus, dass das ThürArchivG gemäß § 20 Nr. 3 ThürArchivG nicht für öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit gilt, die am wirtschaftlichen Wettbewerb teilnehmen, und für deren Zusammenschlüsse. Im genannten Schreiben des UKJ wies dies aber gerade darauf hin, dass es für den Bereich der Krankenversorgung im Wettbewerb mit umliegenden Krankenhäusern im Freistaat Thüringen stehe. Dem TLfDI waren auch keine anderen Sachverhalte bekannt, die an einer Teilnahme des UKJ am wirtschaftlichen Wettbewerb Zweifel begründeten. Deshalb lag nach Auffassung des TLfDI hier der Ausschlussgrund des § 20 Nr. 3 ThürArchivG für dessen Anwendbarkeit auf Patientenunterlagen des UKJ vor. Folglich stellten die Patientenakten auch kein Archivgut im Sinne des § 3 Abs. 1 ThürArchivG dar.

Damit war zugleich auch die zweite Frage des UKJ beantwortet, ob das ThürArchivG aufgrund von § 20 Abs. 3 ThürArchivG überhaupt anwendbar sei.

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

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

11.18 Die Thüringer Krankenhäuser – Heilung in Sicht

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



Die OH KIS richtet sich nicht nur an die Krankenhausbetreiber und Hersteller von Krankenhausinformationssystemen, sondern bildet auch die Grundlage für datenschutzrechtliche Kontrollen der Aufsichtsbehörden des Bundes und der Länder. Auch der TLfDI richtet sich bei seinen Kontrollen nach der OH KIS.

Das Spektrum der festgestellten Mängel ist dabei vielfältig: vom Fehlen konkreter Regelungen zu datenschutzrelevanten Themen, wie Umgang mit Dienst-E-Mail-Zugängen oder den Zugriff auf Patientendaten im Notfall, bis zu unzulässigen Regelungen zur Passwortverwendung und -gültigkeit.

Ein Krankenhaus bearbeitet ein komplexes Feld an Vorgängen, die täglich anfallen. Unter diesen Vorgängen stachen vor allen Dingen einige Probleme hervor, die regelmäßig in vielen Krankenhäusern auftraten. So war zu beobachten, dass sowohl die Ärzte, die Pfleger wie auch das Kostenabrechnungspersonal sehr weitgehende Rechte zur Einsicht in die elektronische Patientenakte hatten. Hier forderte der TLfDI eine Überarbeitung der Zugriffsrechte. Ärzte und Pflegepersonal dürfen grundsätzlich nur auf Patientenakten zugreifen, an deren Behandlung sie auch beteiligt sind. Zu weit reichende Zugriffsrechte können einen Verstoß gegen § 203 Strafgesetzbuch (ärztliche Schweigepflicht) darstellen. Beim Abrechnungspersonal ist die Lage bezüglich der Notwendigkeit der Zugriffe komplizierter – hier ist der TLfDI noch in Diskussion mit den Krankenhäusern. Insgesamt dauert die Umstellung der Zugriffsrechte in den Krankenhäusern noch an, wurde aber durch die Kontrolle des TLfDI angestoßen. Hier muss insbesondere die Gesundheit der Patienten im Vordergrund stehen, was allerdings keinen Freibrief für einen umfassenden Zugriff aller Ärzte darstellt. Eine Möglichkeit der Sicherstellung sowohl der Patientensicherheit als auch der datenschutzrechtlichen Zugriffe auf Patientendaten ist der so genannte Notfallzugriff. Hier kann der Arzt sich über bestehende Zugriffsschranken hinwegsetzen und die Daten dennoch einsehen. Um dies zu tun, muss er allerdings eine Begründung im System hinterlegen, und der Zugriff muss protokolliert werden. Auch dieser Punkt ist noch nicht in allen Krankenhäusern abschließend umgesetzt. So fordert die oben genannte Orientierungshilfe auch insgesamt eine umfassende Protokollierung der Zugriffe auf Patientendaten und deren regelmäßige, stichprobenhafte oder anlassbezogene Auswertung, um Missbrauch zu erschweren. Oft setzt hier die eingesetzte Software dem Krankenhaus Schranken, und die Softwareanbieter sind hier in der Pflicht,

ihre Software entsprechend den datenschutzrechtlichen Anforderungen anzupassen – ein nicht unerheblicher Aufwand und häufig auch Neuland für die Kliniken und Softwarehersteller.

Gleichfalls gibt es von den Softwareherstellern verursachte, ganz grundlegende Probleme. So sind z. B. in den derzeit sechs kontrollierten Krankenhäusern fünf verschiedene Krankenhausinformationssysteme im Einsatz, wobei nur eines dieser Systeme in der Lage ist, Daten entsprechend den gesetzlich vorgeschriebenen Löschrufen auch tatsächlich zu löschen. So fordert der Gesetzgeber beispielsweise, dass Patientendaten nach spätestens 30 Jahren (für einige Daten auch weniger) gelöscht oder anonymisiert werden müssen. Meist besteht die Möglichkeit, Daten zu sperren, um sie vor unberechtigtem Zugriff zu schützen, aber auch dieser Vorgang ist umständlich und noch nicht im notwendigen Maß automatisiert. Auch an dieser Stelle haben die Softwarehersteller in den nächsten Jahren noch Nachholbedarf, die Sperrfunktion im benötigten Umfang komfortabel und datenschutzrechtskonform in ihre Systeme zu integrieren.

Viele organisatorische Mängel konnten bereits beseitigt werden. Die Krankenhäuser sind sich der datenschutzrechtlichen Situation bewusst und sehr kooperativ. Der TLfDI wird entsprechend seiner Kontrollkompetenz weiterhin die Umsetzung der OH KIS fördern und deren datenschutzgerechte Umsetzung beobachten. Heilung ist in Sicht.

Gesundheitsdaten sind sensible personenbezogene Daten. Die Orientierungshilfe Krankenhausinformationssysteme bildet dabei eine gute Grundlage, Krankenhausinformationssysteme datenschutzgerechter zu gestalten und einzusetzen. Die stichpunktartigen Kontrollen ergaben bisher, dass dies aber ein zäher Prozess sowohl bei den Krankenhausbetreibern als auch bei den Herstellern von Krankenhausinformationssystemen ist.

11.19 AlertsNet: Bei Keimen im Blut fließen Daten gut!

Krankenhauskeime sind zunehmend eine echte Gefahr für Patienten, Angestellte und Besucher der Kliniken. Die Übersicht zu behalten, in welchen Stationen welche Keime auftreten, ist nicht immer einfach. Daher ist eine genaue Überwachung dieser Patienten wichtig, wenn ihre Infektion einmal erkannt wurde. Außerdem ist eine statistische Auswertung zur Qualitätssicherung, in welchen Teilen der Kliniken

welche Erreger vorkommen, für das Hygienemanagement der Klinik von Bedeutung. Auch der Vergleich zu anderen Kliniken ist hier für das Qualitätsmanagement der jeweiligen Klinik wichtig.

Das Projekt „AlertsNet“ des Universitätsklinikums Jena erfasst dazu thüringenweit Daten zu auftretenden Fällen von Krankenhauskeimen im Blut. Erhoben werden zum einen Laborbefunde von Blutuntersuchungen, die zuvor von den Laboren als infiziert eingestuft wurden. Im zweiten Schritt werden dann vom Universitätsklinikum zusätzliche Daten zum Betroffenen abgefragt, wie z. B. Name, Vorname, Geburtsdatum, Geschlecht, Krankenhausstation, Behandlungsfokus, Risikofaktoren wie Katheter oder Kanülen, Entlassungsstatus und Schweregrad der Infektion. AlertsNet will neben dem Erfassen von Diagnosen und deren statistischen Auswertungen auch Behandlungshinweise an die entsprechenden Ärzte geben. Ziel ist dabei, auch selten auftretende Infektionen durch das Expertenteam optimal zentral versorgen zu können.

Das System erhebt Gesundheitsdaten und damit besondere Arten von Daten, die vom Gesetz besonders geschützt sind, § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG). Auf das Universitätsklinikum Jena ist im vorliegenden Fall das BDSG anzuwenden, weil es als Krankenhaus am Wettbewerb teilnimmt, § 26 Thüringer Datenschutzgesetz. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nach § 4 Abs. 1 BDSG nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Die Datenerfassung basiert mangels Rechtsgrundlage auf der Einwilligung der betroffenen Person (Patient oder Angestellter). An die Einwilligung sind wegen der Verarbeitung von Gesundheitsdaten hohe Anforderungen zu stellen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform. Da besondere Arten personenbezogener Daten erhoben und verarbeitet werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 4a Abs. 3 BDSG.

Im Rahmen dieses Forschungsprojektes wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) um Stellungnahme zur Einwilligungserklärung sowie zu den Sicherheits- und Anonymisierungsmaßnahmen gebeten. Der TLfDI

wirkte darauf hin, dass die Einwilligungserklärung den gesetzlichen Anforderungen genüge. Im Hinblick auf die Sicherheits- und Anonymisierungsmaßnahmen sieht der TLfDI zwischen den Problemstellungen „statistische Auswertung“ und „Behandlungsvorschläge“ ein gewisses Spannungsfeld. Um nach der ersten Diagnose durch ein Labor auch alle weiteren Daten zu erfassen, muss dem System die betroffene Person zur korrekten Zuordnung bekannt sein. Ebenso muss auch für die Behandlungsvorschläge ein Ansprechpartner bekannt sein. Die Daten werden dazu pseudonymisiert in einer Datenbank gespeichert. Für die statistische Auswertung ist dagegen kein Personenbezug mehr notwendig. Dies bedeutet, dass der Personenbezug aus den gespeicherten Daten gelöscht werden muss, wenn er nicht mehr erforderlich ist. Da für die Nacherfassung und den Behandlungsvorschlag der sinnvoll nutzbare Zeitraum begrenzt ist, werden die personenbezogenen Daten nach sechs Wochen aus der Datenbank gelöscht und liegen dann nur noch in anonymisierter Form zur statistischen Auswertung und Qualitätskontrolle vor. Außerdem prüfte der TLfDI die technischen und organisatorischen Maßnahmen zum Schutz der Datenbank. Hier konnten keine Mängel festgestellt werden.

Die Datenerfassung bei dem Forschungsprojekt AlertsNet beruht auf Einwilligungsbasis. Die übermittelten Daten werden nach Ablauf von sechs Wochen anonymisiert. Das Forschungsprojekt hat frühzeitig die Philosophie der Datensparsamkeit gewählt und diese dadurch in der Programmierung der Software schon mit berücksichtigt.

11.20 Datenschutz vs. Auskunftsrecht

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil die Landesärztekammer Thüringen ihm eine Auskunft verweigere. Er hatte sich mit einer Beschwerde über einen Arzt dort gemeldet und wollte jetzt wissen, wie der Ausgang des Verfahrens war. Die Landesärztekammer teilte ihm mit, dass er aus Datenschutzgründen keine Auskunft erhalten werde.

Vor längerer Zeit hatte sich die Landesärztekammer Thüringen aufgrund der Beschwerde eines Rechtsanwaltes eines Arztes intensiv mit der Fragestellung befasst, welche Informationen ein Beschwerdeführer im Rahmen eines berufsrechtlichen Verfahrens erhalten

darf. In diesem Zusammenhang hatte sich die Kammer auch an den TLfDI gewandt. Die datenschutzrechtliche Prüfung des TLfDI hatte zum Ergebnis, dass das berufsrechtliche Verfahren nach dem Thüringer Heilberufegesetz (ThürHeilBG) als kammerinternes Verfahren ausgestaltet ist und eine Rechtsgrundlage für eine Information an den Beschwerdeführer nicht gegeben ist. Nach § 4 Abs. 1 Thüringer Datenschutzgesetz bedarf nämlich eine Datenübermittlung an den Beschwerdeführer entweder einer gesetzlichen Vorschrift oder der Einwilligung des Betroffenen. Daher kann der Beschwerdeführer lediglich über den Verfahrensstand informiert werden, eine Mitteilung des Ergebnisses des berufsrechtlichen Verfahrens muss aus datenschutzrechtlichen Gründen unterbleiben. Diese Auffassung wird auch von der Rechtsprechung bestätigt. So hat das OVG Lüneburg mit Beschluss vom 29. Januar 2008, Az.: 11 LA 448/07, ausdrücklich festgestellt, dass der Beschwerdeführer nur darüber unterrichtet wird, dass eine berufsrechtliche Prüfung stattfindet. Die Landesärztekammer hatte daher zu Recht auf den Datenschutz verwiesen. Dies wurde dem Beschwerdeführer mitgeteilt.

In berufsrechtlichen Verfahren nach dem ThürHeilBG hat derjenige, der das Verfahren durch seine Beschwerde angestoßen hatte, nur Anspruch auf die Auskunft, dass eine berufsrechtliche Prüfung stattfindet, nicht aber auf das Ergebnis der Prüfung.

11.21 Datenerhebung der Gemeinsamen Prüfungseinrichtung bei Thüringer Ärzten

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bekannt, dass die Gemeinsame Prüfungseinrichtung der Ärzte und Krankenkassen in Thüringen die Übermittlung von Diagnosen und weiterer Angaben zu Krankheiten verlangt, wenn an Ärzte Prüfaufträge gerichtet werden. Die Erhebung dieser Daten seitens der Gemeinsamen Prüfungseinrichtung erfasste dabei auch Gesundheitsdaten der Patienten. Der TLfDI wandte sich an die Gemeinsame Prüfeinrichtung und bat diese, mitzuteilen, auf welcher Rechtsgrundlage diese Datenerhebung erfolgte und welche technisch-organisatorischen Maßnahmen zum Schutz dieser Daten getroffen worden sind.

Die Gemeinsame Prüfeinrichtung ließ wissen, dass die von Kassenärztlicher Vereinigung und Krankenkassen getragenen Prüfungsein-

richtungen (Prüfungsstelle und – für Widerspruchsverfahren – der Beschwerdeausschuss) den in § 106 Sozialgesetzbuch (SGB) Fünftes Buch (V) normierten Auftrag durch Beratungen und Prüfungen erfüllen. Die Wirtschaftlichkeitsprüfung der Vertragsärzte umfasse im Wesentlichen drei Konstellationen, die sich unmittelbar aus dem Gesetz ergäben:

Die Auffälligkeitsprüfung nach § 106 Abs. 2 Nr. 1 SGB V, die auf einer statistischen Überschreitung von Verordnungssummandaten beruht, die Zufälligkeitsprüfung nach § 106 Abs. 2 Nr. 2 SGB V, in die je Quartal zwei vom Hundert der Vertragsärzte für den Zeitraum von vier aufeinanderfolgenden Quartalen einbezogen werden sollen und die auf der Basis von arzt- und versichertenbezogenen Stichproben stattfindet sowie die Einzelfallprüfung nach § 106 Abs. 3 Satz 3 i. V. m. § 11 der Thüringer Prüfvereinbarung. In allen Konstellationen könne es möglich sein, dass die Prüfungsstelle oder auch der Beschwerdeausschuss Diagnosedaten oder weitere Begleitumstände ärztlicher Therapien zu den von einem Prüfverfahren Betroffenen abfordere oder hinterfrage. Die Diagnosedaten seien insbesondere für die Zufälligkeitsprüfung erforderlich, da hier gemäß § 106 Abs. 2a SGB V die medizinische Notwendigkeit ebenso zu beurteilen sei wie die Eignung der Behandlung zur Erreichung des therapeutischen Ziels. Ob eine ärztliche Leistung bzw. Verordnung angemessen, zweckmäßig und effektiv ist, lasse sich nur dann beurteilen, wenn die Indikation und damit auch die Diagnose feststehen.

Im Regelfall prüfe die Prüfungsstelle auf der Grundlage der von der Kassenärztlichen Vereinigung und den Krankenkassen übermittelten Daten. Nur in den Fällen, in denen die regelhaften Datenlieferungen Unklarheiten durch unsachgemäße oder ungenaue Kodierung von Diagnosen, fehlende Diagnosen oder sonstige Unplausibilität der Behandlung (Diagnose passt nicht zur Verordnung) erkennen ließen, fragten die Prüfungsgremien konkret den Arzt nach den patientenindividuellen Behandlungsumständen. Die Mitarbeiter der Prüfungsstelle seien ebenso wie die Mitglieder des Beschwerdeausschusses schriftlich zur Einhaltung des Datenschutzes verpflichtet. Es wurde eine Datenschutzdienstanleitung und eine IT-Sicherheitsrichtlinie übermittelt.

Der TLfDI wies in diesem Zusammenhang darauf hin, dass zwar die gesetzliche Regelung des § 106 SGB V i. V. m. §§ 296, 298 SGB V die Übermittlung von Versichertendaten durch kassenärztliche Vereinigungen bzw. die Krankenkassen vorsehe. Eine Übermitt-

lungsbefugnis der Ärzte an die Gemeinsame Prüfeinrichtung gebe es im Gesetz aber nicht. Auch der vorgelegten Prüfvereinbarung zwischen der kassenärztlichen Vereinigung Thüringen und den Landesverbänden der Krankenkassen konnte eine derartige Übermittlungsbefugnis bzw. -pflicht nicht entnommen werden. Die Gemeinsame Prüfeinrichtung wurde daher zunächst gebeten, künftig in Fällen, in denen die regelhaften Datenlieferungen der kassenärztlichen Vereinigung oder der Krankenkassen Unklarheiten durch unsachgemäße oder ungenaue Codierung von Diagnosen, fehlende Diagnosen oder sonstige Unplausibilitäten der Behandlung erkennen lassen, streng nach dem gesetzlich vorgesehenen Verfahren vorzugehen und diese Daten nur bei den kassenärztlichen Vereinigungen bzw. bei den Krankenkassen zu erheben. Der TLfDI bezog in die Prüfung mit ein, dass die Rechtsprechung (Urteil des LSG Nordrhein-Westfalen vom 14. Dezember 2011 [L11 KA 75/10]; Urteil des BSG vom 13. August 2014 [B 6 KA 41113 R]) eine besondere Mitwirkungspflicht des Vertragsarztes im Wirtschaftlichkeitsprüfverfahren postuliert hat. Außerdem sollte nach der Gesetzesbegründung (Bundestags-Drucksache 12/5187) klargestellt werden, dass der behandelnde Vertragsarzt verpflichtet ist, die im Rahmen von Prüfverfahren notwendigen Unterlagen mit versichertenbezogenen Angaben zu offenbaren und er insofern von seiner Schweigepflicht entbunden ist. Der Gesetzeswortlaut wurde rechtsprechungskonform ausgelegt. Danach bestand eine besondere Mitwirkungspflicht des Vertragsarztes im Wirtschaftlichkeitsprüfverfahren nach § 106 SGB V und der TLfDI sah die Angelegenheit als erledigt an.

Grundsätzlich dürfen auch bei Verfahren nach dem SGB Daten nur verarbeitet werden, wenn die einschlägige gesetzliche Ermächtigungsgrundlage dies vorsieht. Es kommt allerdings vor, dass bestimmte Verfahrensweisen, die sich aus dem Gesetz nicht eindeutig ergeben, durch die Rechtsprechung für zulässig erachtet werden, weil sie das Gesetz unter Berücksichtigung des Willens des Gesetzgebers auslegt.

11.22 Spender-Anamnesebogen für Angehörige von Organspendern

Ein Transplantationsbeauftragter bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um

Hilfe. Seine Aufgabe besteht beispielsweise darin, potentielle Organspender zu identifizieren, die Hirndiagnostik mit durchzuführen und die notwendigen Gespräche mit den Angehörigen im Falle einer Organspende zu führen. Der Transplantationsbeauftragte wünschte eine datenschutzrechtliche Überprüfung eines Spender-Anamnesebogens, der den Angehörigen des verstorbenen Organspenders mit der Bitte um Beantwortung vorgelegt wird. Dieser von der Deutschen Stiftung für Organtransplantation erstellte Spender-Anamnesebogen hat zum Ziel, anamnesische Angaben, also die gesundheitliche Vorgeschichte des Verstorbenen, durch die Befragung der Angehörigen zu erhalten. Wie der TLfDI bei der Prüfung des Bogens feststellen konnte, enthält dieser nicht nur gesundheitliche Fragen zum Organspender, sondern auch die Angabe, ob dieser einer Risikogruppe für AIDS und Hepatitis angehörte und falls ja, welcher. Im Ergebnis gelangte der TLfDI zur Überzeugung, dass sich im Hinblick auf die Anamnese sowie die Lebensumstände des verstorbenen Organspenders die datenschutzrechtlichen Interessen des Verstorbenen und seiner Angehörigen mit denjenigen des potenziellen Organempfängers, der ein schutzwürdiges Interesse daran hat, sein Gesundheitsrisiko durch den Erhalt des Spenderorganes möglichst gering zu halten, widerstritten. Hierbei ist zu berücksichtigen, dass sich Angehörige von Verstorbenen nach der Rechtsprechung nur in sehr geringem Maße auf deren Grundrecht auf informationelle Selbstbestimmung berufen können (siehe BVerfGE 30, 173 (196)). Zum anderen ist das Recht auf körperliche Unversehrtheit (Artikel 2 Abs. 2 des Grundgesetzes) derjenigen, die ein Spenderorgan erhalten sollen, hoch zu bewerten. Der TLfDI hat daher keine grundsätzlichen datenschutzrechtlichen Bedenken gesehen, wenn bestimmte Daten abgefragt werden, die erforderlich sind, um in Erfahrung zu bringen, ob das Spenderorgan für die Transplantation geeignet ist oder nicht.

Der Spender-Anamnesebogen, der den Angehörigen eines verstorbenen Organspenders zur Beantwortung vorgelegt wird, enthält eine Reihe von besonders schutzwürdigen Arten personenbezogener Daten sowohl hinsichtlich des Gesundheitszustandes als auch der ehemaligen Lebensumstände. Insgesamt überwiegt das Recht auf körperliche Unversehrtheit des möglichen Organempfängers das datenschutzrechtliche Interesse des Verstorbenen und seiner Angehörigen,

sodass gegen die Datenerhebung keine durchgreifenden Bedenken geltend gemacht werden.

11.23 ARMIN soll Patienten schützen

Für die AOK Plus ist eigentlich der Sächsische Datenschutzbeauftragte die zuständige Aufsichtsbehörde. Gleichwohl wandte sich die Krankenkasse an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Hintergrund war folgender:

Die Krankenkassen und ihre Verbände können im Rahmen ihrer gesetzlichen Aufgabenstellung zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung Modellvorhaben zur Weiterentwicklung der Verfahrens-, Organisations-, Finanzierungs- und Vergütungsformen der Leistungserbringung durchführen, § 63 Sozialgesetzbuch (SGB) Fünftes Buch (V). Die AOK Plus wollte das Modellprojekt „Arzneimittelinitiative Sachsen-Thüringen“ (ARMIN) initiieren und band den TLfDI frühzeitig ein. Selbstverständlich stimmte sich der TLfDI auch mit dem Sächsischen Datenschutzbeauftragten ab.

Kern des Modells ist ein von Arzt und Apotheker gemeinsam durchgeführtes Medikationsmanagement für Versicherte dieser Krankenkasse, die von so genannter Multimedikation betroffen sind. Hiervon spricht man, wenn eine Vielzahl verschiedener Medikamente eingenommen werden muss. Zwar ist der TLfDI nicht für die datenschutzrechtliche Aufsicht über die AOK Plus zuständig, wohl aber für die Ärzte und Apotheken in Thüringen. Daher war auch eine Abstimmung mit dem TLfDI notwendig.

Das Modellprojekt sieht vor, einen elektronischen Medikationsplan mittels eines Medikationsplanservers bereitzustellen, der Transparenz über das Verordnungsgeschehen herstellt. Damit soll die Arzneimitteltherapiesicherheit verbessert werden. Es kann beispielsweise verhindert werden, dass zwei Ärzte Medikamente verschreiben, die sich nicht miteinander vertragen.

Nach Auffassung des TLfDI ist ein derartiges Projekt nur möglich, wenn eine wirksame Einwilligung des Patienten vorliegt. Nach § 4a BDSG ist der Betroffene auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist

außerdem nur wirksam, wenn sie auf dessen freier Entscheidung beruht. Die Einwilligung bedarf der Schriftform.

Der Versicherte entscheidet sich für die Betreuung durch einen an ARMIN teilnehmenden Arzt und eine an ARMIN teilnehmende Apotheke seiner Wahl. Die Teilnahme an ARMIN ist freiwillig. Teilnahmeberechtigt sind Versicherte der AOK PLUS, sofern sie das 18. Lebensjahr vollendet haben, mittels schriftlicher Erklärung in die Bedingungen des Vertrages einwilligen, nicht dauerhaft in Pflegeeinrichtungen stationär betreut werden und gleichzeitig eine Arzneimitteltherapie mit mindestens fünf Wirkstoffen erhalten.

Personenbezogene Daten werden im Rahmen des Medikationsmanagements dezentral beim behandelnden Arzt und Apotheker erhoben, gespeichert, verarbeitet und genutzt. Hierbei finden die Bestimmungen des Bundesdatenschutzgesetzes Anwendung. Die Einwilligungserklärung wurde mit dem TLfDI abgestimmt. Mit der Einwilligungserklärung räumt der Versicherte seinem gewählten Arzt und Apotheker Zugriff auf seine personenbezogenen Arzneimittelverordnungsdaten der letzten sechs Monate ein. Der Arzt und der Apotheker können diese Angaben nötigenfalls ergänzen, beispielsweise um bestimmte Unverträglichkeiten. Es können auch weitere verordnete Arzneimittel oder solche Mittel mit aufgenommen werden, die der Patient selbst erworben hat.

An dem Modellprojekt teilnehmende Ärzte und Apotheker verpflichten sich bei ihrer Teilnahme, bestimmte technische Mindestanforderungen zu erfüllen, welche neben der Sicherstellung der erforderlichen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes einzuhalten sind. Hierzu zählt u. a. die Verwendung einer vertragskonformen Software. Dabei ist die Vertragskonformität mit einer Zertifizierung nachzuweisen. Mit der Einwilligung erlaubt der Teilnehmer dem Arzt und Apotheker untereinander den Austausch der für die Betreuung erforderlichen Medikationsdaten. Die Medikationspläne werden zwischen Arzt und Apotheker über einen extern gesicherten Server im Netz der Krankenversicherungen, über das bereits die ärztliche Abrechnung läuft, ausgetauscht. Die AOK PLUS kann nach ihren Angaben zu keinem Zeitpunkt die Daten auf dem Medikationsplanserver einsehen.

Der TLfDI wies darauf hin, dass der Versicherte nach § 34 BDSG gegenüber den Ärzten und Apothekern Auskunftsrechte zu den zu ihm gespeicherten personenbezogenen Daten innehat. Die Teilnahme

am Modellprojekt kann gegenüber der AOK PLUS auch wieder gekündigt werden.

Der TLfDI wird das Verfahren weiterhin gemeinsam mit dem Sächsischen Datenschutzbeauftragten begleiten und gegebenenfalls die Einhaltung der schriftlich fixierten Vorgaben vor Ort prüfen.

Wenn die Krankenkassen Modellvorhaben zur Verbesserung der Qualität und der Wirtschaftlichkeit der medizinischen Versorgung durchführen, betrifft dies oftmals auch die Verarbeitung personenbezogener Daten. Es ist ratsam die erforderlichen technischen und organisatorischen Maßnahmen frühzeitig mit dem TLfDI abzustimmen.

11.24 Einsichtnahme in Todesbescheinigungen für eine wissenschaftliche Studie

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom damaligen Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) gebeten, aus datenschutzrechtlicher Sicht zu einer im Universitätsklinikum der Friedrich-Schiller-Universität Jena durchgeführten Studie Stellung zu nehmen. Im Rahmen dieser Studie wollte das Universitätsklinikum die Todesursachen von verstorbenen Patienten, die zuvor an dieser Studie teilgenommen hatten, einer wissenschaftlichen Untersuchung unterziehen. Der TLfDI verwies in seiner Stellungnahme an das TMSFG auf § 15 Abs. 4 Thüringer Bestattungsgesetz (ThürBestG), in dem festgelegt ist, unter welchen Voraussetzungen die für den Wohnort des Verstorbenen zuständige untere Gesundheitsbehörde auf Antrag Auskünfte aus Totenscheinen erteilen kann. Sofern das TMSFG nach § 15 Abs. 4 Satz 1 Nr. 2 Buchstabe b) ThürBestG nicht feststellte, dass ein öffentliches Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, wofür nach dem Dafürhalten des TLfDI nach dem Vorbringen des Universitätsklinikums einiges sprach, kam nur der Erlaubnistatbestand des § 15 Abs. 4 Satz 1 Nr. 1 ThürBestG in Betracht. Danach kann der Antragsteller auf Antrag Auskunft aus Toten- und Sektionsscheinen bekommen, wenn er ein berechtigtes Interesse glaubhaft macht und kein Grund zu der Annahme besteht,

dass durch die Offenbarung schutzwürdige Belange des Verstorbenen oder seiner Angehörigen beeinträchtigt werden. Im vorliegenden Fall wurde nach Auffassung des TLfDI jedoch Auskunft aus einem wissenschaftlichen Interesse heraus begehrt. § 15 Abs. 4 Satz 1 Nr. 2 ThürBestG gestattet unter bestimmten Voraussetzungen die wissenschaftliche Auswertung der bei der für den Wohnort zuständigen unteren Gesundheitsbehörde verwahrten Daten. Die Verwendung von personenbezogenen Daten ohne sofortige Anonymisierung oder Pseudonymisierung bedarf auch nach der Gesetzesbegründung (Landtagsdrucksache 3/3937, S. 33 zu § 15) der Genehmigung des für das Gesundheitswesen zuständigen Ministeriums. Sie darf nur erteilt werden, wenn an dem Forschungsvorhaben ein erhebliches Interesse der Allgemeinheit besteht. Diese gesetzliche Voraussetzung sollte nicht durch eine Anwendung von § 15 Abs. 4 Nr. 1 ThürBestG umgangen werden. Ob die Voraussetzungen des § 15 Abs. 4 Satz 1 Nr. 2 Buchstabe b) ThürBestG vorlagen, unterlag letztlich der fachlichen Entscheidung durch das TMSFG.

Die Auskunft aus Toten- und Sektionsscheinen ist spezialgesetzlich in § 15 des Thüringer Bestattungsgesetzes geregelt. Entweder muss ein Antragsteller bei der für den Wohnort des Verstorbenen zuständigen Gesundheitsbehörde ein berechtigtes Interesse glaubhaft machen und es darf kein Grund zu der Annahme bestehen, dass durch die Offenbarung schutzwürdige Belange des Verstorbenen oder seiner Angehörigen beeinträchtigt werden, oder die Angaben werden für ein wissenschaftliches Vorhaben benötigt. In diesem Fall muss entweder durch sofortige Anonymisierung oder Pseudonymisierung der Angaben sichergestellt werden, dass schutzwürdige Belange des Verstorbenen und seiner Angehörigen nicht beeinträchtigt werden, oder das für das Gesundheitswesen zuständige Ministerium muss feststellen, dass das öffentliche Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Bei einem wissenschaftlichen Vorhaben sollte stets das hier zuständige Ministerium das Vorliegen eines überwiegenden öffentlichen Interesses prüfen und die Auskunft bzw. Einsicht letztlich auf dieser Grundlage erfolgen.

11.25 Grenzenlose Datenerhebung bei Einschulungsuntersuchungen des Kinder- und Jugendärztlichen Dienstes der Gesundheitsämter?

Das Thüringer Landesverwaltungsamt (TLVwA) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Prüfung, ob aus datenschutzrechtlicher Sicht im Rahmen der obligatorischen Einschulungsuntersuchung in Thüringen zukünftig zusätzlich der Parameter „Migrationshintergrund“ erhoben werden darf. Hierzu wurde dem TLfDI ein zum Thüringer Anamnese-Erhebungsbogen zur Einschulungsuntersuchung zusätzlicher Fragebogen zur Erfassung des Migrationshintergrunds vorgelegt, in dem beide Elternteile danach befragt werden, in welchem Land sie geboren wurden, welche Staatsangehörigkeit sie derzeit besitzen und ob ihr Kind in Deutschland geboren wurde. Der TLfDI hatte sich in der Vergangenheit aufgrund von Bürgereingaben bereits mit der Frage auseinandergesetzt, welche personenbezogenen Angaben über das einzuschulende Kind und dessen Eltern erfragt werden dürfen. Die hierbei einschlägigen Rechtsvorschriften enthalten weder einen Musterfragebogen noch einen abschließenden Datenkatalog. Der TLfDI hatte die datenschutzrechtliche Zulässigkeit einer Erweiterung des bisherigen Fragebogens um eine „einheitliche Erfassung des Migrationshintergrundes“ anhand der vorhandenen Rechtsvorschriften in diesem Bereich zu prüfen. Nach § 8 Abs. 1 der Thüringer Verordnung über die Schulgesundheitspflege (ThürSchulGespfVO) darf das Gesundheitsamt zur Erfüllung der ihm aufgrund dieser Verordnung zugewiesenen Aufgaben die dafür erforderlichen Daten verarbeiten und nutzen. Diese Aufgaben sind insbesondere in den in § 1 ThürSchulGespfVO aufgeführten Grundsätzen allgemein beschrieben. Diesen Regelungen ist nicht unmittelbar zu entnehmen, ob die Erfassung des Migrationshintergrundes in diesem Sinne für die Aufgabenerfüllung der Gesundheitsämter erforderlich ist. Es gibt hierzu lediglich eine Empfehlung einer Arbeitsgruppe innerhalb der Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden. Danach ist die Erfassung des Migrationshintergrundes bei der Einschulungsuntersuchung aus gesundheitspolitischer Sicht bedeutsam. Eine Rechtsgrundlage, aus der sich die Zulässigkeit der Verarbeitung dieser Daten ergibt, ist dies jedoch nicht. Der TLfDI hat dem TLVwA als Ergebnis seiner datenschutzrechtlichen Prüfung mitgeteilt, dass eine zusätzliche Erfassung des Migrationshintergrundes bei

den betroffenen Eltern nur dann zulässig ist, wenn die betreffenden Fragen auf dem Bogen eindeutig als freiwillig gekennzeichnet werden und die Eltern gemäß § 4 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG) auf den Zweck, den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung ihrer Daten sowie auf ihre Rechte auf Auskunftserteilung, Berichtigung und Löschung hingewiesen werden. Daraufhin erweiterte das TLVwA seine Anfrage dahingehend, ob der TLfDI grundsätzlich datenschutzrechtliche Bedenken gegen eine Erfassung des Migrationshintergrunds im Rahmen der Vorsorgeuntersuchungen des öffentlichen Gesundheitsdienstes – gemeint sind die anderen Kindertagesstätten- und Schuluntersuchungen, die in Thüringen durchgeführt werden – und die Übermittlung entsprechend aggregierter Daten an die Landesbehörden hat. Der TLfDI verwies in seiner erneuten Antwort wiederum auf die Problematik, dass es, wie vom TLVwA dargestellt, wohl fachliche Gründe für eine Erfassung dieser Daten gebe, eine ausdrückliche Rechtsvorschrift die Verarbeitung und Nutzung dieser personenbezogenen Daten jedoch nicht erlaubt oder anordnet. Soweit die Verarbeitung und Nutzung dieser Daten im Sinne von § 4 Abs. 1 Satz 2 ThürDSG „zur Erfüllung anerkannter Zwecke erforderlich ist“, besteht nach der gegebenen Rechtslage in diesen Fällen ausschließlich die Möglichkeit, bei den Eltern Daten zum Migrationshintergrund auf freiwilliger Basis entsprechend der oben dargestellten Verfahrensweise zu erheben. Gegen eine Übermittlung dieser auf freiwilliger Basis erhobenen Daten in aggregierter Form, die dann nicht mehr personenbezogen sind, bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Wann der Zusatzfragebogen bei der Einschulungsuntersuchung eingeführt wird, ist dem TLfDI noch nicht bekannt.

Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist. Die Erforderlichkeit muss sich vorliegend aus den Regelungen der ThürSchulGespfVO ergeben. Da diese Verordnung die betroffenen Eltern weder zur Auskunft über ihren Migrationshintergrund verpflichtet oder die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen ist, sind die Eltern auf die Freiwilligkeit ihrer Angaben hinzuweisen.

11.26 Datenbohrung bei der Kassenzahnärztlichen Vereinigung Thüringen

Ein Bürger wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ihm die Kassenzahnärztliche Vereinigung Thüringen auf seine bereits vor geraumer Zeit gestellte Frage, wie lange (Vergangenheit und Zukunft) die Daten über die zahnärztlichen Leistungen gespeichert werden, keine Antwort erteilt habe.

Da eine Auskunftsverweigerung im Raum stand, wandte sich der TLfDI an die Kassenzahnärztliche Vereinigung und bat unter Darlegung der Rechtslage um Mitteilung, weshalb denn der Beschwerdeführer keine Antwort erhielt. Der Auskunftsanspruch des Beschwerdeführers richtete sich nach § 83 Abs. 1 Sozialgesetzbuch (SGB) Zehntes Buch (X). Danach ist dem Betroffenen auf Antrag Auskunft zu erteilen über die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten bezieht, über die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und über den Zweck der Speicherung. Die Dauer der Speicherung ist zwar im Gesetz nicht genannt. Durch die Art der Auskunft muss der Betroffene jedoch in die Lage versetzt werden, zumindest in groben Zügen den Verwendungszusammenhang seiner Sozialdaten nachzuvollziehen und dessen Bedeutung bewerten zu können. Hierzu gehört nach Auffassung des TLfDI auch die Speicherdauer.

Die Kassenzahnärztliche Vereinigung teilte dem TLfDI mit, nach ihrem Dafürhalten habe sie dem Beschwerdeführer vollumfänglich die möglichen Auskünfte erteilt. Nachdem nämlich erst zu klären war, auf welcher konkreten Rechtsgrundlage der Beschwerdeführer Auskünfte verlangte (§ 83 SGB X oder § 305 SGB V), sei man zu dem Schluss gekommen, dass ein über die erteilte Auskunft hinausgehendes Informationsinteresse des Beschwerdeführers nicht zu erkennen und auch nicht über § 83 SGB X als Anspruchsgrundlage gedeckt sei. Die Fragestellung nach den Aufbewahrungszeiten von vertragszahnärztlichen Leistungen sei so allgemein gehalten, dass dem Erfordernis der genauen Bezeichnung seitens des Beschwerdeführers nicht nachgekommen worden sei. Hinsichtlich der Speicherung der Daten in der Vergangenheit und Zukunft sei die Anfrage zu unkonkret, sodass hierauf keine Auskunft gegeben werden konnte.

Im Übrigen könne nicht verbindlich beantwortet werden, wie lange in der Zukunft etwas gespeichert werde.

Das überzeugte den TLfDI nicht. Er teilte der Kassenzahnärztlichen Vereinigung mit, dass er nach wie vor die Dauer der Speicherung der Daten über Kassenzahnärztliche Leistungen vom Auskunftsrecht nach § 83 Abs. 1 SGB X umfasst ansehe. Da die Speicherdauer von zahnärztlichen Leistungen festzulegen bzw. gesetzlich festgelegt ist, war nicht nachvollziehbar, weshalb dies denn dem Beschwerdeführer nicht mitgeteilt werden könne. Daraufhin gab die Kassenzahnärztliche Vereinigung ihre Position auf und teilte dem Beschwerdeführer mit, dass sie zur Erfüllung ihrer Aufgaben Abrechnungsdaten zu zahnärztlichen Leistungen sechs Jahre verarbeitungsfähig vorhalte. Darüber hinaus würden bis zur Dauer von zehn Jahren komprimierte Daten zum Zweck der Datensicherung vorgehalten, um entsprechende Auswertungen für die Versorgungssituation in Thüringen vornehmen zu können. Hierbei werde jedoch eine Zuordnung von Daten zu Personen nicht mehr vorgenommen.

Der Beschwerdeführer bedankte sich, dass er letztendlich durch die Intervention des TLfDI zu der begehrten Auskunft über die Speicherdauer kam.

Eine Auskunft nach § 83 SGB X umfasst die zu einer Person gespeicherten Sozialdaten, deren Herkunft und die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, sowie den Zweck der Speicherung. Damit der Betroffene in die Lage versetzt wird, zumindest in groben Zügen den Verwendungszusammenhang seiner Sozialdaten nachzuvollziehen und dessen Bedeutung bewerten zu können, umfasst die Auskunft auch die Speicherdauer.

11.27 Auch zukünftig nur anonyme Daten für die Bundesärztestatistik

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde informiert, dass die Landesärztekammern zukünftig personenbezogene Daten von Ärzten als Einzeldatensätze an die Bundesärztekammer liefern sollen. Dies wäre ein Bruch mit der gegenwärtigen Praxis, bei der Arztdaten nur in aggregierter Form an die Bundesärztekammer fließen und somit kein Bezug zur Einzelperson hergestellt werden kann. Um hier Klärung im Interesse der vielen Thüringer Ärztinnen und Ärzte zu schaffen, die

ja Betroffene nach § 3 Abs. 1 Thüringer Datenschutzgesetz sind, bat der TLfDI die Thüringer Landesärztekammer um Stellungnahme. Dabei vertrat der TLfDI die Rechtsauffassung, dass für eine Weitergabe von personenbezogenen Daten an die Bundesärztekammer keine Rechtsgrundlage bestehe und somit eine Einwilligung des Betroffenen erforderlich wäre. Die Thüringer Landesärztekammer antwortete prompt und stellte klar, dass sie an der bisherigen Verfahrensweise festhalten wolle. Die Rechtsauffassung des TLfDI werde vollumfänglich geteilt. Somit war klar, dass die personenbeziehbaren Daten der Thüringer Ärztinnen und Ärzte auch in Zukunft die Landesärztekammer nicht verlassen müssen, jedenfalls nicht, wenn hierfür keine Rechtsgrundlage besteht oder der Betroffene nicht wirksam eingewilligt hat.

Für statistische Zwecke sind anonymisierte Personendaten hinreichend. Eine Anonymisierung von Arztdaten, die von der Thüringer Landesärztekammer an die Bundesärztekammer geliefert werden, bleibt auch zukünftig gewährleistet. Der TLfDI konnte dies im Interesse der Thüringer Ärzteschaft klären und hat die Datenschutzbehörden des Bundes und der Länder über die Position der Landesärztekammer informiert.

11.28 Vertretung des Amtsarztes durch Private – die Zweite

Mit dem Thema der Vertretung des Amtsarztes durch private Ärzte beschäftigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in seinem 9. Tätigkeitsbericht (dort unter 11.5.). Damals wurde aufgrund einer Eingabe festgestellt, dass in einem Gesundheitsamt die schulzahnärztlichen Reihenuntersuchungen nicht nur von den Schulzahnärzten des Gesundheitsamts, sondern auch von privaten Zahnärzten durchgeführt wurden. Begründet worden war dies damit, dass die regulär beschäftigten Zahnärzte mehrwöchig arbeitsunfähig gewesen waren und die zahnärztliche Aufgabenerfüllung mit den angestellten Zahnärzten des Fachdienstes Gesundheit nicht mehr möglich gewesen war.

Dies begegnete nach Ansicht des TLfDI erheblichen datenschutzrechtlichen Bedenken. Nach § 55 Abs. 3 des Thüringer Schulgesetzes (ThürSchulG) sind die Schüler verpflichtet, sich den Maßnahmen des schulärztlichen und schulzahnärztlichen Dienstes zu unterziehen.

Bei einer Untersuchung durch den „Schul(zahn)arzt“ werden die Schüler nicht nur körperlich untersucht, es werden auch Gesundheitsdaten von ihnen erhoben. Eine zwangsweise Datenerhebung stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Dieser ist nur zulässig, wenn hierfür eine gesetzliche Grundlage besteht. Diese Grundlage ist in § 55 Abs. 3 ThürSchulG sowie in der nach § 55 Abs. 3 Satz 2 ThürSchulG erlassenen Rechtsverordnung zu sehen. Da § 1 Abs. 1 Satz 2 der Thüringer Verordnung über die Schulgesundheitspflege vorsieht, dass die Schulgesundheitspflege von den Schulärzten und Schulzahnärzten der Gesundheitsämter (schulärztlicher und schulzahnärztlicher Dienst) wahrgenommen wird, entspricht die Wahrnehmung dieser Aufgabe durch Private nicht den gesetzlichen Vorgaben. Vielmehr stellt die Schulgesundheitspflege eine hoheitliche Aufgabe dar, die nur durch einen Träger öffentlicher Gewalt wahrgenommen werden darf. Der TLfDI hatte dem damaligen Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) als oberste Aufsichtsbehörde seine Rechtsauffassung dargelegt und gebeten, die Gesundheitsämter in einem entsprechenden Rundschreiben über die Rechtslage aufzuklären. Außerdem sollte mitgeteilt werden, in welchen Gesundheitsämtern in Thüringen ebenfalls private Ärzte mit Aufgaben des schulärztlichen und schulzahnärztlichen Dienstes betraut sind.

Es stellte sich heraus, dass es an einigen Gesundheitsämtern in Thüringen üblich ist, Honorarärzte im schulärztlichen und schulzahnärztlichen Dienst zu beschäftigen. Grund dafür ist oftmals eine längere Krankheit oder Elternzeit des fest angestellten Arztes.

Der TLfDI hat gegenüber dem TMSFG mehrfach deutlich gemacht, dass eine derartige Situation nach seiner Rechtsauffassung mit der geltenden Rechtslage nicht vereinbar ist. Es wurde als unpraktikabel angesehen, im Vorfeld eine Einwilligung der Eltern zur Begutachtung des Kindes durch einen niedergelassenen Arzt einzuholen.

In dem Gesetzentwurf zur Änderung beamtenrechtlicher Vorschriften wurde das Problem aufgegriffen. § 33 Abs. 1 Thüringer Beamtengesetz regelt nun, dass angeordnete ärztliche Untersuchungen von den zuständigen Amtsärzten, beamteten Ärzten oder sonstigen von der zuständigen Stelle bestimmten Ärzten durchgeführt werden. Diese Bestimmung ist aber auf die Durchführung schulärztlicher Untersuchungen nicht direkt anwendbar, weil es sich hier nicht um angeordnete, sondern gesetzlich vorgesehene Untersuchungen han-

delt. So heißt es in der Gesetzesbegründung (Landtagsdrucksache 5/7453): „Absatz 1 regelt, welche Ärzte mit der Durchführung von Untersuchungen beauftragt werden dürfen. [...] Die Möglichkeit zur Bestellung eines anderen ärztlichen Gutachters durch spezialgesetzliche Regelungen bleibt davon unberührt.“

Der TLfDI verschließt sich nicht der Tatsache, dass im Einzelfall aufgrund von faktischen Problemen ein niedergelassener Arzt im schulärztlichen und schulzahnärztlichen Dienst einspringen muss. Diese Situation sollte aber die Ausnahme bleiben. Andernfalls muss es eine eindeutige gesetzliche Regelung geben, die zulässt, dass Aufgaben des schulärztlichen und schulzahnärztlichen Dienstes auch von anderen Ärzten durchgeführt werden können. Der TLfDI wird weiterhin mit dem nunmehr zuständigen Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie und den betroffenen Gesundheitsämtern auf eine gesetzeskonforme Lösung hinarbeiten.

Da die verpflichtend durchzuführenden Schuluntersuchungen einen Grundrechtseingriff sowohl in das Grundrecht auf körperliche Unversehrtheit als auch in das Grundrecht auf informationelle Selbstbestimmung darstellen, dürfen sie nach geltender Rechtslage nur von Trägern hoheitlicher Gewalt durchgeführt werden.

11.29 Klinisches Krebsregister Thüringen

Die Überlebenschancen und die Lebensqualität krebskranker Menschen haben sich in den letzten Jahrzehnten in Deutschland erheblich verbessert. Allerdings steigen die Neuerkrankungsraten. Das Bundesministerium für Gesundheit hat gemeinsam mit der Deutschen Krebsgesellschaft, der Deutschen Krebshilfe und der Arbeitsgemeinschaft Deutscher Tumorzentren am 16. Juni 2008 den Nationalen Krebsplan initiiert. Ein Ziel des Nationalen Krebsplanes ist die Schaffung einer aussagekräftigen onkologischen Qualitätsberichterstattung für Leistungserbringer (wie z. B. Krankenhäuser und ambulant behandelnde Ärzte), Entscheidungsträger und Patienten durch einen flächendeckenden Ausbau der klinischen Krebsregister. Diese Aufgabe wurde mit dem Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (Krebsfrüherkennungs- und -registergesetz – KFRG) in Angriff genommen. Nach § 65c Sozialgesetzbuch (SGB) Fünftes Buch (V) erfolgt die Einrichtung klinischer Krebsregister durch die Län-

der, wobei die Daten flächendeckend und möglichst vollzählig erfasst sowie jährlich landesbezogen ausgewertet werden sollen. Die notwendigen rechtlichen Regelungen für die Einrichtung und den Betrieb klinischer Krebsregister einschließlich der datenschutzrechtlichen Bestimmungen bleiben den Ländern vorbehalten.

Das ursprünglich zuständige Thüringer Ministerium für Soziales, Familie und Gesundheit trat bereits frühzeitig an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran, um datenschutzrechtliche Fragen zur Umsetzung des KFRG abzustimmen. In Thüringen stellt sich, wie in den meisten neuen Bundesländern, die Situation etwas anders dar als in den meisten westlichen Bundesländern. Hier gab es bereits gewachsene Strukturen der klinischen Krebsregistrierung. In Thüringen existieren fünf regionale Klinische Krebsregister an den fünf Tumorzentren Erfurt, Gera, Jena, Nordhausen und Suhl. Diese Strukturen allein erfüllen aber nicht die Aufgaben, die § 65c SGB V dem künftigen Klinischen Krebsregister Thüringen zuweist. Zum einen muss eine nahezu flächendeckende Registrierung sichergestellt werden, es müssen Auswertungen der landesweit vorliegenden Daten möglich sein und die Daten der einzelnen vorhandenen Register müssen miteinander abgeglichen werden können, um Doppel- und Fehlmeldungen zu vermeiden.

Es wurden Verhandlungen darüber geführt, welche Rolle die fünf regionalen Klinischen Krebsregister bei der Erfüllung der gesetzlichen Aufgaben spielen werden und wie im Verhältnis dazu ein zentrales Register ausgestaltet werden soll. Es ist der Grundsatz der Datensparsamkeit zu beachten, es dürfen möglichst keine Daten doppelt vorgehalten werden. Gleichzeitig müssen die Zugriffsrechte der einzelnen Beteiligten wegen der Sensibilität der im Register gespeicherten Gesundheitsdaten sehr trennscharf geregelt werden. Der Prozess ist noch nicht abgeschlossen. Die Anforderungen des § 65c SGB V müssen bis zum 1. Januar 2016 erfüllt sein, allerdings gilt eine Übergangsregelung bis einschließlich 2017 (siehe § 65c Abs. 4 SGB V).

Auch das für die Umsetzung des KFRG in Thüringen notwendige Gesetzgebungsverfahren muss bis dahin abgeschlossen sein. Der TLfDI wird dieses im Hinblick auf die zu schaffenden datenschutzrechtlichen Regelungen begleiten und über das Ergebnis im nächsten Tätigkeitsbericht informieren.

Die klinischen Krebsregister sollen bundesweit flächendeckend ausgebaut werden. In Thüringen ist ein Klinisches Krebsregister Thüringen zu schaffen. Es ist der Grundsatz der Datensparsamkeit zu beachten. Die Zugriffsrechte der einzelnen Beteiligten müssen wegen der Sensibilität der im Register gespeicherten Gesundheitsdaten sehr trennscharf geregelt werden. Die notwendigen Datenübermittlungen bedürfen einer landesgesetzlichen Regelung.

11.30 Ist die Arztqualifikation auch echt?

Sie kennen das sicher: Beim Besuch in der Arztpraxis hängen häufig Urkunden und Fortbildungszertifikate zu Qualifikationen oder zusätzlichen Spezialisierungen und Lehrgängen. Dadurch wird dem Patienten angezeigt, welche Leistungen in der Praxis qualifiziert durch den Arzt oder durch das medizinische Fachpersonal durchgeführt werden können. Doch woher weiß der Patient, dass ein solches Fortbildungszertifikat auch echt ist?



Um dem Bürger die Möglichkeit zu geben, dies schnell und einfach prüfen zu können, betreibt die Landesärztekammer Thüringen mit anderen Ärztekammern ein Online-Portal bei der Bundesärztekammer <https://www.kammerservice.de/>, mit welchem die Prüfung dieser Urkunden möglich ist. Dafür ist auf der Urkunde ein QR-Code

abgedruckt, der eine 64-stellige Zeichenfolge enthält. Diese Zeichenfolge ist die eindeutige Urkundennummer. Gibt man diese Zeichenfolge, welche man sich zuvor beim Arzt notiert oder etwa als Handfoto gespeichert hat, in dem o. g. Portal ein, werden die Daten, welche auf der Urkunde abgedruckt sind, auch online angezeigt. So kann die Urkunde auf Echtheit überprüft werden.

Um diese Überprüfung technisch zu ermöglichen, werden hierzu die Daten von Urkunden und Fortbildungszertifikaten dezentral in den jeweiligen Landesärztekammern vorgehalten. Das Online-Portal, welches über die Bundesärztekammer betrieben wird, leitet die elektronischen Anfragen an die zuständigen Ärztekammern weiter. Anhand des Codes erkennt das Portal die zuständige Landesärztekammer.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) informierte sich über die technische Si-

cherung der Zugänge, was insbesondere die Transportverschlüsselung vom Nutzer zum Portal-Server betraf. Außerdem wurde die Landesärztekammer Thüringen bezüglich der Bildungsvorschrift der Urkundennummer beraten. Hierbei war es vor allen Dingen wichtig, dass die Nummer, welche unter anderem aus dem Namen des Urkundeninhabers und weiteren Urkundendaten gebildet wird, nicht doppelt vorkommen darf, um die Eindeutigkeit der Urkunden zu gewährleisten. Hinsichtlich des Verfahrens in Thüringen steht der TLfDI mit der Landesärztekammer weiterhin in Kontakt, um die Sicherheit des Verfahrens abschließend beurteilen zu können. Das Verfahren selber befindet sich noch in der Testphase.

Wollen Bürger zukünftig die Echtheit einer Urkunde oder eines Fortbildungszertifikates vom Arzt- oder Medizinischem Fachpersonal prüfen, können sie diese über die Identifikationsnummer der Urkunde oder des Fortbildungszertifikates im Portal <https://www.kammerservice.de/> kontrollieren. Wurde ein entsprechendes echtes Dokument gefunden, wird dieses zum Vergleich mit den wichtigsten Daten angezeigt. Der TLfDI prüft den Verifikationsdienst noch, um die Sicherheit abschließend beurteilen zu können.



11.31 Elektronische Gesundheitskarte: runde Sache oder Runder Tisch?

Seit dem 1. Januar 2015 gilt bundesweit ausschließlich die elektronische Gesundheitskarte als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkasse beim Arzt oder Zahnarzt. Hierauf wies der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in seiner Pressemitteilung vom 5. Januar 2015 hin (s. <https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichu>



ngen/pmtlfdi/150105_pm-
gesundheitskarte.pdf). Für die Versicherten
brachte die Einführung zunächst keine gro-
ßen Änderungen mit sich, da auf der Karte
lediglich die Daten abgebildet waren, die
bislang auf der Krankenversichertenkarte
enthalten waren, sowie zusätzlich das Ge-
schlecht und ein Lichtbild des Versicherten.

Diese Daten (außer dem Lichtbild) sind
auch gemäß § 291 Abs. 2 Sozialgesetzbuch (SGB) Fünftes Buch (V)
auf dem Chip der Krankenversicherungskarte gespeichert. Der ge-
plante Onlineabgleich mit den gesetzlichen Krankenkassen sollte ab
Mitte 2015 in verschiedenen Testregionen erprobt werden, zu denen
Thüringen aber nicht zählte. Allerdings ist die elektronische Ge-
sundheitskarte (siehe dazu Nr. 15.8.) darauf ausgerichtet, künftig
zusätzliche Funktionen zu erfüllen, wie beispielsweise das so ge-
nannte E-Rezept und auf Wunsch des Patienten möglicherweise
Notfallversorgungsdaten, elektronische Arztbriefe oder persönliche
Arzneimittellrisiken und Unverträglichkeiten. Eine mögliche weitere
Entwicklung ist zudem der Zugriff auf die elektronische Patientenak-
te. Der TLfDI hat der Landesärztekammer Thüringen und der Lan-
desapothekerkammer Thüringen eine Gesprächsrunde angeboten,
sofern dort Fragen oder Anregungen zur elektronischen Gesund-
heitskarte bestehen. Diese Stellen wollten bei Bedarf auf das Ange-
bot zurückkommen.

Seit 29. Dezember 2015 ist das Gesetz für sichere digitale Kommu-
nikation und Anwendungen im Gesundheitswesen sowie zur Ände-
rung weiterer Gesetze (sog. E-Health-Gesetz) in Kraft (siehe dazu
Nr. 11.7.). Das Sozialgesetzbuch (SGB) Fünftes Buch (V) sieht be-
reits seit 2006 vor, dass auf der elektronischen Gesundheitskarte
unter anderem Notfalldaten, elektronische Arztbriefe, Daten eines
Medikationsplanes, eine elektronische Patientenakte und Erklärun-
gen des Versicherten zur Organspenden gespeichert werden können,
vgl. § 291a Abs. 3 SGB V. Damit allerdings all diese Funktionen der
elektronischen Gesundheitskarte auch genutzt werden können, muss
eine entsprechende Infrastruktur aufgebaut werden, die von allen
Ärzten, Kliniken und Apotheken bundesweit einheitlich genutzt
werden kann. Die verschiedenen Funktionen werden nun zehn Jahre
nach Planung der Gesundheitskarte erst sukzessive zur Verfügung
stehen. Das neue Gesetz stellt für verschiedene Funktionen in § 291b

SGB V einen Zeitplan bis zum 31. Dezember 2018 auf. Wer beruflich die Gesundheitskarte einsetzen muss, z. B. Ärzte, Kliniken und Apotheken, sollte sich daher gegebenenfalls vorab bei seinem Berufsverband informieren.

Das Gesprächsangebot des TLfDI an die Landesärztekammer Thüringen und die Landesapothekerkammer Thüringen, sofern es dort Fragen oder Anregungen zur elektronischen Gesundheitskarte gibt, steht daher nach wie vor.

Da auf der elektronischen Gesundheitskarte künftig Gesundheitsdaten der Patienten gespeichert werden sollen, müssen vor Ort die technischen und organisatorischen Maßnahmen getroffen werden, die zum Schutz dieser Daten erforderlich sind. Der TLfDI bietet den Berufsverbänden in Thüringen hierzu weiterhin seine Gesprächsbereitschaft an.

11.32 Betriebliches Eingliederungsmanagement, ein datenschutzrechtliches Minenfeld

Gemäß § 84 Abs. 2 Sozialgesetzbuch (SGB) Neuntes Buch (IX) ist der Dienstherr beziehungsweise die Dienststelle verpflichtet, betroffenen Beschäftigten, die länger als sechs Wochen krank sind oder waren, ein betriebliches Eingliederungsmanagement (BEM) anzubieten. Hierzu kann von der Personalverwaltung festgestellt werden, wie viele Krankheitstage als Voraussetzung vorliegen.

Zu der Frage, ob denn die Personalverwaltung befugt und berechtigt ist, auf der Grundlage einer Dienstvereinbarung zum BEM Mitteilungen zur Person und der Anzahl der Krankheitstage eines Beschäftigten an das in der Dienstvereinbarung vorgesehene Integrationsteam zu übermitteln, hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Folgendes ausgeführt:

Bei den Krankheitstagen von Beschäftigten handelt es sich um Personalakten Daten, für deren Verarbeitung oder Nutzung die dienstrechtlichen Vorschriften gelten, es sei denn, besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor. Einschlägige Vorschrift zur Vorlage von Personalakten Daten und Auskünften an Dritte ist § 85 Thüringer Beamten-gesetz (ThürBG) in der seit 1. Januar 2015 geltenden Fassung. Eine Datenübermittlung zum Zweck der Durchführung eines BEM ist hier je-

doch nicht speziell geregelt, sodass die Zulässigkeit der Weitergabe/Datenübermittlung auf der Grundlage allgemeiner Vorschriften zu prüfen ist.

Nach § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung personenbezogener Daten zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Datenschutzrechtlich streitig war in der Vergangenheit, ob und zu welchem Zeitpunkt der Personalrat über das Vorliegen der Voraussetzungen für die Durchführung eines BEM zu unterrichten ist. Nach der Rechtsprechung steht dem Personalrat die Möglichkeit zur Überprüfung zu, ob der Dienstherr seiner Verpflichtung zum Angebot eines BEM nachgekommen ist. Zu diesen Prüfzwecken kann unter Umständen auch verlangt werden, dass Namen von Betroffenen genannt werden.

Bezeichnend für das BEM ist, dass es nur auf Freiwilligkeitsbasis des Betroffenen und dessen Einwilligung durchgeführt werden kann und die betroffene Person bestimmt, welche Personen letztendlich damit befasst werden.

Die der Fragestellung zugrundeliegende abgeschlossene Dienstvereinbarung als sonstige Rechtsvorschrift schrieb die Weitergabe der Daten über krankheitsbedingte Fehlzeiten eines Betroffenen an das Integrationsteam vor, dem neben dem BEM-Beauftragten als Vertreter des Arbeitgebers ein Mitglied des Personalrats und gegebenenfalls der Schwerbehindertenvertretung angehören. Damit erhalten diese Personen bereits im Vorfeld, bevor es zu einer Willensäußerung des Betroffenen kommen kann, die Krankheitstage als Daten über das Vorliegen der Voraussetzungen zur Durchführung eines BEM. Willigt der Betroffene nicht ein, so sind dem Personenkreis personenbezogene Daten zu dem Betroffenen bekannt geworden, die letztendlich nicht zu einer weiteren Aufgabenerfüllung erforderlich sind. Die Übermittlung wäre daher nicht erforderlich und damit unzulässig.

Um dies zu vermeiden, sollten die Betroffenen von der Personalverwaltung selbst zum Zweck der Einholung einer Einwilligung zur Durchführung eines BEM angeschrieben werden. Damit würde vermieden, dass Personen, für die die personenbezogenen Daten eines Betroffenen mangels dessen Einwilligung für die weitere Aufgabenerfüllung nicht erforderlich sind, diese in unzulässiger Weise erhalten.

Die anfragende Stelle hat daraufhin die entsprechende Konkretisierung der Dienstvereinbarung zugesagt.

Da die Durchführung des Betrieblichen Eingliederungsmanagements von der Einwilligung des betroffenen Beschäftigten abhängt, bestimmt dieser letztendlich, wer außerhalb der Personalverwaltung seine personenbezogenen Daten über Krankheitstage verarbeiten darf. Es ist darauf zu achten, dass Personen, die mangels Einwilligung des Betroffenen letztendlich nicht mit der Durchführung des BEM befasst werden können, auch keine Informationen über die Krankheitstage erhalten.

11.33 Das Postgeheimnis gilt weiterhin! – Versendung von personenbezogenen Daten per Brief kein Datenschutzverstoß

Ein Rechtsanwalt beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil die Landesärztekammer Thüringen die IBAN und den BIC seines Mandanten mit der Post verschickt hatte. Hierin sah er einen Verstoß gegen das Thüringer Datenschutzgesetz (ThürDSG). Die Landesärztekammer Thüringen teilte auf Nachfrage des TLfDI mit, dass sie Beiträge für ihre Mitglieder erhebe. Hierzu können die Mitglieder der Landesärztekammer Einzugsermächtigungen erteilen. Dies sei auch durch den Mandanten des Beschwerdeführers geschehen. Die Landesärztekammer Thüringen stelle aus aktuellem Anlass das Lastschriftverfahren auf den SEPA-Zahlungsverkehr um und wollte ihrem Mitglied erneut die Möglichkeit anbieten, eine Einzugsermächtigung zu erteilen. Hierfür waren bereits die zutreffende IBAN und die BIC sowie das Kreditinstitut in dem übersandten Formular eingetragen. Dieses Formular war per Standardbrief zugesandt worden.

In der Versendung von personenbezogenen Daten mittels Brief durch die Post konnte der TLfDI keine Verletzung von § 9 Abs. 2 Nr. 1 ThürDSG erkennen. Aufgrund der zu treffenden technischen und organisatorischen Maßnahmen ist sicherzustellen, dass je nach Art der zu schützenden Daten gewährleistet ist, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können – Grundsatz der Vertraulichkeit. Die Vertraulichkeit von Postsendungen ist durch das Briefgeheimnis geschützt. Dieses wird von Artikel 10 des Grundge-

setzes garantiert. Das Postgesetz regelt, dass der Datenschutz bei Postdienstunternehmen nicht nur für Privatpersonen, sondern für alle Postkunden gilt. Weiterhin ist die Verletzung des Briefgeheimnisses nach § 202 Strafgesetzbuch (StGB) eine Straftat. Das Briefgeheimnis umfasst jedes Schriftstück, das verschlossen bzw. durch ein verschlossenes Behältnis gegen Kenntnisnahme gesondert gesichert ist. Damit liegt kein datenschutzrechtlicher Verstoß vor, wenn ein Dokument, das personenbezogene Daten des Empfängers enthält, mit der Post versandt wird. Diese Rechtsauffassung teilte der TLfDI sowohl der Landesärztekammer Thüringen als auch dem Beschwerdeführer mit.

Werden personenbezogenen Daten mit der Post in einem Standardbrief versandt, sind sie auf angemessene Weise vor dem Zugriff unberechtigter Dritter geschützt. Die Vertraulichkeit von Postsendungen ist durch das Briefgeheimnis geschützt, seine Verletzung ist nach § 202 StGB eine Straftat.

11.34 Auch Sozialbehörden dürfen nicht alles wissen

Ein Betreuer wandte sich im Namen des von ihm Betreuten an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Der Betreute erhielt Leistungen zur Rehabilitation und Teilhabe in Form von Eingliederungshilfen für behinderte Menschen. In dem zu ihm erstellten so genannten Gesamtplan war eine Fülle von Angaben enthalten, die der Betreuer für zu umfangreich hielt. Die im Gesamtplan erhobenen Daten dienen dem Sozialamt zur sozialhilferechtlichen und fachlichen Abklärung des individuellen Hilfebedarfs eines Bedürftigen nach Maßgabe von § 9 und § 53 ff. in Verbindung mit § 58 SGB XII. Ein Gesamtplan enthält Angaben zum Lebensbereich des Leistungsberechtigten. Auf dieser Grundlage können die Hilfeleistungen stetig an den Bedarf im Einzelfall angepasst und optimiert werden. Bei der Erstellung des Gesamtplans werden die am Hilfeprozess beteiligten Personen einbezogen.

Nach § 67a Abs. 1 SGB X dürfen Sozialdaten vom Sozialamt nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. An die Erforderlichkeit sind strenge Anforderungen zu stellen. Erforderlich ist die Kenntnis der Daten für das Sozialamt nur dann, wenn ohne diese Daten die Aufgabe nicht, nicht

vollständig oder nicht in rechtmäßiger Weise erfüllt werden kann. Es genügt nicht, wenn eine Angabe zur Aufgabenerfüllung lediglich nützlich ist. Außerdem besteht nach § 67a Abs. 1 Satz 1 SGB X die gesetzliche Verpflichtung, Sozialdaten grundsätzlich beim Betroffenen zu erheben.

Die im Gesamtplan befindlichen Ausführungen zur Beschreibung der aktuellen Situation waren sehr ausführlich, teilweise durch Zitate des Betroffenen ergänzt und wurden an manchen Stellen nicht auf die Überschriften bezogen, unter denen sie sich fanden. Der Sozialhilfeträger wurde vom TLfDI gebeten, die Ausführungen im Gesamtplan nochmals auf die Erforderlichkeit für die Aufgabenerfüllung hin zu prüfen und den Gesamtplan gegebenenfalls zu überarbeiten. Dieses Unterfangen hat zunächst dazu geführt, dass neben kleineren Streichungen der Gesamtplan vom Sozialhilfeträger noch ergänzt und damit insgesamt erweitert worden ist. Hierzu wurde geltend gemacht, nur so könnten die Hilfeleistungen stetig angepasst und optimiert werden. Medizinische Daten beispielsweise dienen dabei als Grundlage für die Einschätzung des Leistungsanspruches und gäben Aufschluss über Defizite und Einschränkungen des Leistungsberechtigten.

Diese Auffassung teilt der TLfDI nicht umfänglich. Denn in den Gesamtplan gehören beispielsweise keine Mutmaßungen des sozialmedizinischen Dienstes hinsichtlich der vermeintlichen Ursachen eines Defizits im Verhalten des Betroffenen. In einem Gespräch mit dem Sozialamt konnte vermittelt werden, dass einige Feststellungen nicht notwendig waren und der Gesamtplan daher auf das erforderliche Maß reduziert werden muss. Ein endgültiges Ergebnis liegt noch nicht vor. Zumindest für die Zukunft ist aufgrund der Einführung der integrierten Teilhabeplanung (ITP), die der TLfDI begleitet hat (siehe dazu Nummer 16.1) davon auszugehen, dass die angesprochenen datenschutzrechtlichen Defizite zukünftig vermieden werden.

Ein ganz wichtiger Punkt ist auch, dass Antragsteller vor der Erstellung eines Hilfeplans regelmäßig schriftlich über alle Umstände informiert werden müssen, insbesondere auch darüber, welche Institutionen an der Beratung zum Hilfeplan in der so genannten Hilfeplankonferenz beteiligt werden. Sollte sich der Betroffene mit der namentlichen Behandlung seines Begehrens in der Hilfeplankonferenz nicht einverstanden erklären, müsste sein Anliegen in anonymer Form vorgestellt und beraten werden. Dieser Hinweis hat der Sozial-

hilfeträger aufgegriffen und die Erarbeitung eines entsprechenden Formulars zugesagt.

Auch bei der Erstellung eines Gesamtplans als Grundlage für Leistungen zur Rehabilitation und Teilhabe nach dem SGB IX dürfen personenbezogene Daten des Bedürftigen nur dann erhoben und verarbeitet werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. An die Erforderlichkeit ist ein strenger Maßstab anzulegen. Einer datenschutzrechtlichen Verbesserung zugeführt wurde die Aufklärung zur Einwilligung durch die Betroffenen.

11.35 Ein Jugendamt tat sich schwer, Auskunft zu erteilen

Mitunter ist die Bearbeitung einer Beschwerde sehr mühevoll. Bereits Mitte 2012 beschwerte sich ein Betroffener beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil er vom Landratsamt keine Auskunft zu den über ihn bei einem Jugendamt verarbeiteten personenbezogenen Daten erhalten habe. Vom Jugendamt wollte er nämlich wissen, was eine Richterin beim Amtsgericht den Mitarbeiterinnen des Jugendamts mitgeteilt habe und was davon über ihn im Jugendamt gespeichert werde. Auf Nachfrage des TLfDI teilte das Landratsamt mit, das Jugendamt sei für den Beschwerdeführer örtlich gar nicht zuständig. Nach einer Anhörung vor dem Familiengericht in einer Kindschaftssache, an dem eine Sachbearbeiterin des Jugendamts teilgenommen hatte, wurde das Landratsamt über einen „Auftritt“ des Beschwerdeführers bei der genannten Richterin per E-Mail informiert. Bis dahin sei der Beschwerdeführer im Landratsamt unbekannt gewesen. Seit diesem Vorfall gingen jedoch beim Landratsamt regelmäßig E-Mails des Beschwerdeführers ein, ohne dass das Landratsamt als Adressat erkennbar sei. Der Auskunftsanspruch des Betroffenen ging nach Auffassung des Landratsamts ins Leere, weil die E-Mail der Richterin gelöscht sei. Auf erneute Nachfrage des TLfDI übersandte das Landratsamt eine Sammlung von E-Mails des Beschwerdeführers und teilte mit, es halte an seiner Auffassung fest. Das Landratsamt verarbeite nämlich gar keine Daten des Betroffenen, es habe sich auch nicht zielgerichtet Daten des Beschwerdeführers beschafft, vielmehr habe der Beschwerdeführer seine personenbezogenen Daten aufgedrängt. Daher könne kein Anspruch des Beschwerdeführers

auf Auskunft nach § 13 Thüringer Datenschutzgesetz (ThürDSG) bestehen.

Nach Ausspruch einer Beanstandung nach § 39 ThürDSG wegen Verweigerung der Auskunft nach § 13 ThürDSG – obwohl keine der dort genannten Gründe vorlagen –, von der auch die Rechtsaufsicht benachrichtigt wurde, folgte ein weiterer umfangreicher Schriftwechsel. Letztendlich informierte die Rechtsaufsicht den TLfDI, das Landratsamt habe eine „Negativauskunft“ mit dem wesentlichen Inhalt erteilt, die E-Mail der Richterin sei vernichtet worden. Es existierten über den Beschwerdeführer dort keine wie auch immer gearteten Informationen, Daten, Unterlagen oder Akten. Zu seiner Person seien zu keinem Zeitpunkt Daten im Sinne des § 3 Abs. 3 ThürDSG verarbeitet worden.

Dies war so auch nicht ganz richtig. Tatsächlich sind selbstverständlich Daten zum Beschwerdeführer verarbeitet worden. Dies betraf zum einen die Löschung der E-Mail der Richterin, da eine Löschung nach der Definition des § 3 Abs. 3 Nr. 6 ThürDSG eine Datenverarbeitung darstellt. Zum anderen wurden personenbezogene Daten des Beschwerdeführers im Rahmen der Bearbeitung seiner Beschwerde zu seinem Auskunftsbegehren verarbeitet. Da aber die Löschung der E-Mail in der Auskunft genannt war und der TLfDI davon ausging, dass zum Jugendamt keine weiteren personenbezogenen Daten des Beschwerdeführers, insbesondere zur Beschwerdebearbeitung, gelangt sind, wurde der datenschutzrechtliche Verstoß als behoben angesehen.

Die Löschung personenbezogener Daten stellt eine Verarbeitung im Sinne des § 3 Abs. 3 Nr. 6 ThürDSG dar. Der Anspruch auf Auskunft nach § 13 ThürDSG geht ins Leere, wenn Daten gelöscht sind. Nach einer Löschung darf nicht mehr nachvollziehbar sein, um was für konkrete Daten es sich gehandelt hat. Im Rahmen der Bearbeitung eines Auskunftsersuchens werden ebenfalls personenbezogene Daten des Antragstellers verarbeitet. Die Auskunft, es seien keine Daten vorhanden, ist daher nicht richtig.

11.36 Aushang von Dienstplänen im Pflegeheim

Die Leitung eines Pflegeheims wandte sich Hilfe suchend an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil es datenschutzrechtliche Bedenken gegen

die Forderung der Heimaufsicht gab, die Dienstpläne der Pflegekräfte für alle Mitarbeiter und damit aufgrund der Gegebenheiten vor Ort auch für Heimbewohner zugänglich auszuhängen. Auf den zu verwendenden Dienstplänen war nämlich zu jedem einzelnen Mitarbeiter eine Vielzahl von Angaben für einen ganzen Monat vorgesehen: Name und Vorname der Pflegekraft, deren Qualifikation, wie viele Stunden und Urlaubstage aus dem Vormonat übertragen waren, wie viele Stunden sie nach dem Arbeitsvertrag zu arbeiten hat, wie viele Arbeitsstunden an welchem Tag geplant sind, an welchem Tag sie wegen Krankheit, eines kranken Kindes, Urlaubs aus verschiedensten Gründen oder wegen Mehrarbeit bzw. Überstunden frei hatte, sich im Mutterschutz oder in Kur, in der Schule oder auf einer Fortbildung befand und vieles mehr.

Mit dem Aushang wäre es nicht zu vermeiden gewesen, dass jeder Mitarbeiter der Pflegeeinrichtung, die Pflegeheimbewohner und deren Besucher diese persönlichen Daten der Beschäftigten zur Kenntnis nehmen konnten, wofür es keinerlei Rechtsgrundlage gab. Auf Nachfrage des TlfdI erklärte das Thüringer Landesverwaltungsamt als zuständige Heimaufsicht, es bestehe die grundsätzliche Anforderlichkeit, dass die Dienstpläne mit dem geschilderten Inhalt an personenbezogenen Daten der Mitarbeiter/innen angelegt würden. Die Pflegeheime seien verpflichtet, über den Einsatz der bei ihnen beschäftigten Mitarbeiter/innen einen Nachweis zu führen. Damit werde zum einen die Ausrichtung des Mitarbeiterereinsatzes entsprechend den Regelungen aus dem Arbeitszeitgesetz, persönlicher, tariflicher oder betrieblicher Vereinbarungen und gegebenenfalls auch aus dem Bundesurlaubsgesetz belegt. Zum anderen werde mit dem Dienstplan die Einhaltung der vertraglichen Verpflichtung (Personaleinsatz laut Leistungs- sowie Vergütungsvereinbarung) nach dem Sozialgesetzbuch (SGB) Zehntes Buch (X) nachgewiesen. Auch bestehe für die Einrichtungsträger die Verpflichtung, den Einsatz der angestellten Mitarbeiter nach § 11 Abs. 1 Zif. 3 Thüringer Wohn- und Teilhabegesetz (ThürWVG) nachzuweisen. Bei aufsichtsrechtlichen Prüfungen in Pflegeeinrichtungen seien die Dienstpläne als wesentliches Qualitätskriterium erforderlich und dienten auch den diensthabenden Pflegekräften dazu, die Organisation der pflegerischen Versorgung sicherzustellen und Mitarbeiterausfälle zu kompensieren. Schließlich wurde vom Thüringer Landesverwaltungsamt ausgeführt, der Dienstplan sei rund um die Uhr für die anwesenden diensthabenden Pflegekräfte erforderlich, um die Organisation der

pflegerischen Versorgung sicherzustellen und Mitarbeiterausfälle kompensieren zu können.

Dass die einzelnen personenbezogenen Daten für unbefugte Dritte nicht einsehbar sein dürfen, war seitens der Heimaufsicht bisher noch nicht problematisiert worden. Der TLfDI hat dem Pflegeheim mitgeteilt, dass die Heimaufsichtsbehörde keinesfalls den Aushang der Dienstpläne mit den genannten Eintragungen zu den einzelnen Mitarbeitern für jedermann einsehbar fordern könne. Erforderlich und damit zulässig ist auch nach Auffassung der Heimaufsichtsbehörde lediglich, die Dienstpläne für aufsichtsrechtliche Kontrollen und intern den zuständigen diensthabenden Pflegekräften zur Sicherstellung der Organisation der pflegerischen Versorgung zur Verfügung zu stellen. Sofern die Dienstpläne nicht computergestützt geführt werden und damit keine technische Möglichkeit zur Verfügung steht, die Lesbarkeit personenbezogen zu beschränken, sind durch die zuständigen Heimleitungen oder Träger andere geeignete technische und organisatorische Maßnahmen zum Schutz der Mitarbeiterdaten vor unbefugter Kenntnisnahme zu treffen. Möglich ist es beispielsweise, gesonderte Dienstpläne zu erstellen und an für Pflegeheimbewohner und Besucher nicht zugänglichen Stellen auszuhängen, die nur die notwendigen Angaben der Anwesenheit enthalten.

Die Inhalte von Dienstplänen sind für aufsichtsrechtliche Prüfungen in Pflegeheimen erforderlich und dienen auch den diensthabenden Pflegekräften dazu, die pflegerische Versorgung sicherzustellen. Die Heimleitungen oder Träger haben entsprechende organisatorische und technische Maßnahmen zum Schutz vor unbefugter Kenntnisnahme der in den Dienstplänen enthaltenen Beschäftigtendaten durch andere Mitarbeiter oder Heimbewohner oder deren Besucher zu treffen. Mangels anderer Möglichkeiten ist der Datenumfang ausgehängter Dienstpläne auf das erforderliche Minimum zu reduzieren.

11.37 Sozialdatenübermittlung an die Staatsangehörigkeitsbehörden

In einem anderen Bundesland hatte sich ein Jobcenter an den zuständigen Landesbeauftragten für den Datenschutz gewandt und auf folgende Problematik hingewiesen:

Das dortige Jobcenter erhielt regelmäßig Anfragen von der im Innenministerium angesiedelten Staatsangehörigkeitsbehörde, um

festzustellen, ob ein Einbürgerungsbewerber, der die deutsche Staatsbürgerschaft erlangen möchte, die geforderten Voraussetzungen erfüllt. Hierzu gehört beispielsweise ein Nachweis, dass er sich in der Vergangenheit um eine Arbeitsstelle bemüht hat und von einer gewissen finanziellen Unabhängigkeit gegenüber dem Staat ausgegangen werden kann. Das zuständige Innenministerium wies darauf hin, dass in anderen Bundesländern hierzu eine mit den jeweiligen datenschutzrechtlichen Aufsichtsbehörden abgestimmte Einwilligungserklärung in die Datenübermittlung herangezogen werde. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) griff die zu dieser Problematik gestartete Länderrumfrage auf und bat das (damalige) Thüringer Innenministerium (TIM) um Informationen zur Handhabung in Thüringen, da keine mit ihm abgestimmte Einwilligungserklärung bekannt war.

Das TIM teilte mit, es gäbe in Thüringen keine generelle Handlungsanweisung. Eine Anfrage an die Jobcenter im Rahmen des Einbürgerungsverfahrens erfolge nur in bestimmten Einzelfällen, wie bei wechselnden Arbeitsverhältnissen, Arbeitslosigkeit, geringen Einkommen und ähnlichen Fallkonstellationen. Für die Anfrage beim Jobcenter werde eine Einwilligung des Einbürgerungsbewerbers eingeholt, wofür ein Muster vorliege. Erteile ein Jobcenter die gewünschten Auskünfte nicht, müsse der Einbürgerungsbewerber aufgrund der allgemeinen Darlegungs- und Beweislast die benötigten Angaben selbst vorlegen. Also liege die Datenübermittlung daher vor allem auch im Interesse des Betroffenen und diene der Verfahrensvereinfachung. Die Vorgehensweise entspreche im Übrigen auch der Praxis in anderen Bundesländern und solle beibehalten werden.

Das übersandte Muster einer Einwilligungserklärung genüge aus Sicht des TLfDI jedoch nicht den Anforderungen an eine rechtswirksame Einwilligung. Vielmehr wurde mit der Unterschrift auf dem Formular eine pauschale Einwilligung erklärt, ohne dass der konkrete Zweck der Datenverarbeitung erkennbar war. Eine Einwilligung setzt aber nach § 4 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) voraus, dass diese in Bezug auf eine bestimmte Verarbeitung oder Nutzung der personenbezogenen Daten erklärt wird. Eine Übermittlung personenbezogener Daten von Seiten der aufgelisteten Behörden auf Grundlage des vorliegenden Musters war somit mangels rechtswirksamer Einwilligung unzulässig.

Zur Konkretisierung hätte daher zu den einzelnen Behörden, die auf dem Muster aufgelistet waren, jeweils eine Ergänzung hinzugefügt

werden müssen, welche konkreten Angaben des Betroffenen zu welchem konkreten Zweck eingeholt werden sollen. Rein praktisch bot es sich aus Gründen der Übersichtlichkeit nicht an, für die aufgelistete Vielzahl von Behörden aus unterschiedlichen Bereichen (Sicherheitsbehörden, Sozialbehörden etc.) dieselbe Mustereinwilligung zu nutzen.

Daraufhin hat das TIM die bis dahin genutzte Einwilligungserklärung zunächst in drei einzelne Erklärungen für Behörden, Sozialbehörden und Auslandsvertretungen des Herkunftsstaates aufgeteilt. Weiterhin war zu beachten, dass für verschiedene Behörden keine Einwilligungen erforderlich waren, weil die Beteiligung der Polizeibehörden, Strafverfolgungsbehörden, Gerichte, der Ausländer- und Ordnungsbehörden, der Auslandsvertretungen der Bundesrepublik, des Bundesamts für Migration und Flüchtlinge (BAMF), der Standesämter, Meldeämter und der Jugendämter auf Grundlage der gesetzlichen Regelungen der §§ 32 und 37 Abs. 2 Staatsangehörigkeitsgesetz (StAG) erfolgte.

Der TLfDI hielt es aber für angemessen, die Betroffenen auf die vielfältigen Anfragemöglichkeiten hinzuweisen, auch wenn dies nicht von ihrer Einwilligung abhing. Daher sollte die zunächst vorbereitete Einwilligung zu Abfragen bei den Meldebehörden, Ausländerbehörden, dem Bundesamt für Justiz, den Sicherheitsbehörden, dem Thüringer Landesamt für Verfassungsschutz, dem BAMF, dem Gewerbeamt, der Wohngeldstelle, dem Auswärtigen Amt und den deutschen Auslandsvertretungen als Merk- und Erläuterungsblatt umgearbeitet und genutzt werden. Dies dient der Transparenz für die Betroffenen, um ihnen die Möglichkeit zu geben, von den Datenübermittlungen Kenntnis zu erlangen.

Die Erhebung von Sozialdaten war nach § 67a Abs. 1 SGB X nur bei gesetzlich vorgesehener Einwilligung auf Einwilligungsbasis möglich. Entsprechend der Wertung nach § 67a Abs. 2 Nr. 1 SGB X war aber nach Auffassung des TLfDI dennoch die Erhebung auf Einwilligungsbasis möglich, um die Betroffenen vom Aufwand zu entlasten, sofern sie dies ausdrücklich wünschen.

Das TIM hat die Hinweise des TLfDI in den nunmehr zu verwendenden Einwilligungsmustern und insbesondere in einem ausführlichen Merkblatt für die betroffenen Einbürgerungswilligen berücksichtigt.

Ist zur Prüfung der Voraussetzungen in einem Verwaltungsverfahren eine Vielzahl von Bescheinigungen und Auskünften anderer Behörden erforderlich, können diese, sofern die gesetzlichen Voraussetzungen hierzu vorliegen, von der entscheidenden Behörde aufgrund von Einwilligungen der Betroffenen eingeholt werden. Besondere Bedeutung kommt hier der Transparenz für die Betroffenen zu.

11.38 Akteneinsicht beim Jugendamt – ein schwieriges Unterfangen?

Die Mutter eines volljährigen Sohnes, der zeitweilig in einem Heim untergebracht war, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ihr die Einsicht in die bzw. die Auskunft aus den beim Jugendamt zu ihrem Sohn geführten Akten verweigert würde. Ihr Akteneinsichts- bzw. Auskunftsrecht, das sie nach dem Bundesdatenschutzgesetz geltend machen wollte, hatte sie gegenüber dem Jugendamt „zum Zweck der Berichtigung und Löschung“ personenbezogener Daten beantragt. Das Jugendamt fragte nach, welche personenbezogenen Daten, die beaskunftet werden sollten, die Beschwerdeführerin als unrichtig ansehe. Trotz der umfangreichen Antwort der Beschwerdeführerin sah sich das Jugendamt immer noch nicht imstande, Akteneinsicht zu gewähren bzw. Auskunft zu erteilen. Dies interpretierte die Beschwerdeführerin als Ablehnung ihres Antrags und bat den TLfDI um Hilfe.

Der TLfDI nahm zur Sachverhaltsklärung Akteneinsicht im Jugendamt. Dabei wurde festgestellt, dass die eingesehenen, zum Sohn geführten Akten auch personenbezogene Daten der Beschwerdeführerin enthielten. Sie enthielten aber jeweils ebenso personenbezogene Daten Dritter, auch des Kindsvaters sowie der mit den einzelnen Sachverhalten beschäftigten Mitarbeiter des Jugendamts und des Heims. Die Akten waren darüber hinaus bereits abgeschlossen. Der Sohn war zwischenzeitlich volljährig, sodass für ihn auch keine weitere Zuständigkeit des Jugendamtes bestand. Es war eine zehnjährige Aufbewahrungsfrist festgelegt worden

Innerhalb eines konkreten Verwaltungsverfahrens beim Jugendamt besteht für die betroffenen Kinder, für die Eltern und Personensorgeberechtigten (gemeinsam oder allein) sowie die übrigen Beteiligten eines solchen Verfahrens ein Anspruch auf Akteneinsicht nach § 25 Zehntes Buch Sozialgesetzbuch (SGB X). Das Jugendamt hat

Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 25 Abs. 1 SGB X). Die Verpflichtung zur Gestattung der Akteneinsicht besteht nicht, soweit die Vorgänge wegen der berechtigten Interessen anderer Beteiligter oder dritter Personen geheim gehalten werden müssen (§ 25 Abs. 3 SGB X).

Da eine Trennung zwischen den personenbezogenen Daten der Beschwerdeführerin und Daten Dritter nicht möglich war, musste der Anspruch auf Akteneinsicht vom Jugendamt sorgfältig geprüft werden. Die Antragstellerin muss darlegen, welche Daten aus welchem Grund für die Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich sind. Außerdem muss das Jugendamt für die dann in Betracht kommenden Daten prüfen, ob sie wegen der berechtigten Interessen anderer Beteiligter oder dritter Personen geheim gehalten werden müssen. Bei Ablehnung der Akteneinsicht steht der Antragstellerin eine rechtsmittelfähige Entscheidung zu.

Der TLfDI hat daher das Jugendamt gebeten, die Antragstellerin aufzufordern, ihren Antrag dahingehend zu konkretisieren, welche Daten aus welchem Grund für die Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich sind.

Daneben hat das Jugendamt dem Betroffenen nach § 83 SGB X auf Antrag Auskunft zu erteilen über die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung.

Im Rahmen der Auskunftserteilung auf dieser Rechtsgrundlage kann es – wie im vorliegenden Fall – ausreichen, der Beschwerdeführerin mitzuteilen, welche Schreiben von ihr in der betroffenen Akte enthalten sind und welche Schreiben an sie gerichtet wurden.

Hierauf wies der TLfDI das Jugendamt hin, dass der Beschwerdeführerin nach der Konkretisierung ihres Antrags unter Berücksichtigung der Rechtsauffassung des TLfDI Auskunft erteilt wird.

Nach § 13 Thüringer Datenschutzgesetz haben Betroffene das Recht auf Auskunft und Akteneinsicht gegenüber den öffentlichen Stellen des Landes. Auskunftsrechte können sich auch auf spezialgesetzliche Rechtsgrundlagen wie §§ 25 Abs. 1 und 83 SGB X stützen. Ein Antrag auf Auskunft muss so hinreichend konkretisiert werden, dass

der auskunftspflichtigen Behörde eine Entscheidung über den Antrag möglich ist.

11.39 Wohngeld nur für gläserne Bürger?

Ein Betroffener, der Wohngeld beantragen wollte, wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil von ihm nicht etwa nur Angaben zu seinen Einkünften, sondern auch eine detaillierte Aufstellung seiner durchschnittlichen monatlichen Ausgaben verlangt wurde. Verlangt wurden Angaben zu Ausgaben für die Ernährung (Frühstück, Mittag- und Abendessen), Neuanschaffung von Bekleidung, Reinigung und Reparatur von Schuhen, Kleidung und Wäsche, Haushaltsgegenständen und Möbeln, für die persönlichen Dinge des täglichen Lebens (einschließlich Kosmetik, Körperpflege, Bücher, Zeitschriften, Vereine, Hobby usw.) bis hin zu Telefon, Hörfunk, Fernsehen, Versicherungen und zu guter Letzt detaillierten Kosten für ein Kraftfahrzeug (Versicherung, Steuer, Treibstoff, Wartung, Reparatur). Am Ende des Merkblatts zum Wohngeldantrag wurde von der zuständigen Sozialbehörde auch gleich darüber informiert, dass unvollständige Angaben zur Ablehnung des Wohngeldantrags führen.

Mit den beschriebenen Angaben wäre der Antragsteller für die Sozialbehörde der gläserne Mensch schlechthin. Sein gesamter Lebenswandel wäre anhand seiner Ausgaben nachvollziehbar. Inwieweit derartige Angaben auf die Ermittlung der Höhe des Wohngelds Einfluss haben können, erschloss sich dem TLfDI nicht. Nach dem Wohngeldgesetz sind lediglich die Einkommensverhältnisse zu klären. Demnach ist eine Datenerhebung als unzulässig anzusehen, die über die im Wohngeldgesetz konkret geregelten Erhebungstatbestände hinausgeht. Der Nachweis monatlicher Ausgaben für den aufgeführten persönlichen Bedarf gehört keinesfalls dazu.

Die zur Stellungnahme aufgeforderte Stadtverwaltung teilte mit, Grundlage der Befragung bilde § 15 Wohngeldgesetz (WoGG). Nach der Allgemeinen Verwaltungsvorschrift zur Durchführung des Wohngeldgesetzes seien die Angaben der wohngeldberechtigten Personen besonders auf ihre Glaubhaftigkeit und Vollständigkeit zu überprüfen (Plausibilitätsprüfung), wenn sich bei der Ermittlung des Jahreseinkommens unter dem Bedarf liegende Einnahmen ergäben. Glaubhaft sei nur, wenn das angegebene, zur Verfügung stehende Einkommen plus Wohngeld 80 % des Bedarfs nach dem Sozialge-

setzungsbuch Zwölftes Buch (SGB XII) ergebe. Mit anderen Worten: Plausibel ist nur, wenn man mit Wohngeld über mehr als 80 % des Sozialhilfesatzes verfügt. Oder anders herum: Wer nicht genügend Einkommen hat oder angibt, kann davon nicht leben und schummelt vielleicht – soll so eine Person Wohngeld bekommen?

Aufgrund des Einschreitens des TLfDI hat das Sozialamt das Standardschreiben geändert. Der Vordruck zur Datenerhebung werde nur noch als Erleichterung und Hilfe für Wohngeldberechtigte angeboten. Die Betroffenen seien nicht verpflichtet, die Angaben zur durchschnittlichen persönlichen Verwendung der schmalen Einkünfte auszufüllen. Machen die Betroffenen aber keine Angaben, würde – soweit aufgrund der eingereichten Unterlagen möglich – das nicht plausibel dargelegte Einkommen geschätzt und die Regelsätze nach dem SGB II und SGB XII als persönlicher Bedarf angesetzt. Dies könne aber im Einzelfall dem Antragsteller dann zum Nachteil erreichen, wenn er die freiwilligen Angaben nicht vornehme.

Diese Maßnahme reichte dem TLfDI natürlich nicht aus. Die Erhebung von Sozialdaten ist nach § 67a SGB X nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe nach dem SGB erforderlich ist. Das Wohngeldgesetz gehört nach § 68 SGB I zum Sozialgesetzbuch und gibt genaue Vorgaben zur Ermittlung der Höhe des Wohngeldes. Das Wohngeld berechnet sich nach der Anzahl der zu berücksichtigenden Haushaltsmitglieder (§§ 5 bis 8 WoGG), der zu berücksichtigenden Miete oder Belastung (§§ 9 bis 12 WoGG) und dem Gesamteinkommen (§§ 13 bis 18 WoGG). Zu diesen Punkten darf die zuständige Stelle grundsätzlich personenbezogene Daten erheben. Welche Daten bei der Einkommensermittlung zugrunde zu legen sind, regeln die §§ 13ff. WoGG. Insoweit steht fest, welche konkreten Angaben hierfür erforderlich sind.

Wird Wohngeld beantragt, besteht für die Antragsteller eine sozialrechtliche Mitwirkungspflicht (§ 60 SGB I). Damit verbunden ist die Obliegenheit, der Wohngeldstelle Auskunft über die Einnahmen und über andere für das Wohngeld maßgebende Umstände zu geben. Demnach ist der Antragsteller verpflichtet, sein Einkommen offenzulegen, nicht jedoch Daten dazu, wie und für welche Dinge er sein Einkommen im Einzelfall ausgibt. Es ist unzulässig, vom Antragsteller Informationen zu verlangen, die weder Einnahmen noch für das Wohngeld maßgebende Umstände betreffen. Also war es völlig unerheblich, welche Beträge speziell für Ernährung, für persönliche Dinge des täglichen Lebens und die Neuanschaffung von Bekleidung

aufgewandt werden. Weshalb diese Angaben eine Plausibilität begründen sollten, war nicht nachvollziehbar. Also forderte der TLfDI das Sozialamt auf, das Formular nicht mehr zu verwenden.

Im Sinne der Bürgerfreundlichkeit entwarf das Sozialamt nun ein neues Schreiben für die Wohngeldempfänger und verlangte immer noch freiwillig Angaben zur Lebensführung, weil diese doch für die Betroffenen günstig seien. Gleichzeitig wurden die Betroffenen aber auf mögliche ungünstige Rechtsfolgen bei Verweigerung der Angaben hingewiesen. Aber auch dies war nicht zu akzeptieren.

Der Hinweis für die Betroffenen auf die Freiwilligkeit der zu ergänzenden Angaben zum Wohngeldantrag am Ende des Vordrucks war nicht hilfreich. Die Freiwilligkeit der Angaben musste klar und deutlich erkennbar sein. Es war nicht davon auszugehen, dass Betroffene zuerst den ganzen Vordruck lesen und sich dann entscheiden, ob sie ihn ausfüllen oder von ihrem Recht Gebrauch machen, die Angaben nicht zu machen. Daher sollte bereits unmittelbar nach der Überschrift hervorgehoben vorangestellt werden, dass die folgenden Angaben freiwillig sind (vgl. § 67a Abs. 3 Satz 2 SGB X). Dabei war auch deutlich darauf einzugehen, dass – wie vom Sozialamt vorgetragen – die Gewährung von Rechtsvorteilen im Vordergrund steht, die Angaben ggf. aber auch im gesetzlichen Rahmen zu Ungunsten ausfallen können.

In einem Gespräch legte das Sozialamt nochmals dar, die beabsichtigte Datenerhebung solle zu dem Zweck erfolgen, dem Antragsteller die richtige Hilfe angedeihen zu lassen. Wenn das angegebene Einkommen deutlich unter dem festgestellten Regeleinkommen liege, spreche viel dafür, dass er entweder Hilfe zum Lebensunterhalt oder Leistungen nach dem SGB II beziehen könne. Dagegen war aus datenschutzrechtlicher Sicht einzuwenden, dass, selbst wenn jemand einen Anspruch nach SGB II hat, dies einem Anspruch auf Wohngeldzahlung nur entgegensteht, wenn er diese Leistung nach SGB II auch empfängt. Es reicht eben nicht immer aus, wenn eine Behörde davon ausgeht, eine Datenerhebung erfolge doch nur im Interesse des Betroffenen. Der TLfDI wies nochmals darauf hin, dass das SGB keinen Raum für die Datenerhebung auf Grundlage einer Einwilligung bietet, es sei denn, das Gesetz sieht dies ausdrücklich vor. Dies ist jedoch im Zusammenhang mit der Beantragung von Wohngeld nicht gegeben. Daher verbleibt es bei dem Grundsatz, dass die Erhebung von Sozialdaten nach § 67a Abs. 1 Satz 1 SGB X nur zulässig

ist, wenn ihre Kenntnis zur Aufgabenerfüllung nach diesem Gesetz-
buch erforderlich ist.

Nach den gesetzlichen Vorschriften muss ein Antragsteller bei der
Beantragung von Wohngeld nur sein Einkommen nachweisen, je-
doch nicht, wofür er dieses verwendet. Auch die vorgetragenen Be-
weggründe für die Datenerhebung zur Plausibilitätsprüfung änderten
daran nichts.

Im Ergebnis hat das Sozialamt mitgeteilt, der streitige Vordruck
werde nicht mehr verwandt. In Fällen, in denen ein großes Missver-
hältnis der angegebenen Einkünfte zu den Bedarfsätzen nach dem
SGB II und SGB XII besteht, wird der Betroffene zukünftig ange-
hört. Er kann dann darlegen, wie er es schafft, „über die Runden zu
kommen“ und wird auf die Möglichkeit des Erhalts weiterer Lei-
stungen hingewiesen. Hiergegen ist aus datenschutzrechtlicher Sicht
nichts einzuwenden.

Die Einwilligung von Betroffenen kann im Sozialrecht nur dann
eingeholt werden, wenn die sozialrechtlichen Vorschriften eine Ein-
willigung ausdrücklich zulassen. Im Rahmen des Antrags auf Wohn-
geld können nur Einkommensnachweise verlangt werden.

11.40 Datenerhebung zur Aufnahme von Klienten anderer Sozialhilfeträger

Ein privater Träger, der betreute Wohngruppen und betreutes Ein-
zelwohnen für Abhängigkeitserkrankte anbot, wandte sich an den
Thüringer Landesbeauftragten für den Datenschutz und die Informa-
tionsfreiheit (TLfDI), weil er datenschutzrechtliche Bedenken zu der
Anforderung des Sozialamtes hatte. Dieses wollte mit einem Form-
blatt zur Datenerhebung Informationen zu Bewohnern erhalten, die
aus anderen Kommunen stammten.

Auf Nachfrage des TLfDI teilte das Sozialamt mit, dass die Datener-
hebung zur Abstimmung der Aufnahme von Klienten anderer Sozi-
alhilfeträger im Rahmen des ambulant betreuten Wohnens für Lei-
stungsberechtigte nach §§ 53 ff. Sozialgesetzbuch (SGB) Zwölftes
Buch (XII) dienen sollte. Damit war vom Wohnheimträger anzuge-
ben, wer der zuständige Sozialhilfeträger eines betroffenen, aller-
dings nicht namentlich zu nennenden Klienten war und ob bzw.
welche Hilfen nach dem SGB XII und anderen Bestimmungen be-
reits erbracht wurden. Darüber hinaus sollte die Notwendigkeit der

Aufnahme des Klienten außerhalb des Zuständigkeitsbereichs des bisherigen Sozialhilfeträgers begründet und der erwartete Hilfebedarf eingefügt werden. Die Problematik bestand darin, dass die geforderten Angaben nicht vom konkret betroffenen Klienten (Grundsatz der Erhebung beim Betroffenen) oder von der bisher für diesen zuständigen Stelle (dem anderen Sozialträger), sondern von der aufnehmenden Einrichtung angegeben werden sollte. Fraglich war auch, ob der Wohnheimträger denn über die Angaben überhaupt verfügte oder diese erst vom Betroffenen erheben musste.

Das Sozialamt legte zur Erläuterung dar, es ginge darum, erst einmal die Bedarfe der „eigenen“ Bürger der Kommune zu decken und festzustellen, inwieweit eine „Eigennutzung“ der vorhandenen Platzkapazität bestehe. Unter dem Blickwinkel des Datenschutzes habe man den Fragebogen bewusst anonym gehalten. Die Praxis habe gezeigt, dass Sozialhilfeträger oder andere zuständige Stellen bei entsprechenden Leistungserbringern vor Ort Kapazitätsanfragen stellten, die meist gekoppelt sind mit Fragen zu konzeptionellen Inhalten, speziellen Ausrichtungen usw. Um die Kapazitätsanfrage in Höhe der gegebenenfalls benötigten Fachleistungsstunden konkret abklären zu können, würden die im Fragebogen enthaltenen Daten benötigt.

Der Fragebogen enthielt keine Namen der Betroffenen und war damit zunächst anonym. Soweit Angaben verlangt wurden und hierzu jeweils ein Stichwort genügte, war die Anonymität nicht aufgehoben. Der TLfDI hat darauf hingewiesen, dass bei den Angaben zur Begründung der Notwendigkeit der Aufnahme des Klienten außerhalb des Zuständigkeitsbereichs des bisherigen Sozialhilfeträgers darauf zu achten ist, dass keine Angaben gemacht werden, die eine Reanonymisierung des Betroffenen ermöglichen. Um dies sicherzustellen, wurde das Sozialamt gebeten, die Träger auf diese Gefahr hinzuweisen.

Damit bestanden keine grundsätzlichen datenschutzrechtlichen Bedenken gegen die Vorgehensweise des Sozialamtes.

Eine Erhebung von Angaben über Dritte ist datenschutzrechtlich unbedenklich, wenn die Anonymität des Betroffenen gewahrt wird, die Daten bei der zur Auskunft berufenen Stelle vorhanden und zur Aufgabenerfüllung der Auskunftsbegehrenden Stelle erforderlich sind.

11.41 Datenschutz und Sorgerechtsstreitigkeiten

Ein Vater (Beschwerdeführer) beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über das Jugendamt eines Landkreises zum Umgang mit seinen personenbezogenen Daten in einer Gerichtsverhandlung. In dem Verfahren ging es um das Sorgerecht für seinen Sohn. Nach der Meinung des Beschwerdeführers hatte nämlich das Jugendamt in der Gerichtsverhandlung von ihm allerdings nicht näher bezeichnete unwahre Angaben über ihn verlautbart. Außerdem vertrat er die Auffassung, das Jugendamt unterliege der Amtsverschwiegenheit und hätte daher nur mit seiner Einwilligung bei Gericht Angaben machen dürfen. Im Übrigen hatte er das Jugendamt unter Fristsetzung aufgefordert, ihm Auskunft zu den über ihn gespeicherten personenbezogenen Daten zu erteilen. Dem sei das Jugendamt nicht nachgekommen.

Der TLfDI wies den Beschwerdeführer zunächst darauf hin, dass dem Jugendamt als Beteiligtem im gerichtlichen Verfahren zum Sorge- und Umgangsrecht mit Kindern eine maßgebliche Rolle zukommt und eine Verpflichtung der Mitarbeiter besteht, auf Fragen des Gerichts Auskünfte zu erteilen. Zu beachten ist, dass es in dem gerichtlichen Verfahren zuvorderst um das Wohl des Kindes geht. Die Rolle des Jugendamts wird nicht von den anderen Prozessbeteiligten bestimmt. Angaben bei Gericht sind somit regelmäßig auch nicht von einer Einwilligung eines anderen Prozessbeteiligten abhängig, und es bedarf hierzu grundsätzlich auch keiner Schweigepflichtentbindung. Daraufhin wollte es der Beschwerdeführer, ohne dass er den Sachverhalt konkret schilderte, genau wissen und verlangte vom TLfDI die Angabe sämtlicher Rechtsgrundlagen, aufgrund derer ein Jugendamt Daten übermitteln darf. Dem nachzukommen hielt der TLfDI weder für zielführend noch für angezeigt, ohne dass eine Stellungnahme des Jugendamts in der Angelegenheit vorlag.

Das Landratsamt teilte dem TLfDI mit, das Jugendamt habe aufgrund seiner Mitwirkungspflicht nach § 50 Sozialgesetzbuch (SGB) – Aches Buch (VIII) das Familiengericht bei allen Maßnahmen, die die Sorge von Kindern und Jugendlichen betreffen, zu unterstützen und sei daher Verfahrensbeteiligter im streitgegenständlichen Verfahren gewesen. In dieser Eigenschaft sei in der nichtöffentlichen Sitzung beim Amtsgericht von einer Mitarbeiterin mündlich Bericht

erstattet worden. Alles, was über den Beschwerdeführer in diesem Zusammenhang an Informationen aufgenommen worden sei, befände sich in der Gerichtsakte. Weitere Daten zu dem Beschwerdeführer seien beim Landratsamt nicht gespeichert. Dem Beschwerdeführer habe das Landratsamt zwischenzeitlich eine entsprechende Auskunft gegeben.

Datenschutzrechtliche Bedenken bestanden zu der vom Landratsamt dargelegten Vorgehensweise nicht.

Ist ein Jugendamt Beteiligter in einem gerichtlichen Verfahren, ist es verpflichtet, in Wahrnehmung seiner gesetzlichen Aufgaben die erforderlichen Angaben zu machen. Datenschutzrechtliche Gründe stehen dem nicht entgegen. Zulässige Angaben bei Gericht sind nicht von der Einwilligung eines anderen Prozessbeteiligten abhängig.

11.42 Sozialhilfe auf falschem Konto: Datenschutz leitet auf richtiges Konto um

Der Betreuer einer in einem Pflegeheim untergebrachten älteren Dame beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Er war der Auffassung, dass der behördliche Beauftragte für den Datenschutz eines Landratsamts (bDSB) zu lax mit seiner Beschwerde umgegangen sei und den Datenschutz bei der Bearbeitung verletzt habe. Der Betreuer schilderte, er habe für die Betreute bei dem zuständigen Landratsamt Sozialhilfe zur Überweisung auf deren Konto beantragt. Die nach seiner Auffassung falsch berechnete Sozialhilfe sei dann aber einschließlich des Taschengelds für die Betreute nicht auf ihr Konto, sondern auf das Konto des Pflegeheimbetreibers überwiesen worden. Das Taschengeld habe der Betreiber des Pflegeheims letztendlich erst auf Intervention des Sozialamts auf das Konto der Betreuten überwiesen.

Gegen den Sozialhilfebescheid hatte der Betreuer Widerspruch eingelegt und diesen gesondert auch an den bDSB versandt, weil er darin auch die Verletzung datenschutzrechtlicher Vorschriften geltend gemacht hatte. Der bDSB hatte hierauf nicht reagiert, was der Betreuer nicht hinnehmen wollte.

Der TLfDI hat dem Betreuer zunächst erläutert, dass er in seiner gesetzlichen Funktion als Kontrollbehörde für öffentliche Stellen keine Weisungsbefugnis gegenüber den nach § 10a Thüringer Daten-

schutzgesetz (ThürDSG) bei den Daten verarbeitenden Stellen bestellten bDSB hat. Der TLfDI konnte daher den bDSB in Person nicht, wie vom Betreuer gewünscht, auffordern, eine Antwort auf den Widerspruch gegen den Sozialhilfebescheid zu geben. Der bDSB ist in seiner Funktion dem Leiter der Daten verarbeitenden Stelle (hier Landratsamt) unmittelbar zu unterstellen und hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung der datenschutzrechtlichen Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken.

Für den TLfDI ist die Arbeitsweise eines Beauftragten für den Datenschutz vor Ort nur beschränkt überprüfbar. Beispielsweise kann die notwendige Fachkenntnis zu den Fragen des Datenschutzes und der Datensicherheit hinterfragt und geprüft werden oder ob seine Tätigkeit keinem unüberwindbaren Interessenskonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt ist. Ansonsten ist für Einhaltung der datenschutzrechtlichen Vorschriften bei der Verarbeitung der personenbezogenen Daten die öffentliche Stelle verantwortlich, und sie unterliegt der Kontrolle des TLfDI nach § 37 ThürDSG.

Der Umgang mit der Beschwerde wegen der Überweisung der Sozialhilfe auf das Konto des Pflegeheims seitens des Landratsamts war also vom TLfDI nach § 11 ThürDSG zu prüfen und zu bewerten. Der TLfDI hat daher das Landratsamt zur Stellungnahme aufgefordert. Mangels einer konkreten Rechtsgrundlage konnte die Überweisung der Sozialhilfe auf das Konto des Pflegeheimbetreibers nämlich nur auf Verlangen des Hilfeempfängers oder mit dessen Einwilligung erfolgen. Das Landratsamt teilte mit, man habe die Angelegenheit geprüft und festgestellt, dass die Überweisung der Sozialhilfe leider ohne die erforderliche Einwilligung der Berechtigten auf das Konto des Pflegeheims erfolgte. Es sei die übliche Verfahrensweise, die direkte Zahlung der Sozialhilfe an das Pflegeheim zu leisten. Zur grundsätzlichen Entlastung der Hilfeempfänger und der Betreuer werde dies in der Regel sehr gerne in Anspruch genommen. In zukünftigen Fällen werde jedoch in Absprache mit dem bDSB sichergestellt, dass ohne die erforderliche Einwilligung des Betroffenen keine Zahlungen unmittelbar an das Pflegeheim bzw. dessen Träger erfolgen. Damit wird zukünftig den datenschutzrechtlichen Erfordernissen Rechnung getragen.

Das Handeln eines bDSB ist der öffentlichen Stelle zuzuschreiben, die der Kontrolle des TLfDI unterliegt. Sozialhilfe darf nicht einfach

ohne Verlangen oder Einwilligung des Betroffenen auf das Konto des Pflegeheims überwiesen werden, auch wenn dies in der Regel gerne von den Hilfeempfängern in Anspruch genommen wird. Der Fall zeigt wieder einmal, dass, auch wenn etwas im Sinne der Betroffenen gut gemeint ist, dies nicht immer auch in seinem Interesse sein muss.

11.43 Illegaler Datenhandel auch bei Thüringer Behörden? – Zur Anwerbung von neuen Krankenversicherten

Gegen Ende des Jahres 2013 informierte der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz über ein Verfahren gegen ein Versicherungsunternehmen wegen des Verdachts des illegalen Datenhandels. Das Versicherungsunternehmen hatte ein bundesweites Netz von Vertrauensleuten aufgebaut, aus dem heraus Hinweise auf mögliche Kunden, insbesondere junge Beamtinnen und Beamte, gegeben werden. Diesem Vertrauensleutesystem gehörten zum erheblichen Teil auch Mitarbeiter des öffentlichen Dienstes an. In der überregionalen Presse war die Rede von mehr als 10.000 Beamten. Insofern war es angeraten, die Landesregierungen auf die Ermittlungen anzusprechen und anzuregen, dass insbesondere bei den personalverwaltenden Stellen des Landes und der Kommunen untersucht wird, in welchem Umfang Mitarbeiter des öffentlichen Dienstes als Vertrauensleute des Versicherungsunternehmens fungierten, wie diese Nebentätigkeit praktisch ausgestaltet war, ob sie angezeigt und vergütet war.

Beschäftigten- und Bewerberdaten im öffentlichen Dienst unterfallen dem Personalaktengeheimnis. Ihre Weitergabe ist an die gesetzlichen Regelungen gebunden. Für die Weitergabe durch Mitarbeiter von Personalverwaltungen an ein Versicherungsunternehmen existiert grundsätzlich keine Befugnis.

Weiteren Pressemeldungen zufolge hatten im Zuge der Bestechungsvorwürfe gegen Mitarbeiter des Versicherungsunternehmens auch Durchsuchungen der Geschäftsstellen in Thüringen stattgefunden. Weiterhin wurde bekannt, dass die Anklagebehörde seit geraumer Zeit gegen unbekannte Mitarbeiter auch der öffentlichen Verwaltung ermittle. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat diese Entwicklung zum Anlass genommen, die Landesregierung auf die Problematik aufmerksam zu machen. Die Nutzung und Weitergabe von perso-

nenbezogenen Daten von Beschäftigten und Bewerbern, die dem Personaldatenschutz unterfallen, würden einen Verstoß gegen datenschutzrechtliche Vorschriften darstellen. Gemäß dem damals gültigen § 93 Abs. 2 und dem seit 1. Januar 2015 gültigen § 85 Abs. 2 Thüringer Beamtengesetz (ThürBG) dürfen Auskünfte an Dritte nur mit Einwilligung des Betroffenen gegeben werden, sofern die dort formulierten Ausnahmen nicht vorliegen. Durch den Verweis auf die dienstrechtlichen Vorschriften in § 33 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gilt dies ebenso für Tarifbeschäftigte. Für die Vermittlungstätigkeit für eine Versicherung gelten keine Ausnahmen von dem Einwilligungserfordernis. Daher regte der TLfDI an, insbesondere die personalverwaltenden Stellen des Landes und der Kommunen auf die Problematik hinzuweisen. Rückinformationen zu tatsächlichen Feststellungen, dass Beschäftigte in personalverwaltenden Stellen unbefugt Personaldaten von dort Beschäftigten übermittelt hätten, gab es nicht.

Das Bußgeldverfahren hatte der LfDI Rheinland-Pfalz Ende des Jahres 2014 einvernehmlich mit dem Versicherungsunternehmen abgeschlossen. Grundlage hierfür war unter anderem die Umstellung des Vertriebs bei dem Versicherungsunternehmen. Die Datenschutzbestimmungen sollen zukünftig insbesondere auch dadurch eingehalten werden, dass neue Kundenwerbungen durch Informationen von Kollegen oder Kontaktaufnahmen ohne das Einverständnis der Betroffenen für die Zukunft ausgeschlossen werden.

Konkrete Hinweise darauf, dass personalverwaltende Stellen in den öffentlichen Stellen des Freistaats Thüringen an dem illegalen Datenhandel beteiligt gewesen sein könnten, sind dem TLfDI nicht zur Kenntnis gelangt.

Der TLfDI nimmt auch hier sachdienliche Hinweise gern entgegen.

Personaldaten unterliegen einem besonderen Schutz. Die Übermittlung von Daten eines Beschäftigten im öffentlichen Dienst an ein Versicherungsunternehmen zum Zweck der Kundenwerbung ist nur mit Einwilligung des Betroffenen zulässig.

11.44 Das Jugendamt hat alles richtig gemacht

Eine Mutter wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Sie habe sich mehrmals in einer Unterhaltssache an das Jugendamt einer Stadt mit

der Bitte um Akteneinsicht gewandt und keine Antwort erhalten. Außerdem habe das Jugendamt die in der Unterhaltssache beteiligte Gegenpartei, den Vater des unterhaltsberechtigten Kindes, angerufen und unaufgefordert über die Inhalte des Schreibens der Bürgerin an das Jugendamt informiert.

Der TLfDI schrieb das Jugendamt mit der Bitte um Stellungnahme an. Nach § 25 Abs.1 Sozialgesetzbuch (SGB) Zehntes Buch (X) muss die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Eine Übermittlung von Sozialdaten ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt.

Das Jugendamt teilte mit, dass die Beschwerdeführerin persönlich im Jugendamt vorgesprochen habe. Dort seien ihr die Entscheidungen zur Unterhaltsberechnung im konkreten Fall erläutert worden. Die von ihr schriftlich gestellten Fragen seien beantwortet worden. Ihr seien die vom Kindsvater nachgereichten Unterlagen vorgelegt und von Akteninhalten Kopien überlassen worden. Der Vorwurf, dass keine Akteneinsicht gewährt worden sei, wurde deshalb vom Jugendamt zurückgewiesen. Zur telefonischen Kontaktierung des Kindesvaters teilte das Jugendamt mit, dass der Kindesvater nach dem letzten Schreiben der Beschwerdeführerin telefonisch informiert worden sei, dass die Kindesmutter weitere Fragen zur Unterhaltsberechnung habe. Des Weiteren seien mit dem Kindesvater die noch offenen Fragen besprochen worden. Er wurde durch das Jugendamt aufgefordert, weitere Unterlagen nachzureichen und im Jugendamt vorzusprechen.

Der TLfDI hat keine Anhaltspunkte dafür gefunden, dass die schriftlichen Erläuterungen des Jugendamtes nicht den Tatsachen entsprachen. Eine unzulässige Übermittlung von Sozialdaten an den Kindesvater erfolgte nach dieser Darlegung nicht. Es gab keine Anhaltspunkte dafür, dass die schriftlichen Erläuterungen des Jugendamtes nicht den Tatsachen entsprachen. Sie waren alle mit konkreten Terminen und weiteren Einzelheiten belegt worden. Dies wurde der Beschwerdeführerin mitgeteilt. Der Aufforderung des TLfDI, sich hierzu nochmals zu äußern, kam sie nicht nach. Daher bestand kein weiterer Handlungsbedarf.

Die Behörde muss den Beteiligten Einsicht in die das Verfahren betreffenden Akten gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. In welcher Weise dies geschieht, ist nicht verbindlich festgelegt. Es reicht gegebenenfalls auch eine mündliche Information und die Übergabe von Kopien aus der Akte.

11.45 Sozialdatenschutz im Eilverfahren

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil eine Stadt Sozialdaten bei Dritten erhoben hatte. Dem lag folgender Sachverhalt zugrunde:

Der Betroffene hatte die Stadt in einem Eilverfahren verklagt, ihm die Kosten der Unterkunft zuzusichern und seine Umzugskosten zu übernehmen. Es handelte sich dabei um den „klassischen“ Ausnahmefall der Vorwegnahme der Hauptsache. Sofern eine positive Entscheidung für den Antragsteller im einstweiligen Verfahren getroffen worden wäre, wäre diese später in einem folgenden Hauptsacheverfahren nicht mehr revidierbar gewesen. Nach dem Eingang der Antragsschrift bei der Stadt betrug die Frist zur Stellungnahme eine Woche. Da der Umzugstermin kurz danach anberaumt worden war, musste die Stadt damit rechnen, dass unmittelbar nach der Antragserwiderung durch die Stadt auch eine gerichtliche Entscheidung folgen würde.

Kurzfristig wurde eine Vorortbesichtigung der neuen Wohnung vom Außendienst der Stadt veranlasst. Es wurde festgestellt, dass das Klingelschild bereits mit dem Namen des Beschwerdeführers sowie mit dem Namen einer weiteren Person beschriftet worden war. Da der andere Name aus der Verwaltungsakte nicht bekannt war, lag die Vermutung nicht fern, dass eine weitere Person mit in der Wohnung lebte, was sich auf die Höhe des Anspruchs nach dem Sozialgesetzbuch (SGB) Zweites Buch (II) ausgewirkt hätte. Die Stadt nahm an, dass eine Nachfrage und direkte Erhebung beim Betroffenen angesichts der anwaltlichen Vertretung nur über den Prozessbevollmächtigten hätte erfolgen können, was innerhalb der Frist zur Stellungnahme nicht mehr aussichtsreich erschien. Sie nahm daher Kontakt mit dem Vermieter auf, um in Erfahrung zu bringen, welche Personen die Wohnung bewohnten. Damit hatte die Stadt Jena Sozialdaten bei einem Dritten erhoben.

Letztendlich kommt es bei der datenschutzrechtlichen Bewertung darauf an, ob der betreffende Mitarbeiter der Stadtverwaltung nach § 67a Abs. 2 Nr. 2 Buchstabe b, bb) SGB Zehntes Buch (X) Sozialdaten bei dem Vermieter hätte erheben dürfen. Dies wäre der Fall, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert hätte und keine Anhaltspunkte dafür bestanden hätten, dass seine überwiegenden schutzwürdigen Interessen beeinträchtigt würden. Schutzwürdige Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten sprechen, sind insbesondere dann gegeben, wenn der Leistungsträger notwendigerweise Sozialdaten des Betroffenen an den Dritten übermitteln muss, um die Datenerhebung zu ermöglichen. So kann auch die direkte Kontaktaufnahme, die damit verbunden ist, dass der Vermieter erfährt, dass eine Person Leistungsempfänger nach dem SGB II ist, Anhaltspunkt für eine Beeinträchtigung seiner schutzwürdigen Interessen sein.

Die Stadt berief sich auf den konkreten Missbrauchsverdacht, weswegen das schutzwürdige Interesse des Betroffenen zurücktreten müsse. In seinem Urteil vom 25. Januar 2102 (Az.: B 14 AS 65/11R) legte das Bundessozialgericht dar, dass schutzwürdige Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten im Rahmen des § 67a Abs. 2 Nr. 2 Buchst. b, bb SGB X sprechen könnten, wegen einer hohen Eilbedürftigkeit der Angelegenheit zurückgestellt werden.

Allerdings hat die Stadt den Wortlaut des § 13 Abs. 3 SGB X nicht vollständig beachtet. Danach muss sich die Sozialbehörde zwar an den Bevollmächtigten wenden, der für das Verfahren bestellt ist. Sie kann sich aber auch an den Beteiligten selbst wenden, soweit er zur Mitwirkung verpflichtet ist. Wendet sich die Behörde an den Beteiligten, muss der Bevollmächtigte verständigt werden. Nach all dem wäre wohl auch eine Erhebung beim Betroffenen möglich gewesen. Angesichts der hohen Eilbedürftigkeit war es aber nicht rechtsfehlerhaft, in der konkreten Situation vom Vorliegen der Voraussetzungen des § 67a Abs. 2 Nr. 2 Buchstabe b, bb SGB X auszugehen.

Die Stadt hat mitgeteilt, dass der vorliegende Sachverhalt deutlich vor Augen geführt habe, dass sich – auch und gerade in Eilsituationen – die Grenzen der zulässigen Datenerhebung in einem Bereich abspielen, der juristisch nur schwer erfassbar ist. Das hier im Streit stehende Verfahren war für die Stadt Anlass, die mit der gerichtlichen Vertretung befassten Mitarbeiter nochmals im Umgang mit Sozialdaten zu sensibilisieren und darauf hinzuwirken, dass in jedem

Einzelfall die Interessen des Betroffenen sorgsam in den Blick zu nehmen sind, bevor sich für ein Abweichen vom Grundsatz der unmittelbaren Datenerhebung entschieden wird.

Sozialdaten dürfen nur in den engen gesetzlich benannten Ausnahmefällen bei Dritten erhoben werden. Schutzwürdige Interessen des Betroffenen, die gegen eine Datenerhebung bei Dritten sprechen, sind insbesondere dann gegeben, wenn der Leistungsträger notwendigerweise Sozialdaten des Betroffenen an den Dritten übermitteln muss, um die Datenerhebung zu ermöglichen. Im Einzelfall kann eine hohe Eilbedürftigkeit für die Zulässigkeit der Datenerhebung bei Dritten sprechen.

11.46 Anonymisierung von Pflegedienstmitarbeitern zum Zweck der Entgeltsatzverhandlungen

Regelmäßig müssen Pflegeheimträger und Pflegedienste im Rahmen der mit dem hierfür zuständigen überörtlichen Sozialhilfeträger (Thüringer Landesverwaltungsamt – TLVwA) geführten Entgeltsatzverhandlungen auf der Grundlage des Sozialgesetzbuchs (SGB) Zwölftes Buch (XII) auch anonymisierte Daten zu den eingesetzten Mitarbeitern vorlegen.

Eine Rehabilitationseinrichtung hatte sich anwaltlich vertreten an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt, mit dem Vorbringen, das TLVwA verlange zur Plausibilisierung der prospektiv zu vereinbarenden Entgeltsätze Einsicht in die Personalakten sämtlicher der für die Einrichtung tätigen Beschäftigten – rückwirkend seit 2012. Darüber hinaus sollten ebenfalls zur Plausibilisierung der nach §§ 75 ff. SGB XII zu verhandelnden Entgeltsätze – nach Personalnummern geordnet – Aufstellungen sämtlicher Beschäftigter über deren Bruttovergütung, die gesetzlichen Gehaltsabzüge, die Nettovergütung sowie Eingruppierung vorgelegt werden.

Der TLfDI schrieb das TLVwA an und vertrat die Auffassung, da es sich bei Personalakten um eine Sammlung personenbezogener Daten über die jeweils Betroffenen handele, sei zu differenzieren, ob die Einsicht in alle Unterlagen erforderlich ist oder ob sich die Kenntnis auf konkret zu bezeichnende Angaben eingrenzen lässt. Unter Umständen reiche die Auskunft zu diesen Angaben aus oder die Einsicht lasse sich auf einzelne Dokumente beschränken. Auf diese Weise

werde eine Verarbeitung personenbezogener Daten vermieden, die in den Unterlagen vorhanden, für die Aufgabenerfüllung der öffentlichen Stelle jedoch nicht erforderlich seien.

Das TLVwA bestritt, Personalakten verlangt zu haben. Ein entsprechendes Verlangen konnte aus dem vorgelegten Schriftwechsel nicht entnommen und daher nicht bewiesen werden. Weiterhin teilte das TLVwA dem TLfDI mit, dass aus der aktuellen Rechtsprechung heraus eine plausible und nachvollziehbare Darlegung der prospektiven „Gestehungskosten“ für die Prüfung vorausgesetzt werde. Die tatsächlichen Personalkosten seien anzuerkennen, wenn sie sich aus der vorliegenden Tarifbindung bei funktionsgerechter Eingruppierung ergeben. Der Träger habe hierzu eine Nachweispflicht. Bislang seien von der Einrichtung die Stellennummern mit Angabe von Funktionsbereich, Eingruppierung und wöchentlicher Arbeitszeit vorgelegt worden, die im Zusammenhang mit dem für den Träger gültigen Tarifwerk eine vorläufige Prüfung zugelassen haben. Es müsse jedoch zusätzlich überprüft werden, ob mit jeder Stellennummer auch eine tatsächliche Stellenbesetzung verbunden sei. Die Stellennummer resultiere nämlich im vorliegenden Fall ausschließlich aus dem Soll-Stellenplan heraus und umfasse auch möglicherweise nicht besetzte Stellen. Deshalb müssten die Personalnummern genannt werden, weil diese den Schluss auf die tatsächliche Besetzung eindeutig zuließen. Dies gehe im Übrigen mit dem Urteil des BSG vom 29. Januar 2009 (B3P7/08R) konform, da bei Zweifeln über die voraussichtlich künftigen Gestehungskosten die Nachweispflicht der Einrichtung bis zum Nachweis der in der Vergangenheit angefallenen Kosten reicht. Eine namentliche Untersetzung der Personalnummer werde nicht verlangt, da dies tatsächlich dem in der Rechtsprechung und in der Schutznorm des § 85 Abs. 3 Satz 5 SGB XI vorgegebenen Grundsatz widersprechen würde, wonach personenbezogene Daten zu anonymisieren sind.

Der TLfDI teilte der Rehabilitationseinrichtung seine datenschutzrechtliche Bewertung unter Einbeziehung des Vorbringens des TLVwA mit. Danach sind Personalnummern unter der Voraussetzung, dass eine konkrete namentliche Mitarbeiterliste vorliegt, personenbeziehbar. Werden nur die Personalnummern ohne Bezüge zu den natürlichen Personen angegeben, kann von einer anonymisierten Darstellung ausgegangen werden. Eine Anonymisierung liegt dann vor, wenn keine oder nur mit unverhältnismäßigem Aufwand mögliche Zuordnung zu den Namen der betroffenen Beschäftigten besteht

(§ 85 Abs. 3 Satz 5 SGB XII). Daher konnten die Angaben der Personalnummern zur weiteren Prüfung der tatsächlich besetzten Stellen vom TLVwA angefordert werden.

Kurze Zeit später meldete sich die Vertretung anderer Einrichtungen und beklagte sich darüber, dass das TLVwA sich mit der bisherigen Praxis der Angabe von Stellennummern oder Kürzeln der einzelnen Mitarbeitern nicht mehr zufriedengebe und ab sofort unter Berufung auf das Schreiben des TLfDI nun die Personalnummern der Mitarbeiter verlange. Sie bat daher den TLfDI um verbindliche Mitteilung, unter welchen Umständen die Benennung von Personalnummern unter den datenschutzrechtlichen Gesichtspunkten zulässig ist und/oder wie anderweitig rechtlich verfahren werden kann, um schützenswerte Belange der Mitarbeiter in ihren Mitgliedseinrichtungen nicht zu verletzen.

Der TLfDI hat hierzu erläutert, dem zitierten Schreiben habe ein zu prüfender Sachverhalt zugrunde gelegen, in dem das TLVwA einen erhöhten Prüfaufwand geltend machte, nachdem es Zweifel an den Angaben einer antragstellenden Einrichtung gab. Unter diesem Blickwinkel wurde die Angabe der Personalnummer als zulässig erachtet. Dies schließe jedoch nicht aus, dass auch Kürzel von Mitarbeitern eine datenschutzgerechte Lösung darstellen können. Der TLfDI hatte in der Bearbeitung der ersten Anfrage auf den dargelegten Sachverhalt abgestellt, jedoch kein allgemeingültiges Erfordernis postuliert. Aus datenschutzrechtlicher Sicht sind daher beide Benennungsmöglichkeiten in der Liste aus Gründen der Unterscheidbarkeit akzeptabel.

Sind nach den Vorschriften des Sozialgesetzbuchs anonymisierte Daten von Beschäftigten zu Prüfungszwecken vorzulegen, muss sichergestellt sein, dass keine oder nur mit unverhältnismäßigem Aufwand eine Zuordnung zu den einzelnen Beschäftigten möglich ist. Soweit die Unterscheidbarkeit der einzelnen Beschäftigten aus Plausibilitätsgründen zu Prüfzwecken erforderlich ist, kann dem nachgekommen werden, indem die Kürzel der Mitarbeiter oder deren Personalnummer oder deren Stellenzeichen angegeben werden. Entscheidend ist, dass der Prüfbehörde grundsätzlich keine Reanonymisierung möglich sein darf.

11.47 Medizinische Diagnose in Behördenbescheid – kein Problem

Ein Bürger wandte sich mit folgendem Anliegen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI): Er hatte von einem Landratsamt einen Bescheid erhalten, in dem sein Antrag auf die Erteilung eines Schwerbehindertenausweises nach § 69 Abs. 5 Sozialgesetzbuch (SGB) Zehntes Buch (X) mit der Begründung abgelehnt worden war, dass festgestellt worden sei, der Betroffene leide an dem Asperger-Syndrom und habe infolgedessen nur leichte soziale Anpassungsschwierigkeiten. In der Benennung der konkreten ärztlichen Diagnose neben den festgestellten Beeinträchtigungen sah der Betroffene einen Datenschutzverstoß.

Diese Auffassung konnte der TLfDI nicht bestätigen. Die Behörde durfte die personenbezogenen Daten des Beschwerdeführers verarbeiten, da aufgrund seines Antrags die Datenverarbeitung zum Aufgabenbereich der Behörde gehört, § 67c SGB X. Für den ablehnenden Bescheid gelten die formalen Anforderungen nach § 33 ff. SGB X. Es handelt sich um einen Verwaltungsakt, der inhaltlich hinreichend bestimmt sein muss, § 33 Abs. 1 SGB X. Er ist außerdem mit einer Begründung zu versehen, § 35 Abs. 1 Satz 1 SGB X. Nach Auffassung des TLfDI waren die Ausführungen zu medizinischen Diagnosen erforderlich, um die von der Behörde getroffene Entscheidung näher zu begründen. Der Bescheid ist an den Betroffenen gerichtet und geht damit auch nur ihm per Post zu. Sofern der Bescheid bei anderen Stellen vorlegt werden muss, kann gegebenenfalls eine Kopie angefertigt werden, in der die Schwärzung medizinischer Angaben möglich ist. Daher bestanden gegen die Aufnahme der Diagnosen in dem konkreten Bescheid keine datenschutzrechtlichen Bedenken.

Wenn der Bescheid einer Behörde an einen Betroffenen gerichtet wird, muss in diesem Bescheid alles stehen, was zur Begründung der Entscheidung erforderlich ist. Das gilt auch, wenn es sich um sensible Angaben wie Gesundheits- oder Sozialdaten handelt.

11.48 Wohin mit dem Schriftverkehr zum Betrieblichen Eingliederungsmanagement (BEM)?

Niemand ist absolut sicher vor Erkrankung: Erkältung, Grippewelle, Rückenprobleme und weitere Beeinträchtigungen führen zur Arbeitsunfähigkeit. Wenn Beschäftigte jedoch innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, hat der Gesetzgeber ein Hilfsangebot vorgesehen. Nach § 84 Abs. 2 Sozialgesetzbuch (SGB) Neuntes Buch (IX) wird der Arbeitgeber mit Zustimmung und Beteiligung der betroffenen Person verpflichtet, mit der zuständigen Interessensvertretung zu klären, wie die Arbeitsunfähigkeit möglichst überwunden und mit welchen Leistungen und Hilfen erneuter Arbeitsunfähigkeit vorgebeugt werden kann. Ziel des so genannten betrieblichen Eingliederungsmanagements (BEM) ist es, den Arbeitsplatz zu erhalten. Die betroffene Person/der Bedienstete kann der Durchführung eines BEM zustimmen oder dies ablehnen.

Dem Angebot an einen Betroffenen zu einem BEM-Gespräch kommt besondere Bedeutung zu, weil die Dienststelle dem Personalrat aufgrund dessen Kontrollfunktion unter Umständen beweisen können muss, dass sie ihrer Verpflichtung nach § 84 Abs. 2 SGB IX nachgekommen ist.

Ein Betroffener fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach, ob es denn in Ordnung sei, dass seine Antwort auf das Angebot, egal, ob er es annehme oder nicht, zur Personalakte genommen werde.

Nach § 50 Beamtenstatusgesetz gehören zur Personalakte alle Unterlagen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden (§ 81 Abs. 1 Satz 1 Thüringer Beamtengesetz – ThürBG). Das Angebot zu einem BEM-Gespräch kann aus Sicht des TLfDI als im unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehend angesehen werden und ist daher konsequenterweise in der Personalakte abzuheften. Die Abheftung in der Personalakte hat den Vorteil, dass damit der Schutz für besonders sensible personenbezogene Daten automatisch hergestellt ist.

Von der Personalakte zu unterscheiden sind andere Akten (Sachakten), in denen auch Schriftstücke mit personenbezogenen Daten Beschäftigter abgelegt werden können, die für das Dienstverhältnis

verarbeitet oder genutzt werden. Da sich im Falle der Ablehnung eines BEM-Gesprächs keine weiteren Konsequenzen für den Betroffenen oder sein Dienstverhältnis ergeben und das Anschreiben an den Betroffenen wie oben ausgeführt nur dem Nachweis des Angebots nach § 84 Abs. 2 SGB IX dient, hat es der TLfDI in der Vergangenheit nicht kritisiert, wenn das Angebot der Dienststelle mit der Ablehnung zu einer hierzu angelegten Sachakte genommen wurde. Dem Betroffenen stehen hierzu ebenfalls Einsichtsrechte zu (§ 84 Abs. 4 ThürBG), sodass für ihn keine Nachteile erkennbar sind. Für den Vorgang sind entsprechende Aufbewahrungsfristen vorzusehen.

Zum Nachweis, dass dem Betroffenen ein Angebot zum Eingliederungsmanagement nach § 84 Abs. 2 SGB IX unterbreitet wurde, kann der Schriftverkehr zur Personalakte genommen werden. Es bestehen aber auch keine durchgreifenden datenschutzrechtlichen Bedenken, die Angebote mit den ablehnenden Antworten von Betroffenen in einer hierzu geführten Sachakte abzuheften.

11.49 Löschungsresistente Daten im Gesundheitsamt

Im Rahmen seiner Kontrolltätigkeit ist der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam gemacht worden, dass der KJÄD (= Kinder- und Jugendärztlicher Dienst) der Gesundheitsämter in Thüringen im Rahmen von Einschulungsuntersuchungen ein Programm verwendet, bei dessen Benutzung datenschutzrechtliche Probleme bei der Datenlöschung bestehen. Zum einen erfolgt in diesem System keine automatische Löschung der hochsensiblen Patientendaten, sondern nur eine Archivierung zum Stichtag des 18. Geburtstags, wobei aber der Zugriff auf diese Daten wohl über diesen Zeitpunkt hinaus weiterhin möglich ist. Zum anderen ist der Zugriff auf eine so genannte Zentralkartei offensichtlich von allen Arbeitsplätzen aus uneingeschränkt möglich. Das bedeutet, dass Mitarbeiter des KJÄD auch auf Patientendaten zugreifen können, die sie zu ihrer Aufgabenerfüllung eigentlich nicht (mehr) benötigen. Die Gesundheitsämter in Thüringen wurden vor diesem Hintergrund vom TLfDI angeschrieben und gefragt, ob das betreffende Programm im Rahmen von Einschulungsuntersuchungen seitens des KJÄD angewandt wird und wenn ja, inwieweit die Möglichkeit für den Dienst besteht, die Zugriffsrechte der Benutzer auf die für sie notwendigen Informationen zu

beschränken. Es wurde auch gebeten mitzuteilen, ob der KJÄD ein Rollen- und Berechtigungskonzept für die Zugriffsrechte erstellt hat oder andere Beschränkungsmöglichkeiten bestehen. Die Gesundheitsämter wurden gebeten darzulegen, ob dort entsprechende Vorkehrungen nach § 9 Thüringer Datenschutzgesetz getroffen wurden oder schriftliche Regelungen zur regelmäßigen Löschung von Patientendaten bestehen. Nach Auffassung des TLfDI muss die Löschung manuell, etwa durch einen Mitarbeiter, erfolgen, sofern es keine Möglichkeit einer automatischen Löschung der nicht mehr benötigten Daten gibt.

Aus den Antworten der Gesundheitsämter ließ sich entnehmen, dass alle Gesundheitsämter sehr bemüht sind, datenschutzrechtliche Vorgaben einzuhalten. Dort ist man sich der Notwendigkeit des sorgsamsten Umgangs mit den Daten sehr bewusst. Bei der „Zentralkartei“ handelt es sich wohl um eine reine Adressdatei. In den Gesundheitsämtern gibt es auch Zugriffs- und Berechtigungskonzepte, allerdings keine einheitlichen landesweiten Vorgaben hierzu.

Große Unsicherheiten bestehen aber in Bezug auf die Notwendigkeit des Löschsens der Daten. Nicht eindeutig klar ist, welche Daten für die Dauer der ärztlichen Aufbewahrungsfrist zu speichern sind und welche Daten nicht hierunter fallen. Hier war ein sehr großer Bedarf an verbindlichen Regelungen festzustellen.

Eine datenschutzkonforme Lösung des Problems konnte derzeit noch nicht erreicht werden. Der TLfDI wird im nächsten Berichtszeitraum die Datenverarbeitung in mindestens einem Gesundheitsamt vor Ort prüfen und dann gemeinsam mit den Gesundheitsämtern und der zuständigen Aufsichtsbehörde Leitlinien zur Aufbewahrung von Daten im Gesundheitsamt erarbeiten.

Grundsätzlich dürfen Daten nur solange gespeichert werden, wie ihre Vorhaltung für die Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist. Zu beachten sind aber auch bestehende Aufbewahrungsfristen. Es ist im Gesundheitsamt konkret zu prüfen, welche personenbezogenen Daten unter die ärztliche Aufbewahrungsfrist fallen.

11.50 Auskunft zu und Löschung von Sozialdaten

Eine Beschwerdeführerin wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI)

und trug vor, sie habe an das Sozialamt eine Anfrage gerichtet und Anträge nach dem Landesdatenschutzgesetz gestellt. Sie wollte die Rechtsgrundlagen und den Sachzweck der Speicherung ihrer personenbezogenen Daten im Zusammenhang mit einem Vorgang wissen, der ihren von ihr getrennt lebenden Ehemann betraf. Gleichzeitig hatte sie die Löschung aller sie betreffenden Daten, die ohne Rechtsgrundlage verarbeitet werden, beantragt. Hierauf habe sie keine Antwort erhalten.

Das Sozialamt teilte auf Nachfrage des TLfDI zunächst mit, es könne leider keine Antwort geben, denn die Akte befände sich aufgrund eines Rechtsstreits beim Sozialgericht. Da sich gerichtliche Streitigkeiten über einen längeren Zeitraum ziehen können, bat der TLfDI nach geraumer Zeit um Sachstandsmitteilung. Da der Abschluss des Verfahrens nicht einzuschätzen war, forderte das Sozialamt die Akte vom Sozialgericht an und nahm gegenüber dem TLfDI Stellung. Danach gestaltete sich die Angelegenheit so, dass für den Ehemann Leistungen nach dem Sozialgesetzbuch beantragt waren. Ob die Ehegatten nun getrennt lebten und ab wann, sollte geklärt werden, weil dies maßgeblich zur Berechnung des Bedarfs war. Dies war gegenüber dem TLfDI schlüssig dargelegt worden. Außerdem teilte das Sozialamt mit, die Beschwerdeführerin, die auch gerichtlich vor einiger Zeit zur Betreuerin ihres Ehemannes bestellt worden war, habe aktenkundig Einsicht in die Akte genommen.

Der TLfDI teilte der Beschwerdeführerin daraufhin mit, dass sie mit der Akteneinsicht vollumfänglich Auskunft zu den zu ihrer Person verarbeiteten Daten erhalten habe und damit auch die Rechtsgrundlagen der Verarbeitung ihrer personenbezogenen Daten aus der Akte entnehmen konnte. Da die Darlegung des Sozialamts zur Datenverarbeitung nach den sozialgesetzlichen Vorschriften schlüssig war, wurde sie gebeten, konkret darzulegen, welche Daten denn aus ihrer Sicht unrichtig oder nicht mehr erforderlich seien, sodass sie nach § 84 Sozialgesetzbuch (SGB) Zehntes Buch (X) zu löschen oder zu sperren wären. Allein der Grund, dass Ehegatten zwischenzeitlich getrennt leben oder geschieden sind, macht die Datenverarbeitung nicht unzulässig oder unrichtig. Auch ist sehr fraglich, ob die bereits erhobenen Daten damit zur Aufgabenerfüllung nicht mehr erforderlich sind und aus diesem Grund einem Lösungsanspruch unterliegen könnten. Schließlich ist zu beachten, dass Sozialakten das behördliche Handeln widerspiegeln und nach Abschluss einer Aufbewahrungsfrist unterfallen. Entfallen Ansprüche oder ändern sich die

Lebensumstände, sind nicht automatisch frühere Sachverhalte zu löschen. Ob die Daten eines inzwischen vom Leistungsempfänger getrennten Ehegatten gelöscht werden müssen oder einer Sperrung unterfallen und damit einer Nutzungsbeschränkung unterliegen, ist im Einzelfall zu beurteilen.

Sobald die Beschwerdeführerin ihr Anliegen konkretisiert, wird der TLfDI der Angelegenheit weiter nachgehen.

Nach § 84 SGB X sind Sozialdaten zu berichtigen, wenn sie unrichtig sind. Sie sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Allein die Änderung des Familienstandes macht die Verarbeitung von personenbezogenen Daten des von einem Sozialleistungsempfänger getrennten Ehepartners grundsätzlich noch nicht unzulässig.

11.51 Thüringer Verordnung über die statistischen Angaben für die Gleichstellung von Frauen und Männern nach dem Thüringer Gleichstellungsgesetz

Das (damalige) Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) stellte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) am Ende des Berichtszeitraumes des 10. Tätigkeitsberichtes den Entwurf der Thüringer Verordnung über die statistischen Angaben für die Gleichstellung von Frauen und Männern in Dienststellen des Freistaats Thüringen (Thüringer Gleichstellungsstatistikverordnung – ThürGleichStatVO) mit der Bitte um summarische Prüfung zur Verfügung. Gleichzeitig bat das TMSFG den TLfDI um Mitteilung, ob Bedenken gegen den genannten Verordnungsentwurf aus datenschutzrechtlicher Sicht bestünden. Nach Information des TMSFG sollte die nach § 5 Abs. 2 Thüringer Gleichstellungsgesetz vorgesehene Anhörung des TLfDI nach Abschluss der Ressortabstimmung erfolgen. Der TLfDI nahm zum Entwurf der ThürGleichStatVO Stellung und merkte aus datenschutzrechtlichen Gesichtspunkten eine Vielzahl von kritischen Textpassagen an.

So teilte der TLfDI dem TMSFG beispielsweise mit, dass nicht für alle der nach § 1 Abs. 2 Nr. 6 bis 8 der Verordnung statistisch zu erfassenden Daten das Thüringer Gleichstellungsgesetz als Ermächtigungsgrundlage herangezogen werden könne und bat in Folge, den jeweiligen Passus in der Verordnung zu streichen.

Nach der Ressortabstimmung übersandte das TMSFG dem TLfDI wiederum den Entwurf der ThürGleichStatVO mit der Bitte um datenschutzrechtliche Stellungnahme. Der TLfDI musste nach Prüfung feststellen, dass seine kritischen Anmerkungen zum vorherigen Entwurf nicht in Gänze übernommen worden waren, sodass diese Punkte aus datenschutzrechtlicher Sicht erneut kritisiert wurden.

Zum Berichtszeitraumende stellte das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMA SGFF) dem TLfDI im Rahmen der Anhörung nach §§ 20, 21 Gemeinsame Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen (ThürGGO) den ressortabgestimmten Entwurf eines Ersten Gesetzes zur Änderung des Thüringer Gleichstellungsgesetzes und den ressortabgestimmten Entwurf der ThürGleichStatVO zur Verfügung. Der TLfDI hatte an diesen nichts mehr zu kritisieren, da seine unterbreiteten Anregungen nunmehr Eingang gefunden hatten.

Die Thüringer Gleichstellungsstatistikverordnung regelt die Erhebung geschlechtsspezifischer Daten zur Beschäftigung in der Landes- und Kommunalverwaltung. Diese Daten sind Grundlage für den von der Landesregierung nach § 14 des Thüringer Gleichstellungsgesetzes alle sechs Jahre zu erstellenden Erfahrungsbericht über die Gleichstellung von Frauen und Männern in den Dienststellen des Freistaates Thüringen. Darüber hinaus dienen die auf der Grundlage dieser Rechtsverordnung erhobenen Daten den personalführenden Dienststellen als Grundlage für die nach § 4 des Thüringer Gleichstellungsgesetzes zu erstellenden Gleichstellungspläne.

Die Anregungen des TLfDI zur Verordnung wurden umgesetzt, sodass diese den datenschutzrechtlichen Bestimmungen genügt.

11.52 Auskünfte über Kontenbewegung

Ein Antragsteller für die Grundsicherung für Arbeitsuchende, auch Arbeitslosengeld (ALG) II oder Hartz IV genannt, beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über eine vom Jobcenter veranlasste Kontenabfrage bei seiner Bank. In diesem Zusammenhang bat er den TLfDI auch um Mitteilung, ob das Jobcenter die Vorlage von ungeschwärtzten Kontoauszügen verlangen darf. In seiner Antwort verwies der TLfDI den Beschwerdeführer zunächst darauf, dass dem

Antragsteller nach § 60 Abs. 1 Sozialgesetzbuch (SGB) Erstes Buch (I) bei der Beantragung von Sozialleistungen eine Mitwirkungspflicht obliegt. Danach hat jeder, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte von Seiten Dritter zuzustimmen und Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen. Klare Vorgaben, welche Angaben gegebenenfalls vom Antragsteller auf Kontoauszügen oder anderen Unterlagen geschwärzt werden dürfen, lassen sich dem Gesetz leider nicht entnehmen. Um sowohl dem Recht auf informationelle Selbstbestimmung des Antragstellers als auch den Interessen des Sozialleistungsträgers angemessen Rechnung tragen zu können, sollte die Anforderung von Kontoauszügen zum Zwecke der Klärung einer konkreten Frage zu der Einkommens- und Vermögenssituation der Hilfesuchenden erforderlich sein, weil sie nicht mit der Vorlage anderer Unterlagen herbeigeführt werden kann oder weil konkrete Zweifel an der Vollständigkeit oder Richtigkeit der Angaben der Hilfesuchenden bestehen. Insbesondere bei Soll-Buchungen über geringere Beträge (regelmäßig bis 50 Euro) kann der Hilfesuchende die zu den Einzelbuchungen aufgeführten Texte in der Regel schwärzen. Der Betrag selbst muss sichtbar bleiben. Schwärzungen können unabhängig vom Betrag grundsätzlich dann vorgenommen werden, wenn die Buchungstexte Angaben über besonders geschützte Daten im Sinne des § 67 Abs. 12 SGB Zehntes Buch (X) enthalten. Dazu zählen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Beispielsweise kann bei Überweisungen von Mitgliedsbeiträgen an eine Partei bzw. eine Gewerkschaft oder bei Zahlungen an eine Religionsgemeinschaft die Bezeichnung der Organisation geschwärzt werden. Der Text „Mitgliedsbeitrag“ oder „Spende“ sollte lesbar bleiben, um Missverständnisse zu vermeiden. Hält das Jobcenter es in Einzelfällen für erforderlich, bestimmte Einzelbuchungen ungeschwärzt zur Kenntnis zu nehmen, ist dies gegenüber dem Betroffenen zu begründen. Dem hingegen kann das Schwärzen von Haben-Buchungen, also von Einnahmen, zu einer Verletzung der Mitwirkungspflicht führen, da grundsätzlich das gesamte Einkommen bei der Hilfeförderung zu berücksichtigen ist. Die Verpflichtung zur Vorlage von

Kontoauszügen gemäß § 60 SGB I stellt allerdings keine Befugnis zur Speicherung dieser Daten dar. Vielmehr dürfen diese nur dann gespeichert werden, wenn die Daten zur Aufgabenerfüllung im Einzelfall erforderlich sind. Grundsätzlich reicht es aus, wenn das Jobcenter in den Akten vermerkt, dass die Kontoauszüge vorgelegen haben und hieraus keine Anhaltspunkte für einen Leistungsmissbrauch ersichtlich sind. Der TLfDI forderte vom Jobcenter eine Stellungnahme, aus welchen Gründen dort bei einer Bank Kontendaten über den Betroffenen erhoben wurden. Wie aus dem Antwortschreiben hervorging, stützte das Jobcenter sein Auskunftersuchen an die Bank auf Regelungen des § 21 Abs. 1 S. 1 SGB Zweites Buch (II). Die Regelung erlaubt der Behörde, sich der Beweismittel zu bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält, wobei sich aus den materiellen Anforderungen des jeweiligen Fachrechts ergibt, welche Maßnahmen zur Beweisermittlung erforderlich sind. Im vorliegenden Fall hatte das Jobcenter ein Kontoabrufersuchen eingeleitet, worüber der Beschwerdeführer unterrichtet wurde. Das Bundeszentralamt für Steuern hatte daraufhin dem Jobcenter die Konten des Beschwerdeführers mitgeteilt. Daraufhin wurde der Betroffene zur Vorlage von Kontoauszügen aufgefordert, der dieser Forderung jedoch nicht nachkam. Der TLfDI teilte dem Beschwerdeführer abschließend mit, dass im begründeten Einzelfall ein Jobcenter bei einer Bank Kontendaten des Antragstellers erheben kann. Die Banken und Sparkassen müssen gemäß § 60 Abs. 2 SGB II Auskunft über Guthaben oder verwahrte Vermögensgegenstände erteilen. Grundsätzlich sind nach § 67a Abs. 2 SGB X die für den Antrag benötigten Daten beim Antragsteller zu erheben. Sind die Informationen, die bei der Antragsstellung vorliegen, nach Auffassung der Behörde nicht ausreichend, muss der Antragsteller aufgefordert werden, weitere Angaben zu machen und diese gegebenenfalls zu belegen. Wie der TLfDI feststellte, war diese Anfrage mit einem Schreiben des Jobcenters an den Antragsteller erfolgt. Weil dieser jedoch die von der Behörde verlangten Informationen nicht erteilte und diese Angaben aber für den TLfDI nachvollziehbar zur Durchführung der Aufgaben des Jobcenters erforderlich waren, durfte das Jobcenter nach § 60 Abs. 2 S. 1 SGB II bei der Bank den Kontostand bzw. die Kontoumsätze für den maßgeblichen Zeitraum erfragen.

Ein Antragsteller hat die zur Antragsbearbeitung der Grundsicherung von Arbeitssuchenden nach SGB II erforderlichen Angaben zu erteilen. Hierzu kann auch die Vorlage von Kontoauszügen gegenüber dem Jobcenter gehören. Alle Daten auf diesen Kontoauszügen, die nicht unbedingt als Nachweis erforderlich sind, dürfen vom Antragsteller geschwärzt werden. Erteilt der Antragsteller jedoch keine Informationen über die von ihm geführten Konten, darf das Jobcenter über eine zentrale Anfrage Informationen darüber enthalten, bei welchen Banken Konten des Betroffenen geführt werden. Kommt der Betroffene seiner Auskunftspflicht hierüber nicht nach, darf das Jobcenter sich an die betroffenen Geldinstitute wenden und dort die zur Aufgabenerfüllung erforderlichen Kontodaten erheben.

11.53 Digitalisierung von Akten im Schwerbehindertenrecht

Ein Landratsamt teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass es beabsichtige, die Akten im Schwerbehindertenrecht zu digitalisieren und fragte an, unter welchen Bedingungen dies aus datenschutzrechtlicher Sicht zulässig ist. In seiner Antwort verwies der TLfDI zunächst darauf, dass das Schwerbehindertenrecht im Sozialgesetzbuch (SGB) geregelt ist, weswegen für die datenschutzrechtliche Bewertung das SGB maßgeblich ist. Nach § 78a SGB Zehntes Buch (X) hat die Akten führende Stelle die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Anforderungen des SGB, insbesondere die in der Anlage zu § 78a SGB X genannten acht Anforderungen, zu gewährleisten. Ebenfalls ist herauszustellen, dass das Sozialgeheimnis nach § 35 SGB Erstes Buch sowohl gegenüber Dritten als auch innerhalb der verantwortlichen Stelle gewahrt bleibt. Daher ist zu gewährleisten, dass nur die Personen, die dazu befugt sind, Zugriff auf die Sozialdaten haben. Für die Digitalisierung der Schwerbehindertenakten muss ein eigenes IT-Sicherheitskonzept nach den Vorgaben des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) erstellt werden. Empfohlen wird, wie auf der Seite https://www.bsi.bund.de/DE/Themen/ITGrundsutz/ITGrundsutzStandards/ITGrundsutzStandards_node.html beschrieben vor-



zugehen und zunächst den Bedarf an Informationssicherheit anhand der festgestellten IT-Grundschutzstufe zu ermitteln, um dann anhand einer Risikoanalyse mögliche Sicherheitsmängel festzustellen und die erforderlichen Maßnahmen zur Risikominimierung schriftlich in Form von Dienstanweisungen festzulegen. Der TLFDI geht dabei davon aus, dass man sich im Bereich des Schwerbehindertenrechts durchweg in der Schutzstufe „hoch“ bis „sehr hoch“ bewegt. Im Internetangebot des BSI sind die BSI-Standards zum IT-Grundschutz unter den Stichwörtern IT-Grundschutz – IT-Grundschutz-Standards sowie die aktuelle Version der IT-Grundschutz-Kataloge unter IT-Grundschutz – IT-Grundschutz-Kataloge zu finden. Die nach dem Baukastenprinzip gegliederten IT-Grundschutz-Kataloge umfassen vom BSI kontinuierlich aktualisiertes Wissen, mit dem die in den BSI-Standards enthaltenen allgemeinen Empfehlungen zum Management von Informationssicherheit in der für die Verarbeitung von Sozialdaten verantwortliche Behörde umgesetzt werden können. In



jedem Fall sollten die digitalisierten Daten auf dem Server gemäß der Anlage zu § 78a SGB X mit dem Stand der Technik entsprechenden Verschlüsselungsverfahren verschlüsselt werden. Zudem ist ein Zugriffs- und Berechtigungskonzept zu erstellen, das auch die Mandantenfähigkeit gewährleistet. Die Orientierungshilfe „Mandantenfähigkeit“ des Arbeitskreises Tech-

nik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist unter:

https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_mandantenfaehigkeit.pdf zu finden. Weiterhin ist zum Beispiel auch festzulegen, auf welche Weise die Daten vor einem unbefugten Zugriff von außen geschützt werden (Beschaffenheit der Serverräume, Einsatz von Firewalls etc.). Auch muss festgelegt werden, wie sichergestellt wird, dass andere Mitarbeiter beim Scanvorgang keine Kenntnis der Sozialdaten erhalten. Wichtig ist auch, Regelungen dazu zu treffen, wie mit den auf dem Kopierer gespeicherten Scans umzugehen ist. Weiterhin ist zu prüfen, ob die Originaldokumente möglicherweise noch zu Beweis Zwecken benötigt werden. In diesem Fall dürfen die Originaldokumente nicht vernichtet werden oder sie müssen mit einer qualifizierten elektronischen Signatur eingescannt werden, da nur dann die Authentizität der Dokumente gewährleistet

ist. Mit dieser Beratung war das Landratsamt zunächst zufrieden. Ihm wurde angeboten, sich bei weiteren Fragen wieder an den TLfDI zu wenden.

Bei der Verarbeitung und Nutzung von Sozialdaten sind nach den Regelungen des § 78a SGB X und der Anlage zahlreiche technische und organisatorische Maßnahmen von der verantwortlichen Stelle zu treffen, um die Ausführungen der Vorschriften dieses SGB zu gewährleisten. Aufgrund des hohen bis sehr hohen Schutzbedarfs der Daten, dem Sozialdaten im Schwerbehindertenrecht unterliegen, sind Maßnahmen besonders sorgfältig auszuwählen.

11.54 Todesursachenrecherche

Im Rahmen einer großangelegten, bundesweiten Studie zur Gesundheit Erwachsener in Deutschland bat das die Studie durchführende Institut die Datenschutzbeauftragten des Bundes und der Länder um ihre datenschutzrechtliche Einschätzung zur Verfahrensgestaltung. Ein Schwerpunkt der Studie ist die Feststellung von Todesursachen für bereits verstorbene Studienteilnehmerinnen und -teilnehmer. Allerdings wird hierfür auf einen Datenpool zugegriffen, der aus einer vorhergehenden Studie in den Jahren 2008 bis 2011 stammt. Zum damaligen Zeitpunkt war eine Todesursachenrecherche noch nicht vom Forschungszweck umfasst. Aufgrund der Unmöglichkeit, bei den verstorbenen Probanden eine Einwilligung in die Verarbeitung ihrer personenbezogenen Daten zum Zweck der Todesursachenauswertung einzuholen, war vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu klären, unter welchen Bedingungen das Institut Auskünfte aus den von der unteren Gesundheitsbehörde geführten Toten- und Sektionsscheinen erhalten darf. Der TLfDI teilte dem Institut mit, dass in Thüringen die für den Wohnort des Verstorbenen zuständige untere Gesundheitsbehörde gemäß § 15 Abs. 4 Nr. 2 des Thüringer Bestattungsgesetzes auf Antrag Auskünfte aus Totenscheinen und Sektionsscheinen im erforderlichen Umfang erteilen kann. Voraussetzung ist, dass der Antragsteller, hier also das Institut, die Angaben für ein wissenschaftliches Forschungsvorhaben benötigt und das für das Gesundheitswesen zuständige Ministerium festgestellt hat, dass ein öffentliches Interesse an dem Forschungsvorhaben das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen erheblich überwiegt

und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigen Aufwand erreicht werden kann. Dem Institut wurde deshalb mitgeteilt, sich zunächst an das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMAS-GFF) zu wenden und sich dort bescheinigen zu lassen, dass ein öffentliches Interesse an der Durchführung des wissenschaftlichen Forschungsvorhabens besteht. Das TMASGFF hat die Auffassung des TLfDI in seiner Stellungnahme an das Forschungsinstitut einbezogen.

Forschungsinstitute dürfen von den örtlichen Gesundheitsämtern Auskunft aus Toten- und Sektionsscheinen erhalten, wenn dies zur Durchführung einer im öffentlichen Interesse liegenden wissenschaftlichen Forschungsarbeit erforderlich ist, das Geheimhaltungsinteresse des Verstorbenen und seiner Angehörigen das Forschungsinteresse nicht überwiegt und der Forschungszweck nicht auf andere Weise oder nur mit unverhältnismäßigen Aufwand erreicht werden kann. Das öffentliche Interesse ist dabei durch das für Gesundheitswesen zuständige Ministerium festzustellen.

11.55 Vaterschaftsfeststellung durch das Jobcenter?

Eine junge Mutter stellte beim Jobcenter den Antrag auf eine Babyerstaussstattung. Zu dem Antrag gehörte auch eine Erklärung, dass die Antragstellerin keinen Unterhalt für das Kind erhalte und auch nicht eingefordert habe, weil keine Vaterschaftsanerkennung vorliege. Daraufhin forderte das Jobcenter die Antragstellerin auf, die Adressdaten des Kindsvaters anzugeben. Im Verlauf des Gesprächs im Jobcenter stellte die Antragstellerin fest, dass sich in den Händen des Sachbearbeiters bereits ein Dokument befand, das Adressdaten des vom Jobcenter offenbar vermuteten Vaters enthielt. Dass hinter ihrem Rücken die Daten zum vermeintlichen Vater recherchiert wurden, fand die Antragstellerin nicht in Ordnung und wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Auf die Nachfrage des TLfDI nach der Rechtsgrundlage der Datenerhebung über den vermeintlichen Kindsvater teilte das Jobcenter mit, man habe bei der Prüfung des Antrags auf Leistungen zur Erstausstattung bei Schwangerschaft und Geburt nach § 24 Abs. 3 Sozialgesetzbuch (SGB) Zweites Buch (II) festgestellt, dass zwischen

den Konten der Beschwerdeführerin und einer männlichen Person Gelder flossen. Weil nun der Verdacht aufkam, dass die Betroffene mit dieser Person vielleicht eine Bedarfsgemeinschaft bildete, deren Vorliegen bei der Prüfung der Hilfsbedürftigkeit nach dem SGB II Auswirkungen haben könnte, habe man pflichtgemäß eine Melderegisterabfrage durchgeführt. Als Grundsicherungsträger nach dem SGB II sei das Jobcenter verpflichtet, Sachverhalte von Amts wegen soweit zu ermitteln, dass alle für den Einzelfall bedeutsamen Umstände in die Bedarfsberechnung einfließen.

Fest steht, dass, soweit eine Unterhaltspflicht des Kindsvaters besteht, diese bei der Babyerstaussstattung durch das Amt zu berücksichtigen ist, denn eine Hilfsbedürftigkeit liegt nur dann vor, wenn der Unterhaltspflichtige nicht herangezogen werden kann. Bildet die Kindsmutter mit einer anderen Person eine Bedarfsgemeinschaft, ist dies ebenfalls bei der Hilfsbedürftigkeit zu berücksichtigen. Zu diesem Zweck kann das Jobcenter eine Melderegisterauskunft einholen, um festzustellen, ob dieselben Wohnadressen vorliegen.

Nach der Darlegung des Jobcenters war kein datenschutzrechtlicher Verstoß festzustellen. Die einfache Melderegisterauskunft zu einer männlichen Person, von der die Antragstellerin Geldmittel erhalten hatte, war von den Amtsermittlungen gedeckt. Dass damit der Versuch einer Vaterschaftsfeststellung verbunden gewesen wäre, konnte aus dem Sachverhalt nicht entnommen werden.

Der Grundsicherungsträger ist verpflichtet, von Amts wegen zu prüfen, ob und in welcher Höhe ein Anspruch auf Leistungen nach dem SGB II besteht. Bestehende Unterhaltsansprüche können die Hilfsbedürftigkeit vermindern oder entfallen lassen. Bestehen Anhaltspunkte dafür, dass Hilfsbedürftige in einer Bedarfsgemeinschaft leben, ist auch dies zu berücksichtigen. Eine Melderegisterabfrage in diesem Zusammenhang ist nicht unzulässig.

11.56 Jugendberufsagenturen und Datenschutz

Um den Übergang von der Schule in eine Ausbildung und in einen Beruf zu begleiten, wurden bundesweit flächendeckend Jugendberufsagenturen eingerichtet, die für unter 25-Jährige Leistungen nach den Sozialgesetzbüchern Zweites Buch – „Grundsicherung für Arbeitssuchende“, Drittes Buch – „Arbeitsförderung“ und Achtes Buch – „Kinder- und Jugendhilfe“ bündeln sollen. Aus der Aufga-

benbündelung der Jugendberufsagenturen ergibt sich ein Datenaustausch zwischen den daran beteiligten Sozialhilfeträgern sowie den staatlichen Schulen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte erfahren, dass das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie (TMASGFF) und das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) die Auffassung vertraten, dass Datenübermittlungen zwischen den Schulen und den Jugendberufsagenturen auf der Grundlage der bisher bestehenden gesetzlichen Vorschriften zulässig seien. Dieser Meinung konnte sich der TLfDI jedoch nicht anschließen, weil sich aus dem eindeutigen Wortlaut des § 57 Abs. 4 Thüringer Schulgesetz (ThürSchulG) die Unzulässigkeit einer Übermittlung von Schülerdaten von der Schule an die Jugendberufsagentur ergab. Beide Ministerien wurden dementsprechend vom TLfDI angeschrieben und um Benennung der Rechtsgrundlage gebeten, aus der sich die Zulässigkeit dieser Datenübermittlung ergeben sollte. In einem Antwortschreiben des TMBJS wurde dem TLfDI zugesagt, dass alle erforderlichen Datenübermittlungen von der Schule an die Jugendberufsagenturen ausschließlich auf der Grundlage einer individuellen Einwilligung nach § 57 Abs. 4 Nr. 3 ThürSchulG durch den betroffenen Schüler bzw. dessen Erziehungsberechtigten erfolgen werden. Der TLfDI hatte gegen eine Datenübermittlung mit Einwilligung der Betroffenen keine datenschutzrechtlichen Bedenken. Er wird aber noch prüfen, ob das Einwilligungsverfahren die Voraussetzungen des § 4 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG) erfüllt. Hiernach ist der Betroffene auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Der Datenaustausch von personenbezogenen Schülerdaten zwischen den Schulen und den Jugendberufsagenturen ist nach der gegebenen Rechtslage ausschließlich auf der Grundlage einer Einwilligung nach § 57 Abs. 4 Nr. 3 ThürSchulG in Verbindung mit § 4 Abs. 3 ThürDSG zulässig.

11.57 Datenerhebung bei Minderjährigen nur mit Einwilligung der Eltern?

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Anfrage eines Wirtschaftsfördervereins zur Erstellung einer Homepage. Diese geplante Homepage des Wirtschaftsfördervereins sollte eine Datenbank mit wesentlichen personenbezogenen Daten wie Namen, Alter, Wohnort, Durchschnittsnote, Interessenfelder sowie Kontaktmöglichkeiten wie E-Mail oder Handynummer zu einer angemeldeten Person und für Dritte, im Regelfall Unternehmen, abrufbar bzw. einsehbar führen. Das Angebot wollte der Wirtschaftsförderverein an Jugendliche und junge Erwachsene ab der 10. Klasse richten. Zugriff auf die Datenbank sollten Unternehmen haben, die auf der Suche nach Fachkräften waren.

Der TLfDI teilte dem Wirtschaftsförderverein mit, dass die angeordnete Datenbank unter datenschutzrechtlichen Gesichtspunkten nicht ohne größeren Aufwand realisiert werden könnte. Neben der Erhebung von Daten ist das Erstellen einer Homepage zwangsläufig auch mit der Speicherung und Übermittlung (Verarbeitung) personenbezogener Daten verbunden. Grundsätzlich ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, soweit das BDSG oder eine andere datenschutzrechtliche Vorschrift dies erlaubt oder der Betroffene (in die konkrete Art des Umgangs) eingewilligt hat. Juristisch wird dies als Verbot mit Erlaubnisvorbehalt bezeichnet.

Für den TLfDI war die einzig praktikable und mit dem BDSG vereinbare Lösung für den geplanten Umgang des Wirtschaftsfördervereins mit personenbezogenen Daten, die Einwilligung jedes einzelnen Betroffenen in die Datennutzung einzuholen. Diese muss den Voraussetzungen des § 4a BDSG entsprechen. Jedoch muss für die Wirksamkeit der Einwilligung von Minderjährigen eine Urteils- und Einsichtsfähigkeit des Betroffenen vorhanden sein, die es erlaubt, Grundrechte selbstständig wahrzunehmen bzw. auf deren Ausübung zu verzichten. Dies ist im Falle der informationellen Selbstbestimmung regelmäßig erst ab einem Alter von frühestens 14 Jahren möglich, weswegen eine Nutzung des Angebots für Kinder nur mit Einwilligung der Eltern möglich wäre. Schließlich hat der TLfDI den Wirtschaftsförderverein noch darauf hingewiesen, dass gemäß § 13

Abs. 2 Nr. 2 Telemediengesetz (TMG) die Einwilligung zu protokollieren ist.

Eine andere Erlaubnisnorm für das Vorhaben des Wirtschaftsfördervereins außer der vorgenannten Einwilligung der Betroffenen war nach Überprüfung der Sach- und Rechtslage vom TLfDI nicht ersichtlich. Soweit ersichtlich, hat der Verein die Idee der geplanten Datenbank verworfen.

Für die Wirksamkeit der Einwilligung von Minderjährigen in den Umgang mit personenbezogenen Daten muss eine Urteils- und Einsichtsfähigkeit des Betroffenen vorhanden sein, die es erlaubt, Grundrechte selbstständig wahrzunehmen bzw. auf deren Ausübung zu verzichten. Dies ist im Falle der informationellen Selbstbestimmung regelmäßig erst ab einem Alter von frühestens 14 Jahren möglich. Vor Erreichen dieser Altersgrenze, die im Einzelfall auch höher liegen kann, bedarf es der Einwilligung der Erziehungsberechtigten.

11.58 Sperren statt löschen

In der Eingabe eines Bürgers an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete dieser, dass er im Zusammenhang mit seiner Teilnahme an einer Eingliederungsmaßnahme in den Arbeitsmarkt gegenüber dem die Maßnahme durchführenden Berufsförderungszentrum zahlreiche Daten zu seiner Person angeben musste und nunmehr nach Ende der Maßnahme dort die sofortige Löschung der ihn betreffenden Daten begehrte. Dieser Forderung sei jedoch das Berufsförderungszentrum nicht nachgekommen. Der TLfDI schrieb daraufhin die genannte Stelle an und bat um Stellungnahme zum Sachverhalt. Das Berufsförderungszentrum teilte dem TLfDI mit, dass die Stelle als Bildungsträger aufgrund vertraglich vorgegebener Aufbewahrungsfristen zur Prüfung der qualitätsgerechten Umsetzung von Ausschreibungsmaßnahmen „Arbeitsmarkt-Dienstleistungen“ nicht berechtigt sei, Daten von Teilnehmern vor Erreichen einer Zwei-Jahres-Frist zu löschen. Die Stelle sei verpflichtet, den Weisungen des Jobcenters zum Umgang mit den Daten nachzukommen. Der TLfDI wies das Berufsförderungszentrum auf die Regelung des § 20 Abs. 3 Nr. 1 Bundesdatenschutzgesetz (BDSG) hin, wonach, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, an die Stelle einer Löschung eine

Sperrung tritt. Wie sich im Nachhinein ergab, verarbeitet das Berufsbildungszentrum jedoch als Auftragnehmer für das Jobcenter Sozialdaten, sodass die Sperrung nach der praktisch wortgleichen Regelung des § 84 Abs. 3 Nr. 1 SGB X zu erfolgen hatte. Der TLfDI forderte die Stelle auf, ihn über die erfolgte Sperrung zu unterrichten und einen entsprechenden Nachweis hierüber vorzulegen. Das Berufsförderungszentrum wurde darüber hinaus ersucht, alle Kopien der Daten auf Arbeitsplatz-PCs zu löschen, soweit die Kenntnis für die Mitarbeiter zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Der Beschwerdeführer wurde abschließend über die zweijährige Aufbewahrungsfrist seiner dort gespeicherten Daten und die vom TLfDI geforderte Sperrung seiner Daten unterrichtet. Das Berufsförderungszentrum teilte auf die vom TLfDI geforderte Sperrung der Daten des Beschwerdeführers mit, dass die automatisiert verarbeiteten Daten verschlüsselt abgelegt und die notwendigen Passwörter zur Entschlüsselung in einem Panzerschrank hinterlegt seien, zu dem lediglich zwei Personen Zugang haben. Alle in Papierform gespeicherten Unterlagen, die personenbezogene Daten des Beschwerdeführers enthalten, befinden sich in einem Archiv der Stelle unter Verschluss. Weitere Kopien dieser Daten seien in der Stelle nicht gespeichert worden. Nach Prüfung der erneuten Stellungnahme des Berufsförderungszentrums kam der TLfDI zu dem Ergebnis, dass die Sperrung der Daten des Beschwerdeführers glaubhaft nachgewiesen wurde. Allerdings fragte der TLfDI nach Beendigung der Aufbewahrungsfrist bei der Stelle nochmals an, ob denn nunmehr die Daten des Bürgers gelöscht wurden. Nach Auskunft der Stelle sei der Teilnehmer vorzeitig aus der Bildungsmaßnahme ausgeschieden. Die zweijährige Aufbewahrungsfrist beginne jedoch erst mit Ablauf des tatsächlichen Ablaufs der Maßnahme, sodass die in Rede stehenden Daten noch nicht gelöscht werden dürften. Der TLfDI widersprach der Stelle und wies auf den zwischen der Stelle und der Bundesagentur für Arbeit geschlossenen Vertrag hin, wonach die zweijährige Aufbewahrung eine Maximalfrist ist. Im Falle des Beschwerdeführers war nicht ersichtlich, wieso eine längere Aufbewahrungsfrist seiner Daten erforderlich sein sollte. Nach § 84 Abs. 2 Satz 2 SGB X sind personenbezogene Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zur Annahme besteht, dass durch die Löschung schutzwürdige Interessen

des Betroffenen beeinträchtigt werden. Der Vorgang konnte im vorliegenden Berichtszeitraum noch nicht abgeschlossen werden, da eine erneute Stellungnahme des Berufsbildungszentrums noch nicht vorlag. Der TLfDI wird aber auf eine schnelle Löschung der Daten des Bürgers dringen.

Nach § 84 Abs. 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Nach § 84 Abs. 3 Nr. 1 SGB X tritt an die Stelle einer Löschung eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

11.59 Mütter und Hebammenleistungen – Befragung „entbindet“ nicht von Datenschutz

Das ehemalige Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um dessen datenschutzrechtliche Stellungnahme zu einer geplanten Mütterbefragung. Hintergrund hierfür war die Erstellung eines Gutachtens des TMSFG zur Beantwortung der Frage, inwieweit sich das vom Hebammenlandesverband sowie von verschiedenen Thüringer Bürgerinnen vorgetragene medizinische Versorgungsproblem mit Hebammenleistungen tatsächlich darstellt. Zu diesem Zweck plante das TMSFG eine Mütterbefragung in Thüringen unter Verwendung eines Erhebungsbogens. Um diesen Fragebogen gemäß einer Stichprobenvorgabe einem ausgewählten Personenkreis von Müttern zukommen lassen zu können, hatte das TMSFG an das damalige Thüringer Innenministerium (TIM) ein Auskunftersuchen nach § 34 Abs. 1 Satz 2 Nr. 4b des Thüringer Meldegesetzes gerichtet. Auf diese Weise sollten die Adressen aller Haushalte in Thüringen nach einer vorherigen Gemeindeauswahl ermittelt werden, in denen im Jahr 2014 Kinder geboren worden waren. Aus diesen Adressen sollte dann eine zufällige Auswahl getroffen und die Haushalte mit einem Fragebogen zur Zufriedenheit der Mütter mit dem bestehenden Hebammenangebot befragt werden. Die Mütterbefragung war aufgrund

einer fehlenden Rechtsgrundlage, die zur Teilnahme verpflichtete, nur auf freiwilliger Basis zulässig. Gleiches galt für die anonyme Beantwortung des Erhebungsbogens durch die betroffenen Mütter. Da das TIM dem Auskunftersuchen zunächst nicht nachkam und die Bewertung dieses Auskunftersuchens auch von der datenschutzrechtlichen Bewertung des TLfDI abhängig machen wollte, erläuterte der TLfDI dem TMSFG die Voraussetzungen für eine Zustimmung durch das TIM. Danach betrieb das Land im Landesrechnungszentrum gemäß § 34 Abs. 1 Satz 1 Thüringer Meldegesetz (ThürMeldeG) – wobei das ThürMeldeG seit dem 1. November 2015 keine Gültigkeit mehr hat und nunmehr durch das für alle Bundesländer gültige neue Bundesmeldegesetz abgelöst wurde – ein landeseinheitliches Verfahren für das Meldewesen. Mit anderen Worten lagen dort die Melderegisterdaten aller Thüringer Meldeämter, wobei dies auch nach der Gesetzesänderung gemäß § 5 Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes weiterhin der Fall ist. Nach § 34 Abs. 1 Nr. 4 Buchstabe c ThürMeldeG bedurfte die Erfüllung von Auskunftersuchen von Behörden oder öffentlichen Stellen der Zustimmung des für das Meldewesen zuständigen Ministeriums. Dem TIM war darzulegen, dass das Auskunftersuchen die überwiegende Zahl der Meldebehörden betrifft und die Daten direkt bei den Meldebehörden nur mit unverhältnismäßig hohem Aufwand beschafft werden können. Weiterhin musste begründet werden, dass das TMSFG ohne Kenntnis der Daten zur Erfüllung seiner gesetzlichen Aufgaben nicht in der Lage gewesen wäre. Der TLfDI bat zur datenschutzrechtlichen Prüfung der Angelegenheit um Zusendung des Fragebogens und um Angaben dazu, wie sichergestellt wird, dass eine anonymisierte Antwort durch die Teilnehmerinnen an dem Verfahren möglich ist. Personenbezogene Angaben waren für die Untersuchung nicht erforderlich. Darüber hinaus hätten möglicherweise auch weniger Mütter an der Untersuchung teilgenommen. Wie sich herausstellte, sollten die Antworten in den Fragebögen durch ein vom TMSFG beauftragtes privates Forschungsinstitut ausgewertet werden. Der Fragebogen enthielt ein Kürzel des Landkreises oder der kreisfreien Stadt, in der die ausgewählten Mütter wohnten, allerdings keine Namens- oder Adressangabe derjenigen Mütter, die auf freiwilliger Basis bereit waren, den Fragebogen auszufüllen und an das genannte Institut zu senden. Somit war sichergestellt, dass das Institut nur anonymisierte Erhebungsbögen zur Auswertung erhielt. Der TLfDI verlangte vom TMSFG, die aus dem Einwohnermeldere-

gister übermittelten Namens- und Adressdaten rechtssicher zu lösen, nachdem die Erhebungsbögen mit dem Kennzeichen des Landkreises oder der kreisfreien Stadt versehen wurden. Auch sollte nicht automatisch die weibliche Person im Haushalt, sondern neutral der gesetzliche Vertreter des Kindes angeschrieben werden. Der TLfDI hatte im Übrigen keine Bedenken gegen die Durchführung des Erhebungsverfahrens. Wie sich aus einem Schreiben des TMSFG an das TIM ergab, welches dem TLfDI nachrichtlich zur Kenntnis gegeben wurde, versicherte das TMSFG, dass alle vom TLfDI genannten Voraussetzungen eingehalten wurden.

Aus datenschutzrechtlicher Sicht bestand gegen die Übermittlung der Meldedaten an das TMSFG aus den Thüringer Einwohnermelderegistern keine Bedenken, da das Erhebungsverfahren zur Erfüllung der Aufgaben des TMSFG erforderlich war und seitens des Ministeriums die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Bestimmungen des Thüringer Datenschutzgesetzes getroffen wurden.

11.60 Gesundheitsdaten von Asylbewerbern

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom Sozialamt Jena auf eine datenschutzrechtliche Problematik im Zusammenhang mit der Abrechnung von notwendigen ärztlichen Behandlungen gegenüber dem Freistaat Thüringen aufmerksam gemacht.

Gemäß § 4 Asylbewerberleistungsgesetz hat das jeweilige Sozialamt die Kosten der notwendigen Untersuchungen von Asylbewerbern zu übernehmen. Soweit die Kosten für diese notwendigen Untersuchungen einen Betrag von 2556,46 Euro pro Person und Jahr überschreiten, hatte das Sozialamt einen Erstattungsanspruch in Höhe der über diesen Betrag hinausgehenden Kosten nach § 2 Abs. 5 der Thüringer Verordnung über die Kostenerstattung nach dem Thüringer Flüchtlingsaufnahmegesetz (ThürFlüKEVO) gegenüber dem Freistaat Thüringen. Solche Erstattungsansprüche hatte das Sozialamt gegenüber dem Thüringer Landesverwaltungsamt (TLVwA) geltend gemacht, worauf dieses die Übersendung der jeweiligen Krankenakten zur Prüfung angefordert hatte. Auf diese Anfrage des TLVwA meldete sich das Sozialamt Jena beim TLfDI, weil es der Auffassung war, dass die Übersendung der Krankenakten gegen das Thüringer

Datenschutzgesetz (ThürDSG) verstoße. Der TLfDI teilte nach datenschutzrechtlicher Prüfung die Auffassung des Sozialamts Jena. Die Datenerhebung seitens des TLVwA sowie die geforderte Übermittlung der Krankenakten durch das Sozialamt würden einen datenschutzrechtlichen Verstoß darstellen.

Gemäß § 4 Abs. 1 ThürDSG ist eine Verarbeitung oder Nutzung personenbezogener Daten nur dann zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine Einwilligung der Betroffenen lag in diesem Fall nicht vor. Das Erheben personenbezogener Daten ist nach § 19 Abs. 1 ThürDSG zulässig, wenn ihre Kenntnis für die Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Die Übermittlung ist Teil der Datenverarbeitung. Maßgeblich für die Zulässigkeit der hier angedachten Übermittlung ist daher § 21 ThürDSG, der die Übermittlung von personenbezogenen Daten zwischen Behörden regelt. Danach ist eine Übermittlung personenbezogener Daten an eine andere öffentliche Stelle nur dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten (Empfängers) liegenden Aufgaben erforderlich ist.

Die Erstattung der Kosten nach § 2 Abs. 5 ThürFlüKEVO hat gegen Einzelnachweis zu erfolgen. Das TLVwA ist nach § 4 Abs. 1 ThürFlüKEVO für die Kostenerstattung zuständig. Für den Einzelnachweis in dem mitgeteilten Fall genügt die Übermittlung der der jeweiligen Person zugeordneten Arztrechnungen. Diese müssen erkennen lassen, welche Person behandelt und welcher Betrag dem Fachdienst Soziales in Rechnung gestellt worden ist. Hinsichtlich Diagnose und einzelner Posten sind die Rechnungen jeweils zu schwärzen. Eine Prüfpflicht hinsichtlich der Notwendigkeit der einzelnen Behandlungen durch den Arzt ist von der ThürFlüKEVO nicht vorgesehen und damit für die Aufgabenerfüllung des TLVwA auch nicht erforderlich. Das Sozialamt gab dem TLVwA die Stellungnahme des TLfDI zur Kenntnis. Daraufhin forderte das TLVwA die Weiterleitung amtsärztlicher Stellungnahmen. Die amtsärztlichen Stellungnahmen sind Bestandteil der Krankenhilfeakten und enthalten nach Angaben des Sozialamtes in der Regel zu Diagnosen, Vorerkrankungen und Prognosen oft weitreichendere Angaben als eine Kostenübernahmeanfrage einer Klinik oder eines niedergelassenen Arztes.

Nach Auffassung des TLfDI kann das TLVwA die Vorlage der amtsärztlichen Stellungnahme zwar fordern. Im vorliegenden Fall

war der Inhalt der amtsärztlichen Stellungnahme allerdings viel zu weitgehend. Dem Sozialamt wurde daher empfohlen, die amtsärztliche Stellungnahme zu übermitteln und die Passagen zu schwärzen, die nicht zur Entscheidung des TLVwA über den Erstattungsantrag erforderlich sind. Um derartige Probleme für die Zukunft zu unterbinden, wurde dem Sozialamt dringend empfohlen, die Auftragserteilung an die amtsärztliche Untersuchung zu konkretisieren, um dem Amtsarzt genau mitzuteilen, welche Informationen erfragt werden.

Sowohl die Erhebung von personenbezogenen Daten als auch ihre Übermittlung muss zum Zweck der Aufgabenerfüllung der öffentlichen Stelle erforderlich sein. Auch bei der Beauftragung eines Amtsarztes ist darauf zu achten, dass nur die Information erfragt wird, die für die konkrete Aufgabe erforderlich ist.

11.61 Einwilligungserklärung und damit Verzicht auf Ausübung des Grundrechts der informationellen Selbstbestimmung durch Minderjährige?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bekommt immer wieder Anfragen, ab welchem Alter ein Minderjähriger selbst eine rechtswirksame Einwilligung erteilen kann und dies, ohne dass es auf die Einwilligung der Erziehungsberechtigten ankommt. In diesem Fall fragte ein Unternehmen an, das internetbasierte Lern- und Arbeitsplattformen vertreibt, bei denen sich die Lehrkraft für ihre Schüler entsprechende Apps (Applikationen, also Anwendungssoftware) aus dem Angebot aussucht, die der Unterrichtsgestaltung und -nachbereitung dienen. Die Nutzung dieser Apps ist mit der Verarbeitung und Nutzung personenbezogener Daten der Schüler verbunden. Das Unternehmen sah die Problematik, dass die Schüler in die Verarbeitung und Nutzung ihrer Daten gegebenenfalls nicht wirksam einwilligen können und bat den TLfDI um Vorgaben und Richtwerte, ab wann eine Einwilligung von einem Schüler wirksam vorgenommen werden kann oder ob bis zur Volljährigkeit grundsätzlich immer zusätzlich die Einwilligung der Erziehungsberechtigten eingeholt werden muss. Das Unternehmen bat auch um Auskunft, ob die Einwilligung immer schriftlich erklärt werden müsse oder ob auch andere Lösungen denkbar seien. Zuletzt wurde die Frage aufgeworfen, ob ein Minder-

jähriger wirksam in den Erhalt von Werbe-Newsletters einwilligen kann. Der TLfDI legte dem Unternehmen dar, dass es im Freistaat Thüringen keine konkreten Vorgaben bzw. Richtwerte für Altersstufen gibt, nach denen eine Einwilligung durch den Minderjährigen selbst erfolgen kann. Die Voraussetzungen einer rechtswirksamen Einwilligung richten sich je nach Fallkonstellation nach § 4 Abs. 2 und 3 Thüringer Datenschutzgesetz (ThürDSG) bei der Einholung einer Einwilligung durch eine öffentliche Stelle in Thüringen bzw. nach § 4a Abs. 1 Bundesdatenschutzgesetz (BDSG) durch eine nicht-öffentliche Stelle mit Sitz in Thüringen. Nach beiden Bestimmungen muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Dies setzt ungeachtet der Frage, ob ein Minderjähriger als nach § 106 Bürgerliches Gesetzbuch in der Geschäftsfähigkeit beschränkte Person überhaupt wirksam einen Vertrag über den Erwerb einer App abschließen kann, keine Geschäftsfähigkeit des Minderjährigen, sondern lediglich dessen Einsichtsfähigkeit in die Tragweite der Einwilligung voraus.

Wann von einer solchen Einsichtsfähigkeit ausgegangen werden kann, lässt sich nicht an abstrakten Altersgrenzen festmachen, sondern bedarf einer Entscheidung im Einzelfall. Die Einsichtsfähigkeit von Minderjährigen dürfte in Abhängigkeit vom Umfang der Erhebung personenbezogener Daten sowie deren Verwendungszweck bei der Nutzung von Apps nur in Ausnahmefällen zu bejahen sein. Zusätzlich war zu berücksichtigen, dass ohne Einwilligung der Eltern wohl der wirksame Vertragsschluss zur Nutzung einer App nicht möglich ist. In der Praxis ist es allerdings gang und gäbe, dass sich Minderjährige Apps aus dem Internet herunterladen, die zu großen Teilen kostenlos sind. Solche Rechtsgeschäfte sind jedoch im Regelfall nicht rechtlich, lediglich vorteilhaft für den Minderjährigen. Deshalb können die Eltern nach Auffassung des TLfDI solche Rechtsgeschäfte ihrer Kinder nachträglich widerrufen. Hierbei handelt es sich aber noch um wenig bearbeitetes Neuland, da bisherige Überlegungen stets nur den finanziellen Aspekt berücksichtigen, das „Bezahlen mit personenbezogenen Daten“ aber außer Acht gelassen wird.

Außerdem wies der TLfDI im vorliegenden Fall darauf hin, dass die erforderliche Schriftform der Einwilligung durch die elektronische Form nach § 3a ThürVwVfG ersetzt werden kann. Dafür benötigt man eine qualifizierte elektronische Signatur nach dem Signaturgesetz. Gemäß § 4a Abs. 1 Satz 3 BDSG bedarf die Einwilligung der

Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Das Gesetz räumt der Schriftform den unbedingten Vorrang ein. Ausnahmen sind zwar möglich, eine ausdrückliche, das Einverständnis des Betroffenen dokumentierende Erklärung bleibt jedoch unerlässlich. Daher erfüllt eine Lösung mit einer Einwilligung per Web-Formular nicht die gesetzlichen Anforderungen. Da eine pauschale Beantwortung der Frage, ob das Einverständnis der Eltern eingeholt werden muss, nicht möglich ist und dies immer vom gegebenen Einzelfall abhängt, sollten die Erziehungsberechtigten bei Minderjährigen in die Einwilligungserklärung einbezogen werden. Ebenso ist die Frage nach der Wirksamkeit einer Werbeeinwilligung ohne Einverständnis der Erziehungsberechtigten nicht pauschal zu beantworten. Als Beispiel sei auf eine Entscheidung des Oberlandesgerichts Hamm verwiesen, welches feststellte, dass Minderjährige ab 15 Jahren nicht die nötige Reife haben, die Tragweite der Einwilligungserklärung zur Datenspeicherung und Datenverwendung zu Werbezwecken abzusehen und daher die Zustimmung der Eltern nötig sei (OLG Hamm, Urteil v. 20. September 2012, I-4 U 85/12).

Es kann kein Alter pauschal angegeben werden, ab dem ein Minderjähriger eine rechtswirksame Einwilligung erteilen kann. Je nach dem konkret vorliegenden Einzelfall ist zu ergründen, ob der Minderjährige die Einsichtsfähigkeit besitzt, die Tragweite seiner Einwilligung für die Verarbeitung und Nutzung seiner personenbezogenen Daten zu erfassen. Dies gilt auch bei Rechtsgeschäften im Zusammenhang mit dem Erwerb von Apps aus dem Internet.

11.62 Anonyme Krankenhäuser

Die datenschutzrechtlichen Probleme in einem Krankenhaus sind wegen der Komplexität der zum Einsatz kommenden Systeme vielfältig. Das stellte auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bei seinen Kontrollen verschiedener Krankenhäuser in Thüringen (vergleiche 10. Tätigkeitsbericht im öffentlichen Bereich, Nummer 11.1) fest. Wegen der Sensibilität der dort verarbeiteten Daten besteht oft eine Scheu, sich an die Aufsichtsbehörde zu wenden, weil eine Frage eventuell schlafende Hunde wecken könnte. Andererseits wusste der TLfDI aus seiner Erfahrung bei den Kontrollen, dass die Kranken-

häuser sehr bemüht sind, sich an die gesetzlichen Vorgaben zu halten. Aus dieser Situation heraus wurde die Idee geboren, ein „anonymes“ Forum für Krankenhäuser zu schaffen. Dieses Forum sollte die Möglichkeit bieten, dass sich Krankenhäuser mit Datenschutzfragen an den TLfDI wenden können, ohne ihre Identität zu offenbaren. Deswegen sollte das Forum auch nicht öffentlich einsehbar, sondern nur den Krankenhäusern in Thüringen zugänglich sein.

Der TLfDI nahm frühzeitig mit der Landeskrankenhausesgesellschaft Thüringen e. V. (LKHG) Kontakt auf, um das Vorgehen abzustimmen. Es gestaltete sich nicht ganz einfach, ein Verfahren abzustimmen, das einerseits garantierte, dass nur registrierte Nutzer zu dem Forum Zugang hatten und andererseits aber dem TLfDI die Identität der anfragenden Stelle verborgen blieb. Es wurde der Weg gewählt, dass jedes Krankenhaus in Thüringen einen Zugang erhalten sollte. Die Registrierung der Teilnehmer erfolgte über die LKHG beim Thüringer Landesrechenzentrum (TLRZ). Die Nutzerverwaltung liegt ausschließlich in der Hand des TLRZ. Dieses erhält von der Landeskrankenhausesgesellschaft eine Liste der zu registrierenden Benutzerkennungen der Krankenhäuser. Die Benutzerkennungen werden zuvor von der LKHG nach einer bestimmten Regel zufällig vergeben und neben dem TLRZ den an die LKHG gemeldeten Teilnehmern mitgeteilt. Durch die von der LKHG vergebene zufällig kreierte Benutzerkennung werden somit seitens des TLfDI Rückschlüsse auf die anfragende Stelle vermieden. Der Nutzer kann nun eigene und fremde Themen innerhalb des Forums beobachten sowie Themen erstellen, d. h. Fragen an den TLfDI richten. Dabei kann der Nutzer auswählen, ob er gegenüber dem TLfDI mit seinem Benutzernamen oder unter „Anonymous“ auftreten möchte. Damit können sich die Thüringer Krankenhäuser nunmehr bei datenschutzrechtlichen Fragestellungen schnell und unkompliziert an den TLfDI wenden. Die Antworten des TLfDI werden nach Prüfung der Fragen und deren Beantwortung dann im Forum eingestellt und sind für alle Forennutzer lesbar. Am 8. Dezember 2015 startete der TLfDI das Forum in einem gemeinsamen Presetermin mit der LKHG (siehe auch https://www.tlfdi.de/imperia/md/content/daten-schutz/veroeffentlichungen/pmtlfdi/151209_gem._pm_zur_blogger_ffiung.pdf).



Der TLfDI hofft, dass die Krankenhäuser das Forum nutzen werden, um sich mit ihren datenschutzrechtlichen Problemen an ihn zu wenden. Mit dem Forum wünscht sich der TLfDI, das Vertrauen der Betreiber der Krankenhäuser zu gewinnen. Denn datenschutzrechtliche Missstände werden nicht nur kritisiert und beanstandet, diese müssen auch aufgearbeitet und verbessert/abgeschafft werden. Dabei wird der TLfDI die konstruktive Zusammenarbeit mit den Thüringer Krankenhäusern vertiefen. Im nächsten Tätigkeitsbericht wird zu lesen sein, wie die Krankenhäuser das Forum angenommen haben.

Mit dem Krankenhausforum hat der TLfDI eine geschlossene Plattform eingerichtet, auf der sich registrierte und freigegebene Benutzer der Krankenhäuser mit ihren Fragen zum Datenschutz an den TLfDI wenden können, ohne dass dieser über die Identität der anfragenden Stelle Kenntnis erlangt. Damit müssen Datenschutzprobleme nicht „hinter dem Berg“ gehalten werden und alle Nutzer können an der Lösung partizipieren.



Landstraße, Windkraft, Umwelt © mahey / Fotolia.com

12 Infrastruktur und Landwirtschaft

12.1 Bekenntnis zur freiheitlichen demokratischen Grundordnung bei Ausschreibungen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum eine Information, dass das Thüringer Liegenschaftsmanagement in seinen Formularen für die Bieter in Ausschreibungsverfahren folgende Formulierung verwenden würde:

„Mir/uns ist nicht bekannt, dass bei den von mir/uns eingesetzten Mitarbeitern Zweifel am Bekenntnis der betroffenen Person zur freiheitlichen demokratischen Grundordnung bestehen. Mir/uns ist nicht bekannt, dass das eingesetzte Personal Mitglied in einer extremistischen/verfassungsfeindlichen Partei, Organisation oder sonstigen Vereinigung ist bzw. diesen nahesteht und Schriftgut extremistischen oder sonstigen verfassungsfeindlichen Inhalts besitzt und/oder derartiges Schrift- oder Gedankengut weiterverbreitet.“

Der TLfDI bat daraufhin das Thüringer Liegenschaftsmanagement um Stellungnahme, auf welcher Rechtsgrundlage die genannte Erklärung von den Bietern in Ausschreibungsverfahren verlangt wird und inwieweit diese erforderlich ist.

Daraufhin teilte das Thüringer Liegenschaftsmanagement mit, dass der Sachverhalt im damals zuständigen Thüringer Ministerium für Bau, Landesentwicklung und Verkehr (TMBLV) im Wege der Fachaufsicht einer Prüfung unterzogen und bis zum Vorliegen einer Entscheidung des Ministeriums von einer solchen Bietererklärung abgesehen werde. Das Thüringer Liegenschaftsmanagement wollte sich, sobald die Ergebnisse vorliegen, unaufgefordert wieder an den TLfDI wenden. Nachdem der TLfDI jedoch mehrere Monate nichts mehr in der Angelegenheit gehört hatte, wandte er sich erneut an das Liegenschaftsmanagement und erinnerte an dessen Unterstützungspflicht gemäß §§ 38 Abs. 1 Satz 1 und Satz 2 Thüringer Datenschutzgesetz (ThürDSG). Prompt folgte eine Reaktion des Thüringer Liegenschaftsmanagements: In Abstimmung mit dem nunmehr zuständigen Thüringer Ministerium für Infrastruktur und Landwirtschaft (TMIL) teilte das Thüringer Liegenschaftsmanagement dem TLfDI mit, dass die Bietererklärung schon seit Mitte 2014 keine Verwendung mehr finde und auch zukünftig nicht gefordert werde. Der TLfDI sah damit die Angelegenheit als erledigt an.

Der TLfDI hat Verständnis dafür, dass das Thüringer Liegenschaftsmanagement im Rahmen von Ausschreibungsverfahren nicht mit Bietern in Kontakt treten möchte, deren Bekenntnis zur freiheitlichen demokratischen Grundordnung fragwürdig erscheint. Gleichwohl barg die zunächst verwendete Erklärung die Gefahr, dass konkret personenbeziehbare Daten hier ohne Rechtsgrundlage verarbeitet werden. Dies zu verhindern, ist gemäß § 4 Abs. 1 in Verbindung mit § 37 Abs. 1 ThürDSG die Aufgabe des TLfDI.

12.2 Smarte Heizung – Datenleck?

Das damalige Thüringer Ministerium für Wirtschaft, Arbeit und Technologie fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, wie die Einführung eines intelligenten Heizsystems mit einer selbstlernenden Einzelraumregelung aus datenschutzrechtlicher Sicht zu beurteilen sei. Der TLfDI geht zunächst davon aus, dass das Ministerium als Daten

verarbeitende Stelle im Sinne von § 3 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) für die beim Betrieb des Heizsystems anfallenden Daten verantwortlich ist. Das System erfasst die Anwesenheit und die Dauer der Anwesenheit sowie das Wärmebedürfnis von Personen in den Büroräumen des Ministeriums. Da diese Büros im Regelfall bestimmten Mitarbeitern zugeordnet werden können, entstehen hierbei zumindest personenbeziehbare Daten, die personenbezogenen Daten gleichzusetzen sind (§ 3 Abs. 1 ThürDSG). Die Verarbeitung und Nutzung personenbezogener Daten sind gemäß § 4 Abs. 1 ThürDSG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder bestimmt oder soweit die betroffene Person eingewilligt hat. Der TLfDI erachtete daher einen Testlauf des Systems im Ministerium mit Einwilligung der betroffenen Mitarbeiter für zulässig. Er hat allerdings ausdrücklich darauf aufmerksam gemacht, dass bei einer späteren allgemeinen und „zwangsweisen“ Einführung des Systems für alle Mitarbeiter sich die Ermächtigungsgrundlage zum Betreiben des Systems nicht mehr aus einer Einwilligung ergeben kann, da diese entgegen der Bestimmung von § 4 Abs. 2 ThürDSG keinesfalls mehr freiwillig erteilt werden würde. Vor einem flächendeckenden Dauerbetrieb des Heizsystems bestehen weiterhin Fragen zur Datensicherheit, die noch nicht beantwortet sind. Diese betreffen z. B. die Sicherheit der Datenübertragung zwischen Raumsensor und Ventilsteuerung sowie die Zugriffssicherheit des Bewegungssensors vor dem unbefugten Auslesen des Anwesenheitsprofils. Nach dem letzten Stand wurde der geplante Testeinsatz des smarten Heizsystems von dem jetzt zuständigen Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft auf unbestimmte Zeit verschoben. Der TLfDI wird die Sache weiter verfolgen.

Die neuen „smarten“ Regeltechniken, bei denen personenbeziehbare Daten entstehen, sind so zu gestalten, dass eine Profilbildung von Personen vermieden wird. Die Einwilligung als Zulässigkeitskriterium scheidet beim Dauerbetrieb eines Regelsystems besonders dann aus, wenn es sich um Bedienstete handelt, da hierbei fraglich ist, ob die Einwilligung in eine vom Dienstherrn eingeführte Regeltechnik tatsächlich freiwillig erteilt wird.

12.3 LPG – nicht datengeschützt

In einer Antwort des ehemaligen Thüringer Ministeriums für Landwirtschaft, Forsten, Umwelt und Naturschutz (TMLFUN) auf die Kleine Anfrage Nr. 3718 (Drucksache 5/7507) vom 15. März 2014 zu „Unwirksamen Umwandlungen von Landwirtschaftlichen Produktionsgenossenschaften“ hieß es in der Beantwortung der Frage 1 „Liegen der Landesregierung die Namen der betroffenen Betriebe vor?“:

„Die Prüfung durch den Landesdatenschutzbeauftragten ergab, dass eine namentliche Auflistung der 28 unwirksamen Umwandlungen in Thüringen aus datenschutzrechtlichen Gründen nicht möglich war.“

Hintergrund war der datenschutzrechtliche Umgang mit den Angaben zu einzelnen Genossenschaften im Rahmen eines Forschungsprojektes mit dem Titel „Rechtsprobleme der Restrukturierung landwirtschaftlicher Unternehmen in den neuen Bundesländern nach 1989“. In diesem Zusammenhang hatte die frühere Landesbeauftragte für den Datenschutz im Jahr 2001 tatsächlich die Rechtsauffassung vertreten, dass es datenschutzrechtlich nicht vertretbar sei, Einzelangaben zu den betroffenen Landwirtschaftlichen Produktionsgenossenschaften (LPG) zu veröffentlichen.

Hierzu stellte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nach erneuter datenschutzrechtlicher Prüfung im Berichtszeitraum fest, dass eine Übermittlung personenbezogener Daten, insbesondere die namentliche Auflistung von 28 unwirksam umgewandelten Thüringer Betrieben durch den Leiter des Forschungsprojekts an das TMLFUN aus datenschutzrechtlicher Sicht zulässig sei. Mangels gegenteiliger Hinweise ging der TLfDI davon aus, dass es sich bei den 28 fehlerhaft umgewandelten Thüringer Betrieben um juristische Personen handle. Gemäß § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) sowie gemäß § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten aber gerade Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Angaben über juristische Personen und Personengruppen wie Personengesellschaften, Vereine und Gruppen hat der Gesetzgeber bewusst aus dem Anwendungsbereich von BDSG und ThürDSG ausgenommen (vgl. für das BDSG: Dammann in: Simitis, Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 3, Rz. 18). Juristische Personen sind Personenvereinigungen oder

Zweckvermögen mit vom Gesetz anerkannter rechtlicher Selbstständigkeit.

Folglich unterlagen nach Ansicht des TLfDI die hier infrage stehenden Daten zu den einzelnen früheren LPG nicht dem Schutzbereich des BDSG oder des ThürDSG und konnten daher aus datenschutzrechtlicher Sicht grundsätzlich ohne Weiteres genutzt werden. Diese – revidierte – Rechtsauffassung teilte der TLfDI auch dem TMLFUND mit. Sofern künftig Anfragen an dieses Ministerium zur beschriebenen Problematik herangetragen werden, wird die Rechtsauffassung des TLfDI dort berücksichtigt werden.

Nicht alle Daten werden vom Datenschutzrecht geschützt. Unter den Schutzbereich von § 3 Abs. 1 ThürDSG / § 3 Abs. 1 BDSG fallen nur Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (also jeder lebende Mensch). Die Daten von juristischen Personen oder Personengesellschaften fallen also nicht unter die genannten Regelungen.

12.4 Bodennutzungshaupterhebung

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum darüber, dass er im Rahmen der vom Thüringer Landesamt für Statistik (TLS) durchgeführten Bodennutzungshaupterhebung, einer Agrarstatistik, bei der Abfrage von Flächenveränderungen nach dem Namen und der Anschrift des Flächenabgebers bzw. des Flächenübernehmers gefragt wurde. Diese Vorgehensweise des TLS hielt er für datenschutzrechtlich unzulässig und für eine Statistik unnötig und bat den TLfDI deswegen um Hilfe.

Der TLfDI unterzog den Sachverhalt unter Einbeziehung des TLS einer datenschutzrechtlichen Prüfung und teilte dem Beschwerdeführer Folgendes mit:

Die Bodennutzungshaupterhebung als Bestandteil der Bodennutzungserhebung wird nach Maßgabe des Agrarstatistikgesetzes (AgrStatG) als Bundesstatistik durchgeführt (§ 1 Nr. 1 AgrStatG). Für die Erhebungen zu den Agrarstatistiken nach § 1 AgrStatG besteht gemäß § 93 Abs. 1 AgrStatG Auskunftspflicht. Die Vor- und Familiennamen sowie Anschriften der bisherigen Flächenbewirtschafter sowie der neuen Flächenbewirtschafter oder der jeweiligen Eigentümer

sind nach § 92 Nr. 6 AgrStatG als Hilfsmerkmale bei der Bodennutzungshaupterhebung gesetzlich festgelegt.

Im Ergebnis informierte der TLfDI den Beschwerdeführer, dass das Verarbeiten (dazu zählt auch das Erheben) seiner personenbezogenen Daten gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) datenschutzrechtlich zulässig war, da das Agrarstatistikgesetz (§ 1 Nr. 1 AgrStatG i. V. m. § 92 Nr. 6 AgrStatG) eine derartige Verarbeitung der Daten erlaubt bzw. anordnet. Der TLfDI informierte den Beschwerdeführer ferner darüber, dass die genannten Hilfsmerkmale vom TLS nach abgeschlossener Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit gemäß § 12 Bundesstatistikgesetz zu löschen sind.

Im Rahmen der Bodennutzungshaupterhebung ist bei der Abfrage von Flächenveränderungen das Verarbeiten der personenbezogenen Daten des Flächenabgebers und Flächenübernehmers (Vor- und Familiennamen sowie Anschriften) gemäß § 4 Abs. 1 ThürDSG datenschutzrechtlich zulässig, da das Agrarstatistikgesetz (§ 1 Nr. 1 AgrStatG i. V. m. § 92 Nr. 6 AgrStatG) eine derartige Verarbeitung der Daten erlaubt bzw. anordnet.

12.5 Veröffentlichung personenbezogener Daten in Überwachungsberichten der Immissionsschutzbehörde im Internet

Aufgrund der Anfrage eines behördlichen Beauftragten für den Datenschutz wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass die für den Emissions- und Immissionsschutz zuständigen Thüringer Behörden Überwachungsberichte gemäß § 52a Bundes-Immissionsschutzgesetz in Verbindung mit § 9 Industriekläranlagen-Zulassungs- und Überwachungsverordnung sowie den entsprechenden Anlagen der Verordnung im Internet veröffentlichten. Diese Überwachungsberichte wurden nach der Durchführung einer Vor-Ort-Besichtigung von betroffenen Anlagen erstellt und dann der Öffentlichkeit zur Verfügung gestellt. Außer der Bezeichnung der Anlage selbst wurden auch der Name und die Firmenform des Unternehmens aufgeführt. Hierbei ist nicht auszuschließen, dass dabei auch personenbezogene Daten veröffentlicht werden. Dem Schutz des ThürDSG unterfallen nur personenbezogene Daten. Hierbei

handelt es sich nach § 3 Abs. 1 ThürDSG um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener). Eine gleiche Regelung findet sich in § 3 Abs. 1 Bundesdatenschutzgesetz. Das bedeutet, dass das Datenschutzrecht grundsätzlich nur auf natürliche Personen und nicht auf juristische Personen anwendbar ist. Juristische Personen können sich allenfalls auf ihr Recht am eingerichteten und ausgeübten Gewerbebetrieb bzw. auf ihr Grundrecht auf Eigentum aus Artikel 14 Grundgesetz berufen. Die diesbezügliche Prüfung unterfällt indes nicht der Zuständigkeit des Datenschutzbeauftragten. Es ist jedoch nicht auszuschließen, dass sich unter den betroffenen Firmen auch Einzelkaufleute befinden. Aus den dem TLfDI zum damaligen Zeitpunkt vorliegenden Unterlagen war nicht eindeutig zu entnehmen, ob es sich bei den aufgeführten Firmen ausschließlich um juristische Personen handelt oder ob hinter den Firmen teilweise auch Einzelkaufleute stehen. Grundsätzlich gilt das so genannte Verbot mit Erlaubnisvorbehalt des § 4 Abs. 1 ThürDSG, nach dem die Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Aus den einschlägigen Regelungen des Bundesimmissionsschutzgesetzes ergibt sich nur eine Pflicht zur Erstellung der Überwachungspläne bzw. Überwachungsprogramme der zuständigen Behörden. Nach § 10 Abs. 1 des Thüringer Umweltinformationsgesetzes (ThürUIG) ergreifen die informationspflichtigen Stellen die notwendigen Maßnahmen, um in angemessenem Umfang eine aktive und systematische Verbreitung von Umweltinformationen in der Öffentlichkeit zu fördern. Nach Einschätzung des TLfDI kann § 10 Abs. 2 Nr. 2 ThürUIG nicht als Rechtsgrundlage für die Veröffentlichung personenbezogener Daten herangezogen werden. Nach dieser Vorschrift sind politische Konzepte sowie Pläne und Programme mit Bezug zur Umwelt zu veröffentlichen. Eine Veröffentlichungspflicht unter Nennung der betroffenen Anlagenbetreiber der jeweils zuständigen Behörden ergibt sich hieraus aber nicht. Das damalige Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz (TMLFUN) bestätigte auf Nachfrage des TLfDI, dass bei der Veröffentlichung von Überwachungsprogrammen personenbezogene Daten nicht veröffentlicht werden dürfen. Das Ministerium hatte aufgrund der Anfrage des TLfDI eine Kontrolle des im Internet veröffentlichten Überwachungsplans des Freistaats Thüringen veranlasst. Die Kontrolle hatte ergeben, dass in geringem

Umfang trotz aller Prüfung auch personenbezogene Daten in der Anlagenliste enthalten waren. Das TMLFUN hatte die Herausnahme von personenbezogenen Daten aus der Liste veranlasst, alle zuständigen Behörden auf die Rechtslage hingewiesen und zu einer Anonymisierung von personenbezogenen Daten vor der Veröffentlichung aufgefordert. Der TLfDI hat sich damit einverstanden erklärt, dass die Anlagenbetreiber in anonymisierter Form, also auch ohne die Vergabe von eindeutigen Kürzeln oder Initialen der Betroffenen im Überwachungsplan aufgenommen werden.

Überwachungsberichte nach dem Bundesimmissionsschutzgesetz, die im Internet nach den Thüringer Vorschriften veröffentlicht werden müssen, dürfen keine personenbezogenen Daten zum Betreiber der Anlage, zu seinen Mitarbeitern und zu weiteren Dritten enthalten.

12.6 Grundstücksgrenzen sind auch personenbezogene Daten

Ein Grundstückseigentümer beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass der zuständige Katasterbereich ihm keine Einsicht in die vollständigen, zu seinem Grundstück gespeicherten Daten gewährte. Darüber hinaus führte der Beschwerdeführer aus, dass die im Liegenschaftskataster eingetragenen Grundstücksgrenzen seines Grundstücks falsch seien. Der TLfDI teilte dem Beschwerdeführer zunächst mit, dass nach § 13 Thüringer Datenschutzgesetz (ThürDSG) die Daten verarbeitende Stelle dem Betroffenen auf Antrag Auskunft und Akteneinsicht über die zu seiner Person gespeicherten Daten zu erteilen habe und unrichtige personenbezogene Daten gemäß § 14 ThürDSG zu berichtigen seien. Unter Umständen habe der Betroffene darüber hinaus nach § 15 bzw. § 16 ThürDSG einen Anspruch auf Löschung von unrichtigen personenbezogenen Daten oder zumindest auf Sperrung der Daten, wenn ihre Richtigkeit vom Betroffenen bestritten werde. Allerdings wurde der Beschwerdeführer darauf aufmerksam gemacht, dass der TLfDI nicht berechtigt ist, die rein fachliche Arbeit einer Behörde zu überprüfen. Diesbezüglich wurde dem Bürger geraten, sich an die für die Katasterbereiche zuständige Aufsichtsbehörde, das Thüringer Landesamt für Vermessung und Geoinformation (TLVermGeo), zu wenden. Auf Bitte des Beschwerdeführers erfolgte ein persönliches Gespräch

beim TLfDI zum Sachverhalt, in dessen Verlauf dieser dem TLfDI mehrere Kopien von Unterlagen aus dem Liegenschaftskataster vorlegte, aus denen erkennbar sei, dass die Grenzen des betroffenen Grundstücks im Laufe der Jahre ohne erkennbaren Grund mehrfach geändert worden sein sollen. Außerdem sei die zu seinem Grundstück bestehende maßgebliche Liegenschaftskarte verfälscht worden, indem mehrere Längenmaße durch neue Maßangaben ersetzt worden sein sollen. Der TLfDI bat daraufhin die zuständige Katasterbehörde um Aufklärung des Sachverhalts. Eine Antwort erhielt der TLfDI aus dem TLVermGeo als obere Kataster- und Vermessungsbehörde, dem der Vorgang bereits bekannt war. Zunächst wurde die Auffassung des TLfDI nicht geteilt, dass es sich bei Grundstücksdaten, wie Größe und Grenzlängen um personenbezogene Daten handele. Der TLfDI verwies das Landesamt auf § 3 Abs. 1 ThürDSG, wonach alle Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person personenbezogene Daten sind. Da auch bei Grundstücksdaten ein Bezug zum betroffenen Grundstückseigentümer gegeben ist, sind dies personenbezogene Daten. Zum konkreten Sachverhalt führte das TLVermGeo gegenüber dem TLfDI aus, dass ein öffentlich bestellter Vermessungsingenieur eine erneute Vermessung der Grundstücksgrenzen vorgenommen und dabei festgestellt hätte, dass eine über 40 Jahre alte Vermessung des Grundstücks fehlerhaft gewesen sei. Im Ergebnis dieser Vermessung wurden einige Grenzmarken des Grundstücks zuungunsten des Beschwerdeführers verändert. Die Messergebnisse wurden dann dem betroffenen Grundstückseigentümer mit Bescheid bekannt gegeben. Wie sich durch Nachfrage des TLfDI beim Beschwerdeführer bestätigte, war der Bescheid bestandskräftig geworden. Da der Beschwerdeführer sich aber nach wie vor gegenüber dem TLfDI dahingehend äußerte, dass die aktuell durchgeführte Vermessung seiner Grundstücksgrenzen fehlerhaft gewesen sei, bat der TLfDI um ein gemeinsames Gespräch mit dem Beschwerdeführer, dem TLVermGeo und dem Katasterbereich, zu dem diese sich auch bereit erklärt hatten und bei dem auch die entsprechenden Katasterunterlagen vorgelegt werden sollten. Zur Abstimmung des Gesprächstermins wurde der Beschwerdeführer um Terminvorschläge gebeten.

Dafür schrieb ihn der TLfDI zwei Mal an, erhielt aber in beiden Fällen keine Antwort vom Beschwerdeführer. Deshalb konnte der TLfDI in diesem Fall leider nicht weiter tätig werden.

Grundstücksdaten über eine bestimmte oder bestimmbare Person sind personenbezogene Daten. Der Katasterbereich hat deshalb dem Betroffenen Auskunft über die dort zu seiner Person verarbeiteten Daten zu erteilen und ihm Einsicht in die ihn betreffenden Unterlagen zu gewähren. Grundsätzlich hat die öffentliche Stelle unrichtige Daten gemäß § 14 ThürDSG zu berichtigen, unzulässig gespeicherte Daten gemäß § 16 Abs. 1 Nr. 1 ThürDSG zu löschen und Daten, bei denen sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt, gemäß § 15 Abs. 1 Nr. 1 ThürDSG zu sperren. Wenn ein Bescheid über eine Grundstücksvermessung durch einen öffentlich bestellten Vermessungsingenieur bestandskräftig wird, kann die verantwortliche Stelle davon ausgehen, dass die im Liegenschaftskataster eingetragenen Grundstücksdaten den Tatsachen entsprechen.

12.7 Thüringen in 3-D

Die Daten des amtlichen Vermessungswesens (z. B. Gebäude, Grundstücke, Straßen, Landschaftsbeschaffenheit usw.) werden als



Geobasisdaten bezeichnet und müssen vom amtlichen Vermessungswesen beschrieben und nachgewiesen werden. Bisher erfolgte die Bereitstellung der Geobasisdaten seitens der Katasterverwaltung in zweidimensionaler Darstellung. Zur Einführung der Darstellung von dreidimensionalen Geobasisdaten, die jedermann ohne Zugangsbeschränkung über den Geoclient des Geoproxy

(http://www.geoproxy.geoportal-th.de/geoclient/start_geoproxy.jsp) verfügbar gemacht werden, wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfD) um eine datenschutzrechtliche Stellungnahme gebeten. Der TLfDI nahm hierzu an einer Beratung im Thüringer Landesamt für Vermessung und Geoinformation (TLVermGeo) teil, in der das um die dritte Dimension erweiterende Verfahren vorgestellt wurde. Nach Ausführung des TLVermGeo werden die Gebäudemodelle in einer ersten Stufe derzeit als einfaches Klötzchenmodell (so genannte LoD 1=Level of Detail Stufe 1) dargestellt. Mittelfristig ist dann die Einführung eines dreidimensionalen Gebäudemodells mit standardisierten Dachformen geplant (LoD 2), das dann ebenfalls in Geoproxy zur Verfügung

gestellt werden soll. Die Gebäude- und Landschaftshöhen werden mithilfe eines Laserscannings mittels Befliegen ermittelt. Nach Auffassung des TLVermGeo erfülle der Freistaat Thüringen mit der Bereitstellung des Zugangs zu den Geobasisdaten die Forderungen der EU-Richtlinie „INSPIRE“, die den Rahmen für eine gemeinsame Geodateninfrastruktur in Europa vorgibt. Nach Prüfung des vorgetragenen Sachverhalts, der vorgeführten dreidimensionalen Beispielsbilder von Gebäudemodellen mit standardisierten Dachformen sowie unter Berücksichtigung der hierzu bestehenden Rechtsvorschriften, insbesondere von § 5 Abs. 1 des Thüringer Geodateninfrastrukturgesetzes, wonach Geodaten, Metadaten und Geodatendienste „... öffentlich verfügbar und über das Internet ... zugänglich sein“ müssen, hat der TLfDI keine datenschutzrechtlichen Bedenken gegen die Einführung solcher dreidimensionalen Darstellungen von Geobasisdaten geltend gemacht.

Die öffentliche Verfügbarmachung von Geobasisdaten für jedermann ist in Thüringen wie auch in den anderen Bundesländern erlaubt. Hiermit werden die Forderungen der EU-Verordnung „INSPIRE“ umgesetzt. Der Detaillierungsgrad der Geobasisdaten wird weiter voranschreiten. Der TLfDI wird diese Entwicklung verfolgen.

12.8 Videoüberwachung im ÖPNV – Videogaga 4

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde vom damaligen Thüringer Ministerium für Bau, Landesentwicklung und Verkehr (TMBLV) um Beratung gebeten, welche Rechtsvorschriften bei der Förderung von Videoüberwachungsanlagen in Bussen, Straßenbahnen, Zügen, auf dem Busbahnhof oder Bahnhof sowie bei der Ausschreibung von Verkehrsleistungen im Schienenpersonennahverkehr zu beachten sind. Der TLfDI legte dem Ministerium dar, dass für die Datenschutzaufsichtsbehörde immer die verantwortliche Stelle Ansprechpartner ist. Dies sind die Unternehmen oder Stellen, die die Videoüberwachungsanlage betreiben. Diese sind nach dem Gesetz verpflichtet, die geltenden Datenschutzbestimmungen einzuhalten. Eine Einwilligung kommt bei einer Videoüberwachung nicht in Betracht, da die gesetzlichen Voraussetzungen hierfür nicht eingehalten werden können, etwa hinsichtlich der Freiwilligkeit, der schriftlichen Einwilligung, der umfassenden Aufklärung über die Maßnahme etc.

Eine Videoüberwachung ist daher nur zulässig, wenn eine Rechtsvorschrift sie ausdrücklich erlaubt. In Betracht kommt hier in erster Linie die Bestimmung des § 6b Bundesdatenschutzgesetz. Die Videoüberwachung ist danach nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Nach Auffassung des TLfDI ist nach dem geltenden Recht jedenfalls eine flächendeckende Videoüberwachung in Fahrzeugen des ÖPNV unzulässig. Dem TMBLV wurde empfohlen, im Rahmen der Ausschreibung von Förderungen den verantwortlichen Stellen keine detaillierten Vorgaben für eine ausnahmslose Videoüberwachung zu machen, da deren Zulässigkeit immer nur anhand der Umstände des Einzelfalls beurteilt werden kann. In jedem Fall sind der Umstand einer Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen, im Regelfall durch gut sichtbar angebrachte Schilder, erkennbar zu machen. Der TLfDI hatte das TMBLV auch darüber informiert, dass in aller Regel die verantwortliche Stelle, die eine Videoüberwachung mittels digitaler Aufzeichnung durchführt, einen Beauftragten für den Datenschutz zu bestellen hat. Dieser hat vor Inbetriebnahme der Videoüberwachungsanlage eine so genannte Vorabkontrolle durchzuführen. Zusätzlich wurde das Ministerium auf die Empfehlung „Videoüberwachung in öffentlichen Verkehrsmitteln“ sowie auf die Orientierungshilfe „Videoüberwachung“ (siehe Nummer 2.6) des Düsseldorfer Kreises verwiesen. Inzwischen wurde die Empfehlung „Videoüberwachung in öffentlichen Verkehrsmitteln durch die Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ mit Stand 16. September 2015 ersetzt. Sämtliche Papiere wurden dem TMBLV bzw. dem jetzt zuständigen Thüringer Ministerium für Infrastruktur und Landwirtschaft zur Kenntnis gegeben. Die Dokumente sind auch auf der Homepage des TLfDI unter <https://www.tlfdi.de/tlfdi/themen/orientierungshilfen> veröffentlicht worden.



Da eine Erforderlichkeit des Einsatzes von Videoüberwachung im ÖPNV von zahlreichen Faktoren bestimmt wird und nur anhand der

Umstände im Einzelfall beurteilt werden kann, sollten in einem öffentlichen Ausschreibungstext den verantwortlichen Stellen keine detaillierten Vorgaben zur ausnahmslosen Videoüberwachung gemacht werden.

12.9 PKW-Maut ohne flächendeckende Datenerhebung

Ein Landesdatenschutzbeauftragter bat seine Bundes- und Landeskollegen und -kolleginnen um Stellungnahme zur geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen. Die Bundesregierung schlug als Verfahren eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer an flächendeckend installierten elektronischen Kontrollpunkten vor. Der genannte Entschließungsentwurf forderte von der Bundesregierung, auf die Einrichtung eines solchen elektronischen Verfahrens, mit dem hunderttausende Kfz-Kennzeichen erfasst werden würden, zu verzichten. Zum einen widerspricht diese Verfahrensweise den verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und der Datensparsamkeit, zum anderen ist die Maßnahme zur Mauterhebung nicht erforderlich. Für Abrechnungs- und Kontrollzwecke des Staates stehen z. B. mit der Einführung einer Vignette nach dem Vorbild anderer Staaten mildere und ebenso effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte in seiner Stellungnahme den Entschließungsentwurf mitgetragen und insbesondere die Vignettenlösung bevorzugt, da hierbei nur ein geringer Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen erfolgt. Gleichzeitig brachte der TLfDI zum Ausdruck, andere Lösungen, mit denen Kfz-Kennzeichen oder sogar ein Bild der Fahrzeuge erhoben, verarbeitet und genutzt werden, in der Entschließung grundsätzlich nicht anzusprechen, da unabhängig davon, wie ein solches Verfahren technisch gestaltet ist, bei den Sicherheitsbehörden Begehrlichkeiten geweckt würden, die mit der Vignettenlösung von vornherein vermieden werden könnten. Der TLfDI erinnerte dabei an die Probleme von Zweckerweiterungen der Fotoaufnahmen der Fahrzeuge im Zusammenhang mit der damaligen Einführung der LKW-Maut. In Auswertung der Stellungnahme aller Datenschutzbeauftragten des Bundes und der Länder wurde in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

mit Datum vom 14. November 2014 die Entschließung „Keine PKW-Maut auf Kosten des Datenschutzes!“ verabschiedet und vom TLfDI in einer Pressemitteilung veröffentlicht (siehe dazu Anlage 42).

Bei der Einführung einer PKW-Maut ist aus datenschutzrechtlicher Sicht die Vignetten-Lösung zu bevorzugen. Der Eingriff in das Recht auf informationelle Selbstbestimmung ist hierbei gering. Gleichzeitig hat sich die Vignette bei der Erhebung von Mautgebühren in anderen Ländern bewährt.

12.10 Amtshilfe wegen MPU-Gutachten

Ein behördlicher Datenschutzbeauftragter einer Kommune setzte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber in Kenntnis, dass die Steuerfahndungsstelle eines Finanzamtes im Rahmen der Amtshilfe von Fahrerlaubnisbehörden personenbezogene Daten zu Gutachten zur Fahrtüchtigkeit fordere. Im Einzelnen sollten der Name, die Anschrift, das Geburtsdatum der Begutachteten genannt sowie die Daten der jeweiligen Gutachten in „geeigneter Weise“ belegt werden.

Als Rechtsgrundlage für das Amtshilfeersuchen verwies das Finanzamt auf § 111 Abgabenordnung (AO), der in seinem Abs. 5 auch § 105 AO für entsprechend anwendbar erklärt. Diese Vorschrift greift dann ein, wenn die ersuchte Behörde durch die Amtshilfe ihre Verschwiegenheitspflicht verletzen würde. Die o. g. Daten dürfen nach § 2 Abs. 9 Satz 1 Straßenverkehrsgesetz ausschließlich zur Feststellung oder Überprüfung der Eignung oder Befähigung zur Fahrtüchtigkeit verwendet werden. Zudem enthalten Gutachten zu Fahrtüchtigkeit in der Regel hochsensible Sozialdaten, die dem Sozialgeheimnis nach § 35 Sozialgesetzbuch I unterliegen.

Auf die Anfrage des TLfDI teile das Finanzamt u. a. mit, dass die Daten Name, Vorname und Geburtsdatum der Begutachteten und das Datum des Gutachtens für Vorermittlungen im Besteuerungsverfahren erforderlich seien. Hierbei gehe es insbesondere darum, die zu begutachtenden Personen eindeutig zu identifizieren und den Zeitraum der Rechnungslegung des Gutachters einzugrenzen. Demgegenüber sei der Inhalt der Gutachten nicht erforderlich, weshalb sie nicht vorzulegen seien.

Da die Formulierung in den Amtshilfeersuchen, dass neben den o. g. konkret bezeichneten personenbezogenen Daten auch die Daten der jeweiligen Gutachten „in geeigneter Weise“ zu belegen seien, bei den Fahrerlaubnisbehörden zu Irritationen führte, forderte der TLfDI das Finanzamt auf, dafür Sorge zu tragen, dass künftig gegenüber den ersuchten Stellen nur die im Besteuerungsverfahren benötigten, konkret bezeichneten Daten angefordert werden. Dies würde die in datenschutzrechtlicher Hinsicht gebotene Transparenz des Verfahrens erhöhen und ausschließen, dass für die Aufgabenerledigung nicht benötigte sensible personenbezogene Daten in unzulässiger Weise übermittelt werden.

Das Finanzamt erklärte daraufhin gegenüber dem TLfDI, dass die Verwendung der Formulierung „in geeigneter Weise“ im konkreten Fall des Steuerfahndungsverfahrens die Gefahr von Unklarheiten barg. Daher seien die Mitarbeiter der Steuerfahndungsstelle entsprechend sensibilisiert und im Sinne des Hinweises des TLfDI belehrt worden. Überdies sei das zuständige Fachreferat der Thüringer Landesfinanzdirektion hiervon in Kenntnis gesetzt worden.

Eindeutige Formulierungen hinsichtlich der benötigten personenbezogenen Daten sind sowohl in Amtshilfeersuchen, in Formularen zur Datenerhebung als auch in der Software zur Dateneingabe unabdingbar. Dadurch können das datenschutzrechtliche Transparenzgebot garantiert und unzulässige Datenerfassungen bzw. -übermittlungen sowie etwaige Irritationen bei „Datenlieferanten“ vermieden werden.

12.11 Das Wageninnere: von Interesse auch für die Ordnungskräfte

Aus dem Rundschreiben eines anderen Landesdatenschutzbeauftragten hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfahren, dass im dortigen Bundesland in einigen Kommunen die für die Parkraumüberwachung eingesetzten kommunalen Mitarbeiterinnen und Mitarbeiter Parkverstöße mittels Digitalaufnahmen dokumentieren. Wenn der Parkschein oder die Parkscheibe offensichtlich fehlte, wurde darüber hinaus das gesamte Wageninnere fotografiert. Nach Angaben der angefragten Ordnungsbehörde könne man mit diesen Fotobeweisen besser Behauptungen entgegentreten, der Parkschein bzw. die Parkscheibe sei ins Wageninnere gefallen. Nach Auffassung des TLfDI ist eine sol-

che Verfahrensweise aus datenschutzrechtlichen Gründen völlig inakzeptabel. Gemäß § 13 Abs. 1 Satz 1 der Straßenverkehrsordnung (StVO) muss der Parkschein am oder im Fahrzeug von außen gut lesbar angebracht sein, Gleiches gilt nach § 13 Abs. 2 Nr. 2 StVO auch für die Parkscheibe. Als gut lesbare Orte kommen im Fahrzeug grundsätzlich nur das Armaturenbrett und die Front-, Seiten- oder Heckscheiben (da einige Parkscheiben Saugnäpfe haben), eventuell auch noch die so genannte Hutablage oder bei Kombis die Kofferraumabdeckung infrage. Falls eine Ordnungsbehörde tatsächlich meint, einen ausführlichen Fotobeweis des gesamten einsehbaren Innenraums eines Fahrzeugs anfertigen zu müssen, ist dies aus datenschutzrechtlicher Sicht unzulässig. Für den Nachweis, dass ein Parkschein oder die Parkuhr eben nicht von außen gut lesbar angebracht war, ist das Fotografieren in das Innere des Autos und damit die Dokumentation, wie es darin ausgesehen hat, für die Aufgabenerfüllung nicht erforderlich, § 19 Abs. 1 Thüringer Datenschutzgesetz. Falls ein Parkschein oder eine Parkscheibe ins (nicht gut einsehbare) Autoinnere gefallen ist, geht dies nach Ansicht des TLfDI zulasten des Fahrzeughalters. Darüber hinaus sind die Ordnungsamtsmitarbeiter, die die schriftliche Verwarnung ausstellen, auch ohne Fotobeweis gleichzeitig Zeugen hinsichtlich des fehlenden Parkscheins bzw. der Parkscheibe. Der TLfDI kann sich weder vorstellen, dass die Zahl der Einsprüche mit der in Rede stehenden Begründung, wonach der Parkschein ins Innere gefallen sei, hoch ist, noch dass ein entsprechendes Gericht einer solchen Einlassung eines Kfz-Halters folgen wird. Der TLfDI geht davon aus, dass die Ordnungskräfte in Thüringen die Fahrzeuginnenräume in den dargelegten Fällen nicht fotografisch zu Beweiszwecken dokumentieren. Zumindest sind keine diesbezüglichen Beschwerden laut geworden.

Soweit eine Erforderlichkeit hierfür besteht, dürfen Ordnungsbehörden mittels eines Kamerabeweises einen Parkverstoß dokumentieren. Das Abfotografieren des Innenraums ist hiervon keinesfalls erfasst und deshalb unzulässig.

12.12 Im Tower alles im Blick – Videogaga 5 – Videoüberwachung am Flughafen

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte im Berichtszeitraum die

Videoüberwachung an einem Flughafen in Thüringen. Naturgemäß gab es an dem Flughafen einige Kameras. Ein Flughafen besitzt auch immer ein hohes Sicherheitsrisiko, dem auch mit dem Einsatz von Videoüberwachung begegnet werden soll. Die Kameras, die von der Bundespolizei eingesetzt und auch nur von dieser eingesehen werden können, unterliegen nicht der Kontrolle des TLfDI. Er prüfte die Zulässigkeit der Kameras, die im Parkhaus und auf dem Flughafengelände von dem Betreiber des Flughafens genutzt wurden. Auf den Flughafen ist das Bundesdatenschutzgesetz (BDSG) anwendbar. Zwar handelt es sich nach § 2 Absatz 2 Thüringer Datenschutzgesetz (ThürDSG) um eine öffentliche Stelle. Allerdings bestimmt § 26 ThürDSG, dass, soweit öffentliche Stellen am Wettbewerb teilnehmen, auf sie von den Bestimmungen des ThürDSG nur der 5. Abschnitt, ausgenommen § 34 Abs. 2, anzuwenden ist, im Übrigen gelten für sie die Bestimmungen des BDSG mit Ausnahme des 2. Abschnitts und des § 38. Die Flughäfen stehen, zumindest soweit sie sich in räumlicher Nähe befinden, untereinander im Wettbewerb im Hinblick auf die potenziellen Fluggäste.

Wie es bei dem Einsatz einer Vielzahl von Kameras erforderlich ist, gab es für den Flughafen einen Datenschutzbeauftragten, der auch die nach § 4d Abs. 5 BDSG erforderliche Vorabkontrolle durchgeführt hatte. Ziel dieser technisch-organisatorischen Analyse ist die Bewertung der Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung. Geprüft werden muss dabei, ob der geplante Einsatz jeder einzelnen Kamera jeweils den gesetzlichen Anforderungen entspricht und welche technischen und organisatorischen Maßnahmen zu ihrer Einhaltung zu ergreifen sind. Lassen sich erkannte Restrisiken nicht hinreichend sicher ausgestalten, darf ein Verfahren so nicht zum produktiven Einsatz kommen. Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte. Die Zulässigkeit der Videoüberwachung beurteilte sich nach § 6b Absatz 1 BDSG. Danach ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen.

Zunächst fiel dem TLfDI auf, dass die Speicherdauer der Aufzeichnungen mit einer Woche zu lang war. Gemäß § 6b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen,

wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht mehr notwendig ist. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können, da der Flughafen 24 Stunden an sieben Tagen in der Woche geöffnet ist. Das bedeutet, dass Videoaufzeichnungen grundsätzlich nach 48 Stunden zu löschen sind (vgl. Gesetzesbegründung, Bundestagsdrucksache 14/5790, Seite 63). Für einen Großteil der Kameras wurde daher eine Speicherdauer von maximal 48 Stunden als ausreichend angesehen. Etwas anderes galt für die Kameras, die sich im Schrankenbereich des Parkhauses sowie der Parkplätze befinden. Der Betreiber des Flughafens hatte glaubhaft dargelegt, dass es zahlreiche Urlauber gibt, die den Parkplatz für einen längeren Zeitraum nutzen und es bei Verlust des Parkscheines häufiger zu Problemen wegen der Nichtbeweisbarkeit der Standdauer des PKW komme. Für die Einfahrt in die Parkgarage bzw. auf den Parkplatz wurde daher eine längere Speicherdauer für zulässig erachtet.

Alle für die jeweiligen Kameras angegebenen Zwecke wurden geprüft. Jede einzelne Kamera muss tatsächlich für den festgelegten Zweck geeignet und erforderlich sein. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel, erreicht werden kann. Nicht alle angegebenen Zwecke rechtfertigten eine Videoaufzeichnung. In einigen Bereichen sollte die Videoaufzeichnung Zugänge sichern und die Zufahrt für Not- und Rettungseinsätze sichern. Für diese Zwecke würde es ausreichen, wenn ein reines Monitoring, also die Beobachtung der Liveaufnahmen, stattfindet. In der Vorabkontrolle war angeführt, dass eine permanente Überwachung der Mitarbeiter nicht stattfindet, und außerdem wurde bei den jeweiligen Kameras mit angegeben, welche Personen Einsicht nehmen dürfen. Es fehlte jedoch eine schriftliche Festlegung, unter welchen Voraussetzungen überhaupt Zugriff auf die Videoaufzeichnungen genommen werden darf. In diesen Punkten hat der TLfDI Nachbesserung gefordert. Das Verfahren ist noch nicht abgeschlossen.

Auch wenn auf einem Flughafen ein erhöhtes Sicherheitsrisiko besteht, darf eine Videoüberwachung nur stattfinden, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen, § 6b BDSG. Die Speicherdauer von Videoaufzeichnungen kann in einem Flughafenparkhaus länger sein, weil es dort viele über einen längeren Zeitraum parkende Nutzer gibt.

12.13 Video im Bus – kein Muss – Videogaga 6

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine anonyme Anzeige gegen ein Busunternehmen in Thüringen ein. Der Eigentümer des Unternehmens habe kürzlich neue Fahrzeuge angeschafft und in diesen Videotechnik installiert. Dabei werde das komplette Innere des Busses einschließlich des Sitzes des Busfahrers selbst überwacht. Außerdem werde auch noch ein Teil des Straßenbereichs vor dem Bus aufgenommen. Der TLfDI stattete dem Busunternehmen einen Besuch ab und kontrollierte dort die vom Unternehmen durchgeführte Videoüberwachung. Dabei stellte sich heraus, dass zur Objektsicherung des Betriebsgeländes 14 Kameras zum Einsatz kamen. Die in der anonymen Anzeige gemachten Angaben bestätigten sich vor Ort. Die modernen Busse des Unternehmens waren mit einer Videoüberwachung ausgestattet, die sowohl die Fahrgäste als auch den Busfahrer überwachte. Auch ein Teil des Straßenbereichs vor dem Bus wurde mit aufgezeichnet. Der Inhaber des Unternehmens teilte mit, dass er hinsichtlich der Überwachung in den Bussen davon ausgegangen sei, dass diese unproblematisch sei, da die Fahrzeuge mit der entsprechenden Ausstattung angeboten worden seien und die Ausrüstung der Fahrzeuge auch durch ein Förderprogramm des Freistaates Thüringen mit 75 Prozent der Anschaffungskosten gefördert worden sei.

Im Rahmen des Arbeitskreises Verkehr erfuhr der TLfDI zwischenzeitlich, dass die Videoüberwachungen in Bussen und sonstigen Unternehmen des öffentlichen Personennahverkehrs auch in anderen Ländern deutlich zugenommen hat. Auch die Aufsichtsbehörden der anderen Länder sahen das Bedürfnis, für diesen Bereich einheitliche Festlegungen zu treffen. Die Aufsichtsbehörden beschlossen daher,

eine Orientierungshilfe für die Videoüberwachung im öffentlichen Personennahverkehr zu erarbeiten (siehe Nummer 12.8).

Der TLfDI stellte das Verfahren der Prüfung der Videoüberwachung des Busunternehmens aus diesem Grund zunächst zurück, um das Ergebnis der Beratungen über die Orientierungshilfe abzuwarten. Nachdem die Orientierungshilfe vom Düsseldorfer Kreis beschlossen wurde, trat der TLfDI erneut an das Busunternehmen heran und bat dieses zunächst, die auf dem Betriebsgelände und in den Dienstbussen aktuell durchgeführte Videoüberwachung nochmals darzulegen. Es war nicht ausgeschlossen, dass sich aufgrund des Zeitablaufs zwischenzeitlich Änderungen ergeben hatten. Der TLfDI wird die durchgeführte Videoüberwachung anhand der Festlegungen der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ prüfen. Es ist davon auszugehen, dass eine lückenlose Überwachung des Busfahrers jedenfalls nicht zulässig sein wird, da nach § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz personenbezogene Daten eines Beschäftigten zur Aufdeckung von Strafdaten nur dann erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Für das Unternehmen wird außerdem schwer zu begründen sein, warum der öffentliche Verkehrsraum mitüberwacht werden muss und eine nahezu lückenlose Überwachung der Busse durchgeführt wird. Das weitere Verfahren bleibt abzuwarten.

Auch im öffentlichen Personennahverkehr ist eine Videoüberwachung nicht grundsätzlich zulässig, sie muss im Rahmen geltender Datenschutzgesetze durchgeführt werden. Der TLfDI wird die in der Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ festgelegten Grundsätze bei der Prüfung zugrunde legen.

12.14 Tunnelblick

Ende Oktober/Anfang November 2014 wurde der Jagdbergtunnel der Autobahn A 4 bei Jena eröffnet und für den Verkehr freigegeben. Aus diesem Anlass wandte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an das zuständige Landesamt für Bau und Verkehr Thüringen und bat um Auskunft über die in den Tunnelröhren eingesetzten Videokameras,

deren Anzahl und die Übertragung von Videobildern an öffentliche Stellen.

Das Landesamt Bau und Verkehr antwortete prompt und teilte mit, dass die Videodaten zur Gefahrenabwehr an die zentrale Betriebsleitstelle für alle Straßentunnel in Thüringen nach Zella-Mehlis übertragen würden. Daneben erfolge eine Übermittlung für alle Straßentunnel an die Autobahnpolizeiinspektion (API) in Schleifreisen und die Autobahnpolizeistation Süd in Zella-Mehlis, welche für die Tunnelkette Thüringer Wald zuständig sei. Auch an die Feuerwehr der Stadt Suhl und an die Feuerwehr der Stadt Jena finde eine Übertragung der Videodaten statt. Insgesamt seien 127 Kameras im Tunnel eingesetzt.

Daraufhin forderte der TLfDI das Thüringer Ministerium für Inneres und Kommunales (TMIK) auf, ihm die Rechtsgrundlage für eine Übermittlung der Videobilder aus dem Jagdbergtunnel an die API zu nennen.

Eine Rechtsgrundlage für die Übermittlung dieser Videobilder war aus der Sicht des TMIK nicht erforderlich. Das Ministerium begründete seine Rechtsauffassung unter Hinweis darauf, dass es sich bei den Videobildern um Übersichtsaufnahmen handele, auf denen weder Personen noch amtliche Kfz-Kennzeichen erkennbar seien. Deshalb würden keine personenbezogenen Daten mittels der Videobilder erhoben, sodass kein Grundrechtseingriff statfinde und daher auch keine Rechtsgrundlage für die Übermittlung der Videobilder erforderlich sei.

Der TLfDI konnte sich mit dieser Antwort noch nicht zufriedengeben: Für ihn war es entscheidend, ob auf den erhobenen Videobildern aus dem Jagdbergtunnel tatsächlich keine personenbezogenen oder personenbeziehbaren Daten enthalten waren. Deshalb wollte er vom TMIK wissen, welche Auflösung die Videobilder besitzen, die mit den Kameras aus dem Jagdbergtunnel angefertigt werden. Ferner interessierte den TLfDI auch der Öffnungswinkel der im Jagdbergtunnel eingesetzten Kameras.

Die Antworten des TMIK auf diese datenschutzrechtlich relevanten Fragen lagen bis zum Redaktionsschluss für den 11. Tätigkeitsbericht noch nicht vor. Der TLfDI wird daher im nächsten Tätigkeitsbericht darüber informieren, welche Bilder in welcher Auflösung im Jagdbergtunnel erhoben werden.

Mit der Kfz-Kennzeichenerfassung in Thüringer Tunneln hat der TLfDI schon datenschutzrechtlich negative Erfahrungen gesammelt: Erinnert sei hier nur an die „automatische Kennzeichenerfassung“ im Rennsteigtunnel trotz fehlender Rechtsgrundlage (siehe dazu den 5. Tätigkeitsbericht, Nr. 7.5 – Automatische Gesichts- und Kennzeichenerfassung, Seite 86 f.). Deshalb ist bei einer Bild- oder Videoübermittlung aus einem Tunnel an die Polizei besonderes datenschutzrechtliches Augenmerk geboten: Erst wenn klar ist, dass tatsächlich keine personenbezogenen oder personenbeziehbaren Daten von den Kameras aus dem Jagdbergtunnel erhoben werden, bedarf es dafür auch keiner Rechtsgrundlage. Dies ergibt sich aus § 4 Abs. 1 Satz 1 ThürDSG und für die Polizei insbesondere aus § 31 Abs. 1 Polizeiaufgabengesetz. Ob im Jagdbergtunnel tatsächlich keine personenbezogenen Daten mittels Kamera erhoben werden, hat der TLfDI im Rahmen seiner Aufgaben gemäß § 37 Abs. 1 ThürDSG zu prüfen.

12.15 Erforschung der Energieeffizienz

Eine Universität wandte sich mit der Bitte um Beratung an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Es war ein Forschungsprojekt „Energieeffizienz in der Stadt“ geplant. Ziel war, in einer bestimmten Modellregion ein Planungsinstrument zur Verfügung zu stellen, welches es ermöglichen sollte, Effizienzmaßnahmen in die kommunale Stadtentwicklung zu integrieren. Hierfür beabsichtigte die Universität, über die Bereitstellung von Kennzahlen eine hinreichende Abschätzung des Verbrauchs zu ermöglichen. Zur Erarbeitung dieser Kennzahlen wurden Geobasisdaten der Region zur Analyse und Visualisierung funktioneller Zusammenhänge sowie gebäudescharfe Energieverbrauchsdaten und die gebäudespezifische Einwohnerzahl ohne Nennung der Namen benötigt. Außerdem wurde zur notwendigen Ermittlung der anfallenden Abwassermengen der Wasserverbrauch pro Gebäude benötigt. Die aus diesen Daten zu generierenden gebäudespezifischen Kennzahlen sollten lediglich über statistische Angaben wie die Gesamtheit gleicher Gebäudetypen, bestimmte Baublöcke (ein von vier Straßen umgebenes Quartier) oder noch größer über Stadträume (mehrere Blöcke gleichen Typs) veröffentlicht werden. Die Universität hatte alle am Projekt Beteiligten im Hinblick auf den Datenschutz geschult, und sie waren auf das Datengeheimnis ver-

pflichtet worden. Die Daten sollten auf einem separaten, nur dafür vorgesehenen Rechner ohne Zugriff auf das Internet verarbeitet werden. Die Festplatte sollte zudem verschlüsselt werden.

Der TLfDI teilte der Universität mit, dass das Erheben personenbezogener Daten zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist, § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG). Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden, § 25 Abs. 1 ThürDSG. Nach § 25 Abs. 3 ThürDSG sind die personenbezogenen Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Die Universität hatte nachvollziehbar dargelegt, aus welchen Gründen die zu erhebenden Daten nicht in anonymisierter Form ausreichen. Allerdings hat sie sicherzustellen, dass die gespeicherten personenbezogenen Daten entsprechend den Vorgaben des § 25 Abs. 1 ThürDSG nur für die verfolgten Forschungszwecke verwandt und die gewonnenen Erkenntnisse in anonymisierter Form dargestellt werden. Die Mitglieder der Forschungsgruppe sind darauf hinzuweisen, dass eine Weitergabe der personenbezogenen Daten an Dritte nicht zulässig ist.

Problematischer gestaltete sich die Übermittlungsbefugnis der Stellen, bei denen die benötigten Daten vorhanden sind, beispielsweise Einwohnermeldeämter der betroffenen Kommunen und Energieversorger.

Der TLfDI ging davon aus, dass die Universität die Geobasisdaten der betroffenen Gemeinden über den Geoproxyserver des Thüringer Landesamtes für Vermessung und Geoinformation erhalten würde, insoweit bestanden keine datenschutzrechtlichen Bedenken. Auch Geobasisdaten stellen personenbezogene Daten dar, da sie sich immer auf ein Grundstück beziehen und damit Rückschlüsse auf den Eigentümer des Grundstücks zulassen. Nach § 5 Abs. 1 des Thüringer Geodateninfrastrukturgesetzes müssen Geodaten öffentlich verfügbar und über das Internet und andere geeignete Kommunikationsmittel zugänglich sein.

Für die Übermittlung der gebäudescharfen Energieverbrauchsdaten als Sachdaten sowie der Einwohnerzahl für die jeweiligen Adressen gab es keine spezielle Ermächtigungsgrundlage, daher galten die allgemeinen Bestimmungen des ThürDSG. Da die Universität eine öffentliche Stelle im Sinne von § 2 Abs. 1 ThürDSG ist, gilt für die

Datenübermittlung durch die Kommune § 21 ThürDSG. Fraglich ist, ob die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden. Danach muss die Übermittlung für Zwecke erfolgen, für die die Daten bei der Daten erhebenden Stelle erhoben worden sind. Dies war nicht der Fall, da die Daten ursprünglich nicht für die Übermittlung an die Universität erhoben wurden, sondern für andere Zwecke. Eine Übermittlung für andere Zwecke ist nur unter den Voraussetzungen des § 20 Abs. 2 ThürDSG zulässig. In Betracht kam hier § 20 Abs. 2 Nr. 9 ThürDSG. Danach muss die Übermittlung dann zur Durchführung von wissenschaftlicher Forschung erforderlich sein, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens muss das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegen und der Zweck der Forschung muss auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können. Die Erforderlichkeit der Daten für die wissenschaftliche Forschung lag auf der Hand und es bestand auch kein Zweifel daran, dass der Zweck der Forschung auf andere Weise nicht bzw. nur mit unverhältnismäßigem Aufwand erreicht werden konnte. Fraglich war, ob das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt. Bei den Daten zum Strom-, zum Wasserverbrauch sowie zum Abfall- und Abwasseranfall handelt es sich um personenbezogene Daten, die Auskunft über das Verbrauchsverhalten der Personen geben, die unter einer Adresse gemeldet sind. Die Namen der Einwohner werden nicht genannt, nur die Zahl der Einwohner, die unter einer bestimmten Adresse gemeldet sind. Eine eindeutige Zuordnung des Verbrauchsverhaltens ist daher nur in den Fällen möglich, in denen unter einer bestimmten Adresse nur eine Person gemeldet ist. In allen anderen Fällen ist die Zuordnung umso mehr erschwert, je mehr Personen unter einer Adresse gemeldet sind. Unter folgenden Voraussetzungen erschien die Übermittlung der Daten dem TLfDI noch als von § 20 Abs. 2 Nr. 9 ThürDSG gedeckt:

Es muss sich um eine einmalige Datenlieferung zu einem bestimmten Zeitraum für ein abgegrenztes Gebiet (beispielsweise das Gebiet einer Gemeinde) handeln. Es werden keine Einwohnernamen erhoben, sondern die Daten lediglich zu den Adressen zugeordnet. Zugriff auf diese Daten haben nur die Mitglieder der Forschungsgruppe, wobei diese auf das Datengeheimnis nach § 6 ThürDSG zu ver-

pflichten sind. Die Forschungsergebnisse dürfen keine Rückschlüsse auf den Energieverbrauch bestimmter Personen oder Adressen zulassen. Die statistisch aufbereiteten Daten sollen immer nur aggregiert für eine gewisse Anzahl von Adressen übermittelt werden. Die Daten müssen auf dem Server der Universität in einem gesonderten Mandanten vorgehalten werden, zu dem nur die Mitglieder der Forschungsgruppe Zugang haben. Die Festplatte ist zu verschlüsseln. Nach Ablauf des Projekts müssen die Daten gelöscht werden, sobald sie zu Forschungszwecken nicht mehr benötigt werden.

Nachdem den Forschern die Einhaltung der datenschutzrechtlichen Anforderungen von hoher Bedeutung war, geht der TLfDI davon aus, dass die Anforderungen umgesetzt werden. Eine datenschutzrechtliche Prüfung behält der TLfDI sich vor.

Weil die Forschung mit personenbezogenen Daten oftmals unerlässlich ist, um einen bestimmten Forschungszweck zu erreichen, sieht das ThürDSG ein so genanntes Forschungsprivileg vor. Nach § 20 Abs. 2 Nr. 9 ThürDSG ist die Übermittlung von personenbezogenen Daten an öffentliche Forschungseinrichtungen zulässig, wenn sie zur Durchführung von wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

12.16 Wolf unter Beobachtung – zu Wildkameras

Das Thüringer Ministerium für Umwelt, Energie und Naturschutz (TMUEN) wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um datenschutzrechtliche Beurteilung einer geplanten Videoüberwachung durch so genannte Wildkameras zur Wolfsbeobachtung in einem bestimmten Thüringer Waldgebiet, in dem der Wolf bereits gesichtet worden war.

Die Videoüberwachung sei zur Beobachtung der vermuteten und nachgewiesenen Aufenthaltsorte und Laufwege aus wissenschaftlichen Zwecken erforderlich und für die wissenschaftliche Auswertung unverzichtbar. Insbesondere die Fauna, Flora, Habitat (FFH)-Richtlinie (Richtlinie 92/43/EWG) und § 6 in Verbindung mit

§ 7 Abs. 2 Nr. 14 des Bundesnaturschutzgesetzes (BNatSchG) verpflichtet das Land, über den Haltungszustand durch Beobachtung zu berichten. In Bezug auf wildlebende Wölfe sind alle erforderlichen Maßnahmen zu treffen, um die natürlichen Lebensräume und die Population zu erhalten oder diese wiederherzustellen. Gemäß Artikel 11 der FFH-Richtlinie sind die Mitgliedstaaten zur Überwachung des Erhaltungszustandes der Arten verpflichtet, die eine Beobachtung auch der Wölfe voraussetzt. Die Durchführung ist in § 6 BNatSchG niedergelegt. Das Thüringer Ministerium für Umwelt, Energie und Naturschutz (TMUEN) hatte hierzu die Installation von 10 Wildkameras vorgesehen.

Die Problematik ist äußerst vielschichtig, da die Verantwortlichkeit für die Videoüberwachung in einem Waldgebiet mit unterschiedlichen Eigentümern teils beim TMUEN und teils bei einer Bundesstelle liegt. Soweit es sich zu großen Teilen um ein nicht öffentlich betretbares Waldgebiet handelt, ist dort der Einsatz von Videoüberwachung durch eine öffentliche Bundesstelle aus Sicht des TLfDI datenschutzrechtlich nicht problematisch. Wenn ein bestimmtes Gebiet für die Öffentlichkeit erkennbar gesperrt ist, muss dort im Regelfall nicht von einem überwiegenden schutzwürdigen Interesse des von der Videoüberwachung Betroffenen ausgegangen werden. Bei den öffentlich zugänglichen Waldgebieten kommt als Rechtsgrundlage für eine Videoüberwachung lediglich § 6b Abs. 1 Nr. 3 Bundesdatenschutzgesetz (BDSG) zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke, nämlich der Berichtspflicht an die öffentlichen Stellen nachkommen zu können, in Betracht. Es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Da die Beobachtung eines Wolfes im öffentlichen Interesse liegt, kann das schutzwürdige Interesse betroffener Spaziergänger, die durch Zufall eine Wildkamera auslösen, zurücktreten. Allerdings gilt die Rechtsgrundlage nur für nicht-öffentliche Stellen, also für private Jagdpächter oder den Besitzer des Waldstückes.

Soll für Zwecke des Monitorings durch das Land als öffentliche Stelle eine Beobachtung zur Feststellung des Bewegungsradius⁷ eines Wolfes stattfinden, kommt § 25a Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) als Rechtsgrundlage in Betracht. Danach ist die Videoüberwachung zulässig, soweit sie zur Wahrnehmung des Hausrechts der verantwortlichen Stelle erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Be-

troffenen überwiegen. Ein Hausrecht des Landes in den Jagdgebieten, die im gemischten Eigentum stehen, besteht jedoch nicht. Da sich vorliegend die Videoüberwachung also nicht auf § 25a Abs. 1 ThürDSG stützen kann, wird die Videoüberwachung als wissenschaftliches Monitoring im Auftrag des Freistaats Thüringen auf der Grundlage von § 8 ThürDSG in Verbindung mit § 6 BNatSchG von nach § 7 BNatSchG streng geschützten Arten durchgeführt.

Aus Gründen der Transparenz für potentiell betroffene Waldspaziergänger muss auf die Videoüberwachung und die entsprechenden Rechtsgrundlagen sowie die verantwortliche Stelle deutlich sichtbar an den Zugängen zu dem betreffenden Waldstück hingewiesen werden. Das TMUEN hat nach Rücksprache mit dem TLfDI eine ausführliche Handlungsanleitung entworfen, die den o. g. Kamerabetreuern genaue Anweisungen gibt, wie mit den Aufnahmen der Kameras umzugehen ist. Insbesondere sind Aufnahmen von zufällig erfassten Spaziergängern ohne weitere Auswertung sofort zu löschen. Der vom TMUEN vorgeschlagene Inhalt des Hinweisschildes für die betroffenen Waldbesucher entsprach den Erfordernissen.

Der Einsatz von Videoüberwachung ist für öffentliche Stellen des Freistaats Thüringen ausschließlich zur Wahrnehmung des Hausrechts im eigenen Zuständigkeitsbereich zulässig. Ohne eine spezielle Rechtsvorschrift, die die Videoüberwachung zur Tierbeobachtung für naturschutzrechtliche Zwecke in öffentlich zugänglichen Bereichen ausdrücklich erlaubt, ist der Einsatz von Wildkameras nur ausnahmsweise und nur unter sehr engen Bedingungen zulässig. Auf der Grundlage von § 8 ThürDSG in Verbindung mit § 6 BNatSchG kann im Auftrag des Freistaats Thüringen die Videoüberwachung von nach § 7 BNatSchG streng geschützten Arten als wissenschaftliches Monitoring durchgeführt werden.



Globalization computer technology — © red150770 / Fotolia.com

13 Wirtschaft, Wissenschaft und digitale Gesellschaft

13.1 Auch Handwerkskammer unterliegt Auskunftsanspruch

Ein Handwerkskammermitglied wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und beschwerte sich darüber, dass die für ihn zuständige Handwerkskammer (HWK) ihm trotz mehrerer Wochen Wartezeit keine Auskunft über die zu seiner Person gespeicherten Daten erteilte. Daraufhin schrieb der TLfDI die HWK an und forderte diese auf, dem Betroffenen gemäß § 13 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ohne unzumutbare Verzögerung Auskunft zu erteilen über die dort zu seiner Person verarbeiteten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten und deren Empfänger oder die Kategorien der Empfänger, soweit diese Angaben gespeichert sind. Obwohl die HWK kurz darauf die Erledigung der Angelegenheit mitteilte, meldete sich der Betroffene erneut beim TLfDI, da er immer noch keine Auskunft über die zu seiner Person gespeicherten Daten erhalten habe. Wie sich bei der daraufhin vom TLfDI nochmals kontaktierten HWK herausstellte, hatte diese das Kammermitglied zwar über die entsprechenden Rechtsgrundlagen unterrichtet, die die Verarbeitung seiner personenbezogenen Daten erlaubten, die konkreten Daten wurden dabei

aber nicht aufgeführt. Der TLfDI forderte die HWK auf, dies unverzüglich beim Betroffenen nachzuholen, was bald darauf auch von der HWK bestätigt wurde.

Das Auskunfts- und Einsichtsrecht des Betroffenen gemäß § 13 ThürDSG ist als eine der datenschutzrechtlichen Kernforderungen anzusehen. Hierdurch kann sich der Betroffene Kenntnis von den ihn betreffenden Datenverarbeitungsvorgängen verschaffen. Die öffentlichen Stellen haben zu beachten, einem solchen Antrag auf Auskunft und Akteneinsicht zeitnah und umfassend nachzukommen.

13.2 Datenübermittlung einer Handwerkskammer ohne Einverständnis des Betroffenen

Ein Bürger beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Übermittlung seiner Mobilfunknummer seitens der Handwerkskammer an Dritte. Nach Schilderung des Betroffenen beantragte dieser daraufhin bei der Handwerkskammer Auskunft nach § 13 Thüringer Datenschutzgesetz (ThürDSG) über die zu seiner Person dort gespeicherten Daten, die er aber nicht erhielt. Der TLfDI schrieb daraufhin die Handwerkskammer an und bat um Auskunft zum Sachverhalt. In ihrer Stellungnahme führte die Handwerkskammer aus, dass die Mobilfunknummer an einen ehemaligen Dozenten des Beschwerdeführers herausgegeben wurde. Danach wollte sich dieser Dozent mit dem ehemaligen Lehrgangsteilnehmer über den Inhalt des Lehrgangs unterhalten. Die Handwerkskammer hatte es versäumt, vorab den Betroffenen um seine Einwilligung in die Datenübermittlung zu ersuchen. Die Kammer versicherte, dass es sich um einen bedauerlichen Einzelfall gehandelt habe. Dem TLfDI wurde Auskunft zu den Datenarten gegeben, die über den Beschwerdeführer bei der Handwerkskammer gespeichert waren. Der Grund der gespeicherten Daten ergab sich danach aus einer von dem Beschwerdeführer dort absolvierten Fortbildungsprüfung. Der TLfDI forderte die Kammer auf, den Vorfall zum Anlass zu nehmen und die Kammermitarbeiter nochmals darüber zu unterrichten, dass personenbezogene Daten nur zur Erfüllung der erforderlichen Zwecke genutzt werden und nicht ohne ausdrückliches Einverständnis des Betroffenen an Dritte übermittelt werden dürfen. Nach Angaben der Handwerkskammer wurde in einer Dienstberatung der Sachverhalt zum Anlass genommen, die

verantwortlichen Mitarbeiter über die Einhaltung der datenschutzrechtlichen Vorschriften zu belehren. Der TLfDI informierte den Beschwerdeführer abschließend über die Stellungnahme der Handwerkskammer und die zu seiner Person gespeicherten Datenarten. Ob die Handwerkskammer auch dem Betroffenen noch die erforderliche Auskunft nach § 13 ThürDSG erteilte, ist dem TLfDI nicht bekannt. Der TLfDI sah im Ergebnis von einer Beanstandung der Handwerkskammer ab, da diese den Fehler sofort eingeräumt hatte, alle Mitarbeiter nochmals über die Einhaltung datenschutzrechtlicher Vorschriften belehrt hatte und im Übrigen versicherte, dass es sich lediglich um einen Einzelfall gehandelt habe.

Eine Handwerkskammer darf ebenso wie jede andere öffentliche Stelle personenbezogenen Daten an Dritte nur dann übermitteln, wenn das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt. In allen anderen Fällen ist der Betroffene um seine Einwilligung in die Datenübermittlung zu ersuchen. Weiterhin hat die Daten verarbeitende Stelle dem Betroffenen nach § 13 ThürDSG auf Antrag ohne zumutbare Verzögerung Auskunft über die zu seiner Person verarbeiteten Daten sowie weitere dort genannte Sachverhalte zu erteilen.

13.3 Widersprechende Angaben zur Einhaltung des Datenschutzes bei der GFAW mbH Erfurt

Ein Unternehmensgründer beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den unzulässigen Umgang mit seinen personenbezogenen Daten seitens der Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen mbH (GFAW Thüringen). Nach Schilderung des Betroffenen habe er im Rahmen der Beantragung des vom Europäischen Sozialfonds für Deutschland (ESF) geförderten Existenzgründerpasses gemäß der damaligen GFAW-Richtlinie termingerecht seine Teilnahme an den zu absolvierenden Beratungen (z. B. von Steuerberatern, Rechtsanwälten, Marketingberatern usw.) mit Originalbelegen nachgewiesen. Ihm seien danach auch die Fördermittel ausgezahlt worden. Daraufhin habe die GFAW vom Betroffenen verlangt, geeignete Nachweise für die tatsächlichen Zahlungen in Form von Originalquittungen oder Originalkopien von Kontoauszügen vorzulegen. Die GFAW habe dem Unternehmensgründer

mitgeteilt, dass die vorgelegten, in einigen Teilen unkenntlich gemachten Kontoauszüge zur Prüfung nicht ausreichen würden und nur ungeschwärzte Kontoauszüge vorzulegen seien. Darüber hinaus beschwerte sich der Betroffene darüber, dass er ein Gespräch zur Klärung der genannten Angelegenheit neben dem Eingangsbereich der GFAW habe führen müssen, sodass alle ankommenden Besucher die Möglichkeit gehabt hätten, den vertraulichen Inhalt des Gespräches zu verfolgen. Der TLfDI wandte sich deshalb an die GFAW und bat um Stellungnahme zu dem vom Betroffenen vorgetragenen Sachverhalt. Im Antwortschreiben der GFAW bestritt diese, dass vom Betroffenen ungeschwärzte Kontoauszüge verlangt worden wären. Vielmehr habe der Zuwendungsempfänger im Rahmen der Abrechnung von Fördermitteln Kopien von Kontoauszügen eingereicht. Tatsächlich sei es nicht um die Unkenntlichmachung von Zahlungsvorgängen gegangen, die mit der Förderleistung in keinem Zusammenhang stehen, sondern um den Umstand, dass der GFAW anstelle der Originale nur Kopien vorgelegt worden sein sollen. Die GFAW habe dem Zuwendungsempfänger diesen Unterschied mehrfach erläutert und diesen auf die für die Förderung geltenden Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P), die Bestandteil der Verwaltungsvorschriften zu § 44 Thüringer Landeshaushaltsordnung sind, hingewiesen. Hiernach seien zum Nachweis der Verwendung die Originalbelege vorzulegen, wobei es den Zuwendungsempfängern dabei unbenommen bleibe, die Originale zu schwärzen oder abgedeckt vorzulegen. Dem Zuwendungsempfänger wurde daher auch mehrfach angeboten, anstelle der Übersendung der Originalkontoauszüge diese unter Abdeckung der für die Förderung nicht relevanten Vorgänge zur Einsichtnahme vorzulegen. Eine unzulässige Erhebung personenbezogener Daten liege deshalb nicht vor. Zum zweiten vom Betroffenen geäußerten Vorwurf der nicht gewährleisteten Vertraulichkeit von Gesprächen, verwies die GFAW zunächst darauf, dass persönlich abgegebene Unterlagen am Empfang von Mitarbeitern entgegengenommen würden. Der zuständige Mitarbeiter werde hierzu im Regelfall nicht hinzugezogen. Wenn bei einem Zuwendungsempfänger Beratungs- oder Klärungsbedarf bestehe, erfolge vorab eine Terminvereinbarung mit dem zuständigen Sachbearbeiter. Die Terminvereinbarung erfolge dann in Abhängigkeit von der Verfügbarkeit der Beratungsräume und finde zum Schutz von vertraulichen Daten nicht am Empfang statt. Vorliegend sei der Beschwerdeführer jedoch ohne vorherige

Terminvereinbarung in der GFAW erschienen, da er lediglich Unterlagen abgeben wollte. Jedoch bat der Betroffene die Mitarbeiter des Empfangsbereiches um die persönliche Abgabe der Unterlagen, weshalb umgehend die für den Fall zuständige Sachbearbeiterin am Empfang erschienen sein soll. Diese habe dem Betroffenen mitgeteilt, dass die Unterlagen als Kopie nicht anerkannt werden können und auf die Notwendigkeit von Originalbelegen hingewiesen. In solchen „Ad-hoc Fällen“ werde die Sitzgruppe im Servicebereich abseits des Empfangstresens genutzt. Diese besitzt einen Sichtschutz, damit Dritte keine Einsicht in die Unterlagen eines Zuwendungsempfängers erlangen. Ebenso stelle der Abstand zum Tresen des Empfangs sicher, dass Gespräche in normaler Zimmerlautstärke vom Empfangstresen aus nicht ohne Weiteres mitgehört werden können. Im Ergebnis waren sowohl die Schilderungen des Beschwerdeführers als auch die Stellungnahme der GFAW als plausibel anzusehen. Da die dem TLfDI zur Verfügung stehenden Aufklärungskompetenzen mithin erschöpft waren, war es nicht möglich, den Vorgang abschließend zu klären. Einen datenschutzrechtlicher Verstoß seitens der GFAW konnte der TLfDI nicht feststellen. Dem Beschwerdeführer wurde das für ihn sicherlich nicht zufriedenstellende Ergebnis mitgeteilt. Er hat sich daraufhin aber nicht mehr gemeldet.

Die Pflicht des Zuwendungsempfängers zur Vorlage von Originalbelegen bei der GFAW ergibt sich für zahlreiche Förderleistungen aus den Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P). Wenn bestimmte Vorfälle von einem Betroffenen einerseits und einer Daten verarbeitenden Stelle andererseits unterschiedlich dargestellt werden, die dem TLfDI beide plausibel erscheinen, so kann kein datenschutzrechtlicher Verstoß der Stelle festgestellt werden.

13.4 Gewerbedaten im Internet – nicht für unsichere Drittstaaten bestimmt!

In seinem zehnten Tätigkeitsbericht (hier unter Gliederungspunkt 5.30) hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ausgeführt, dass eine Übermittlung der Grunddaten Name/Firma, Tätigkeit und Anschrift gemäß § 14 Abs. 5 Satz 2 Gewerbeordnung (GewO) innerhalb eines Land-

ratsamtes vom Gewerbeamt an die Wirtschaftsförderung zulässig sei, nicht jedoch deren Veröffentlichung im Internet.

Zu dieser Rechtsauffassung des TLfDI äußerte sich im März 2015 das Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) dahin gehend, dass die Übermittlung der o. g. Grunddaten über das Internet nicht gegen das Thüringer Datenschutzgesetz verstoße.

Das TMWWDG begründete seine Auffassung, die in diesem Sinne auch vom Bund-Länder-Ausschuss „Gewerberecht“ vertreten werde, im Kern damit, das nach Art. 8 Abs. 2 Buchstabe e. der EU-Datenschutzrichtlinie 95/46/EG ein Schutz personenbezogener Daten dann nicht erforderlich sei, wenn der Betroffene sie selbst öffentlich bekannt mache. Um einen solchen Fall handele es sich nach Auffassung des TMWWDG auch bei den o. g. Grunddaten, da die Gewerbebetriebe diese ohnehin im Rechtsverkehr für jedermann offenlegen würden. Zudem seien diese Daten auch im Handelsregister einsehbar.

Weiterhin wies das TMWWDG darauf hin, dass die Dienstleistungsrichtlinie 2006/123/EG in Art. 22 Abs. 1 die Mitgliedstaaten verpflichte, sicherzustellen, dass ein Dienstleistungserbringer Informationen über seinen Namen, seinen Rechtsstatus, seine Rechtsform, seine Anschrift und Informationen darüber, wie eine schnelle Kontaktaufnahme und direkte Kommunikation mit ihm zu ermöglichen sei, zur Verfügung stellen müsse.

Nach eingehender Prüfung der Angelegenheit teilte der TLfDI dem TMWWDG mit, dass er an seiner bisherigen Rechtsauffassung festhalte. Grund hierfür war, dass die Voraussetzungen für eine Datenübermittlung in unsichere Drittstaaten gemäß § 23 Abs. 1 Satz 2 oder Abs. 2 ThürDSG im konkreten Fall gerade nicht vorlagen. Auch vor dem Hintergrund des Safe-Harbor-Urteils des EuGHs vom 6. Oktober 2015 zeige sich die Wichtigkeit des Ausschlusses von Datenübermittlungen in datenschutzrechtlich unsichere Drittstaaten.

Der Grundsatz des Übermittlungsverbots von personenbezogenen Daten in unsichere Drittstaaten, wie er in § 23 ThürDSG zum Ausdruck kommt, kann nur durch normenklare spezialgesetzliche Ausnahmenregelungen durchbrochen werden. Solange diese nicht existieren, hält der TLfDI an seiner Auffassung fest, dass auch Gewerbegrunddaten nicht im Internet veröffentlicht werden dürfen. Die Safe-

Harbor-Entscheidung des Europäischen Gerichtshofs vom 6. Oktober 2015 bestätigt diese Auffassung.

13.5 Verarbeitung von Teilnehmerdaten bei EU-geförderten Projekten

Die EU fördert etliche Bildungsmaßnahmen. Allerdings muss geprüft werden, ob die zur Verfügung gestellten EU-Mittel auch zweckentsprechend eingesetzt wurden. Dazu müssen personenbezogene Daten von Teilnehmern erfasst und verarbeitet werden. Das ist altbekannt. Die technische Entwicklung macht aber auch vor der EU-Förderung nicht Halt. Die EU forderte daher eine Umstellung auf elektronische Verfahren. Diesem Anliegen nahm sich das Thüringer Ministerium für Wirtschaft und Arbeit und Technologie (TMWAT, heute TMWDDG) zuständigkeitshalber an. Es entwickelte das Projekt „Datenschutz und Fraud-Management im eCohesion-Projekt der Operationellen Programme EFRE/ESF“. Fraud-Management bezeichnet übersetzt Technologien zur Betrugserkennung, e-Cohesion bedeutet die weitgehende elektronische Umsetzung der Abwicklung der Strukturförderung. In diesem Verfahren sollen neue IT-gestützte Arbeitsabläufe entstehen, Betrugsfälle leichter aufgedeckt und eine Effektivitätskontrolle ermöglicht werden. Wird ein Projekt bzw. eine Maßnahme aus Mitteln des Europäischen Sozialfonds (ESF) mitfinanziert, bestehen für die im TMWWDG angesiedelte Verwaltungsbehörde Berichtspflichten gegenüber europäischen Institutionen. Hierfür werden personenbezogene Daten der Teilnehmer an den Maßnahmen benötigt.

Das damalige TMWAT beteiligte hierzu den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Dieser stellte fest, dass Grundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verbindliche Rechtsvorschriften der Europäischen Union waren. Hier sind die Verordnungen VO (EU) Nr. 1303/2013 und VO (EU) Nr. 1304/2013, insbesondere der Anhang I, der die zu erfassenden Daten näher bestimmt, und das Operationelle Programm des Europäischen Sozialfonds für die Förderperiode 2014 bis 2020, in welchem festgelegt wurde, mit welchen Indikatoren die Ergebnisse der Förderung gemessen werden, maßgeblich. Da die Gewährung der finanziellen Mittel nach diesen Vorschriften von der vorgeschriebenen Berichterstattung abhängt, wird auch die Teilnahme an der Maßnahme von der voll-

ständigen Angabe der erforderlichen personenbezogenen Daten abhängig gemacht. Hierzu wurde vom zuständigen Ressort ein Erhebungsbogen erarbeitet. Bei Eintritt in das Projekt werden Angaben zur persönlichen und beruflichen Situation der Teilnehmer erhoben. Hierzu gehören auch Fragen zu Behinderungen oder zum Migrationshintergrund. Die Beantwortung dieser beiden Fragen ist freiwillig, eine fehlende Angabe führt nicht zum Ausschluss von der Maßnahme. Wenn die Maßnahme beendet ist, werden auch noch Angaben zur veränderten beruflichen Situation und zum Bildungsabschluss erhoben. Sechs Monate nach Austritt des Teilnehmers aus dem Projekt wird dann stichprobenmäßig von der Verwaltungsbehörde (im Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie [TMSGFF]) bei den Teilnehmern eine weitere Befragung zur beruflichen Situation durchgeführt. Mit der Durchführung der Datenerhebung wird der jeweilige Träger des Projekts beauftragt, der die datenschutzrechtlichen Vorgaben einzuhalten hat. Er darf die Daten also nur zu dem vorgegebenen Zweck erheben und verarbeiten. Im Auftrag des nach dem Regierungswechsel zuständigen TMSGFF werden die Daten über das Portal der Gesellschaft für Arbeits- und Wirtschaftsförderung (GFAW) erfasst und bei der Thüringer Aufbaubank (TAB) in einer Datenbank gespeichert. Der Europäischen Kommission wird durch das TMSGFF in Erfüllung der Berichtspflichten eine Zusammenfassung ohne Namen und Adressen der Teilnehmer übermittelt. Der Personenbezug in der bei der TAB geführten Datenbank ist für eine Zuordnung zum Zweck der oben erwähnten späteren Befragung nach sechs Monaten erforderlich.

Der TLfDI hat den Fragebogen auf dem Teilnehmerportal aus dem datenschutzrechtlichen Blickwinkel überprüft. Wichtig war vor allem die Aufklärung der von der Datenerhebung Betroffenen (=Teilnehmer), um die doch schwierige und komplexe Angelegenheit transparent zu machen. Jeder muss erkennen können, zu welchem konkreten Zweck er welche konkreten Daten anzugeben hat und zu welchem Zweck sie durch wen weiter verarbeitet werden. Eindeutig muss auch erkennbar sein, welche Daten Pflichtangaben sind, welche Angaben freiwillig gemacht werden können und welche Rechtsfolgen eine fehlende Angabe hat.

Den Anregungen und Forderungen des TLfDI wurde in diesem Zusammenhang vollständig nachgekommen. Damit ist auch wichtige Vorarbeit geleistet, denn diese Art der Datenverarbeitung soll in

Zukunft auf weitere Anforderungen von Daten nach Europäischen Vorschriften ausgeweitet werden.

Besonders bei der Umstellung auf automatisierte Verfahren zur Datenerhebung und -verarbeitung kommt der Aufklärung der Betroffenen erhebliche Bedeutung zu. Jeder muss erkennen können, zu welchem konkreten Zweck er welche konkreten Daten anzugeben hat und zu welchem Zweck sie durch wen weiterverarbeitet werden. Eindeutig muss auch erkennbar sein, welche Daten Pflichtangaben sind, welche Angaben freiwillig gemacht werden können und welche Rechtsfolgen eine fehlende Angabe hat.

13.6 Feuer (daten-) frei – Datenerhebung beim Bezirksschornsteinfeger

Die Schornsteinfegerinnung Thüringen informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass eine Untere Immissionsschutzbehörde plane, bei den Bezirksschornsteinfegern in zahlreichen Fällen personenbezogene Daten von Eigentümern, die Feuerungsanlagen betreiben, zu erheben. Aus datenschutzrechtlicher Sicht ist ein solches Übermittlungersuchen jedoch nach derzeitigem Kenntnisstand des TLfDI unzulässig und daher von den Bezirksschornsteinfegern abzulehnen. Eine Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 Thüringer Datenschutzgesetz (ThürDSG) – [Rechtsvorschrift, Einwilligung, im Interesse des Betroffenen liegend, allgemein zugängliche Quellen, Strafverfolgung usw.] zulassen würden. Nach Auffassung des TLfDI ist die Zulässigkeit bereits deshalb nicht gegeben, weil die Datenerhebung nicht zur Erfüllung der in der Zuständigkeit des Bezirksschornsteinfegers und der Unteren Immissionsschutzbehörde liegenden Aufgaben erforderlich ist. Es gibt weder eine Rechtsgrundlage für das personenbezogene Erheben der vom Bezirksschornsteinfeger festgestellten Messwerte der Feuerungsanlagen, noch ist die Überprüfung der rechtmäßigen Durchführung der dem Bezirksschornsteinfeger zugewiesenen Aufgaben zur Erfüllung der Aufgaben der Unteren Immissionsschutzbehörde erforderlich. Aus der Ersten Verordnung zur Durchführung des Bundesimmissi-

onsschutzgesetzes ergibt sich, dass der Bezirksschornsteinfeger die Feuerstättenschau für die Feuerungsanlagen vornimmt. Somit erfolgt die Überwachung grundsätzlich durch den Bezirksschornsteinfeger. Dieser hat dem Eigentümer einer Feuerstätte Mängel an kehr- und überprüfungspflichtigen Anlagen mitzuteilen und zur Behebung innerhalb von sechs Wochen aufzufordern. Erst wenn der Eigentümer einer Feuerungsanlage der Behebung des Mangels nicht nachkommt, hat der Bezirksschornsteinfeger den Mangel der zuständigen Behörde anzuzeigen (§ 5 Abs. 1 Schornsteinfeger-Handwerksgesetz). Zusammenfassend ist festzuhalten, dass die Untere Immissionsschutzbehörde nicht ohne begründete Anhaltspunkte den Bezirksschornsteinfeger auffordern darf, ihr personenbezogenen alle Eigentümer einer Feuerungsanlage einschließlich der technischen Daten der Anlage sowie der dort gemessenen Werte vorzulegen. Dies stellt zum einen alle Feuerstättenbetreiber unter einen gewissen Generalverdacht, und zum anderen ist gegebenenfalls hier auch ein Misstrauen gegenüber den Bezirksschornsteinfegern dahingehend abzuleiten, ob diese ihrer Anzeigepflicht nachkommen. Gegen eine Übermittlung von statistischen Daten zu Feuerungsanlagen (Alter, Leistung, Immissionswerte usw.) bestehen aus datenschutzrechtlicher Sicht hingegen keine Bedenken. Eine endgültige Stellungnahme der betroffenen Unteren Immissionsschutzbehörde hinsichtlich des dort Veranlassten steht noch aus. Diese wurde vom TLfDI bereits mehrfach angemahnt und steht kurz vor der Beanstandung wegen mangelnder Unterstützung nach § 38 Abs. 1 Nr. 1 ThürDSG.

Die bevollmächtigten Bezirksschornsteinfeger führen als beliehene Unternehmer in den ihnen anvertrauten Kehrbezirken hoheitliche Tätigkeiten aus. Eine Übermittlung von personenbezogenen Daten der Feuerstättenbetreiber an die Untere Immissionsschutzbehörde, ohne dass eine Rechtsvorschrift dies eindeutig vorsieht, ist unzulässig. Nur wenn ein Bezirksschornsteinfeger einen Feuerstättenmangel dort anzeigt, dürfen die erforderlichen personenbezogenen Daten an die Untere Immissionsschutzbehörde übermittelt werden.



Dozent hilft Studierenden © Robert Kneschke / Fotolia.com

14 Bildung, Jugend, Sport

14.1 Arbeitskreis (AK) Datenschutz und Bildung

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) tagte der Arbeitskreis Datenschutz und Bildung im vorliegenden Berichtszeitraum dreimal in Erfurt. Um einige wichtige Punkte herauszugreifen, die in den Sitzungen behandelt wurden, soll zunächst auf Projekt „Young Data“ verwiesen werden (siehe dazu Nummer 14.16). Die anwesenden Arbeitskreismitglieder diskutierten darüber, auf welche Weise das Jugendportal in die Verantwortung der Datenschutzbeauftragten des Bundes und der Länder übergeben werden kann. Unter anderem wurde hierbei festgelegt, wie sich die finanzielle Unterstützung des Bundes und der Länder gestaltet. Darüber hinaus wurden an den Bund und die Länder Arbeitsaufgaben hinsichtlich der inhaltlichen Betreuung der Menüpunkte des Internetauftritts verteilt. Weitere Punkte waren die formale Gestaltung von bestimmten Menüpunkten und die Klärung der presserechtlichen Verantwortlichkeiten für den Inhalt von „Young Data“. Die Seite ging dann als gemeinsames Kinder- und Jugendportal der Datenschutzbeauftragten des Bundes

und der Länder anlässlich des Safer Internet Day am 10. Februar 2015 recht erfolgreich an den Start. Der Arbeitskreis beschäftigte sich auch mit dem Thema „Medienkunde als Schulfach“ und hier schwerpunktmäßig mit der Umsetzung des im Beschluss der Kultusministerkonferenz (KMK) zur Medienbildung in der Schule vom 8. März 2012 geäußerten Willens, dass Medienbildung in Lehrplänen und in der Lehrerbildung verbindlich festgeschrieben werden sollte. Es wurde aus dem Arbeitskreis vorgeschlagen, einen medienpolitischen Kongress zu dieser Problematik durchzuführen. Man einigte sich dann darauf, dass der TLfDI zum Safer Internet Day am 10. Februar 2015 eine derartige Veranstaltung durchführt. Der TLfDI organisierte daraufhin eine Fachtagung unter Beteiligung zahlreicher Experten auf dem Gebiet der Medienkompetenz und zahlreicher interessierter Zuschauer (siehe hierzu Anlage 48). Auf Einladung des TLfDI nahm auch der frühere Staatssekretär des ehemaligen Thüringer Ministeriums für Bildung, Wissenschaft und Kultur Stellung zum Stand der Vermittlung von Medienkompetenz in den Thüringer Schulen und hob hierbei auch die Wichtigkeit der Berücksichtigung dieses Themas in der grundständigen Lehrerbildung vor. Er verwies diesbezüglich auf den dabei geplanten Ausbau in Kooperation mit dem TLfDI. Der TLfDI erwähnte in diesem Zusammenhang, dass der Beschluss der KMK aus dem Jahr 2012 in den Ländern aus Sicht der Landesdatenschutzbeauftragten nicht hinreichend umgesetzt werde und eine Evaluierung der gegenwärtigen Standards bei der Umsetzung von Medienbildungskonzepten im Schulunterricht und in der Lehrerbildung nicht stattfinde.

Weiterhin tauschten sich die Arbeitskreismitglieder darüber aus, wie das Thema Medienbewusstsein tatsächlich unter die Menschen gebracht werden könne. Die Landesdatenschutzbeauftragten berichteten hierzu über ihre Aktivitäten in Form von Veranstaltungen, Vorträgen, Aktionen, Kampagnen usw., um die Wichtigkeit des Anliegens herauszustellen. Der TLfDI berichtete von seiner Idee, die Abgeordneten für die Sache zu interessieren und z. B. einen runden Tisch zusammen mit Informatikern, Datenschützern und auch Lehrern zu installieren.

Zur Arbeitskreissitzung am 1. Dezember 2015 hatte der TLfDI zum Thema „Medienbildung in der Schule“ unter Berücksichtigung des Beschlusses der Kultusministerkonferenz mehrere Fachleute eingeladen, die zu dem Thema sachkundig Stellung nehmen konnten. Die

Staatssekretärin des Thüringer Ministeriums für Bildung, Jugend und Kultur berichtete, dass im Zusammenhang mit dem Beschluss der Kultusministerkonferenz vom 8. März 2012 eine Arbeitsgruppe auf Staatssekretärsebene eingerichtet wurde, die bereits erste Vorschläge zur Umsetzung der Forderungen des Beschlusses entwickelt habe. Es sei geplant, bis Ende des Jahres 2016 ein Ergebnis vorzulegen. Zur Situation in Thüringen verwies die Staatssekretärin auf die externe Evaluation des Kurses Medienkunde, die vom TLfDI unterstützt werde. Es gebe auch einen „Runden Tisch Medienkompetenz“ als interministerielle Arbeitsgruppe, die für eine bessere Vernetzung sorgen solle. Ein Ergebnisbericht an den Thüringer Landtag sei für das Jahr 2017 geplant.

In einem weiteren Gastvortrag wurde die derzeitige Erarbeitung einer Strategie der Kultusministerkonferenz zur „Bildung in einer digitalen Welt“ bis Ende 2016 unter Einbeziehung der verschiedenen Kultusministerkonferenz-Ausschüsse vorgestellt. Danach werden dort Vorschläge erarbeitet, auf welche Weise die Lehrpläne der Schulen ergänzt werden müssen, um mehr Medienkompetenz zu schaffen. Es soll eine bundesweite Verständigung über gültige verbindliche Anforderungen in den Bereichen der Qualifizierung von Erziehenden und Lehrenden geben. Die Arbeitskreismitglieder signalisierten die Bereitschaft zum Dialog mit der Kultusministerkonferenz und begrüßten die künftige intensive Kooperation ausdrücklich. Der TLfDI als Vorsitzender des AK Datenschutz und Bildung wird nach Abschluss des Koordinierungsprozesses innerhalb des Generalsekretariats der Kultusministerkonferenz in die weitere Planung einbezogen werden. Die unmittelbare Zusammenarbeit der Kultusministerkonferenz mit dem Arbeitskreis Datenschutz und Bildung zum Thema „Medienbildung in der Schule“ stellt dabei ein Novum dar, von dem sich der TLfDI eine stärkere Einflussnahme des Datenschutzes auf die zukünftige Medienbildung in den Schulen verspricht.

In einem wissenschaftlichen Vortrag wurde der Einsatz von digitalen Medien in der Bildung beleuchtet. Die Vortragende plädierte dafür, dass digitale Medien und die pädagogische Arbeit besser verbunden werden und ein Lernen und Lehren mit digitalen Medien nicht reicht. Nur die Hälfte der Lehrenden schätze die Potentiale digitaler Medien. In Deutschland gebe es einen negativen Zusammenhang zwischen der Häufigkeit der Computernutzung in der Schule und digitalen Kompetenzen der Schüler. Nach einer Studie habe das Lernen

mit digitalen Medien im Schnitt einen relativ geringen nachweisbaren Effekt auf den Lernerfolg. Der Lernerfolg hänge danach eher von Faktoren wie Weiterbildung der Lehrkräfte, der Einbindung in Unterrichtskonzepte und der Art der eingesetzten Software ab. Schließlich verwies die Wissenschaftlerin auf die Notwendigkeit des Einsatzes von digitalen Medien als Bildungsmedien und stellte die Chancen dar, die der richtige Einsatz von digitalen Medien für Lernprozesse biete. Hierzu gehöre nicht nur das Lernen über die richtige Benutzung von digitalen Medien, sondern vielmehr das Verständnis und die Auseinandersetzung darüber, wie digitale Medien funktionieren. Lehrende sollen ein digitales Medium nicht nur von seiner Oberfläche und Funktion kennen, sondern auch die dahinter stehenden Prozesse wie Algorithmen berücksichtigen und dieses an die Schüler weitergeben. Es besteht die Forderung nach einer verpflichtenden Medienbildung für pädagogische Fachkräfte in der Jugend- und der Lehrerbildung sowie der entsprechenden Verankerung in den Schullehrplänen und in der beruflichen Bildung.

Insgesamt sieht der TLfDI den Arbeitskreis Datenschutz und Bildung weiterhin auf einem guten Weg. Die Vermittlung von Medienkompetenz durch Medienbildung bei Lehrern und Schülern, aber auch in der Bevölkerung insgesamt und die Stärkung des datenschutzrechtlichen Bewusstseins werden dem Arbeitskreis Datenschutz und Bildung als Schwerpunktthemen erhalten bleiben.

Der Arbeitskreis Datenschutz und Bildung hat weiterhin das Thema Datenschutz als Bildungsaufgabe als Schwerpunkt seiner Arbeit. Dabei stehen der Austausch der Arbeitskreismitglieder über Aktivitäten zur Förderung der Medienkompetenz und auch die aktive Beteiligung am fachlichen und politischen Prozess der Umsetzung dieses Ziels in den Ländern im Vordergrund. Die Kooperation des Arbeitskreises mit der Kultusministerkonferenz zu Fragen der Umsetzung von Medienbildung in Schule, Lehrerbildung und Lehrerweiterbildung wird zukünftig erstmals die Möglichkeit bieten, den datenschutzrechtlichen Aspekt verstärkt einzubringen.

14.2 Unterarbeitskreis Datenschutz und Schule

Im vergangenen Berichtszeitraum fanden unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zwei weitere Sitzungen der Arbeitsgruppe

Datenschutz und Schule der Konferenz der Datenschutzbeauftragten des Bundes und der Schule, die nunmehr Unterarbeitskreis (UAK) Datenschutz und Schule des Arbeitskreises Datenschutz und Bildung heißt, statt. Nach wie vor herrscht in den Bundesländern an datenschutzrechtlichen Themen im Schulbereich kein Mangel. Dementsprechend wurden auf den Sitzungen zahlreiche Tagesordnungspunkte besprochen. Ein Schwerpunkt war die Einführung von Online-Lernplattformen an Schulen. Hierbei stellen die Schulen eine Software zur Verfügung, die für Unterrichtszwecke eingesetzt wird. Hierauf werden Lernmaterialien für den Zugriff abgelegt, Lernvorgänge organisiert und die Kommunikation zwischen den Lehrerinnen/Lehrern und den Schülerinnen/Schülern über das Internet ermöglicht. Inzwischen gibt es zahlreiche Anbieter von Online-Lernplattformen, die ihre Software den Schulen zur Nutzung anbieten. Die Landesdatenschutzbeauftragten berichteten dabei im Kollegenkreis über die Ergebnisse ihrer datenschutzrechtlichen Prüfung von bestimmten Online-Lernplattformen. Ebenfalls wurden jeweils die Rechtsgrundlagen vorgestellt, die das Betreiben von Online-Lernplattformen im eigenen Bundesland erlauben und entweder die Teilnahme hieran nur auf freiwilliger Basis gestatten oder aber die Nutzung des Systems als verpflichtend vorschreiben. Der UAK war sich einig darüber, dass ein solches System nur eingeführt werden darf, wenn die faktische Teilnahme der Lernenden hieran durch die Schule gewährleistet werden kann. Aufgrund der datenschutzrechtlichen Komplexität der Nutzung von Online-Lernplattformen erarbeitet der Arbeitskreis Datenschutz und Bildung zurzeit eine entsprechende Orientierungshilfe (siehe dazu Nr. 14.33.), die noch in diesem Jahr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgelegt werden wird und den Schulen dann zur Verfügung gestellt werden soll. Diese können sich anhand der Orientierungshilfe einen Überblick darüber verschaffen, welche datenschutzrechtliche Mindestkriterien sie in Online-Lernplattformen erfüllen müssen. Als weiteres großes Thema wird darüber diskutiert, dass Lehrer in zunehmendem Maße private Datenverarbeitungsgeräte für den Einsatz von schulischen Anwendungen nutzen. Gemeint sind hier die zahlreich angebotenen Apps, die es den Lehrkräften ermöglichen, ihre privaten mobilen Datenverarbeitungsgeräte für dienstliche Zwecke einzusetzen und hiermit personenbezogene Schüler-, Eltern- und Lehrerdaten zu verarbeiten. Im Ergebnis stellte der UAK fest, dass in den meisten Bundesländern, so auch in Thüringen,

noch keine Vorschriften bestehen, die speziell die dienstliche Nutzung von privaten mobilen Endgeräten regeln. Aus dem UAK hat sich eine Ad-Hoc-Arbeitsgruppe gebildet, die eine Handreichung „Einsatz von schulischen Anwendungen auf privaten Datenverarbeitungsgeräten bei Lehrkräften“ für Schulleiter und Lehrer erarbeitet hat (siehe dazu Nr. 14.40.) und diese ebenfalls noch in diesem Jahr den Schulen zur Verfügung stellen wird. Weiteres Thema des UAK war der Umgang mit Schülerdaten bei Kindern von beruflich Reisenden. Bedingt durch den ständigen Schulwechsel müssen unterschiedliche Schulen, die die Kinder jedes Jahr besuchen, auf die betroffenen Schülerdaten zugreifen. Die erforderlichen Datenflüsse zwischen der jeweiligen Stammschule dieser Schüler und den übrigen besuchten Schulen sowie die hierzu verwendete Software müssen datenschutzrechtlich begleitet werden. Im Zusammenhang mit den zahlreichen bundeslandübergreifenden Schul- und Bildungsuntersuchungen, zu denen in den meisten Bundesländern die Landesdatenschutzbeauftragten um eine datenschutzrechtliche Stellungnahme der jeweiligen Untersuchung gebeten werden, wurde aus Kreisen der Bildungsforscher der Vorschlag unterbreitet, das datenschutzrechtliche Prüfverfahren zu vereinfachen. In diesem Zusammenhang gab es auch einen Austausch über die gesetzlichen Bestimmungen in den einzelnen Ländern, wenn in wissenschaftlichen Schülerbefragungen auch Fragen enthalten sind, die den Kernbereich privater Lebensgestaltung betreffen. In manchen Bundesländern besteht die gesetzliche Regelung, dass die Beantwortung solcher Fragen nur mit Einwilligung der Betroffenen erfolgen darf. Einige Landesdatenschutzbeauftragte sind der Auffassung, dass auch mit ausdrücklicher Regelung eine Einwilligung zur Beantwortung der Fragen erforderlich ist, da hier die schutzwürdigen Belange des Betroffenen immer überwiegen. In anderen Bundesländern existieren Verordnungen, die einen Datenkatalog enthalten, in dem geregelt ist, welche Daten erhoben werden dürfen. Besprochen wurden auch die neuen Entwicklungen im Schuldatenschutzrecht in den Ländern. Hier bauen einige Länder die dort bestehenden speziellen Schuldatenschutzverordnungen weiter aus und passen diese an die gegebenen technischen Entwicklungen an. Hinsichtlich einer Nutzung von sozialen Netzwerken für den Unterricht ergibt sich in den Ländern ebenfalls ein uneinheitliches Bild. Teilweise besteht von Kultusseite ein Verbot für schulische Kontakte über soziale Netzwerke zwischen den Lehrkräften und den Schülern, in anderen Fällen warnen Landesdatenschutzbeauftragte

generell vor einer Nutzung sozialer Netzwerke zu schulischen Zwecken und beraten hierzu die Schulen oder geben selbst erstellte Handreichungen heraus. Weitere Themen waren z. B. die Videoüberwachung an Schulen, das Erstellen von Videoaufnahmen im Unterricht, die Sozialarbeit an den Schulen, die schulische Nutzung von Cloud-Diensten, Datenübermittlung von den Schulen an die Jugendberufsagenturen, das Blockieren oder Orten von Mobilfunk durch Schulen bei Prüfungen usw. Es ist abzusehen, dass dem UAK Datenschutz und Schule die Arbeit nicht ausgehen wird.

Der UAK Datenschutz und Schule hat sich auch in den letzten zwei Jahren mit zahlreichen Datenschutzthemen auseinandergesetzt, die bei der Verarbeitung von Schüler-, Eltern- und Lehrerdaten durch die Schule entstehen. Durch den Austausch mit den Kollegen aus den anderen Bundesländern gewinnt der TLfDI wertvolle Hinweise für die eigene Arbeit im Schulbereich.

14.3 Medienbildung tut not – TLfDI sorgt für Futter!

„Wir haben nichts!“ – So schallte es dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bei seinen Besuchen in Thüringer Schulen entgegen. Der Hilfeschrei kam von Lehrern und bezog sich auf geeignete Unterrichtsmaterialien zu den Themen Datenschutz und Datensicherheit. Vor allem jene Lehrerinnen und Lehrer, die an der Umsetzung des Kurses Medienkunde beteiligt sind, fühlten sich alleingelassen. Dem TLfDI war natürlich klar, dass sich hier etwas tun muss und handelte, unter anderem, indem er einen Lehrer an seine Behörde holte, der sich darum kümmert. Seitdem ist einiges geschehen. Nach intensiver Internetrecherche waren schnell geeignete Videos, Broschüren usw. gefunden. Bei besonders geeigneten Materialien sorgte der TLfDI für die Nutzungsrechte für Thüringer Schulen. Die Angebote landeten dann umgehend in der Mediothek des Thüringer Schulportals zum kostenfreien Download. Links zu anderen Quellen im Netz füllen eine eigens beim TLfDI entwickelte Mediendatenbank. Sie erlaubt dem Lehrer, alters- und schlagwortspezifisch nach „Futter“ für seine Schüler zu suchen. Die Datenbank ist auf der Internetseite des TLfDI online. Dort ist auch schon ein Video abrufbar, das Teil eines komplexen Unterrichtsprojektes ist, das beim TLfDI selbst entwickelt wurde. In sechs Unterrichtsstunden können und sollen

sich Schüler im Rahmen des Sozialkundeunterrichts mit der Frage „Videouberwachung – In Ordnung oder nicht?“ auseinandersetzen. Das umfangreiche Material ist so ausgearbeitet, dass ein Lehrer den Unterricht für seine Schüler auch dann erfolgreich gestalten kann, wenn er sich zuvor noch nicht mit diesem Thema beschäftigt hat. Erfolgreich sein heißt hier, dass die Jugendlichen ihre Sensibilität für den Wert des Grundrechts auf informationelle Selbstbestimmung und ihre Bürgerrechte entwickeln und „nebenbei“ auch ihre Medienkompetenz. Beide Aspekte sind dem TLfDI Grundanliegen, die er mit Nachdruck gegenüber den politisch Verantwortlichen in Thüringen und der Kultusministerkonferenz (KMK) vertritt. Denn hier besteht Handlungsbedarf in unserer digitalisierten Welt, insbesondere was die Befähigung der jungen Generation zur reflektierten(!) Interaktion mit Medien betrifft. Der Schutz von und der sensible Umgang mit personenbezogenen Daten sind hier zentrale Herausforderungen.

Der TLfDI setzt sich offensiv für Veränderungen in den Schulen ein. Unabdingbar ist auch, dass eine solide Medienbildung endlich in den Lehramtsstudiengängen der Hochschulen Eingang findet und zwar für alle Schulfächer aller Bildungsgänge. Der TLfDI fordert nicht nur, sondern hat dem Bildungsministerium konkrete Unterstützungsangebote unterbreitet, beispielsweise für die Einbindung von Datenschutz- und Datensicherheitsinhalten in die Lehrerbildung an den Thüringer Studienseminaren. Darüber hinaus hat er seine Bereitschaft zur Mitwirkung bei der Evaluation des Kurses Medienkunde erklärt, die vom Bildungsministerium auch angenommen wurde.

Auch landesübergreifend engagiert sich der TLfDI für eine zeitgemäße Medienbildung. Auf einer KMK-Fachkonferenz im September 2015 stieß der TLfDI mit seinem Beitrag über den Datenschutz als Zukunftskompetenz im digitalen Zeitalter auf große Resonanz. In der Folge entwickelte sich eine Zusammenarbeit zwischen dem Arbeitskreis Datenschutz und Bildung der Datenschutzbeauftragten des Bundes und der Länder – dessen Vorsitzender der TLfDI ist – und Vertretern der KMK (siehe dazu Nr. 14.1).

Handeln ist angesagt! Strategiepapiere, an deren Umsetzung es häufig mangelt, gibt es bereits genug.

Datenschutzaspekte sind wesentlicher Bestandteil von Medienkompetenz. Der TLfDI sieht hier Handlungsbedarf und sorgt auf verschiedenen Ebenen dafür, dass sich etwas bewegt.

14.4 Medienschulen in Thüringen – kein Auslaufmodell!

„Thüringer Medienschule“ – mit Stolz brachten etliche Thüringer Schulen in den 2000er-Jahren ein solches Schild an’s Schulhaus an. Allen „draußen“ sollte es klar machen: Hier zieht das Informationszeitalter nicht an der Schultür vorbei, sondern hält Einzug in die Klassenräume und vor allem in die Köpfe von Lehrern und Schülern. 47 Schulen machten sich damals von 2000 bis 2006 auf den Weg und bildeten ein thüringenweites Netzwerk. Dabei waren Schulen aller allgemeinbildenden Schularten, angefangen von Grundschulen über Regelschulen, Gesamtschulen bis hin zu Gymnasien. Auch Förderschulen reihten sich ein, weil sie erkannten, dass eine möglichst solide Medienkompetenz für Beruf und gesellschaftliche Teilhabe unverzichtbar ist. Die beteiligten Schulen waren nicht allein. Sie erhielten Ausstattungsunterstützung. Zudem konnten sich die Lehrkräfte in zahlreichen zentralen Fortbildungen des Thüringer Instituts für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) und regional in den Schulamtsbereichen fortbilden. Die Medienschulen selbst strahlten mit ihren Erfahrungen in ihr regionales Umfeld aus. Alles in allem ein guter Anfang.

Was ist draus geworden? Sind inzwischen weitere Medienschulen hinzugekommen? – Diese Fragen standen 2015 auch auf der Agenda des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Bekanntermaßen steht dort die Medienkompetenzentwicklung der Thüringer Schülerinnen und Schüler ganz oben auf der Liste, denn Datenschutz und Datensicherheit sind heute ein untrennbarer Aspekt dieser Schlüsselqualifikation.

Anfragen beim Thüringer Ministerium für Bildung, Wissenschaft und Sport zeigten, dass der Schwung nachgelassen hat. Seit 2010 gibt es noch sieben offiziell geführte Medienschulen in ganz Thüringen. Man muss fragen, ob Initiativreichtum und Kraft dieser sieben besonders engagierten Schulen ausreichen können, um auf die anderen 811 allgemeinbildenden Schulen Thüringens (ohne Schulen in freier Trägerschaft) wirkungsvoll auszustrahlen. Das Ministerium teilte auf Anfrage des TLfDI mit, dass die Schulleiter eine stärkere Vernetzung wünschten und dass beim nächsten Thüringer Schulmedientag angesprochen werden soll, wie „im Rahmen unserer Möglichkeiten gezielter Unterstützung“ geleistet werden kann. Der TLfDI wird diesen Prozess nach Kräften unterstützen, auch im Rahmen

des im Oktober 2015 konstituierten „Runden Tisches Medienkompetenz“.

Der TLfDI stellt insgesamt fest, dass in puncto Medienkompetenz in Thüringen Aufbruchstimmung herrscht. Konzentriertes Vorgehen wird Thüringen auch hier wieder einen Spitzenplatz verschaffen. Medienschulen zeichnen sich durch besonderes Engagement für die Medienkompetenzentwicklung ihrer Schüler aus. Sie sind Impulsquelle für andere Schulen der Region.

14.5 Lernmanagementsystem neu denken!

Aufgrund des großen Engagements des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu dem Thema Medienkunde wurden im Berichtszeitraum zahlreiche allgemeine Anfragen aus dem Schulbereich an den TLfDI herangetragen. Die Schulen möchten einerseits auf Augenhöhe mit den Schülern kommunizieren und dafür die modernen Medien nutzen. Die gängigen sozialen Netzwerke bieten aber andererseits für den Schulbereich keine datenschutzgerechten Lösungen an. Daher versuchen etliche Schulen, eigene Lösungen zu finden. Im Zuge eines derartigen Projektes trat ein Lehrer an den TLfDI heran und bat um fachliche Begleitung. Im Gespräch stellte sich heraus, dass die Schule ein Open-Source-Lernmanagementsystem ins Auge gefasst hatte, das die Funktion sozialer Netzwerke abbilden und diese datenschutzkonform umsetzen sollte. Das System sei bereits von einem Landesbeauftragten für den Datenschutz begutachtet und für gut befunden worden. Diese Angaben konnten bei konkreter Nachfrage bei diesem Landesbeauftragten für den Datenschutz leider nicht bestätigt werden. Es stellte sich heraus, dass vermutlich der Datenschutzbeauftragte der Stelle, die das Lernmanagementtool entwickelt hatte, diese Prüfung vorgenommen hatte. Dem Lehrer wurde erklärt, dass der TLfDI gerne bereit ist, das Lernmanagementsystem zu prüfen, sofern die Schule sich für einen Einsatz entscheidet und den TLfDI um eine Prüfung bittet. Hierzu ist es im Verlauf des weiteren Verfahrens noch nicht gekommen.

Nach Auffassung des TLfDI besteht im Bereich der Lernmanagementsysteme Handlungsbedarf. Da bei der Kommunikation zwischen Schule und Schülern mit diesen Mitteln zahlreiche daten-

schutzrechtliche Probleme geklärt werden müssen, wird es künftig vermehrt Aufgabe des TLfDI sein, derartige Systeme auf die Vereinbarung mit den geltenden Datenschutzregeln zu prüfen.

14.6 Datenschutz im Hort

Die Mutter eines Schulkindes beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über den in einer Stadtverwaltung herausgegebenen Erhebungsbogen zur Anmeldung eines Kindes im Schulhort. Insbesondere hielt die Beschwerdeführerin die Frage zur Angabe der genauen Hortbetreuungszeit und die Abfrage des Ermäßigungstatbestands, auch wenn dieser gar nicht genutzt werden sollte, für unzulässig. Bei der Berechnung der Hortgebühr wird das Einkommen der Eltern sowie die Zahl der kindergeldberechtigten Kinder in einer Familie berücksichtigt. Wer weiß, dass der Ermäßigungstatbestand nicht erfüllt wird und ohnehin die Höchstgebühr zu entrichten hat oder dies freiwillig tut, muss diesen Teil des Erhebungsbogens wegen mangelnder Erforderlichkeit nicht ausfüllen. Der TLfDI konfrontierte die verantwortliche Stadtverwaltung mit den von der Beschwerdeführerin angeführten Kritikpunkten und wies gleichzeitig auf § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) hin, wonach die Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Nach § 4 der Thüringer Hortkostenbeteiligungsverordnung wird lediglich danach unterschieden, ob eine Betreuung von mehr oder weniger als 10 Stunden in der Woche erfolgen soll. Sofern ein Elternteil sein Kind für mehr als 10 Stunden in der Woche anmeldet, hat es Anspruch auf Betreuung während der gesamten Öffnungszeit des Hortes. Auf Grundlage dieser Vorschrift war es nicht zulässig, bei den Erziehungsberechtigten verpflichtend die genaue Zeit zu erheben, in der das Schulkind den Hort besucht.

Der TLfDI forderte die Stadtverwaltung deshalb zunächst auf, diese Angaben lediglich auf freiwilliger Basis zu erheben und dies im Erhebungsbogen deutlich zu kennzeichnen oder aber die Frage aus dem Formular herauszunehmen. Die Stadtverwaltung wies in ihrer Stellungnahme dann darauf hin, dass die erhobenen Daten alle zwei Jahre an das zu diesem Zeitpunkt zuständige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) übermittelt werden mussten und insofern die Verantwortlichkeit für die Zulässigkeit

dieser Datenerhebung dort lag. Tatsächlich bat das TMBWK einige Zeit später den TLfDI und die Stadtverwaltung für die Klärung des Sachverhalts zu einem Gespräch. Aus diesem Gespräch ergab sich, dass die Stadtverwaltung als Schulträger im vorliegenden Fall nicht nach dem Thüringer Schulgesetz, sondern als Träger des Schulhortes handelte. Damit richtete sich die Zulässigkeit der Datenerhebung nach dem ThürDSG. Gemäß § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist. Zusätzlich wurden nach Nr. 4.2.2 der zu diesem Zeitpunkt gültigen Verwaltungsvorschrift des TMBWK vom 12. Dezember 2013 (Gz: 1B 4/4025) den Grund- und Gemeinschaftsschulen im Rahmen der dem Schulamt zur Verfügung gestellten Stellen die Erzieherwochenstunden für die Hortarbeit von den Schulämtern zugewiesen. In einer Planungsphase wurde zunächst ein durchschnittlicher Wert für die Berechnung des Erzieherbedarfs ermittelt, der dann zum Schuljahresbeginn endgültig abgeglichen wurde. Um die Zahl der benötigten Erzieher und die anfallende Betreuungszeit möglichst sachgerecht ermitteln zu können, war es für den Schulträger hilfreich zu wissen, zu welchen Zeiten ein Kind regelmäßig den Hort aufsucht. Hintergrund hierfür war die Teilnahme der Stadtverwaltung an einem Erprobungsmodell des Landes, welches seit mehreren Jahren durchgeführt wurde. Hier erstattete das Land den Trägern die Differenz, die zwischen dem für das Hortpersonal bereitgestellten Geld und dem tatsächlichen Bedarf bestand. Um den Differenzbetrag festzustellen, war es notwendig, dass der Schulträger Daten erhebt. Auch unter Berücksichtigung der vom TMBWK erlassenen, oben genannten Verwaltungsvorschrift, die sich an die Schulverwaltungsämter, nicht aber an die Bürger richtete, kam der TLfDI erneut zur Auffassung, dass die Antragsteller auf einen Schulhortplatz gesetzlich nicht verpflichtet waren, hierzu verbindliche Angaben zu machen. Gleichwohl hat der TLfDI auf eine Kennzeichnung dieser Frage als freiwillig verzichtet, da der Träger des Schulhortes zur Übermittlung der Summe der konkreten Stundenzahl einer Hortnutzung an das TMBWK verpflichtet war. Lediglich die nach der Thüringer Hortkostenbeteiligungsverordnung erforderliche Angabe, ob eine Betreuung von mehr oder weniger als 10 Stunden wöchentlich erfolgte, war durch die Eltern zu machen. Der Beschwerdeführerin wurden deshalb die Möglichkeiten aufgezeigt, der Stadtverwaltung entweder mitzuteilen, dass sie keine Angaben machen kann oder aufgrund der

Tatsache, dass ihr genaue Angaben nicht möglich sind, den Höchstbetreuungszeitraum anzugeben. Der TLfDI wies die Beschwerdeführerin darauf hin, dass die gemachten Angaben in keinem Fall Auswirkungen auf ihren Anspruch auf Betreuung des Kindes im Hort haben. Selbstverständlich bestand auch keine Verpflichtung, Angaben zur Ermäßigung der Hortgebühren zu machen, wenn eine Ermäßigung, aus welchen Gründen auch immer, nicht beantragt wird. Auf eine aktuelle Anfrage des TLfDI bei der Stadtverwaltung teilte diese mit, dass nach wie vor das nunmehr zuständige Thüringer Ministerium für Bildung, Jugend und Sport die benötigten Hortzeiten stundengenau im Rahmen des Erprobungsmodells erfragt. Der TLfDI hat die Stadtverwaltung aufgefordert, auf dem Erhebungsbogen die Frage nach der konkreten zeitlichen Inanspruchnahme des Hortes als freiwillig zu kennzeichnen.

In einem Erhebungsbogen zur Anmeldung für einen Betreuungsplatz im Schulhort dürfen nur diejenigen Daten erhoben werden, die für die Aufgabenerledigung des Aufgabenträgers unbedingt erforderlich sind. Sind bestimmte Daten der Antragsteller für den Träger oder wie im beschriebenen Fall für die Durchführung eines Erprobungsmodells erforderlich, ohne dass eine Rechtsgrundlage die Antragsteller hierzu verpflichtet, so müssen die Angaben nicht gemacht werden. Ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, ist der Betroffene hierauf hinzuweisen, wobei aber auch hier keine Auskunftspflicht besteht.

14.7 Schüler unter Beobachtung? – Videogaga 7

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte eine Beschwerde über eine Berufsschule. Die Schule würde die Eingangsbereiche zu ihrem Grundstück und zum Gebäude videoüberwachen. Besonders störte den Beschwerdeführer, dass sich die Zugangsrampe, über die man statt der Treppe das Gebäude erreichen kann, im Aufnahmebereich der Kamera befand. Der TLfDI wandte sich an die Berufsschule und stellte die Fragen, deren Beantwortung zur datenschutzrechtlichen Prüfung der Videoüberwachung notwendig ist. Als die Antwort der verantwortlichen Stelle einging, ergab sich ein weiteres Problem: Der von der Schule verwendete Kopfbogen des Antwortschreibens legte nahe, dass es sich bei der Schule um ein Unternehmen handel-

te, an dem eine Stadt zumindest teilweise beteiligt war. Für das Tätigwerden des TLfDI ist wegen der anzuwendenden Rechtsgrundlagen entscheidend, ob es sich bei der verantwortlichen Stelle um eine öffentliche oder eine nicht-öffentliche Stelle handelt. Nach § 2 Abs. 2 des Thüringer Datenschutzgesetzes (ThürDSG) gelten als öffentliche Stellen auch juristische Personen oder sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine Gemeinde beteiligt ist. Nach § 26 ThürDSG gilt allerdings, dass für den Fall, dass öffentliche Stellen am Wettbewerb teilnehmen, grundsätzlich die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) anzuwenden sind. Der TLfDI ging zunächst davon aus, dass die Schule als Unternehmen zwar Aufgaben der öffentlichen Verwaltung wahrnahm, hierbei aber im Wettbewerb zu anderen Unternehmen stand und auf sie daher die Bestimmungen des BDSG mit Ausnahme des zweiten Abschnitts und des § 38 anzuwenden waren, § 26 ThürDSG. Mit der Einordnung als öffentliche Stelle hat der TLfDI nicht mehr die Handlungsmöglichkeiten des § 38 BDSG, nach dem er Anordnungen treffen und mittels Verwaltungszwang durchsetzen kann. Bei öffentlichen Stellen kann er festgestellte Verstöße gegen das Datenschutzrecht lediglich beanstanden und die zuständige Aufsichtsbehörde informieren. Die Schule äußerte sich bislang nicht zur möglichen Beteiligung der Stadt und wurde nochmals zur Äußerung aufgefordert, da sie trotz Erinnerung nicht reagierte. Der TLfDI wird an die Stadt herantreten, falls die Schule die gestellten Fragen nicht innerhalb der neu gesetzten Frist beantwortet.

Zur Zulässigkeit der Videoüberwachung ist Folgendes festzustellen: Auf dem Gelände der Schule befanden sich drei Kameras. Eine Aufzeichnung fand nur in der Zeit von 16:00 bis 06:30 Uhr und am Wochenende 24-stündig, also außerhalb der Öffnungszeiten, statt. Gegen den Aufnahmebereich einer Kamera bestanden keine datenschutzrechtlichen Bedenken, weil sie lediglich auf den Innenhof der Schule gerichtet war. Bei den anderen beiden Kameras waren aber jeweils Teile der öffentlichen Straße bzw. des Bürgersteigs auf den Aufnahmen zu erkennen. Die Aufzeichnungen hatten einen sehr geringen Auflösungsgrad, weswegen Personen nicht ohne Weiteres eindeutig zu erkennen waren. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Entscheidend ist daher, ob Personen, die sich im Aufnahmebe-

reich der Kamera befinden, zumindest bestimmbar sind. Dies hielt der TLfDI auch bei der geringen Auflösung nicht für grundsätzlich ausgeschlossen. Die Schule wurde daher gebeten, die Kameras so auszurichten, dass die öffentliche Straße nicht mehr aufgezeichnet wird. Sollte dies nicht möglich sein, müsste geprüft werden, ob dieser Bereich bei den Aufnahmen jeweils ausgepixelt werden kann. Sollte die Schule den Forderungen des TLfDI nicht nachkommen, wird er – je nachdem, ob es sich um eine öffentliche oder eine nicht-öffentliche Stelle handelt – den Verstoß entweder beanstanden oder eine Anordnung nach § 38 Abs. 5 Satz 1 BDSG treffen.

Für die Handlungsmöglichkeiten des TLfDI ist es entscheidend, ob eine öffentliche oder eine nicht-öffentliche Stelle für die Datenverarbeitung verantwortlich ist. Für die Beurteilung von Videoaufzeichnungen kommt es bei einem sehr geringen Auflösungsgrad der Aufnahmen darauf an, ob die Personen, die sich im Aufnahmebereich der Kamera befinden, zumindest bestimmbar sind.

14.8 Handreichung zur Schulsozialarbeit

Mit dem Erlass der „Richtlinie über die Gewährung von Zuwendungen an örtliche Träger der öffentlichen Jugendhilfe für Vorhaben der schulbezogenen Jugendsozialarbeit vom 27. Mai 2013“ sind bis August 2015 über 260 Fachkräfte in den 23 Thüringer Landkreisen und kreisfreien Städten eingestellt worden. Für die Umsetzung der in der Richtlinie beschriebenen Ziele ist eine enge Kooperation mit den an der Schule tätigen Personen notwendig. Nach der Richtlinie sollen die individuellen und sozialen Kompetenzen der Kinder und Jugendlichen gefördert werden, soziale Benachteiligungen abgebaut und Lehrkräfte und Personensorgeberechtigte beraten werden. Vor dem Hintergrund eines präventiven Arbeitsansatzes sollte der Austausch zwischen den einzelnen Fachkräften (Lehrkräfte und schulbezogene Jugendsozialarbeiter) reibungslos funktionieren. Dabei ergaben sich jedoch zahlreiche datenschutzrechtliche Fragestellungen.

Da es in der Praxis immer wieder Fragen dazu gab, welche Daten unter welchen Voraussetzungen zwischen Schulsozialarbeitern und an der Schule tätigen Personen ausgetauscht werden dürfen, führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) mehrere Schulungen zu diesem Thema für Schulleiter und Schulsozialarbeiter durch. Dabei ging es beispiels-

weise um die Fragen, welche Daten zwischen Schulsozialarbeitern und an der Schule tätigen Personen ausgetauscht werden dürfen, ob Beratungen von Schülern trotz Verneinung durch die Personensorgeberechtigten durchgeführt werden dürfen oder wie lange Gesprächsakten aufzubewahren sind. Wichtig ist in diesem Zusammenhang vor allem, genau danach zu unterscheiden, wer personenbezogene Daten an wen übermittelt. Je nachdem gelten unterschiedliche Regelungen. Schulsozialarbeit als eine Aufgabe der Jugendhilfe wird ausschließlich nach den Regeln des Sozialgesetzbuches (SGB) erfüllt. Das Thüringer Schulgesetz regelt in § 57 Abs. 4 die Voraussetzungen der Übermittlung von personenbezogenen Daten an Dritte, zu denen auch die Schulsozialarbeiter gehören.

Dem TLfDI ist es aufgrund seiner knappen personellen Kapazität leider nicht möglich, alle von der Richtlinie Betroffenen zu schulen. Da die Inhalte der Schulung aber möglichst allen Betroffenen zur Verfügung stehen sollen, haben sich das Thüringer Ministerium für Bildung, Jugend und Sport als verantwortliches Ministerium sowie die fachliche Begleitung im entsprechenden Landesprogramm, die durch ein privates Unternehmen durchgeführt wird, dazu entschlossen, eine Handreichung zu dem Thema zu entwickeln. Grundlage war die vom TLfDI durchgeführte Schulung. Die Handreichung wurde inhaltlich mit dem TLfDI abgestimmt und wird im kommenden Berichtszeitraum als „Handreichung zum Datenschutz in der Schulsozialarbeit“ veröffentlicht. In diesem Dokument geht es neben den allgemeinen Regelungen und Begriffsklärungen insbesondere um die rechtliche Einordnung der Übermittlung von personenbezogenen Daten zwischen den Lehrkräften und den Schulsozialarbeitern beziehungsweise umgekehrt. Diese Bestimmungen werden in den einzelnen Kapiteln anhand von kleinen Fallbeispielen praktisch dargestellt.

Da für Schulsozialarbeiter das SGB gilt, für Schulen hingegen das Thüringer Schulgesetz, gestaltet sich die Beantwortung der Frage, welche Daten unter welchen Voraussetzungen zwischen Schulsozialarbeitern und an der Schule tätigen Personen ausgetauscht werden dürfen, als nicht ganz einfach. Die Verantwortlichen haben gemeinsam mit dem TLfDI eine „Handreichung zum Datenschutz in der Schulsozialarbeit“ entwickelt, die Erläuterungen anhand von konkreten Fallbeispielen enthält.

14.9 Erhebung von personenbezogenen Daten im Kultusbereich – zur Integration erforderlich

Zur Fünften Verordnung zur Änderung der Thüringer Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich nahm auch der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Anfang des Jahres 2014 Stellung.

Die Thüringer Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich sollte mit Ablauf des 31. Juli 2014 außer Kraft treten. Für Zwecke der Bildungsplanung war von Seiten des ehemaligen Thüringer Ministeriums für Bildung, Wissenschaft und Kultur (TMBWK) die Erhebung der Daten „Geburtsland (Staat); bei nichtdeutschem Geburtsland: Jahr des Zuzugs nach Deutschland; Staatsangehörigkeit; bei überwiegend nichtdeutscher Verkehrssprache in der Familie: Sprache bzw. Sprachengruppe“ über den 31. Juli 2014 hinaus erforderlich, da die erhobenen Daten die Grundlage für Meldungen an die Kultusministerkonferenz und das Statistische Bundesamt bilden würden. Zugleich war eine Ergänzung der bisher fehlenden Merkmale „Geburtsland und Jahr des Zuzugs nach Deutschland bei nichtdeutschem Geburtsland“ sowie „bei überwiegend nichtdeutscher Verkehrssprache in der Familie: Sprache“ entsprechend dem Beschluss der Kultusministerkonferenz zum „Kerndatensatz für schulstatistische Individualdaten der Länder“ notwendig. Bei diesen in Artikel 1 Nr. 1 des Verordnungsentwurfes ergänzten Merkmalen sollte demnach nur eine Lücke geschlossen werden, wie es bei der Mehrheit der Bundesländer bereits geschehen war.

Für den TLfDI war es noch fraglich, aus welchem Grund die Erhebung des Geburtslandes und die Erhebung des Jahres des Zuzugs nach Deutschland bei nichtdeutschem Geburtsland erforderlich seien. Das Ministerium teilte mit, dass im Rahmen der Beurteilung und der Analyse von Lernerfolgen beide Merkmale relevant seien. Aus dem Merkmal „Jahr des Zuzugs nach Deutschland“ könne die Verweildauer im deutschen Schulsystem ermittelt werden. Bei der statistischen Betrachtung, inwieweit das Schulsystem die Schüler zu einem bestimmten Abschluss führen kann, sei es durchaus von Bedeutung, ob bei den Migranten die Schullaufbahn überwiegend in Deutschland oder im Ausland absolviert wurde. Der Lernerfolg sei auch abhängig von der Verweildauer im deutschen Schulsystem. Bei

der genaueren statistischen Analyse der Migrantengruppen gäbe es große Unterschiede in den Lernerfolgen für verschiedene Herkunftsgebiete. Da viele Migranten bereits die deutsche Staatsbürgerschaft besäßen, sei das Merkmal „Geburtsland“ ein Merkmal zur Bestimmung der Unterschiede innerhalb der Migrantenpopulation. Diese Ausführungen sah der TLfDI als plausibel an.

Bei Verfahren zum Erlass bzw. Änderungen von Verordnungen, die datenschutzrechtliche Fragestellungen betreffen, ist auch der TLfDI einzubinden, damit sichergestellt ist, dass auch datenschutzrechtliche Belange hinreichend Berücksichtigung finden.

14.10 Anhörung zum Entwurf der Thüringer Fachschulordnung für die Bildungsgänge im Sozialwesen (ThürFSO-SW)

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Gelegenheit, zu dem in der Überschrift genannten Entwurf Stellung zu nehmen. Gegenüber dem Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) merkte er an, dass in dem Entwurf zwar die beim Antrag auf Aufnahme in die Fachschule einzureichenden Unterlagen im Einzelnen aufgelistet werden, nicht geregelt ist aber, wie mit diesen Unterlagen im Verlauf einer Ablehnung des Bewerbers durch die Fachschule umzugehen ist. Der TLfDI hat vorgeschlagen, in die Vorschrift eine Regelung aufzunehmen, wonach abgelehnte Bewerber die Unterlagen nach Abschluss des Aufnahmeverfahrens zurückerhalten. Ob dieser Vorschlag vom TMBJS berücksichtigt werden wird, ist bislang nicht bekannt, da der Entwurf sich derzeit noch in der Prüfung befindet und danach in den Bildungsausschuss zur Beratung überwiesen wird. Der TLfDI wird den weiteren Verlauf der Angelegenheit beobachten.

Um Irritationen hinsichtlich des weiteren Umgangs mit Antragsunterlagen im Zusammenhang mit dem Aufnahmeverfahren bei einer Fachschule zu vermeiden, sollte zusätzlich geregelt werden, wie mit solchen Unterlagen bei einer Ablehnung des Bewerbers umzugehen ist.

14.11 Kein Muster für Schulleistungsuntersuchungen

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erfolgte auf der Sitzung der Arbeitsgruppe Datenschutz und Schule am 16./17. September 2014 ein Meinungsaustausch über das Thema „Datenschutzrechtliche Prüfung bundeslandübergreifender Schulleistungsuntersuchungen“. Hintergrund hierfür war eine Anfrage des Deutschen Instituts für Internationale pädagogische Forschung bei den Landesbeauftragten für den Datenschutz (LfD), ob man das Verfahren der datenschutzrechtlichen Prüfung von wissenschaftlichen Bildungsforschungsvorhaben durch die LfD der jeweils an der Untersuchung teilnehmenden Bundesländer nicht vereinfachen könnte. So sollten Studienprojekte, die sich regelmäßig wiederholen, nur bei der ersten Genehmigung ausführlich geprüft werden. Als Ergebnis der Erörterung war festzustellen, dass eine abschließende Lösung der Problematik nicht erreicht werden konnte. Es bestehen Bedenken, pauschal dem Muster einer datenschutzrechtlichen Unbedenklichkeitserklärung gegenüber Schulleistungsuntersuchungen zuzustimmen. Dies insbesondere auch wegen der unterschiedlichen Rechtsvorschriften in den Ländern. In einigen Bundesländern, wie etwa auch in Thüringen, teilt der LfD seine datenschutzrechtliche Einschätzung zu einem Verfahren dem verantwortlichen Forschungsinstitut direkt mit, und das zuständige Thüringer Ministerium für Bildung, Jugend und Sport erteilt erst danach dem Institut die Genehmigung zur Durchführung der Untersuchung in den staatlichen Schulen. In anderen Bundesländern führt das jeweilige Kultusministerium die datenschutzrechtliche Prüfung des Verfahrens selbstständig durch und der zuständige LfD wird dann nur bei speziellen datenschutzrechtlichen Problemen beteiligt. Darüber hinaus können bei einzelnen datenschutzrechtlichen Fragestellungen durchaus unterschiedliche Rechtsauffassungen herrschen. Die Bildungsforscher schlugen auch vor, bei sich regelmäßig wiederholenden Projekten nur bei der erstmaligen Vorlage eine ausführliche datenschutzrechtliche Prüfung für die Prüfbehörde durchzuführen und bei nachfolgenden Genehmigungsverfahren geänderte oder neu eingefügte Sachverhalte entsprechend zu markieren, um auf diese Weise das Prüfverfahren abzukürzen. Fraglich ist aber, ob man sich tatsächlich auf solche Markierungen verlassen kann und die Forscher alle

von den LfD als erforderlich angesehenen Änderungen umgesetzt haben.

Schulleistungsuntersuchungen und andere Bildungsforschungsvorhaben, bei denen personenbezogene Schüler-, Eltern- und Lehrerdaten verarbeitet werden, müssen die Anforderungen der jeweiligen Datenschutzgesetze und anderer Rechtsvorschriften über den Datenschutz erfüllen. Für den Bereich der Thüringer Schulen hat der TLfDI gemäß § 37 Thüringer Datenschutzgesetz die Einhaltung dieser Bestimmungen zu kontrollieren.

14.12 Noten gehen nur die Betroffenen etwas an

Ein Schwarzes Brett findet sich in jeder Hochschule. Es birgt manchmal Gefahren für den Datenschutz. Hochschulangehörige baten den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Mitteilung, unter welchen Voraussetzungen der öffentliche Aushang von Prüfungsergebnissen am Schwarzen Brett von Hochschulen und auch die Veröffentlichung solcher Ergebnislisten im Internet unter Nennung der Matrikelnummer sowie der dazugehörigen Note zulässig sind. Die Anfrage wurde zum Anlass genommen, alle Thüringer Hochschulen auf eine datenschutzgerechte Verfahrensweise bei der Veröffentlichung von Prüfungsergebnissen hinzuweisen. Prüfungsergebnisse, die einer konkreten Person zugeordnet werden können, sind personenbezogene Daten, deren Verarbeitung und Nutzung gemäß § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Durchsicht von einigen Hochschulsatzungen ergab, dass die Bekanntgabe von Noten unter Nennung der Matrikelnummer der betroffenen Studierenden dort als anonym bezeichnet wird. Grundsätzlich fallen anonyme Daten nicht mehr in den Anwendungsbereich des ThürDSG. Allerdings ist durchaus fraglich, ob die Matrikelnummer einen Personenbezug für Dritte praktisch tatsächlich ausschließt. Da Matrikelnummern in Verbindung mit den Namen der Studierenden innerhalb der Hochschule und auch außerhalb dieses Bereichs bei vielen Gelegenheiten Verwendung finden, etwa bei der Eintragung von Studierenden für eine Lehrveranstaltung, bei der Beantragung eines Login für einen Computerarbeitsplatz, bei der Beantragung eines Bibliothek-Benutzerkontos, bei der

Bearbeitung von Formularen in den BAföG- und Kindergeldstellen durch die Unterhaltspflichtigen sowie zum Nachweis der Studierendeneigenschaft gegenüber Verkehrsunternehmen, Zeitschriftenabonnements, Krankenversicherungen usw., ist ein Rückschluss auf eine bestimmte Person mit einer bestimmten Wahrscheinlichkeit durchaus möglich. Wenn Prüfungsergebnisse darüber hinaus nicht nur örtlich begrenzt am Schwarzen Brett des jeweiligen Fachbereichs, sondern auch zusätzlich im Internetauftritt der Hochschule, ohne persönliche Zugangsvoraussetzungen, etwa ein Login mit Nutzernamen und Passwort, veröffentlicht werden, so erweitert dies den Übermittlungsbereich (weltweit) beträchtlich. Der TLfDI hat den Hochschulen daher dringend empfohlen, die Studierenden bei der Aufnahme des Studiums darauf hinzuweisen, die Matrikelnummer Dritten gegenüber nicht bekanntzugeben. Weiterhin darf die Matrikelnummer von der Hochschule in keinem Zusammenhang mit personenidentifizierenden Merkmalen der Studierenden veröffentlicht werden. Ebenfalls darf eine Veröffentlichung von Prüfungsergebnissen mit Matrikelnummern im Internet ohne weitere Zugangsvoraussetzung nur dann erfolgen, wenn die Studierenden hierzu ausdrücklich ihre schriftliche Einwilligung erteilt haben. Die Hochschulen sollten Verfahren den Vorzug geben, bei denen z. B. durch Einrichten eines Benutzernamens mit Passwort sichergestellt ist, dass nur der Berechtigte auf seine Prüfungsergebnisse Zugriff hat. Eine datenschutzrechtliche, wenn auch für die Hochschulen aufwendige Verfahrensweise liegt schließlich darin, für jede einzelne Prüfung einmalige, zufällig erzeugte Klausurnummern zu vergeben, die sich die Studierenden merken müssen, um das Prüfungsergebnis später bei der Veröffentlichung zuordnen zu können.

Matrikelnummern sind bei der Angabe in einem Aushang der Hochschule nur dann als ausreichend anonym anzusehen, wenn sie weder von den Studierenden noch von der Hochschule im Zusammenhang mit personenidentifizierenden Merkmalen des Betroffenen veröffentlicht werden. Eine Veröffentlichung von Prüfungsergebnissen unter Nennung der Matrikelnummer im Internet sollte von der Hochschule grundsätzlich nur in Form eines Logins mit Benutzernamen und Passwort erfolgen.

14.13 Tresen-Lösung im Prüfungsamt

In einer Eingabe an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) beschwerte sich ein Student über die Organisation eines Prüfungsamtes der Hochschule. Auf Anfrage des TLfDI nach dem entsprechenden Sachverhalt, teilte die Hochschule mit, dass in diesem Prüfungsamt mehrere tausend Studierende mit ihren Prüfungen verwaltet werden. Man habe sich dort für eine als „Tresen-Lösung“ bezeichnete Organisation entschieden. Hierbei warten mehrere Studierende in einem Raum und werden durch Bedienstete des Prüfungsamtes an jeweils eine der nebeneinanderliegenden Bearbeitungsstellen gerufen, wobei diese lediglich durch einen kleinen Sichtschutz voneinander getrennt sind. Die Hochschule macht geltend, dass aufgrund der Einführung dieser Verfahrensweise die durchschnittlichen Wartezeiten der Studierenden von 90 Minuten auf etwa 10 Minuten reduziert werden konnten. Nach Angaben der Hochschule habe man die Anforderungen des Datenschutzes an die Wahrung der Vertraulichkeit bei einer solchen Lösung berücksichtigt und unter Beteiligung des behördlichen Datenschutzbeauftragten (bDSB) der Hochschule von Anfang an entsprechende Maßnahmen getroffen. Danach ist an der Eingangstür ein deutlich sichtbarer Hinweis angebracht, wonach Studierende, die für das Gespräch mit dem betreffenden Mitarbeiter oder der Mitarbeiterin Vertraulichkeit wünschen, dies zu Beginn des Gesprächs deutlich machen können, woraufhin der Mitarbeiter oder die Mitarbeiterin dann mit dem Studierenden das Gespräch in einem separaten Raum weiterführt. Diese Praxis habe sich bewährt, werde allerdings bislang selten von den Studierenden in Anspruch genommen. Dem beschwerdeführenden Studenten wurde vom TLfDI mitgeteilt, dass die gewählte Verfahrensweise aus datenschutzrechtlicher Sicht angesichts der hohen Zahl an Studierenden und des beschränkten Personal- und Platzangebotes sowie der gegebenen Möglichkeit, bei Bedarf vertrauliche Gespräche führen zu können, als akzeptabel anzusehen ist.

Auch bei der Durchführung von Massenverfahren an einer Hochschule haben die verantwortlichen Stellen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die bestehenden datenschutzrechtlichen Bestimmungen zu gewährleisten.

Hochschulen müssen deshalb den Studierenden eine Möglichkeit einräumen, die Vertraulichkeit des Wortes zu wahren.

14.14 Betrugsverdacht bei Klausur – Einsicht in Smartphoneverläufe zulässig?

In einer anonymen Anfrage wandte sich ein Bürger mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob ein Dozent den Browserverlauf auf dem Smartphone eines Studierenden überprüfen darf. Hintergrund war ein Verdacht des Dozenten, dass der Student während einer Klausur unter Verwendung eines Smartphones einen Betrugsversuch unternommen hatte. Um diesen Verdacht zu widerlegen, forderte der Dozent noch in der laufenden Klausur beim Betroffenen die Herausgabe des Smartphones zur Offenlegung des Browserverlaufs, was der Student unter Verweis auf den Datenschutz ablehnte. Der TLfDI führte gegenüber dem Anfragenden aus, dass die vom Dozenten geforderte Einsicht in den Browserverlauf nur mit Einwilligung des Studenten erfolgen durfte. Da diese Einwilligung vom Betroffenen nicht erteilt wurde, bestand für den Dozenten keine Möglichkeit, den Browserverlauf durchzusehen, denn es gibt keine Befugnisnorm für Dozenten oder Lehrer zur Beschlagnahme und zum Auslesen eines Handys. Gegen den Willen des Betroffenen dürfen daher Inhalte auf Smartphones nicht ausgewertet werden. Im Rahmen der datenschutzrechtlichen Grundsätze von Datenvermeidung und Datensparsamkeit hätte der Dozent auch mit Einwilligung des Betroffenen lediglich Einsicht in den die prüfungsrelevante Zeit betreffenden Teil des Browserverlaufs nehmen dürfen. Welche Konsequenzen sich aber für den Studenten aus der nicht erteilten Einwilligung ergaben, entzog sich der datenschutzrechtlichen Beurteilung. Um solche Konflikte bei der Nachweisführung von Täuschungsversuchen zu verhindern, haben viele Schulen und Hochschulen in ihren Prüfungsordnungen oder schulinternen Ordnungen festgelegt, dass bei förmlichen Prüfungen bereits ein mitgeführtes Handy bzw. Smartphone als Täuschungsversuch gewertet werden kann.

Handys bzw. Smartphones von Studierenden und Schülern dürfen von Lehrkräften nicht ohne Einwilligung des Betroffenen eingesehen werden. Um Konflikte von vornherein auszuschließen, bietet es sich an, in Prüfungsordnungen und internen Schulordnungen zu regeln,

dass zur Prüfung keine eingeschalteten Handys bzw. Smartphones mitgeführt werden dürfen.

14.15 E-Mail zwischen Schule und Schulamt

In einer Eingabe wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, dass zwischen den Schulen und dem zuständigen staatlichen Schulamt regelmäßig personenbezogene Schuldaten im unverschlüsselten E-Mail-Verkehr übermittelt wurden. Es handelte sich um Schülerdaten, etwa sonderpädagogische Gutachten, Aufnahmeanträge von Schülern, Daten der Personalplanung der Lehrer sowie dienstliche Beurteilungen von Lehrkräften. Der TLfDI wandte sich mit dieser Problematik an das damalige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) und wies dort auf die Regelungen des § 9 Thüringer Datenschutzgesetz (ThürDSG) hin, wonach öffentliche Stellen bei der Verarbeitung personenbezogener Daten die erforderlichen technischen und organisatorischen Maßnahmen zu treffen haben, um die datenschutzrechtlichen Bestimmungen zu gewährleisten. Eine Übermittlung personenbezogener Daten mit einer E-Mail kann die Vertraulichkeit und Integrität der übermittelten personenbezogenen Daten nicht gewährleisten. Der E-Mail-Inhalt kann von Dritten mitgelesen oder sogar verändert bzw. verfälscht werden. Daher sind Texte, die personenbezogene Daten enthalten, vom Absender zu verschlüsseln. Die verschlüsselten Texte müssen dann vom Empfänger entschlüsselt, also in den Klartext zurückverwandelt werden. Das TMBWK teilte dem TLfDI in einer Stellungnahme mit, dass für die Übermittlung personenbezogener Daten zwischen den Schulen, Schulämtern und dem Ministerium innerhalb der Verwaltungsplattform Schulwesen (THVPS) ein Austauschserver eingerichtet wurde. Dokumente, die hierüber übermittelt werden, unterliegen einer dreifachen Sicherung des THVPS, nämlich in Form einer PIN, einer Autorisierungskarte und einem eindeutigen Authentifizierungstoken. Wer keinen Zugriff auf das THVPS besitzt, soll die Papierform verwenden. Das TMBWK hatte dem TLfDI zugesagt, bei einer Schulamtsleiterberatung die Problematik zu thematisieren und dort darum zu bitten, dies auch an die Schulleiter weiterzugeben. Der TLfDI teilte dem TMBWK mit, dass aus datenschutzrechtlicher Sicht keine Bedenken gegen die Verwendung des THVPS bestehen und hat angeregt, an die Problematik des

Versands von personenbezogenen Daten per E-Mail regelmäßig in Beratungen mit den Schulamtsleitern zu erinnern.

Personenbezogene Daten dürfen per E-Mail zwischen öffentlichen Stellen, im vorliegenden Fall zwischen Schule und Schulamt, nur übermittelt werden, wenn ein anerkanntes Verschlüsselungsverfahren eingesetzt wird. Andernfalls stellt die unverschlüsselte Übermittlung einen Verstoß gegen die Regelungen des § 9 ThürDSG dar.

14.16 Fakten, Fakten, Fakten: www.youngdata.de – nicht nur für Jugendliche!



Am 10. Februar 2015 wurde im Rahmen einer Veranstaltung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zum Safer Internet Day mit dem Thema „Medienkunde als eigenes Schulfach – Neuland in Sicht?“ per symbolischem Knopfdruck der Startschuss für das gemeinsame Kinder- und

Jugendportal der Datenschutzbeauftragten des Bundes und der Länder <http://www.youngdata.de/> gegeben, wobei der Start der Seite große Resonanz in den Medien fand. Mit diesem Internetauftritt wollen die Datenschutzbeauftragten die Aufmerksamkeit von Kindern und Jugendlichen für die Themen Datenschutz und Datensicherheit stärken und gegen mangelndes Wissen in diesen Bereichen vorgehen. Das Portal bietet dabei aktuelle Datenschutz-Nachrichten, Videos, Cartoons, Quiz und Tipps, wie man seine Daten am besten schützen kann. Die Betreuung der verschiedenen Hauptmenüpunkte haben die Datenschutzbeauftragten der Länder unter sich aufgeteilt. Der TLfDI hat dabei die inhaltliche Pflege und Betreuung der Hauptmenüpunkte „Videoüberwachung“ und „Informationsfreiheit“ übernommen. Unter einem weiteren Hauptmenüpunkt „Was gibt’s in deiner Nähe?“ haben alle Datenschutzbeauftragten die Möglichkeit, auf jeweils eigene Bildungs- und Informationsangebote hinzuweisen. Inzwischen wurde das Portal durch jugendspezifische Angebote zum Thema „Selbstdatenschutz“ unter dem Menüpunkt „Digitale Selbstverteidigung“ erweitert. Hierin werden konkrete Tipps gegeben, was Jugendliche tun können, um ihre Daten besser zu schützen, z. B. in

einem sozialen Netzwerk, bei der Nutzung eines Messenger-Dienstes oder auf dem eigenen Smartphone.

Zutritt zur Seite haben natürlich auch Erwachsene ;-)

Mit <http://www.youngdata.de/> haben die Datenschutzbeauftragten des Bundes und der Länder ein gemeinsames Internetportal geschaffen, das sich besonders an Kinder und Jugendliche richtet und Informationen zum Datenschutz, zur Datensicherheit und zur Informationsfreiheit gibt.

14.17 Hänseleien bei der Bekanntgabe von Schulnoten vor der Klasse

Die Mutter eines 11-jährigen Schulkindes wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und berichtete von einigen Lehrkräften, die bei Schülerinnen und Schülern im Unterricht anfragten, ob diese in die Bekanntgabe ihrer Endjahresnote vor der Klasse einwilligen. Bei dem Schulkind im vorliegenden Fall wurden nach dessen Zustimmung die durchweg sehr guten Noten angesagt. Dies hatte zur Folge, dass das Kind nunmehr den Hänseleien der anderen Schülerinnen und Schüler ausgesetzt war und von diesen auch ausgegrenzt wurde. Die Mutter bat den TLfDI daraufhin um Aufklärung, unter welchen Voraussetzungen Zensuren vor der Klasse mitgeteilt werden dürfen und ob sie aufgrund ihrer Erfahrung die öffentliche Bekanntgabe der Noten ihres Kindes verhindern kann. Der TLfDI legte der Beschwerdeführerin dar, dass es sich bei Schulnoten aus datenschutzrechtlicher Sicht um personenbezogene Daten im Sinne von § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) handelt. Die Bekanntgabe von Schulnoten vor der Klasse stellt eine Übermittlung personenbezogener Daten an Dritte dar und ist somit nach § 3 Abs. 3 ThürDSG eine Verarbeitung personenbezogener Daten. Das Verarbeiten und Nutzen personenbezogener Daten ist gemäß § 4 Abs. 1 ThürDSG nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die spezialgesetzliche Regelung des Thüringer Schulgesetzes (ThürSchulG) führt in § 57 Abs. 4 Nr. 3 aus, dass eine Übermittlung personenbezogener Daten an Dritte nur zulässig ist, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. Darüber hinaus bestimmt § 57 Abs. 1 ThürSchulG, dass das Verarbeiten und Nutzen

personenbezogener Daten der Schüler zur Erfüllung der den Schulen zugewiesenen Aufgaben zulässig ist, soweit dies für den jeweils mit den Aufgaben verbundenen Zweck erforderlich ist. Ob die Bekanntgabe von (Zeugnis-)Noten im Unterricht überhaupt zulässig ist, muss aus pädagogischer Sicht beurteilt werden. Gemäß § 48 Abs. 3 Thür-SchulG ist die Transparenz der Notengebung für Schüler und Eltern zu gewährleisten. Fraglich ist allerdings, ob die Transparenz der Notengebung personenbezogen erfolgen darf oder aber, ob hierfür nicht ein anonymer Notenspiegel diese Aufgabe ausreichend erfüllt. Soweit eine Schule die Notenbekanntgabe vor der Klasse aus pädagogischer Sicht für sinnvoll erachtet, kann dies aus datenschutzrechtlicher Sicht ausschließlich auf der Grundlage einer rechtswirksamen Einwilligung der Betroffenen erfolgen. Voraussetzung für eine wirksame Einwilligung ist, dass der Schüler die Tragweite seiner Entscheidung überblicken kann. Verbindliche Altersgrenzen für die Erteilung einer Einwilligungserklärung gibt es somit nicht. Der TLfDI geht aber davon aus, dass ein 11-jähriges Kind nur in den wenigsten Fällen selbst genügend Einsichtsfähigkeit hat, um eine verbindliche Einwilligungserklärung selbst abgeben zu können. Als grober Anhaltspunkt ist hier je nach vorliegendem Sachverhalt zumindest das 14. Lebensjahr anzusehen. In Zweifelsfällen sollte die Schule daher die Einwilligung der Eltern einholen.

Da die Mutter im vorliegenden Fall die Schule nicht benannte, konnte der TLfDI nicht tätig werden.

Die schulgesetzlichen Bestimmungen enthalten keine Regelung zur Bekanntgabe von Zeugnisnoten vor der Klasse. Wird dies aus pädagogischen Gründen für erforderlich gehalten, ist dies nur auf der Grundlage einer Einwilligung zulässig. Die Erteilung einer rechtswirksamen Einwilligung erfordert eine entsprechende Einsichtsfähigkeit der Schülerinnen und Schüler. Hierfür gibt es keine starre Altersgrenze, in Zweifelsfällen sollte jedoch der Elternwille beachtet und die Eltern um die Einwilligung ersucht werden.

14.18 Lehrkräfte führen privates Girokonto zu Schulzwecken?

Aufgrund der Anfrage eines anderen Landesdatenschutzbeauftragten wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) darüber informiert, dass es in Schulen dort üblich sei, dass Lehrkräfte im Zusammenhang mit der fiskali-

schen Abwicklung von zum Beispiel Klassenfahrten für diese Zwecke ein Privatkonto eröffnen. Hier sind auch datenschutzrechtliche Aspekte berührt, etwa bei der Datenerhebung durch die Banken bei der Kontoeröffnung und einer möglichen Übermittlung personenbezogener Daten an die Schufa oder die Erhebung personenbezogener Daten Dritter, die als zusätzliche Verfügungsberechtigte eingetragen werden. Der TLfDI nahm den geschilderten Sachverhalt zum Anlass, sich an das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) zu wenden und nachzufragen, ob auch in Thüringen Privatkonten von Lehrkräften zu schulischen Zwecken geführt werden. In seiner Antwort wies das TMBJS darauf hin, dass es einen Entwurf einer Verwaltungsvorschrift zur Einrichtung und Führung von Schulkonten erarbeitet hatte, hierzu aber Dissens zur Frage entstand, ob diese Konten in der Inhaberschaft der Schulträger oder aber des Landes Thüringen zu führen seien. Bis zum gegenwärtigen Zeitpunkt konnte keine Klärung erreicht werden, ob die Kontoinhaberschaft für Girokonten der Schulen beim Land oder bei den Schulträgern liegt. Das TMBJS stimmte dem TLfDI zu, dass Kontoinhaberschaften durch Lehrkräfte als Privatpersonen auf keinen Fall vorgesehen sind. Der TLfDI wird weiterhin beobachten, wann eine Verwaltungsvorschrift die Einrichtung und Führung von Schulkonten regelt. Offenbar ist aber in Thüringen kein flächendeckender Handlungsbedarf in der Frage gegeben.

Die Eröffnung und Führung von Privatkonten durch Lehrkräfte zu schulischen Zwecken ist aus datenschutzrechtlicher Sicht bedenklich. Das Land hat dafür Sorge zu tragen, dass bei Zahlungsverkehr für schulische Angelegenheiten keine privaten Konten zum Einsatz kommen.

14.19 Schülerdaten im Netz

Besorgte Eltern berichteten dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) von einer im Internet ohne weitere Zugangsvoraussetzungen zugänglichen Excel-Tabelle, in der die Namen, die Adressen und Telefonnummern aller Schülerinnen und Schüler einer Grundschule sowie die Namen der Elternteile, teilweise mit entsprechenden Hinweisen auf die Sorgeberechtigten, enthalten waren. Der TLfDI wandte sich umgehend an die Schule mit der Forderung, die Seite unverzüglich aus dem Inter-

net zu entfernen. Aus datenschutzrechtlicher Sicht liegt in einer Internetveröffentlichung von Schüler- und Elterndaten eine weltweite Datenübermittlung. Eine solche Übermittlung personenbezogener Daten im Internet ist nur dann zulässig, wenn eine der in § 23 Abs. 2 Thüringer Datenschutzgesetz (ThürDSG) aufgeführten Voraussetzungen vorliegt, was in diesem Fall nicht ersichtlich war. Wie die Schule in ihrer Stellungnahme mitteilte, war die Seite völlig unbeabsichtigt im Thüringer Schulportal veröffentlicht worden. Das Thüringer Schulportal ist eine Arbeitsplattform für den Kultusbereich in Thüringen, die zum Beispiel Schulporträts, Neuigkeiten aus der Bildungslandschaft Thüringen, Unterrichtsmaterialien für Lehrkräfte usw. veröffentlicht. Nach Angaben der Schulleiterin war die eigentliche Absicht, die Klassenlisten für Zwecke des Krisenmanagements nach § 136 Abs. 10 der Thüringer Schulordnung in das Schulportal zu übertragen. Hierbei besteht eine Zugriffsmöglichkeit nur seitens des zuständigen Schulamts. Ein Zugriff ist nur im Falle von Krisen- oder Notfällen zulässig. Aus für die Schulleiterin unerklärlichen Gründen sei ihr bei der Übermittlung an das Portal offenbar ein Fehler unterlaufen. Sie bedauerte den Vorfall und sagte dem TLfDI zu, in Zukunft noch genauer auf korrekte Datenübertragungen von personenbezogenen Daten zu achten. Noch während der Klärung des Sachverhalts konnte der TLfDI feststellen, dass die Schülerliste nicht mehr im Internet öffentlich abrufbar war. Der TLfDI hatte in dem vorliegenden Fall von einer Beanstandung abgesehen, da die Schule den Fehler eingeräumt hatte, der Mangel sofort beseitigt wurde und eine noch sorgfältigere Beachtung der datenschutzrechtlichen Vorschriften versichert wurde.

Die Schule hat bei der Verarbeitung von personenbezogenen Schüler- und Elterndaten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen des ThürDSG zu gewährleisten (§ 9 Abs. 1 ThürDSG). Der TLfDI kann nach § 39 Abs. 4 ThürDSG von einer Beanstandung absehen, insbesondere wenn es sich um inzwischen beseitigte Mängel handelt.

14.20 Soziale Netzwerke in der Ausbildung im Vorbereitungsdienst für die Lehrämter

Das für die Lehrerbildung ehemals zuständige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Prüfung einer Community-Plattform, die ein Seminarschulverbund einführen wollte. Die Plattform sollte als Kommunikationsmedium über das Internet zwischen den Fachleitern und den Lehramtsanwärtern dienen. Hiermit sollte diesem Personenkreis ein Zugang zu Lerninhalten und -angeboten sowie der Austausch von Materialien ermöglicht werden. Der TLfDI teilte im Ergebnis die im TMBWK bereits bestehenden Bedenken gegen die Nutzung der Community-Plattform. Nach wie vor rät der TLfDI von der Nutzung vieler angebotener sozialer Netzwerke zur Aufgabenerfüllung öffentlicher Stellen im Hinblick darauf ab, dass die meisten Anbieter und Betreiber in der USA ansässig sind und nunmehr amtlich ist, dass das Safe-Harbor-Abkommen zum Schutz personenbezogener Daten den datenschutzrechtlichen Anforderungen in der Europäischen Union nicht gerecht geworden ist (vgl. Urteil des EuGH vom 6. Oktober 2015). Im vorliegenden Fall war insbesondere die Nutzung der Online-Plattform über Drittanbieter, z. B. Facebook oder Twitter, kritisch anzusehen. Die Plattform sah eine Verknüpfung mit anderen sozialen Netzwerken in der Form vor, dass man sich auch über diese Drittanbieter in die Plattform einloggen konnte. Somit war nicht auszuschließen, dass zumindest beim Login Daten an das gewählte soziale Netzwerk dieses Drittanbieters übertragen werden. Der Seminarschulverbund schlug deshalb vor, die Nutzung der Plattform auf der Grundlage einer Einwilligung durch die Teilnehmer zu ermöglichen. Da der Einsatz dieses Verfahrens zwar dienstlich nicht vorgeschrieben werden sollte, den Lehramtsanwärtern jedoch nach dem geplanten Konzept mit Einstieg in den Vorbereitungsdienst zur Nutzung als Mittel zur Ausbildung angeboten wurde, hätte die Verantwortung für die datenschutzgerechte Verarbeitung und Nutzung der Daten auf der Community-Plattform allein beim Seminarschulverbund und nicht beim einzelnen Nutzer gelegen. Der TLfDI wies weiter darauf hin, dass der Seminarschulverbund als verantwortliche Stelle mit dem die Online-Plattform anbietenden Unternehmen einen Vertrag über eine Auftragsdatenverarbeitung nach § 8 Thüringer Datenschutzgesetz (ThürDSG)

abschließen müsse. Die verantwortliche Stelle als Auftraggeber hat beim Auftragnehmer die von diesem getroffenen technischen und organisatorischen Maßnahmen zu prüfen. Auch hiernach wäre der Hochschulverbund für die Einhaltung der Bestimmungen des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich geblieben. Nach Kenntnissen des TLfDI wurde der Einsatz der Online-Plattform durch den Seminarschulverbund nicht weiter verfolgt.

Bei der Nutzung einer Online-Plattform eines externen Dienstleisters hat die verantwortliche Stelle zu prüfen, ob dieser die datenschutzrechtlichen Anforderungen erfüllt. Die verantwortliche Stelle muss „Herrin der Daten“ bleiben. Sie muss gegenüber dem Auftragnehmer ein Weisungsrecht hinsichtlich der Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen.

14.21 Weltweite Veröffentlichung von Schülernamen und Abiturprüfungszeiten

In der Eingabe eines Schülers beschwerte dieser sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die Veröffentlichung von Prüfungszeiten für das mündliche Abitur im Internetauftritt einer Schule. Man erhielt auf dieser Seite Einblick in eine Liste, aus der ersichtlich war, welcher Prüfling mit Namen und Vornamen an welchem Tag zu welcher Zeit und in welchem Fach mündlich geprüft wurde. Die weitere Durchsicht der Schulhomepage ergab, dass die Stundenpläne aller Schulklassen unter Nennung des Namens der Klassenlehrer/innen sowie die entsprechenden Klassenfotos eingestellt waren. Weiterhin waren Vertretungspläne abrufbar, in denen unter Angabe der jeweiligen Klasse und des Fachs ersichtlich war, durch welche Lehrkraft ein abwesender Lehrer vertreten wird. Der TLfDI schrieb die Schule an und wies darauf hin, dass eine namensbezogene Veröffentlichung von Prüfungslisten und Vertretungsplänen im Internet eine weltweite Übermittlung personenbezogener Daten darstelle, die nicht zur Aufgabenerfüllung der Schule erforderlich sei. Nach § 57 Abs. 4 Thüringer Schulgesetz (ThürSchulG) ist eine Übermittlung personenbezogener Daten an Dritte nur unter den dort genannten Voraussetzungen zulässig. Eine dieser Voraussetzungen ist die Einwilligung durch die Betroffenen. Da nach § 4 Abs. 1 Satz 2 Thüringer Datenschutzgesetz

(ThürDSG) eine Verarbeitung und Nutzung personenbezogener Daten mit Einwilligung der Betroffenen nur dann zulässig ist, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist, war bereits aus diesem Grund die Zulässigkeit der Datenveröffentlichungen im Internet fraglich. Insbesondere ist die Zulässigkeit einer Veröffentlichung personenbezogener Daten mit Einwilligung durch die Lehrkräfte zweifelhaft, da aufgrund des Beschäftigtenverhältnisses der Lehrkräfte mit der Daten verarbeitenden Stelle ein Abhängigkeitsverhältnis besteht und daher nicht von einer freiwilligen Einwilligung ausgegangen werden kann. Zur Veröffentlichung von Klassenfotos verwies der TLfDI auf § 56 Abs. 1 Satz 6 Thüringer Schulgesetz, wonach die Mitwirkung an Klassenfotos freiwillig ist. Nach § 4 ThürDSG ist eine Verarbeitung und Nutzung der personenbezogenen Daten nur zulässig, wenn der Betroffene (hier Schüler/in) bzw. die Erziehungsberechtigten eingewilligt haben. Die Einwilligung bedarf der Schriftform oder der elektronischen Form mit einer qualifizierten elektronischen Signatur, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 4 Abs. 3 Satz 2 ThürDSG). Die Schulleitung erläuterte, dass eine Veröffentlichung von Prüfungslisten für das mündliche Abitur ein Ausnahmefall wäre, der einer besonderen schulischen Situation geschuldet gewesen sein soll und in vorheriger mündlicher Absprache mit den Schülern erfolgt sei. Die Schule sagte zu, solche Listen zukünftig nicht mehr zu veröffentlichen. Hinsichtlich der Veröffentlichung von Klassen- und Schülerfotos gab die Schule an, jährlich eine Fotoerlaubnis schriftlich bei allen Eltern einzuholen. Bei der Veröffentlichung von Namen der Lehrkräfte im Vertretungsplan sei diese nach einem Schreiben aus dem ehemaligen Thüringer Ministerium für Bildung, Wissenschaft und Kultur vom 21. März 2010 an die staatlichen Schulämter durch Einholung einer rechtswirksamen Einwilligung bei den Lehrkräften zulässig. Den Lehrkräften sei auch das Recht eingeräumt worden, die Einwilligung jederzeit schriftlich zu widerrufen. Die Schulleitung sagte dem TLfDI aber zu, zukünftig auf die Nennung der Nachnamen zu verzichten und nur noch Kürzel zu verwenden. Da der TLfDI bei der Durchsicht des Internetauftritts feststellen musste, dass die Liste der mündlichen Abiturkandidaten noch immer abrufbar war, wurde die Schule erneut aufgefordert, die Seite unverzüglich zu entfernen und dem TLfDI das hierzu Veranlasste mitzuteilen. Dies wurde daraufhin von der Schule erledigt.

Bei der Veröffentlichung personenbezogener Daten auf der Schulhomepage hat die Schule als verantwortliche Stelle vorab zu prüfen, ob dies zulässig ist. Im Regelfall müssen die Betroffenen vor der Veröffentlichung ihrer Daten im Internet von der Schule um eine schriftliche Einwilligung ersucht werden. Bei der Veröffentlichung von Vertretungsplänen dürfen keine Namen der vertretenen oder der vertretenden Lehrkräfte genannt werden. Idealerweise sind auch Kürzel so zu wählen, dass diese für Dritte außerhalb der Schule nicht personenbeziehbar sind.

14.22 Elektronisches Klassenbuch: datenschutzrechtlich nicht ohne

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten einige Anfragen zur Nutzung des elektronischen Klassebuchs in staatlichen Schulen des Freistaats Thüringen. Dabei erfolgten die bisherigen Anfragen nicht seitens der Schulen oder Schulaufsichtsbehörden, sondern von den Schulverwaltungsämtern, also den kommunalen Schulträgern, die unter anderem den für den Schulbetrieb und Unterricht erforderlichen Sachaufwand tragen (§ 3 Abs. 2 Thüringer Gesetz über die Finanzierung der staatlichen Schulen). Hierzu gehört auch die Beschaffung und Finanzierung der in der Schule verwendeten Soft- und Hardware und damit auch die Einführung des elektronischen Klassenbuchs. Hierunter ist eine Software zu verstehen, die die Führung des herkömmlichen Klassenbuchs in Papierform ergänzen oder ersetzen soll. Dabei gehen die Möglichkeiten des elektronischen Klassenbuchs weit über die Funktionen des bisherigen Klassenbuchs hinaus. Es können viel mehr Angaben als bisher erhoben werden.

Welche personenbezogenen Schüler- und Elterndaten zu welchen Zwecken verarbeitet werden dürfen, ist aber in § 136 Abs. 4 und 10 der Thüringer Schulordnung abschließend geregelt. Somit darf die Schule alle anderen Funktionen der Software nicht nutzen und muss diese deaktivieren. Darüber hinaus werden beim elektronischen Klassenbuch die personenbezogenen Daten im Regelfall nicht von der Schule selbst oder einer staatlichen Stelle, sondern bei einem privaten Dritten oder in einer Cloud in Auftragsdatenverarbeitung gemäß § 8 Thüringer Datenschutzgesetz gespeichert. Deshalb muss die Schule bzw. ein staatliches Schulamt eine Vereinbarung über die Verarbeitung der personenbezogenen Daten mit dem Anbieter des

elektronischen Klassenbuchs schließen. Sowohl der Speicherplatz als auch der Übertragungsweg vom Schulrechner auf den Speicher bedürfen einer vorherigen ausführlichen datenschutzrechtlichen Prüfung. Genau diese Problematik war dem Hinweis eines Schulverwaltungsamtes zu entnehmen, wonach dort angedacht war, die Daten in einer Cloud zu speichern und den Lehrkräften der jeweiligen Klasse einen lesenden und schreibenden Zugriff einzurichten. Auch den Eltern der Schülerinnen und Schüler sollte über ein Login ein lesender Zugriff ermöglicht werden, damit sie sich über An- und Abwesenheiten vom Unterricht ihres Kindes, Fehlzeiten, Klassenbucheinträge, Prüfungen etc. auf elektronischem Wege informieren konnten. Das Schulverwaltungsamt gab dabei an, für die datenschutzrechtliche und die datensicherheitstechnische Zulässigkeit des Verfahrens keine Verantwortung tragen zu können. Die Verantwortung für den Umgang mit Schüler-, Lehrer- und Elterndaten zu schulischen Zwecken liege bei der Schule bzw. bei den Schulaufsichtsbehörden. Diese Auffassung teilt der TLfDI bereits seit Längerem und stand hierzu bereits mit dem ehemaligen Thüringer Ministerium für Bildung, Wissenschaft und Kultur in Kontakt. Eine vollständige Klärung des Sachverhalts steht noch aus. Zum konkreten Sachverhalt teilte das zuständige staatliche Schulamt mit, dass es sich lediglich um schulinterne Vorüberlegungen handele und Informationen gesammelt werden sollten. Der TLfDI hatte das Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) gebeten, aufzulisten, wie viele staatliche Schulen in Thüringen ein elektronisches Klassenbuch nutzen. Inzwischen hat das Ministerium eine solche Liste, basierend auf den Rückmeldungen der Schulen, an den TLfDI übersandt. Danach nutzen erst ca. 100 Schulen ein elektronisches Klassenbuch. Die nähere Auswertung der dabei genutzten Systeme muss noch erfolgen. Der TLfDI bleibt in der Sache am Ball und wird die zukünftige Entwicklung verfolgen. Er hat das TMBJS gebeten, alle Schulen auf die Rechtslage hinzuweisen, dass die Funktionen der Software nicht genutzt werden dürfen, die die Anforderungen des § 136 Abs. 4 und 10 der Thüringer Schulordnung nicht erfüllen.

Nicht alles, was das elektronische Klassenbuch kann, darf von der Schule auch genutzt werden. Bei Dateninhalten und Zugriffsregelungen müssen die gesetzlichen Regelungen, die für das herkömmliche Klassenbuch in Papierform gemäß § 136 Abs. 4 und 10 Thüringer Schulordnung gelten, gleichfalls beachtet werden.

14.23 Alte Klassenbücher: Oldies sind datenschutzrechtlich keine Goldies

Aus Anlass des 50-jährigen Schulabschlusses wollten einige der Ehemaligen in den alten Klassenbüchern stöbern, um in geselliger Runde den einen oder anderen Klassenbucheintrag zum Besten zu geben. In diesem Zusammenhang brachte eine Beschwerdeführerin gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ihre Empörung zum Ausdruck, dass einige Schulen sich geweigert hatten, die Einsicht in die mindestens 50 Jahre alten Klassenbücher zuzulassen. Die Bürgerin war der Auffassung, dass so alte Daten in den Klassenbüchern unmöglich noch schützenswert sein können. So sehr der Unterhaltungswert von alten Klassenbucheinträgen nachvollziehbar ist, musste der TLfDI der Beschwerdeführerin mitteilen, dass auch personenbezogene Daten in 50 Jahre alten Klassenbüchern personenbezogene Daten bleiben. Auch in diesen Fällen darf eine Schule nach § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz personenbezogene Daten an Dritte nur dann übermitteln, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Auch das Thüringer Schulgesetz erlaubt in § 57 Abs. 4 Nr. 3 die Übermittlung personenbezogener Daten an Dritte nur, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. Eine Einsichtnahme in diese Klassenbücher wäre demnach lediglich auf der Grundlage einer Einwilligung aller noch lebenden ehemaligen Schülerinnen und Schüler zulässig gewesen. Darüber hinaus war der TLfDI davon überrascht, dass eine Schule noch Klassenbücher aufbewahrte, die vor 50 Jahren ihren Abschluss gefunden hatten. Nach § 136 Abs. 8 Thüringer Schulordnung sind personenbezogene Daten in nicht automatisierten Dateien und Akten nach Maßgabe der hierfür geltenden Bestimmungen aufzubewahren und nach Ablauf der jeweiligen Frist zu vernichten oder zu archivieren. In Thüringen ist nach einem Schreiben des ehemaligen Thüringer Kultusministeriums vom 24. Juni 2014 für Klassenbücher eine Aufbewahrungsfrist von 2 Jahren vorgesehen. Diese sind danach den örtlichen bzw. kreislichen Archiven anzubieten. Da dem TLfDI der Name der Schule nicht bekannt geworden war, konnte er die Schule nicht auf die entsprechende Regelung hinweisen.

Auch auf personenbezogene Daten von Schülerinnen und Schülern in alten Klassenbüchern finden datenschutzrechtliche Regelungen Anwendung. Ohne eine spezielle Rechtsvorschrift, die eine Übermittlung dieser Daten an Dritte erlaubt, kann sich die Zulässigkeit der Übermittlung nur aus einer rechtswirksamen Einwilligung ergeben. Die Schulen sind angehalten, ihren Datenbestand laufend daraufhin zu überprüfen, ob Aufbewahrungsfristen abgelaufen sind und die Unterlagen dem zuständigen Archiv angeboten oder vernichtet werden müssen.

14.24 BAföG21, Dialog21 und Kasse21

Das Bundesausbildungsförderungsgesetz (BAföG) regelt die staatliche Unterstützung für die Ausbildung von Schülern und Studenten. Mit dem Ziel, das Verfahren der Erhebung personenbezogener Daten beim Antragsteller bis zur Prüfung, Berechnung und Auszahlung der Förderleistung zu beschleunigen, hat der Freistaat Thüringen die Verfahren BAföG21, Dialog21 und Kasse21 eingeführt. In den meisten anderen Bundesländern werden diese automatisierten Verfahren ebenfalls genutzt. Es wird seit dem Jahr 2014 in Thüringen eingesetzt. Es handelt sich um eine Modernisierung der vormals bestehenden IT-Verfahren. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat das neue Verfahren aus datenschutzrechtlicher Sicht begleitet und war bereits im Jahr 2009 hiermit beschäftigt. Der Verfahrensgang stellt sich so dar, dass zunächst die Beantragung von Leistungen nach dem BAföG in dem Amt für Ausbildungsförderung bei den kreisfreien Städten und den Landkreisen sowie beim Studentenwerk Thüringen an den Hochschulstandorten erfolgt. Die dort erhobenen Daten des Antragstellers werden dann in einem zentralen Hauptverfahren im Thüringer Landesrechenzentrum im Auftrag des damaligen Thüringer Ministeriums für Bildung, Wissenschaft und Kultur (TMBWK) und jetzigen Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft (TMWWDG) weiterverarbeitet. In diesem Hauptverfahren erfolgen eine Plausibilitätsprüfung, die Berechnung der Förderleistung, die Bescheiderstellung und die Zahlungsanweisung. Der TLfDI prüfte zunächst den Entwurf des für das Verfahren erstellten Sicherheitskonzepts. Der im Ergebnis erforderliche Ergänzung- und Änderungsbedarf wurde vom Thüringer Landesrechenzentrum im Auftrag des TMBWK in das Sicherheitskonzept eingear-

beitet. Die Forderungen in diesem zentral erstellten Sicherheitskonzept müssen von allen beteiligten Thüringer Ämtern für Ausbildungsförderung umgesetzt und das Verfahren von den Ämtern als Daten verarbeitende Stellen nach § 10 Thüringer Datenschutzgesetz (ThürDSG) in das Verfahrensverzeichnis aufgenommen werden. Die Freigabe des Verfahrens nach § 34 Abs. 2 ThürDSG erfolgte für alle Ämter für Ausbildung zentral seitens des TMWWDG, das jedoch keinen Zugriff auf die verarbeiteten Daten der Antragsteller hatte.

Seit dem Jahr 2014 werden die personenbezogenen Daten der Antragsteller und Bezieher von Förderleistungen nach dem BAföG mit den Verfahren BAföG21, Dialog21 und Kasse21 verarbeitet. Nach Prüfung des TLfDI bestehen gegen den Einsatz nach derzeitigen Erkenntnissen keine datenschutzrechtlichen Bedenken.

14.25 Novellierung des Thüringer Gesetzes über Schulen in freier Trägerschaft

Im Rahmen der geplanten Novellierung des Thüringer Gesetzes über Schulen in freier Trägerschaft (ThürSchfTG) bat das damalige Thüringer Ministerium für Bildung, Wissenschaft und Kultur den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Auskunft und Stellungnahme zu einem möglichen Widerspruch zwischen der Regelung des § 5 Abs. 10 Satz 4 ThürSchfTG und der Bestimmung des § 72a Abs. 5 Sozialgesetzbuch (SGB) Achtes Buch (VIII). Konkret stellt sich die Rechtslage so dar, dass nach § 72a Abs. 5 SGB VIII die Träger der öffentlichen und freien Jugendhilfe für die Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine Personen beschäftigen oder vermitteln dürfen, die rechtskräftig wegen einer Straftat im Zusammenhang mit Kindern und Jugendlichen (z. B. Verletzung der Fürsorge- und Erziehungspflichten, sexueller Missbrauch oder Misshandlungen von Kindern und Jugendlichen usw.) verurteilt worden sind. Um dies zu überprüfen, sind die Träger gehalten, sich bei der Einstellung und in regelmäßigen Abständen von diesen Personen ein Führungszeugnis nach § 30 Abs. 5 und § 30a Abs. 1 des Bundeszentralregistergesetzes vorlegen zu lassen. Es handelt sich hierbei um Regelungen zu einem erweiterten Führungszeugnis, welches über Personen erteilt werden kann, die beruflich, ehrenamtlich oder in sonstiger Weise kinder-

oder jugendnah tätig sind oder tätig werden sollen. Der TLfDI bat um eine Änderung der in § 5 Abs. 10 des Entwurfs zur Änderung des ThürSchfTG gewählten Formulierung, da diese nahelegte, dass der private Träger der Schule das erweiterte Führungszeugnis nach der Vorlage durch die Lehrkraft bei sich speichert. Dies war nach Auffassung des TLfDI nicht zulässig und nach der Gesetzesbegründung auch offensichtlich nicht gewollt. Der TLfDI sah darüber hinaus keinen Grund, das erweiterte Führungszeugnis beim Träger auf Dauer aufzubewahren. Es reicht danach völlig aus, wenn in den Akten vermerkt ist, dass das Zeugnis vorgelegt wurde und keine Einträge vorhanden sind. Das am ersten Januar 2016 in Kraft getretene Gesetz hat die Änderungsvorschläge des TLfDI berücksichtigt.

Schulen in privater Trägerschaft müssen sich bei der Einstellung von Lehrkräften ein erweitertes Führungszeugnis vorlegen lassen und die Vorlage sowie die Tatsache, dass keine relevanten Eintragungen hierin enthalten sind, in Akten speichern. Danach ist das Führungszeugnis an die betroffene Lehrkraft zurückzugeben.

14.26 Schule erhebt Gesundheitsdaten

Die Eltern eines Schulkindes beschwerten sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass die Schule eine Liste führte, in der die Namen von erkrankten Kindern und die jeweilige Krankheitsursache eingetragen wurden. Daraufhin wandte sich der TLfDI an die betreffende Schule und forderte diese zu einer Stellungnahme zu dem erhobenen Vorwurf auf. Die Schule verwies in ihrer Antwort auf § 5 Abs. 1 der Thüringer Schulordnung, wonach die Schule über den Grund des Fernbleibens vom Unterricht unverzüglich zu informieren ist. Die Schule legte die Liste bei, in der die Sekretärin entsprechende Krankmeldungen der Eltern fortlaufend mit Datum, Klasse, Name, Vorname sowie Bemerkungen eingetragen hatte. Der TLfDI stimmte insoweit mit der Auffassung der Schule überein, als die Eltern die Schule unverzüglich über den Grund des Fernbleibens ihres Kindes zu unterrichten haben. Hierfür reicht es aber im Regelfall, wenn die Schule lediglich die Information erhält, dass das Kind erkrankt ist. Krankheitsnamen oder Symptome darf die Schule nicht verarbeiten (z. B. speichern) oder nutzen. Ausnahmen sind nur dann denkbar, wenn ein Kind häufig aus Krankheitsgründen im Unterricht fehlt

oder regelmäßig nicht am Sportunterricht teilnimmt. Hier darf die Schule bei den Eltern eine Begründung für die Nichtteilnahme verlangen, um zu entscheiden, ob das von der Schule akzeptiert oder aber die Vorlage eines ärztlichen Zeugnisses verlangt wird. Gemäß § 5 Abs. 2 Thüringer Schulordnung darf die Schule bei einer Erkrankung des Kindes von mehr als zehn Tagen die Vorlage eines ärztlichen Zeugnisses verlangen. Häufen sich die krankheitsbedingten Schulversäumnisse oder bestehen an der Erkrankung Zweifel, kann die Schule die Vorlage eines ärztlichen oder schulärztlichen Zeugnisses verlangen. Darüber hinaus besteht nach §§ 33, 34 Infektionsschutzgesetz (IfSG), z. B. bei Kopflausbefall, für Eltern die Pflicht, die Schule über die Krankheit zu unterrichten (§ 34 Abs. 5 IfSG). Gemäß § 16 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Vermerke über Krankheitsfehltag eines Kindes, vorliegend also die Krankheitsliste, sind daher dann zu löschen, wenn im Zeugnis die entschuldigten und unentschuldigten Fehltage eingetragen wurden. Der TLfDI forderte die Schule auf, grundsätzlich nur die Krankmeldung des Kindes durch die Eltern zu vermerken, keinesfalls aber den Grund der Erkrankung zu speichern. Dies gilt auch dann, wenn die Eltern der Schule freiwillig die Art der Erkrankung mitteilen. Die Schule hat dem TLfDI zugesagt, dies entsprechend umzusetzen.

Schulen dürfen nur speichern, welches Kind aus welcher Klasse wann und für wie lange von den Erziehungsberechtigten krankgemeldet wurde. Eine Speicherung von Krankheitsnamen oder Symptomen in den Schulunterlagen ist im Regelfall nicht zulässig. Im Falle einer Erkrankung des Kindes an einer nach dem Infektionsschutzgesetz meldepflichtigen Krankheit haben die Erziehungsberechtigten dies der Schule mitzuteilen. Die Schulleitung hat „das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen“. Gegen eine allgemeine Information der Eltern über eine in der Einrichtung aufgetretene, meldepflichtige Erkrankung, um auf bestimmte Symptome hinzuweisen, bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

14.27 Schüler an den Pranger gestellt: nichts dazu gelernt!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr durch die Beschwerde eines Schulleiternsprechers von einem Vorfall in der Schule, der sich als ungeheuerlich herausstellte und bei dem das Verhalten der Schulleitung böse Erinnerungen an eine längst überwunden geglaubte Vergangenheit weckte, in deren Mittelpunkt die Erziehung der Jugend zu staatsbürgerlicher Disziplin stand. Danach mussten sich auf Anweisung der Schulleitung in einer fünften Unterrichtsstunde alle anwesenden Schüler und Lehrkräfte vor dem Speisesaal der Schule versammeln. Die Schulleitung verkündete daraufhin den Grund für die kurzfristig einberufene Versammlung und führte dabei drei Punkte auf. Im letzten Punkt wurde die Erteilung eines Schulverweises angekündigt. Nach Schilderung des Elternsprechers hatten im Vorfeld bereits viele Schüler große Angst davor gehabt, ob sie das Kind sein könnten, welches den Schulverweis erhalten wird. Tatsächlich wurde dann ein bestimmter Schüler namentlich aufgerufen, neben die Schulleitung zu treten und erhielt dort vor allen Anwesenden einen strengen Schulverweis unter Benennung des Fehlverhaltens und weiterer möglicher disziplinarischer Schritte. Der TLfDI schrieb daraufhin die Schule an und wies auf die bestehenden datenschutzrechtlichen Regelungen hin. Die Regelungen zum Datenschutzgesetz ergeben sich insbesondere aus § 57 des Thüringer Schulgesetzes (ThürSchulG), der Thüringer Schulordnung sowie für ungeregelte Sachverhalte aus dem Thüringer Datenschutzgesetz (ThürDSG). Die Erteilung eines Verweises an einen Schüler vor der gesamten Schulköfentlichkeit stellt eine Übermittlung personenbezogener Daten an Dritte dar. Eine Übermittlung ist nur unter den in § 57 Abs. 4 ThürSchulG genannten sehr engen Voraussetzungen (rechtliches Interesse eines Dritten, an die Gesundheitsämter zur Durchführung schulärztlicher Untersuchungen, Vorliegen einer rechtswirksamen Einwilligung des Betroffenen) zulässig. Auch nach Auswertung der Stellungnahme der angefragten Schule hatte sich der geschilderte Sachverhalt im Großen und Ganzen bestätigt. Der TLfDI kam zu dem Ergebnis, dass es sich bei der Verfahrensweise um einen erheblichen datenschutzrechtlichen Mangel handelte. Zum einen sollte die Maßnahme nach Schilderung des Beschwerdeführers einen nachhaltigen Eindruck sowohl bei dem betroffenen Schüler als auch bei den übrigen anwesenden Schülern hinterlassen. Zum anderen erfolgte die

öffentliche Erteilung des Verweises nicht aus einem fahrlässigen Versehen heraus, sondern durchaus in der Absicht, die dabei entstandene Prangerwirkung der Situation dafür zu nutzen, ein Exempel zu statuieren und für die anderen Schüler als abschreckendes Beispiel zu dienen. Der TLfDI sprach der Schule eine Beanstandung gemäß § 39 Abs. 1 ThürDSG aus. Wie zu erfahren war, wurde der Vorfall ebenfalls fachaufsichtlich vom zuständigen Staatlichen Schulamt geprüft und der Schulleitung eine dienstliche Rüge erteilt.

Schulen haben vor einer Übermittlung personenbezogener Schüler-, Eltern- und Lehrerdaten die rechtlichen Voraussetzungen für die Zulässigkeit der Übermittlung zu prüfen. Zumindest aus datenschutzrechtlicher Sicht ist eine Übermittlung personenbezogener Schülerdaten an die Schulöffentlichkeit zum Zwecke der Disziplinierung von Schülern grundsätzlich unzulässig. In Zweifelsfällen sollte die Schule sich an den im jeweiligen Schulamt für die Schulen zuständigen Beauftragten für den Datenschutz oder gerne auch an den TLfDI wenden.

14.28 Datenschutzrechtliches O. K. für Schulportal?

Das Medienzentrum Jena bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beurteilung einer konkreten Schulportallösung. Es ist angedacht, das Verfahren als Kommunikationsplattform zwischen den Schülerinnen, Schülern und Lehrkräften in den Schulen der Stadt Jena einzusetzen. Das Schulportal bietet dabei zahlreiche Funktionen zur Nutzung an, etwa Zugriffe auf von der Schule bereitgestellte Informationen und Unterlagen, Unterrichtsmaterialien, Vertretungspläne, Stundenpläne, Aktuelles etc. Weiterhin können Lehrkräfte sowohl von der Schule aber auch von zu Hause aus in Hausaufgaben und andere Arbeitsergebnisse von Schülern Einblick nehmen, diese kommentieren oder bewerten. Die Schülerinnen und Schüler haben die Möglichkeit, bei der Bildung einer Lern- oder Projektgruppe eigene virtuelle Räume mit Chat und Blogfunktion einzurichten. Der TLfDI hatte das Verfahren anhand der vom Medienzentrum Jena vorgelegten Unterlagen einer ersten datenschutzrechtlichen Prüfung unterzogen. Zunächst wurde dabei festgestellt, dass im Gegensatz zu den Angaben des Medienzentrums das Schulportal nicht von einem anderen Landesdatenschutzbeauftragten bereits eine Zustimmung erhalten hatte. Die

weitere Systemprüfung ergab, dass die Datenübertragung auf allen Übertragungswegen mit einer TLS / SSL Verschlüsselung – es handelt sich um ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet – abgesichert werden kann, wozu auch ein eigenes Zertifikat vorhanden ist. Aus technischer Sicht gibt es nur wenige Einwände gegen das System. Die getroffenen technischen und organisatorischen Maßnahmen entsprechen insoweit dem Stand der Technik. Offen ist hier noch, ob Nutzer bei der Rechte- und Passwortübernahme explizit ausgenommen werden können, etwa aufgrund einer fehlenden Einwilligung. Ebenfalls ist ungeklärt, wie das Löschkonzept aussieht, also ob z. B. nach Ausscheiden von Schülerinnen und Schülern eine automatische Löschung des Nutzers erfolgt oder ob dies von den Betroffenen beantragt werden muss und wer die Einhaltung von Löschfristen überwacht. Soweit die Schulen dieses Schulportal einführen wollen, müssen diese mit dem Unternehmen, welches für das Verfahren Dienstleistungen hinsichtlich der IT-Systembetreuung für die Hard- und Software erbringt und bei denen Mitarbeiter des Unternehmens mit personenbezogenen Daten der Schulen in Kontakt kommen können, etwa bei der Wartung, einen Auftragsdatenverarbeitungsvertrag gemäß § 8 Thüringer Datenschutzgesetz (ThürDSG) abschließen. Die Schulen haben auch zu prüfen, ob die schulrechtlichen Voraussetzungen für die Einführung dieses Verfahrens gegeben sind. Das Schulportal bedarf vor der Nutzung gemäß § 34 Abs. 2 ThürDSG zunächst hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung der vorherigen schriftlichen Freigabe durch die Stelle, die nach Absatz 1 den Datenschutz sicherzustellen hat. Dies sind vorliegend die staatlichen Schulämter oder das Thüringer Ministerium für Bildung, Jugend und Sport. Ebenfalls muss das Schulportal zum Verfahrensverzeichnis nach § 10 ThürDSG aufgenommen werden. Zusätzlich ist ein Sicherheitskonzept nach § 9 Abs. 2 Satz 1 ThürDSG zu erstellen und eine Dienstanweisung zur Nutzung des Systems anzufertigen. Darüber hinaus muss von den Schulen beachtet werden, dass in Verfahren die Verschlüsselung mittels HTTPS als Transportverschlüsselung sichergestellt wird. Weiterhin ist die Schule selbst für die Datensicherung der Nutzerdateien zuständig. Außerdem müssen vor der Systemeinrichtung die Nutzungsbedingungen bekannt gemacht und die Einwilligungserklärungen eingeholt werden. Der TLfDI hält eine verpflichtende Teilnahme an dem Schulportal ohne eine schulgesetzliche Ergänzung nicht für zulässig. Das Medienzentrum Jena teilte

dem TLfDI auf der Grundlage seiner datenschutzrechtlichen Prüfung mit, das Projekt weiterzuverfolgen und den TLfDI hierüber zu unterrichten.

Auch wenn ein Schulportal aus datenschutzrechtlicher Sicht grundsätzlich die Ausführung der Bestimmungen des ThürDSG gewährleistet, hat die Schule bei der konkreten Nutzung eines solchen Systems zahlreiche technische und organisatorische Maßnahmen zu treffen, um einen datenschutzgerechten Verfahrensablauf zu gewährleisten.

14.29 Datenunfall bei Schülern? – Prüfung einer Panelstudie

Im Vorfeld einer an mehreren Thüringer Schulen geplanten Panelstudie, also einer Langzeit- und Längsschnittstudie, die über einen Zeitraum von sechs Jahren (5. bis 10. Klassenstufe) angelegt ist, wandte sich ein Forschungsinstitut an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte um datenschutzrechtliche Prüfung des Forschungsvorhabens. Die Zielsetzung der Studie war es, zu untersuchen, aus welchen Gründen es bei Schülerinnen und Schülern zu Unfällen sowie Verletzungen im schulischen Bereich kommt und welche Möglichkeiten der Vorbeugung ergriffen werden können. Die Forscher gingen dabei von der These aus, dass Unfälle sich nicht allein zufällig ereignen, sondern dass auch das familiäre und soziale Umfeld der Jugendlichen einen Einfluss ausübe. Die Datenerhebung erfolgte auf freiwilliger Basis, wobei Schüler und Eltern gebeten wurden, ihre schriftliche Einwilligung zur Teilnahme an der Studie zu erklären. Die Datenerhebung am Befragungstag wurde computergestützt mit Tablet-PCs im Offline-Modus durchgeführt, wobei jedem teilnehmenden Jugendlichen ein Gerät ausgehändigt wurde, auf dem der dort aufgespielte Fragebogen direkt bearbeitet werden sollte. Die Antworten wurden lokal auf den Tablets abgespeichert. Die Jugendlichen mussten bei der Beantwortung der Fragen ihre Namen nicht nennen, jedoch einen individuellen Code generieren. Das Forschungsinstitut bezeichnete die Befragung als faktisch anonym. Aufgrund der Vielzahl der Angaben konnte aber mit Zusatzwissen eine Personenbeziehbarkeit nicht vollständig ausgeschlossen werden. Auf Anfrage des TLfDI, ob und auf welche Weise sichergestellt sei, dass eine Einsicht in die Antworten des befragten Jugendlichen nach

Rückgabe des Tablets durch Dritte verhindert wird, teilte das Forschungsinstitut mit, dass das Anwendungsprogramm keine Möglichkeit zulässt, mit herkömmlichen Anwendungen Zugriff auf die gespeicherten Antworten zu erhalten. Ebenfalls fragte der TLfDI nach, welche Zugriffsrechte auf die Rechner des Instituts bestanden, nachdem die Befragungsergebnisse von den Tablets dorthin zur weiteren Auswertung hochgeladen worden waren. Nach Angaben des Instituts war der Zugriff auf die gespeicherten Daten nur durch die Benutzung persönlicher passwortgeschützter Anmeldezugänge möglich, wobei sich die Rechner in abschließbaren Büros befanden. Der TLfDI informierte das für die Genehmigung zur Durchführung der Studie an den staatlichen Thüringer Schulen zuständige Thüringer Ministerium für Bildung, Jugend und Sport über sein Schreiben an das Institut und erhielt vom Ministerium die Antwort, dass die Befragung genehmigt worden sei. Inzwischen hat das Forschungsinstitut dem TLfDI Unterlagen über die zweite Erhebungswelle der Panelstudie mit der Bitte um erneute Prüfung vorgelegt. Wie sich zeigte, wurden lediglich einige Änderungen im Schülerfragebogen vorgenommen, während die organisatorische und technische Durchführung der Untersuchung praktisch gleich blieb. Der TLfDI hat deshalb gegen die Fortführung der Studie keine Bedenken geäußert.

Auch wenn bei Schulstudien an den staatlichen Schulen des Freistaats Thüringen eine Einwilligung der Erziehungsberechtigten und der Schülerinnen und Schüler vorliegt, dürfen die Studien nur durchgeführt werden, wenn von der verantwortlichen Forschungsstelle die nach § 9 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten.

14.30 Schule – Videogaga 8

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichte im Berichtszeitraum die Anfrage einer Berufsfachschule zu einer geplanten Videoüberwachung im Erdgeschoss ihres Schulgebäudes. Die geplante Videoüberwachung sollte nur außerhalb der Unterrichtszeiten der Berufsfachschule erfolgen. Während des Schulbetriebes sollten das System deaktiviert und die Videokameras für jedermann ersichtlich

auf die Wand ausgerichtet werden. Die Speicherung der erhobenen Daten sollte nicht länger als maximal sieben Tage betragen.

Zunächst stellte der TLfDI fest, dass die Berufsfachschule als Schule in freier Trägerschaft den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes (BDSG) unterliegt. Rechtsgrundlage für den Einsatz von Videoüberwachung in öffentlich zugänglichen Bereichen ist § 6b BDSG, für nicht öffentlich zugängliche Bereiche gilt § 28 BDSG. Außerhalb der Schulzeit ist das Schulgebäude nicht öffentlich zugänglich. Die Videoüberwachung in nicht öffentlich zugänglichen Räumen außerhalb der Schulzeit richtet sich nach § 28 Abs. 1 Nr. 2 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Da außerhalb der Schulzeit die Schule nicht dazu bestimmt ist, von einem unbestimmten Personenkreis betreten und genutzt zu werden, bestand nach Auffassung des TLfDI kein Grund zur Annahme, dass schutzwürdige Interessen von Betroffenen berührt sind. Die Videoüberwachung war daher zu diesen Zeiten grundsätzlich als zulässig anzusehen.

Etwas anderes ergibt sich dann, wenn außerhalb der Schulzeiten Räume oder Flächen der Schule für die Öffentlichkeit freigegeben werden. Hierzu zählen etwa die Aula bei öffentlichen Konzerten oder Feierstunden, eine Sporthalle, die von Vereinen genutzt wird, die Vermietung von Klassenräumen für außerschulische Kurse usw. Auch sollte dabei an eine Reinigungsfirma gedacht werden, die die Schulräume außerhalb der Unterrichtszeiten reinigt und somit bei der Erledigung der Arbeit beobachtet und aufgezeichnet werden würde. Ebenso liegt eine Videoüberwachung von öffentlich zugänglichen Räumen vor, wenn die Beobachtung sich auf weitere Bereiche über die Schule hinaus erstreckt, in denen sich Personen zulässigerweise aufhalten dürfen, z. B. auf öffentlichen Verkehrswegen rund um das Schulgebäude oder innerhalb und außerhalb des Schulgebäudes, wenn diese Bereiche nach dem erkennbaren Willen des Grundstückseigentümers oder des Trägers von jedermann genutzt oder betreten werden dürfen. In den vorgenannten Fällen liegt eine Beobachtung öffentlich zugänglicher Räume vor, die gemäß § 6b Abs. 1 Nr. 2 und 3 BDSG nur zulässig ist, soweit sie zur Wahrnehmung des Haus-

rechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Da in den genannten Beispielen schutzwürdige Interessen von Betroffenen bestehen, darf hier die Videoüberwachung nur erfolgen, wenn z. B. Vorkommnisse nachgewiesen werden (Einbrüche, Vandalismus), aus denen sich eine Erforderlichkeit der Videoüberwachung ergibt.

§ 6b Abs. 2 BDSG verlangt außerdem, dass auf jede Form der Videoüberwachung und auf die verantwortliche Stelle hingewiesen wird. Ausdrücklich vorgesehen ist dies zwar nur für die Videoüberwachung öffentlich zugänglicher Räume. Es empfiehlt sich jedoch auch bei einer Videoüberwachung nicht öffentlich zugänglicher Räume, aus Gründen der Transparenz entsprechende Hinweisschilder oder Piktogramme anzubringen, vgl. § 4 Abs. 3 BDSG.

Die von der Berufsfachschule geplante Löschrfrist von sieben Tagen war nach Auffassung des TLfDI zu lang. Eine Löschung der Aufnahmen sollte regelmäßig nach 48 Stunden erfolgen, es sei denn, es liegen besondere Gründe für eine längere Speicherung vor (Feiertage, Wochenende).

Diese Rechtsauffassung wurde der Berufsfachschule mitgeteilt, die sich daraufhin nicht mehr gemeldet hat.

Eine Videoüberwachung an und in Schulen kann nur ausnahmsweise und grundsätzlich nur außerhalb der Unterrichtszeiten gerechtfertigt sein. Auch dann müssen allerdings die schutzwürdigen Interessen von Personen, die sich zu dieser Zeit zulässigerweise auf dem Schulgelände oder in den Schulgebäuden aufhalten, hinreichend berücksichtigt werden.

14.31 Sicheres soziales Netzwerk für Thüringer Schulen!

In unserer digitalen Welt richten Datensammler wie Datenschützer ihre Augen auf die neuen Kommunikationswege. Sichere Briefpost ist fast out. Ohne E-Mail und Kurznachrichten, ohne Chat und Cloud geht heute praktisch nichts mehr. Auch Lehrer mailen natürlich mit ihren Schülern und deren Eltern, zu ihren Kollegen und Schulleitern, das Bildungsministerium mailt zu Schulämtern, Schulämter zu Schulen, zu Schulverwaltungen usw., usw. Geht es da immer datenschutzgerecht zu? Auf jeden Fall bestehen datenschutzrechtliche

Hürden, wenn die Inhalte solcher Nachrichten personenbezogene Daten enthalten. Und das dürfte bei einem Großteil schulbezogener Mitteilungen der Fall sein. Dass soziale Netzwerke wie Facebook für die Nachrichtenübermittlung in schulischem Kontext keine Rolle spielen dürfen, hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits Mitte 2013 in einer Pressemitteilung öffentlich klargestellt und alle Thüringer Schulen besonders informiert. Das heißt natürlich nicht, dass soziale Netzwerke im Unterricht keine Rolle spielen dürfen. Im Gegenteil: Neue Kommunikationsformen mit ihren Möglichkeiten und Gefahren müssen Thema in zeitgemäßem Unterricht sein.

Aber auch E-Mails sind bekanntermaßen wie Postkarten, die jeder lesen kann, wenn er das notwendige Know-how besitzt, um sie aus dem Netz zu fischen. Abhilfe schafft hier die Ende-zu-Ende-Verschlüsselung, die aber den meisten Lehrern noch immer unbekannt ist oder zu kompliziert erscheint. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bietet deshalb Schulungen zur E-Mailverschlüsselung für Lehrer an (siehe dazu Anlage 86). Ein anderer Ansatz des TLfDI besteht darin, für alle o. g. Personengruppen eine einheitliche, handhabbare Kommunikationsplattform zu empfehlen – einen geschützten Raum, der den gezielten Informationsaustausch ermöglicht, aber die Nachrichten vor fremden Blicken sicher schützt. Dieses Rad muss nicht neu erfunden werden, denn moderne Lernplattformen, die teilweise auch an Thüringer Schulen als „virtuelle Klassen- oder Lehrerzimmer“ genutzt werden, besitzen die notwendigen Funktionen für einen gezielten Nachrichtenaustausch zwischen Einzelpersonen und Personengruppen bereits. Selbstverständlich sind dabei eine verlässliche Nutzerregistrierung und angemessene Rechtevergabe erforderlich, damit die elektronische Post, z. B. mit einer Zeugnisbeurteilung oder einem Sonderpädagogischen Gutachten, keine Abwege gehen kann. Der TLfDI prüft seit Anfang 2015 solche Plattformen mit dem Ziel, dem zuständigen Bildungsministerium konkrete Vorschläge zu unterbreiten, die schul- und datenschutzrechtskonform sind. Ziel ist es, eine datenschutzgerechte Lösung für Thüringer Schulbehörden und alle Schulen in Thüringen zu schaffen, die öffentliche Stellen im Sinne des Thüringer Datenschutzgesetzes sind.

Auf Bundesebene beschäftigt sich derzeit auch der Arbeitskreis Datenschutz und Bildung der Datenschutzbehörden des Bundes und der Länder, dessen Vorsitzender der TLfDI ist, mit dieser Frage.

Nachrichten werden heute in der Regel elektronisch ausgetauscht. Das gilt auch für den dienstlichen Austausch zwischen Lehrern, Schülern, Eltern, Schulbehörden usw. Hier bestehen datenschutzrechtliche Hürden, weil dabei regelmäßig personenbezogene Daten verarbeitet (erhoben, übermittelt, gespeichert) werden. Facebook und andere soziale Netzwerke sind hier tabu. Der TLfDI prüft seit 2015, ob eine geschützte Lernplattform für alle Thüringer Schulen und Schulbehörden eine datenschutzgerechte Alternative sein kann.

14.32 Schweigepflichtentbindung an einer Schule

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Anfrage einer Staatlichen Regelschule aus Thüringen. Sie bat um Überprüfung des Formulars zur Einwilligungserklärung zur Übermittlung personenbezogener Daten der Schüler von den Erziehungsberechtigten an andere Stellen, wie Ärzte, Schulpsychologen, Sozialarbeiter und Ehe-, Familien- und Schwangerschaftsberater. Dabei ging es nicht um die Frage, wer die Einwilligung im Einzelfall zu erteilen hat, die Eltern oder (auch) die Schüler, sondern um den notwendigen Inhalt der Einwilligungserklärung.

Da das Thüringer Schulgesetz keine spezielle Regelung zur Einwilligung des Betroffenen in die Verarbeitung seiner Daten enthält, findet das Thüringer Datenschutzgesetz (ThürDSG) Anwendung. Nach § 4 Abs. 2 ThürDSG ist die Einwilligung eine auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung und der Nutzung zuzustimmen. Wird die Einwilligung beim Betroffenen eingeholt, ist er auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folge der Verweigerung der Einwilligung hinzuweisen, § 4 Abs. 3 ThürDSG. Die Verarbeitung oder das Nutzen von Daten über die Gesundheit ist nur zulässig, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht, § 4 Abs. 5 Nr. 2 ThürDSG.

Aus der Sicht des TLfDI erfüllte die von der Staatlichen Regelschule vorgelegte Form der Einwilligung nicht die gesetzlichen Voraussetzungen. Es handelte sich um eine pauschale Einwilligung, in der

bestimmte Stellen angekreuzt werden konnten. Der Zweck der Datenverarbeitung war sehr allgemein damit bezeichnet, die schulischen Leistungen des Kindes zu fördern und eine soziale Eingliederung zu unterstützen. Sofern ein Arzt von seiner Schweigepflicht entbunden und die datenschutzrechtliche Einwilligung zur Datenverarbeitung gegeben werden sollte, müssten der Arzt sowie der Schulpsychologe oder der Sozialarbeiter konkret namentlich benannt werden. In dem Formular war für den TLfDI nicht eindeutig dargelegt, ob in die Datenerhebung bei dem Arzt, Schulpsychologen und bei den sonstigen genannten Stellen eingewilligt werden sollte oder ob in die Datenübermittlung an diese Stellen eingewilligt wurde. Außerdem gab es entgegen der gesetzlichen Regelung in dem zur Überprüfung vorgelegten Formular keine Angaben zur Dauer der Speicherung sowie keinen Hinweis auf die Rechte der Auskunftserteilung, Berichtigung oder Löschung.

Im Ergebnis empfahl der TLfDI der Staatlichen Regelschule, in den Fällen, in denen eine Datenerhebung bei Dritten zukünftig erforderlich ist, diese Stelle konkret zu benennen und den konkreten Zweck der Erhebung zu bezeichnen. Die möglicherweise zu erhebenden Daten könnten dann, wie es in dem Formblatt bereits angelegt war, jeweils angekreuzt werden. Diese Stellungnahme teilte der TLfDI der Staatlichen Regelschule mit.

Nach § 4 Abs. 2 ThürDSG ist die Einwilligung eine auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung und der Nutzung zuzustimmen. Wird die Einwilligung beim Betroffenen eingeholt, ist er auf den Zweck und den Umfang der Verarbeitung oder Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folge der Verweigerung der Einwilligung hinzuweisen, § 4 Abs. 3 ThürDSG.

14.33 Schulunterricht online

Der unter Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) tagende Unterarbeitskreis Datenschutz und Schule der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat im vorliegenden Berichtszeitraum sehr intensiv an einer gemeinsame Orientierungs-

hilfe für Online-Lernplattformen gearbeitet. Damit wollten die Datenschutzbeauftragten auf die Entwicklung reagieren, dass immer mehr Bildungsinstitutionen und hierunter insbesondere die Schulen auf die internetgestützte Vermittlung von Wissen und den elektronischen Kontakt zwischen Schülern und Lehrern setzen. Für Online-Lernplattformen hat sich inzwischen ein großer Markt gebildet, auf dem Schulbuchverlage sowie Computer- und Softwarehersteller zahlreiche Produkte anbieten. Eine Online-Lernplattform ist ein Softwaresystem, das den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation des Schulstoffes ergänzt oder sogar ersetzt. Der Zugriff auf die Software erfolgt ortsunabhängig mit einem Endgerät (PC, Tablet, Smartphone) über einen Web-Browser (Computerprogramm zur Darstellung von Webseiten im Internet). Die computerbasierte Lernumgebung kann von der Schule auf unterschiedliche Weise gestaltet werden, etwa durch das Einrichten von Kommunikationswegen zwischen Lehrer und Schüler, der Durchführung von Gruppenarbeit, der Erteilung von Aufgaben zur Übung oder zur Lernkontrolle. Grundsätzlich besteht für die Schule die Möglichkeit, eine Online-Lernplattform in Form einer freiwilligen Beteiligung der Schüler oder aber als verpflichtende Teilnahme zu organisieren. In letzterem Fall hat die Schule die faktische Teilnahme der Schüler zu gewährleisten. Aus datenschutzrechtlicher Sicht werden mit dem Verfahren auch viele personenbezogene Schüler- und Lehrerdaten internetbasiert verarbeitet. Aus diesem Grund soll die Orientierungshilfe als Hilfestellung für die Schulverwaltung und die Schulen dienen, welche datenschutzrechtliche Mindestkriterien Online-Lernplattformen erfüllen müssen. Zusätzlich werden den Anbietern von Online-Lernplattformen Kriterien an die Hand geben, wie ihr jeweiliges Produkt gestaltet oder angepasst werden muss, damit eine Nutzung durch die Schulen auf zulässige Weise erfolgen kann. Jeder Schüler muss sich als Zugangsvoraussetzung zunächst im Onlineverfahren auf der Lernplattform anmelden. In aller Regel melden sich die Benutzer einer Plattform personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. Hierdurch entsteht die Gefahr, dass Persönlichkeitsprofile über Schüler und Lehrkräfte erstellt und Informationen ermittelt werden. Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung der Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen den Lehr-

kräften erheblich mehr Daten zur Verfügung, als für die Aufgabewahrnehmung erforderlich ist und sind daher entsprechend anzupassen. Beim Einsatz von Online-Lernplattformen wird Lehrkräften die Möglichkeit eingeräumt, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wann, wie oft und zu welchen Zeiten ein Schüler in der Online-Lernplattform an bestimmten Aufgaben gearbeitet hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Bei der Nutzung von Lernplattformen bleibt die Schule – oder je nach Bundesland die Schulaufsichtsbehörde – verantwortliche Stelle für die Datenverarbeitung und -nutzung. Dies setzt voraus, dass sie die Art und Weise der Datennutzung und -verarbeitung maßgeblich bestimmen kann, also „Herrin der Daten“ bleibt. Bei der Auswahl bzw. Anschaffung einer Online-Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser Anbieter die schuldatenschutzrechtlichen Anforderungen erfüllen kann oder ob die Schule / die Schulaufsichtsbehörde gegebenenfalls ein eigenes Lernportal erstellt. Weiterhin ist das Verfahren nach § 34 Abs. 2 ThürDSG zuvor von der Schulaufsichtsbehörde schriftlich freizugeben und nach § 10 ThürDSG in das Verfahrensverzeichnis aufzunehmen. Schüler, Eltern und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich zu unterrichten. Sie sind darüber aufzuklären, dass sie nach § 10 Abs. 3 Thüringer Datenschutzgesetz berechtigt sind, das Verfahrensverzeichnis der Lernplattform einzusehen. Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht hinzuweisen. Außerdem sind die Lehrkräfte und Administratoren zu schulen und die Schüler zu unterweisen.

Eine endgültige Fassung der Orientierungshilfe konnte erst nach dem Berichtszeitraum fertiggestellt werden. Sie ist unter <https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh-lernplattformen.pdf> veröffentlicht.



Der Einsatz von Online-Lernplattformen in der Schule liegt im Trend. Da mit diesen Verfahren zahlreiche personenbezogene Schü-

ler- und Lehrerdaten verarbeitet und genutzt werden, sind alle erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die datenschutzrechtlichen Bestimmungen zu gewährleisten. Eine Orientierungshilfe „Online-Lernplattformen“ gibt sowohl den Anbietern als auch den Nutzern dieser Systeme wertvolle Hinweise, welche datenschutzrechtlichen Mindestkriterien beim Einsatz zu beachten sind.

14.34 Daten-Wolken auch für Schulen?

Datenwolken wabern überall und sind bereit, ganze Festplatteninhalte in sich aufzusaugen, wenn das der Kunde will. Es ist ja auch ganz vorteilhaft, von jedem Ort der Welt auf seine Daten zugreifen zu können. Das könnte auch für Schulen und Schüler interessant sein, wenn es darum geht, z. B. Unterrichtsvideos und andere datenintensive Inhalte für sich und seine Schüler verfügbar zu haben. Auch für die Schulverwaltung könnten aktuelle, gemeinsam nutzbare Datenbestände hilfreich sein. Aber wie sieht's da mit dem Datenschutz aus? Gibt es Regelungen, ob und wie kommerzielle Cloud-Angebote, wie „Microsoft Office 365“ oder „Google Docs“ durch staatliche Schulen genutzt werden können oder nicht? Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde durch eine Anfrage einer deutschen Universität mit der Frage konfrontiert, ob und wie Cloud-Lösungen an Thüringer Schulen eingesetzt werden. Dem TLfDI war hierzu nichts bekannt. Das für Schulen zuständige Ministerium teilte auf Nachfrage mit, dass es hierzu derzeit keine Richtlinie oder Empfehlungen für Schulen gäbe, weil ein Cloud-Einsatz an Schulen bislang kaum erfolge. Das könne sich aber schnell ändern. Das Bildungsressort regte deshalb an, gemeinsam mit dem TLfDI eine Empfehlung für die datenschutzgerechte Cloud-Nutzung zu erarbeiten, um zu verhindern, dass personenbezogene Daten von Thüringer Schülern, Lehrern und Eltern aus trüben Wolken ausländischer Server irgendwo abregnen. Nach § 9 Thüringer Datenschutzgesetz (ThürDSG) hat die Daten verarbeitende Stelle die technischen und organisatorischen Maßnahmen zu ergreifen, die erforderlich sind, um die bestehenden datenschutzrechtlichen Regelungen einzuhalten. Bei Cloud-Angeboten aus dem außereuropäischen Ausland besteht immer die Frage, ob dort ein angemessenes Datenschutzniveau im Sinne von § 23 Abs. 1 Satz 2 ThürDSG besteht. Nach dem Aus für Safe-Harbor bestehen hier bei

Angeboten aus den Vereinigten Staaten erhebliche Zweifel (siehe dazu Nr. 3.1). Es gilt zu vermeiden, dass die Schule als verantwortliche Stelle Rechtsverstöße begeht. Der sinnvolle Vorschlag des Bildungsministeriums wird derzeit vom TLfDI geprüft.

Die Nutzung internetbasierter Datenspeicher gewinnt allgemein an Bedeutung. Der Trend geht vermutlich auch an Schulen und Schulbehörden nicht vorbei. Um solche Möglichkeiten datenschutzgerecht zu gestalten, bedarf es Vorkehrungen und fundierter Empfehlungen für die Nutzer. Der TLfDI prüft den Vorschlag des Bildungsressorts, gemeinsam eine Empfehlung für die Schulen zu erarbeiten.

14.35 Behördliche Datenschutzbeauftragte an Schulen

Wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits in den letzten zwei Tätigkeitsberichten (9. Tätigkeitsbericht unter Punkt 13.2 und 10. Tätigkeitsbericht unter 13.2) dargestellt hatte, wurde in jedem staatlichen Schulamt jeweils eine dort beschäftigte Person als Beauftragter für den Datenschutz (bDSB) nach § 10a Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) für alle staatlichen Schulen im Zuständigkeitsbereich bestimmt.

Hinsichtlich der in den Schulen eingesetzten Hard- und Software zur Verarbeitung von Schüler-, Eltern- und Lehrerdaten bestand zwischen dem TLfDI und dem ehemaligen Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) weiterhin Uneinigkeit darüber, ob die Schule oder aber der kommunale Schulträger Daten verarbeitende Stelle im Sinne von § 3 Abs. 5 ThürDSG ist. Dies ist aber entscheidend für die Frage, welche Stelle die Verantwortung für die Sicherstellung des Datenschutzes trägt und damit die Verfahren nach § 34 Abs. 2 ThürDSG vor dem erstmaligen Einsatz freizugeben hat. Der Zweck der datenschutzrechtlichen Freigabe liegt in der Vorabkontrolle der Zulässigkeit der automatisierten Verarbeitung personenbezogener Daten. Automatisierte Verfahren dürfen grundsätzlich erst nach der vorherigen schriftlichen Freigabe eingesetzt werden. Weiterhin hat die Daten verarbeitende Stelle gemäß § 10 ThürDSG ein Verzeichnis der automatisierten Verfahren zu führen, mit denen personenbezogene Daten verarbeitet werden. Dies dient der Eigenkontrolle der Behörde und als Grundlage für die Kontrollen des TLfDI. Es dient darüber hinaus der Transparenz der Datenverar-

beutung innerhalb der öffentlichen Stelle. Entsprechend § 10a ThürDSG ist dem Beauftragten für den Datenschutz die Führung des Verzeichnisses und folglich die Zuständigkeit für die Publizität der automatisierten Verfahren als Aufgabe übertragen worden. Zusätzlich hat die Daten verarbeitende Stelle nach § 9 Abs. 2 ThürDSG ein Sicherheitskonzept zu erstellen, auf dessen Grundlage die in der Schule zur Gewährleistung von Datenschutz und Datensicherheit zu treffenden technischen und organisatorischen Maßnahmen ermittelt werden müssen. Eine weitere Zuständigkeitsproblematik ergab sich aus der Wartung, der Ergänzung oder durch den Austausch der in der Schule eingesetzten automatisierten Datenverarbeitungsanlagen, die im Regelfall entweder vom Schulträger selbst oder von einer privaten Stelle vorgenommen werden. Nach der Argumentation des TMBWK finanziert der Schulträger die Infrastruktur der Schule, wozu auch die angeschaffte Hard- und Software gehört, und hat den laufenden Betrieb sicherzustellen. Aufgrund des kommunalen Selbstverwaltungsrechts steht es in eigener Verantwortung des Schulträgers, was er wann auf welche Weise beschafft und wie er den Betrieb sicherstellt, um den schulgesetzlichen Vorgaben gerecht zu werden. Aber bereits aus der gesetzlichen Definition des § 3 Abs. 5 ThürDSG wird deutlich, dass die Daten verarbeitende Stelle Daten in eigener Verantwortung für sich selbst verarbeitet oder nutzt oder dies im Auftrag durch andere vornehmen lässt. Der Schulträger verarbeitet aber keine schulischen Daten der Schüler, Eltern und Lehrer. Hierfür ist ausschließlich die Schule zur Erfüllung ihrer Aufgaben zuständig. Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt gemäß § 8 Abs. 1 ThürDSG der Auftraggeber für die Einhaltung der Bestimmungen dieses Gesetzes verantwortlich. In § 8 Abs. 7 ThürDSG ist ausdrücklich geregelt, dass die Vorschrift auch entsprechend für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen gilt, soweit ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann. Daher ist die Schule als Auftraggeber verpflichtet, mit dem Schulträger als Auftragnehmer eine vertragliche Vereinbarung über die Wartung abzuschließen. Zu den Aufgaben der bDSB gehört es, die Schulen bei der Ausführung des ThürDSG und anderer Rechtsvorschriften über den Datenschutz zu unterstützen und auf deren Einhaltung hinzuwirken. Aus diesem Grund lud der TLfDI die bDSB der staatlichen Schulämter wie ein Jahr zuvor zu einer Gesprächsrunde ein, in der besprochen wurde,

welchen Stand bis dahin die Erstellung der datenschutzrechtlichen Freigaben, Verfahrensverzeichnisse, Sicherheitskonzepte und Verträge über Auftragsdatenverarbeitungen zwischen Schule und Schulträger erreicht hatte. Weitere Themen waren die Frage nach der Verantwortung für den Betrieb einer Schulhomepage, die wahrgenommenen Weiterbildungsmaßnahmen zur Erweiterung der Fachkunde für bDSB und das von den staatlichen Schulämtern zur Verfügung gestellte Zeitkontingent für die Erledigung der Aufgaben des bDSB. Aus den Darlegungen der bDSB konnte der TLfDI entnehmen, dass die Fortschritte bei der Umsetzung der erforderlichen Freigaben und Verfahrensverzeichnisse im Vergleich der staatlichen Schulämter sich voneinander unterschieden, insgesamt aber nur eine sehr geringe Anzahl von automatisierten Schulverwaltungsverfahren bereits freigegeben und in das Verfahrensverzeichnis eingetragen waren. Hinsichtlich der Erstellung eines IT-Sicherheitskonzeptes für die Schulen, musste der TLfDI konstatieren, dass bis dahin für keine Schule ein solches Konzept vorlag. Mit der Problematik der Wartung der automatisierten Datenverarbeitungsanlagen der Schulen durch die kommunalen Schulträger in Auftragsdatenverarbeitung hatten sich die bDSB bis dahin ebenfalls nicht beschäftigt. Aufschlussreich für den TLfDI war der Hinweis einiger bDSB darauf, dass die Beschaffung der Schulsoftware nicht vom Schulträger, sondern teilweise von der Schule selbst wahrgenommen wurde. Allerdings sei es den Schulen untersagt, selbstständig Computer zu beschaffen und mit dem internen Schulcomputernetz zu verbinden. Weiterbildungsmaßnahmen im Bereich des Datenschutzes wurden lediglich von einigen bDSB bereits wahrgenommen. Die Teilnehmer wurden gebeten, mitzuteilen, ob ihnen für die Aufgabe des bDSB der Schulen ein ausreichendes Zeitbudget eingeräumt wurde. Aber auch hier gab es je nach staatlichem Schulamt unterschiedliche Regelungen. Dies war in den staatlichen Schulämtern unterschiedlich ausgestaltet. Die Spanne reichte hier von 20% der Arbeitszeit bis zu 5 % für die Aufgabe des bDSB. Aufgrund der zahlreichen übrigen Arbeitsaufgaben konnten die vom jeweiligen Schulamt eingeräumten Zeitanteile zur Wahrnehmung der Aufgabe des bDSB nicht verwendet werden. Die bDSB waren sich darin einig, dass man als bDSB zunächst mindestens 50 % der gesamten Arbeitszeit benötige. Die Festlegungen der Aufgabe eines bDSB und des eingeräumten Zeitbudgets ergaben sich nach Kenntnis der bDSB zu diesem Zeitpunkt weder aus den Geschäftsordnungen noch aus den Geschäftsverteilungsplänen der

staatlichen Schulämter. Der TLfDI nahm dies zum Anlass, die Geschäftsordnungen und -verteilungspläne bei den staatlichen Schulämtern anzufordern. Den bDSB wurde mitgeteilt, dass diese sich bei Problemen, etwa aufgrund eines nicht ausreichenden Zeitbudgets oder bei mangelnder Unterstützung durch die Behördenleitung, selbstverständlich an den TLfDI wenden können. Um sich ein Bild davon zu machen, welche Schulsoftware von den Schulen in Thüringen verwendet wird, hatte der TLfDI alle kommunalen Schulträger angeschrieben und um Mitteilung gebeten, welche Schulverwaltungssoftware dort jeweils eingesetzt wird. In Auswertung der Rückmeldungen der Schulträger war festzustellen, dass überwiegend an den Thüringer Schulen zwei unterschiedliche Schulverwaltungsprogramme eingesetzt werden, mit denen personenbezogene Schüler- und Eltern Daten verarbeitet werden. Darüber hinaus wird vereinzelt weitere Schulverwaltungssoftware verwendet. Zusätzlich gibt es Teilanwendungen der Schulverwaltung, z. B. Unterrichtsplanung, Abiturverwaltung, Bibliotheksverwaltung, Notenbuch, Klassenbuch usw. Trotzdem gestaltet sich die vollständige Übersicht über die verwendeten Schulverwaltungsprogramme schwierig, da trotz grundsätzlich gleicher Programme diese mit unterschiedlichen Modulen ausgestattet sind, etwa Stundenplan, Zensur, Statistik, Haushalt, Archiv, Vertretungsplan, Datenex- und -import usw. Darüber hinaus enthalten die Programme schulartspezifische Datenbestände, je nachdem, ob das Verfahren in einer Grundschule, Regelschule, in einem Gymnasium, einer Fachschule oder Berufsschule zur Anwendung kommt. Besonderes Interesse des TLfDI weckte die Mitteilung eines Schulträgers, wonach dort nicht bekannt sei, welche Schulverwaltungssoftware eingesetzt werde, da die Schulen die Programme in eigener Verantwortung anschafften. Auch die Wartung der Programme erfolge nicht über den Schulträger. Der TLfDI gab den bDSB in den staatlichen Schulämtern dieses Ergebnis seiner Abfrage bekannt. Für eine lückenlose Erstellung der Freigaben und der Aufnahme in das Verfahrensverzeichnis müssen sich die zuständigen bDSB deshalb teilweise direkt an die Schulen in ihrem Zuständigkeitsbereich wenden. Dies insbesondere deshalb, weil die Schulen entweder das Schulverwaltungsprogramm oder zumindest Zusatzmodule hierzu selbst angeschafft haben und auch nicht bekannt ist, wer die Wartungsarbeiten der Hard- und Software durchführt. Der TLfDI wird die bDSB erneut zu einer Gesprächsrunde einladen und den bis dahin vorliegenden Stand über die erfolgten Freigaben, die

Aufnahme von Schulverwaltungssoftware in das Verzeichnisse, die Erstellung von IT-Sicherheitskonzepten sowie die Vereinbarungen über Auftragsdatenverarbeitung erfragen und für den kommenden Tätigkeitsberichtszeitraum auf die Erledigung der noch offenen Forderungen hinwirken.

Schulen dürfen Schulverwaltungsverfahren, mit denen personenbezogene Daten verarbeitet werden, nur einsetzen, wenn bestimmte formale Voraussetzungen hierfür erfüllt sind. Dies sind insbesondere die vorherige schriftliche Freigabe, das Führen eines Verzeichnisses, das Erstellen eines IT-Sicherheitskonzeptes sowie der Abschluss von vertraglichen Vereinbarungen im Rahmen einer Auftragsverarbeitung. Den bDSB der Schulen ist für die Erledigung ihrer Aufgaben vom Dienstherrn ein ausreichendes Arbeitszeitbudget zur Verfügung zu stellen und die Möglichkeit einzuräumen, sich die notwendige Fachkenntnis anzueignen bzw. diese zu erweitern.

14.36 Veröffentlichung personenbezogener Daten des Promovenden

Ein Bürger fragte beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob personenbezogene Daten des Verfassers einer Promotion im Internet veröffentlicht werden dürfen, obwohl der Betroffene dieser Veröffentlichung widersprochen hat. Da die näheren Umstände der Anfrage dem TLfDI nicht bekannt waren, konnte nur eine allgemeine Auskunft erteilt werden. Grundsätzlich ergibt sich aus den Promotionsordnungen der Thüringer Hochschulen, dass Dissertationen zu veröffentlichen sind. Dies betrifft neben dem Text der Dissertation auch den Namen des Promovierenden bzw. des Promovierten, das Datum der Promotion sowie den Namen der Hochschule, an der die Dissertation erfolgte. Im Regelfall wird die Veröffentlichung von Dissertationen in der Weise geregelt, dass der Promovend eine bestimmte Anzahl von Druckexemplaren im jeweiligen Fachbereich abzugeben hat bzw. die Verbreitung der Arbeit über den Buchhandel nachweisen muss. Weiterhin wird der Doktorand teilweise verpflichtet, das Recht auf Veröffentlichung seiner Dissertation in elektronischer Form in Datenbanken der Hochschule und der Deutschen Bibliothek in Frankfurt am Main und Leipzig einzuräumen. Einige Promotionsordnungen fordern zusätzlich die Abgabe von Pflichtexemplaren an die Hoch-

schule, denen der Promovend einen Lebenslauf beizufügen hat. Aus datenschutzrechtlicher Sicht muss dieser Lebenslauf lediglich über den Bildungsweg Auskunft geben. Gemäß den Promotionsordnungen sind auch die mündlichen Prüfungen öffentlich. Da eine Dissertation grundsätzlich öffentlich zugänglich ist, dürfen aus datenschutzrechtlicher Sicht die Hochschulen Namen und Vornamen sowie das Dissertationsthema im Internet veröffentlichen und das Werk zum Beispiel in der Hochschulbibliothek als Buch oder in elektronischer Form zur Verfügung stellen. Mehr noch, die Dissertation soll einen Beitrag zur Wissenschaft in einem bestimmten Gebiet leisten und der wissenschaftlichen Forschung zur Verfügung stehen. Voraussetzung hierfür ist der freie Zugang zu Dissertationen. Einer weltweiten Verfügbarkeit, also auch in Ländern, in denen kein angemessenes Datenschutzniveau gewährleistet ist, steht nichts entgegen, denn die Veröffentlichung stellt eine Datenübermittlung dar, die nach § 23 Abs. 2 Nr. 4 Thüringer Datenschutzgesetz im öffentlichen Interesse erforderlich ist. Von einem überwiegenden schutzwürdigen Interesse des Betroffenen, dessen personenbezogene Daten, soweit diese die Dissertation betreffen, nicht zu veröffentlichen, ist regelmäßig nicht auszugehen.

Ein Promovend muss davon ausgehen, dass seine Dissertation veröffentlicht wird und somit als allgemein zugängliche Quelle für wissenschaftliche Zwecke genutzt werden darf.

14.37 Sicherheitslücken bei „thoska“

Seit inzwischen 15 Jahren ersetzt die Chipkarte „thoska“ (Thüringer Hochschul- und Studentenwerkkarte) den herkömmlichen Studentenausweis in Papierform. Die Karte vereint mehrere Funktionsweisen, z. B. die Ausweisfunktion zur Sichtprüfung, sie dient als Zugriffs- und Zugangsberechtigungsnachweis, um an speziell eingerichteten Terminals zum Beispiel Ergebnisse von Prüfungsleistungen abrufen zu können. Die Karte hat auch eine Bestell- und Ausleihfunktion für Druckerzeugnisse in der Hochschulbibliothek, über sie kann der Zutritt zu Räumen oder die Durchfahrt zu Parkflächen gewährt werden. Zudem besitzt sie eine Geldbörsenfunktion bei Kopierern, in der Mensa oder beim Bezahlen von Semestergebühren. Außerdem dient sie Bediensteten der Hochschule als Zeiterfassungssystem. Presseberichten war zu entnehmen, dass die bisher teilweise

noch verwendete ältere Version der Hochschulchipkarte (Mifare Classic) von Hackern geknackt worden sei, sodass ein Missbrauch dieser Karte nicht auszuschließen ist. Die Karte konnte ausgelesen und anschließend geklont werden. Mit diesen Kopien könnten z. B. auf dem Kartenchip Geldbeträge erzeugt werden, mit denen dann in den Mensen der Studentenwerke oder an Kopierern bezahlt werden könnte. Aus datenschutzrechtlicher Sicht bedeutsam ist insbesondere die Möglichkeit der Überwindung von Türöffnungssystemen, der Identitätserschleichung beim Ausleihen von Büchern aus den Hochschulbibliotheken und der mögliche Zugriff auf Prüfungsergebnisse sowie auf weitere personenbezogene Daten, die auf der Karte gespeichert sind. Weiterhin kann die Chipkarte, da diese mit RFID-Technologie kontaktlos in einer Distanz von bis zu zehn Zentimetern arbeitet, durch ein Portemonnaie oder eine Tasche hindurch ausgelesen werden. Auf diese Weise ist es möglich, die Identität einer Person festzustellen.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) schrieb daher die Hochschulen des Landes an und forderte diese auf, alle „thoska“-Chipkarten, die mit der veralteten Technik arbeiten, sofort auszusondern und durch neue Karten mit einer sicheren Technik zu ersetzen sowie die alten Karten zur Vermeidung von Missbrauch einzuziehen. Die Hochschulen haben sich nun für eine Karte entschieden, die mit einem weiterentwickelten Chip ausgestattet ist (Mifare DESFire), der mit aktuellen Kryptoalgorithmen wie zum Beispiel 2KDES, 3KDES oder AES128 arbeitet. Die 3DES beziehungsweise „Triple-DES“-Verschlüsselung ist dabei wesentlich sicherer, als die ursprünglich verwendete Authentifizierung über Schlüsselabgleich. Die neuen Karten sind sowohl hinsichtlich der Funktionalität als auch der Vertrauenswürdigkeit des technischen Systems nach einem internationalen Standard zertifiziert worden (Common Criteria EAL 4+). Aufgrund der Rückmeldungen der Hochschulen an den TLfDI kann die Aussage getroffen werden, dass bis Ende 2015 alle Hochschulen, die mit „thoska“ arbeiten, die alten Karten eingezogen und durch neue ersetzt haben. Dies gilt sowohl für die Studenten- als auch die Mitarbeiterkarten.

Beim Einsatz von auf RFID-Technologie basierenden Chipkarten der Thüringer Hochschulen ist der jeweilige Stand der Technik zu be-

achten, um den Schutz von personenbezogenen Daten der Hochschulangehörigen zu gewährleisten.

14.38 Prüfungsamt mit medizinischen Fähigkeiten?

In einer Kleinen Anfrage wandte sich ein Abgeordneter an die Landesregierung, weil Studierende dazu verpflichtet sind, gegenüber den Prüfungsausschüssen der Hochschulen zur Feststellung der Prüfungsunfähigkeit ihre krankheitsbedingten Beschwerden offenzulegen. Der Abgeordnete wandte sich zu dieser Problematik auch an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Darüber hinaus beschwerten sich einige Studierende über diese Verfahrensweise in ihrer Hochschule beim TLfDI. Aus datenschutzrechtlicher Sicht stellt sich die Sachlage so dar, dass das Thüringer Hochschulgesetz (ThürHG) zur Feststellung einer Prüfungsunfähigkeit an den Thüringer Hochschulen keine eigenen Regelungen enthält, sondern die Hochschulen nach § 49 Abs. 1 ThürHG fachübergreifende Bestimmungen für das Prüfungsverfahren (Rahmenprüfungsordnung) erlassen können. Der TLfDI schrieb daraufhin alle Thüringer Hochschulen an und bat um eine Darstellung des jeweils dort festgelegten Verfahrens zur Feststellung einer Prüfungsunfähigkeit. Die eingegangenen Antworten zeigten ein uneinheitliches Bild. Einigen Hochschulen reicht es zur Nachweisführung aus, wenn der Arzt auf einem von der Hochschule herausgegebenen Vordruck die Prüfungsunfähigkeit des Studierenden erklärt, während andere Hochschulen erheblich mehr Daten zum Gesundheitszustand des Prüfungskandidaten beim behandelnden Arzt erheben, etwa zur Einschätzung des Leistungsvermögens, zu den bestehenden Krankheitssymptomen bzw. der Art der Leistungsminderung sowie – als freiwillig gekennzeichnet – die Bezeichnung der Krankheit.

Gegen Verfahren derjenigen Hochschulen, die lediglich ein ärztliches Attest von Prüflingen verlangen, in dem der Arzt feststellt, dass der Prüfling wegen gesundheitlicher Beeinträchtigungen nicht an einer Prüfung teilnehmen kann, hat der TLfDI keine Bedenken. Bei den anderen Hochschulen, die vom behandelnden Arzt zusätzlich eine Beschreibung der gesundheitlichen Beeinträchtigungen verlangen, ist die Erforderlichkeit und Verhältnismäßigkeit dieser Datenerhebung von Krankheitsauswirkungen aus datenschutzrechtlicher Sicht nicht unmittelbar erkennbar. Die Hochschulen begründen die

Erforderlichkeit mit der Aufgabe der Prüfungsausschüsse, selbstständig über den Antrag in eigener Verantwortung darüber entscheiden zu müssen, ob im konkreten Fall eine Prüfungsunfähigkeit vorliegt. Darüber hinaus wurde auf einen Beschluss des Bundesverwaltungsgerichts vom 6. August 1996, Az.: 6 B 17.96 verwiesen. Darin stellte das Gericht hinsichtlich der Nachweisführung einer Prüfungsunfähigkeit in der ersten Juristischen Staatsprüfung fest, dass nicht der Arzt, sondern das Landesjustizprüfungsamt entscheidet, ob die nachgewiesenen Gründe es rechtfertigen, dass der Prüfling verhindert ist. Es gibt also eine höchstrichterliche Entscheidung darüber, welche formalen und inhaltlichen Anforderungen von der Prüfungsverwaltung an ein ärztliches Attest gestellt werden dürfen. Wenn eine Hochschule eine Satzung erlassen hat, in der bestimmt wird, in welcher Weise die Studierenden eine Prüfungsunfähigkeit gegenüber dem Prüfungsausschuss nachweisen müssen und sich der Umfang der verlangten gesundheitlichen Informationen in einem durch das oben genannte Urteil erforderlichen Datenumfang hält, so ist dieses zunächst auch aus datenschutzrechtlicher Sicht nicht zu beanstanden. Gegen Datenerhebungen, die im Umfang über den unbedingt erforderlichen Datenrahmen hinausgehen, wird der TLfDI aber von seiner Prüfkompetenz gegenüber den Hochschulen Gebrauch machen. In einer Hochschule wird das Verfahren zur Feststellung der Prüfungsunfähigkeit zurzeit einer Neubewertung unterzogen. Dies erfolgt in Abstimmung mit dem rechtsaufsichtlich zuständigen Ministerium für Wirtschaft, Wissenschaft und digitale Gesellschaft. Der TLfDI hat das Ministerium gebeten, ihn in das Verfahren mit einzubinden. Ergebnisse zum Verfahrensstand sind dem TLfDI noch nicht bekannt.

Zum Nachweis einer Prüfungsunfähigkeit sollte es den Hochschulen grundsätzlich genügen, wenn der Betroffene dem Prüfungsamt ein Attest vorlegt, in dem sein behandelnder Arzt die Prüfungsunfähigkeit bestätigt.

14.39 Erhebung von Täternamen bei sexueller Gewalt?

Im März 2010 hat das Bundeskabinett die Einrichtung des Runden Tisches „Sexueller Kindesmissbrauch in Abhängigkeits- und Machtverhältnissen in privaten und öffentlichen Einrichtungen und im familiären Bereich“ beschlossen. Die Mitglieder des Runden Tisches

hatten im November 2011 ihren Abschlussbericht verabschiedet. In diesem wurde unter anderem die Einrichtung eines Ergänzenden Hilfesystems (EHS) für diejenigen empfohlen, die in ihrer Kindheit bzw. Jugend sexuellen Missbrauch in der Familie oder in Institutionen erlitten haben und noch heute an diesen Folgewirkungen leiden. Der Bund stellte für den familiären Bereich 50 Mio. Euro bereit. Daher gibt es seit dem 1. Mai 2013 den „Fonds Sexueller Missbrauch im familiären Bereich“. Aus Mitteln des Fonds können Betroffene Sachleistungen bis zum 30. April 2016 beantragen. Hierfür entwickelte der Bund ein einheitliches Antragsformular. Die Geschäftsstelle des „Fonds Sexueller Missbrauch im familiären Bereich“ übernimmt die Entgegennahme sämtlicher Anträge und leitet diese an das zuständige Land weiter, wenn Gegenstand des Antrages ein Missbrauch in einer Institution des Landes ist. In diesem institutionellen Bereich übernehmen die Länder ihre Arbeitgeberverantwortlichkeit für Missbrauchsfälle, die durch Beschäftigte des Landes und der Kommunen zu verantworten sind.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ging davon aus, dass es im Verfahren für die Prüfung der Arbeitgeberverantwortung in der Vielzahl der Fälle notwendig sein würde, Informationen über den Täter zu erlangen. Dies ist aus Sicht des TLfDI aber nicht ohne Weiteres zulässig. Die zu erhebenden Daten sind sehr sensibel und nicht alle Betroffenen möchten wegen der damit verbundenen Folgen (z. B. der Notwendigkeit einer Aussage als Zeuge) den Täternamen benennen. Nach einer ersten Einschätzung des TLfDI kann eine Datenerhebung ausschließlich im Wege der Einwilligung der Betroffenen erfolgen. Es ist nicht erkennbar, dass die Datenerhebung des Täternamens für die Erfüllung der Aufgabe des EHS erforderlich ist. Diese besteht darin, „noch andauernde Belastungen als Folgewirkungen des Missbrauchs auszugleichen bzw. zu mildern“, nicht aber in der Ermittlung und gegebenenfalls Sanktionierung der Täter.

An die Bestimmtheit einer derartigen Einwilligungserklärung und die Darstellung der mit der Datenverarbeitung verfolgten Zwecke sind besonders hohe Anforderungen zu stellen. In jedem Einzelfall ist eine strenge Erforderlichkeitsprüfung notwendig. Der TLfDI setzte sich Anfang des Jahres 2015 mit dem zuständigen Ressort in Verbindung, um zu erfahren, in welcher Weise eine Umsetzung des EHS für den institutionellen Bereich im Freistaat Thüringen erfolgen und wie das Verfahren der Prüfung der Arbeitgeberverantwortung

ausgestaltet werden soll. Dem Thüringer Ministerium für Bildung, Jugend und Sport (TMBJS) wurde mehrmals Fristverlängerung gewährt. Dieses teilte noch im Mai 2015 mit, zwischen den Ländern habe sich Diskussionsbedarf entwickelt und die notwendigen Beschlüsse und Vereinbarungen lägen noch nicht vollständig vor. Es war nicht in Erfahrung zu bringen, bis wann mit einer Antwort auf die vom TLfDI gestellten Fragen zu rechnen ist. Nach § 38 Abs. 1 Nr. 1 ThürDSG sind der Landesbeauftragte für den Datenschutz und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis insbesondere Auskunft zu ihren Fragen zu gewähren. Unter Hinweis auf diese Unterstützungspflicht aller öffentlichen Stellen in Thüringen gegenüber dem TLfDI wandte sich dieser an die zuständige Abteilung des TMBJS. Bis zum Ende des Berichtszeitraums ging beim TLfDI keine Antwort ein. Der TLfDI wird die Angelegenheit weiterverfolgen und eine Beanstandung wegen mangelnder Unterstützung des TLfDI androhen. Über den Ausgang des Verfahrens wird im nächsten Tätigkeitsbericht informiert werden.

Nach § 38 Abs. 1 Nr. 1 ThürDSG sind der Landesbeauftragte für den Datenschutz und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Die Erfüllung der Beantwortungspflicht erleichtert dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit die Wahrnehmung seiner Kontrollaufgabe. Nur wenn er alle notwendigen Informationen enthält, kann er die Einhaltung datenschutzrechtlicher Vorgaben prüfen.

14.40 Lehrer-Apps: kritisch

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat in seiner Eigenschaft als Vorsitzender der Unterarbeitsgruppe des Arbeitskreises Datenschutz und Bildung der Datenschutzbeauftragten das Thema des Einsatzes von Apps auf privaten IT-Systemen von Lehrern aufgegriffen und erstellt zurzeit gemeinsam mit anderen Landesdatenschutzbeauftragten in dieser Arbeitsgruppe ein Informationsblatt, welches sich an Schulleiter und Lehrkräfte richtet und die einschlägigen datenschutzrechtlichen Vorschriften darstellen sowie die erforderlichen technischen und organi-

satorischen Maßnahmen erläutern soll, die von den Lehrkräften zu ergreifen sind, um Schüler-, Eltern- und Lehrerdaten zulässigerweise mit Mobilgeräten verarbeiten und nutzen zu können. Im Rahmen der weiten Verbreitung von mobilen Datenverarbeitungsgeräten, wie Smartphones, Tablets und Notebooks, besteht bei den Lehrkräften das Bedürfnis, diese in erster Linie für die private Nutzung vorgesehenen Geräte auch für ihre dienstliche Arbeit einzusetzen. Der Einsatz von im privaten Besitz befindlichen Geräten zu dienstlichen Zwecken wird auch als „bring your own device“ (BYOD) bezeichnet. In Thüringen gibt es, wie in den meisten anderen Bundesländern, bislang noch keine Vorschriften, die speziell die dienstliche Nutzung von privaten, mobilen Endgeräten regeln. Da die vorhandenen Thüringer Vorschriften zur Verarbeitung personenbezogener Daten von Schülern auf privaten Rechnern der Lehrkräfte bereits vor 15 Jahren erstellt wurden, beziehen sich diese ausschließlich auf die Verwendung des heimischen stationären PC. Es ist davon auszugehen, dass trotz fehlender rechtlicher Voraussetzungen die dienstliche Nutzung von mobilen Endgeräten durch Lehrkräfte durchaus verbreitet ist oder zumindest ins Auge gefasst wird. Die Privatwirtschaft stellt für die dienstlichen Bedürfnisse der Lehrerinnen und Lehrer eine immer mehr anwachsende Zahl von „Lehrer-Apps“ (App ist die Abkürzung für das englische „Application“ und meint eine Anwendersoftware) zur Verfügung, die das bisherige „Notenbüchlein“ oder den Terminkalender in Papierform ersetzen. Die Funktionalitäten und Verwendungsmöglichkeiten gehen dabei weit über die bisherige analoge Verarbeitung und Nutzung von personenbezogenen Schüler-, Eltern- und Lehrerdaten hinaus. Neben der Leistungsfähigkeit der Apps haben Mobilgeräte auch den Vorteil, diese ständig mit sich führen zu können und unabhängig von einem festen Arbeitsplatz Schülerdaten verarbeiten und nutzen zu können. Allerdings ergeben sich aus den genannten Vorteilen von Mobilgeräten auch zahlreiche datenschutzrechtlich relevante Sicherheitsprobleme. Dies fängt an bei der Gefahr, die kompakten und ständig im mobilen Gebrauch befindlichen Geräte zu verlieren und geht über nicht genutzte Sicherheitseinstellungen, ungeprüft installierte Apps bis hin zur unkritischen Verwendung des Gerätes in der Öffentlichkeit. Der TLfDI wird nach der Fertigstellung des Informationsblatts dieses den Lehrkräften über die Schulen zukommen lassen.

Die Verwendung von privaten mobilen Geräten durch Lehrkräfte zu schulischen Zwecken ist aus datenschutzrechtlicher Sicht kritisch zu sehen und erfordert das Ergreifen zahlreicher technischer und organisatorischer Maßnahmen, um die datenschutzrechtlichen Bestimmungen zu gewährleisten. Mit einem hierfür erarbeiteten Informationsblatt wird der TLfDI die Lehrerschaft auf die bestehenden Gefahren hinweisen und Lösungsmöglichkeiten beschreiben.



Online Security Technology © GKSD / Fotolia.com

15 Entwicklungen der automatischen Datenverarbeitung

15.1 Verschlüsselung mit TrueCrypt

Lange galt TrueCrypt als sicheres Programm zum Verschlüsseln von Daten auf der Festplatte, auf Datenträgern oder aber auch zum Verschlüsseln der Daten vor einer Datenübermittlung. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl dieses Programm. Doch die Weiterentwicklung dieses Programms wurde durch die Entwickler Ende Mai 2014 eingestellt, sodass nunmehr keine Empfehlung seitens des BSI mehr erfolgt.

Da einige Programmteile von TrueCrypt auch in anderen Programmen verwendet werden, hatte das BSI das Fraunhofer-Institut für sichere Informationstechnologie (SIT) mit der Durchführung einer Sicherheitsanalyse von TrueCrypt in der Version 7.1a beauftragt. Das Ergebnis dieser Sicherheitsanalyse wurde vom BSI im November 2015 unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Truecrypt/Truecrypt.pdf?__blob=publicationFile&v=2 veröffentlicht.



In der Studie wird u. a. festgestellt, dass TrueCrypt nur dann noch einen wirksamen Schutz entfaltet, wenn das Gerät, auf dem die Daten gespeichert sind, sich im ausgeschalteten Modus befinden. Dies ist bspw. bei Verlust des USB-Sticks oder Laptops der Fall.

Die Studie kommt zum Schluss, dass in den anderen Fällen, also bspw. im Online-Modus, kein sicherer Schutz mehr besteht. Grund dafür ist, dass der Einsatz eines heimlich installierten Key-Logger-Programms, also eines Programms, welches die Eingabe an der Tastatur mitschneidet, den Schutz unterlaufen könnte. Ebenso kann andere installierte Schadsoftware den Schutz von TrueCrypt unterlaufen.

Was bedeutet dies nun für die Anwender? Wieso wird hier auf einmal die Gefahr des Key-Loggers problematisiert und bei anderen sicherheitsrelevanten Prozessen bewusst ausgeblendet?

Die Datenschutzbeauftragten des Bundes und der Länder haben beispielsweise bei der Einführung des elektronisch lesbaren Personalausweises die unsicheren Lesegeräte ohne eigenständige Tastatur genau aus diesem Grund kritisiert und vor Key-Loggern gewarnt. Weder die Bundesregierung noch das BSI änderten daraufhin das Verfahren dahingehend, dass nur Lesegeräte mit eigener Tastatur zugelassen werden.

Auch darf der Bürger sich fragen, wenn er die von der Bundesregierung favorisierte De-Mail benutzt (siehe Nummer 5.51), ob diese vor einem Key-Logger geschützt ist. Diesbezügliche Aussagen sind für den Bürger derzeit nicht zu finden.

Welche Alternative schlägt nun das BSI hinsichtlich TrueCrypt vor? Muss man gänzlich auf TrueCrypt verzichten? Aus datenschutzrechtlicher Sicht ergibt sich aus der vorliegenden Sicherheitsanalyse, dass TrueCrypt durchaus weiter Anwendung finden kann, wenn die Daten auf einem Gerät nur bei Verlust oder Diebstahl des Gerätes vor unberechtigtem Zugriff gesichert werden sollen. Auch für ausgelagerte Datensicherungen scheint es gemäß der oben zitierten Studie des Fraunhofer-Instituts weiterhin geeignet. Nur für den Zugriff auf Daten in laufenden Systemen kann die Verschlüsselung allein keinen ausreichenden Schutz gewährleisten.

Man muss also vor dem Einsatz immer schauen, welche Empfehlungen derzeit das BSI

ausspricht

(https://www.bsi.bund.de/DE/Home/home_no



de.html). Wichtig ist, dass man immer dem Stand der Technik entsprechende Verschlüsselungssoftware einsetzt, um nicht fahrlässig zu handeln.

Verschlüsselungssoftware ist immer entsprechend dem aktuellen Stand der Technik einzusetzen. Daher sollte man sich regelmäßig beim Bundesamt für Sicherheit in der Informationstechnik (BSI) informieren.

15.2 Ein Schritt vor, zwei zurück – ist die Verschlüsselung politisch wirklich gewollt?

Durch die zunehmende digitale Vernetzung und die Erkenntnis, dass Sicherheitsbehörden heimlich Daten abgreifen und die Wirtschaftsspionage zunimmt, gewinnt die Verschlüsselung von Daten bei der Datenübermittlung und Datenspeicherung verstärkt an Bedeutung.

Das Sicherheitsbedürfnis, dass nur Befugte Daten zur Kenntnis nehmen sollen, haben Bürger, Unternehmen und auch die öffentliche Verwaltung. Insbesondere Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie z. B. Ärzte, Anwälte, Psychologen und Steuerberater, müssen die Vertraulichkeiten der Daten gewährleisten. Aber auch Journalisten und Abgeordnete haben großes Interesse daran, dass sich jedermann vertraulich an sie wenden kann.

Wie wichtig eine zuverlässige und sichere Verschlüsselung von Daten ist, hatte auch die Bundesregierung im Dokument „Digitale Agenda 2014-2017“ deutlich gemacht.

So heißt es in der Agenda:

„Ohne Vertrauen in die Sicherheit und Integrität der digitalen Welt wird es nicht gelingen, die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen. Das Vertrauen zu stärken heißt daher zum einen, die Kommunikation über digitale Netze zu schützen und dafür den Zugang zu sicheren und einfach zu nutzenden Verschlüsselungsverfahren zu fördern.

Zum anderen bedeutet es, dass wir unsere kritischen Infrastrukturen schützen. Wir wollen mit der Digitalen Agenda einen wesent-

lichen Beitrag dazu leisten, dass unser Land einer der sichersten digitalen Standorte weltweit bleibt.“

„Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungs-Standort Nr. 1 auf der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden.“

„Wir fördern und fordern den Einsatz von vertrauenswürdigen IT-Sicherheitstechnologien, insbesondere von mehr und besserer Verschlüsselung in der elektronischen Kommunikation.“

Das war allerdings im August 2014.

Im Zusammenhang mit dem Anschlag in Paris am 7. Januar 2015 wurde dann sofort seitens der Politik über die Notwendigkeit einer Schwächung von Verschlüsselungstechnologien diskutiert, um so dem Terrorismus wirksam zu begegnen.

So konnte man schon im gleichen Monat einer Meldung bei <http://www.heise.de/> entnehmen, dass – neben dem britischen Premier David Cameron und US-Präsident Obama – auch der Bundesinnenminister Thomas de Maizière nun Zugang zu verschlüsselten Daten wünscht. So forderte er, dass deutsche Sicherheitsbehörden befugt sein und in die Lage versetzt werden müssen, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen, wenn dies für ihre Arbeit und zum Schutz der Bevölkerung notwendig ist.



Aus diesem Grund wendete sich im März 2015 die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer ihrer Entschließungen an die Politik und forderte sie auf, sich aktiv für das Brief-, Post- und Fernmeldegeheimnis und bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschrän-

ken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich (siehe Anlage 23).

Kryptographische Verfahren dienen der Gewährleistung der Vertraulichkeit und Integrität. Insbesondere ist eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeit Dritter bereitzustellen. Kryptographische Verfahren durch staatliche Regulierungen zu unterbinden, würde unter Umständen auch dem Brief-, Post- und Fernmeldegeheimnis entgegenwirken.

15.3 Betriebssysteme mit Cloud-Anbindung – immer online

„Daten in der Cloud“ sind in aller Munde und unsere Gesellschaft hat diesen Begriff in den täglichen Gebrauch aufgenommen. Doch was ist eine Cloud und was hat sie mit Betriebssystemen zu tun?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) berichtete bereits im 10. Tätigkeitsbericht (Punkt 14.4) über die Risiken des Cloud Computing. Allgemein gesprochen ist die „Cloud“ ein Ersatzkonstrukt, welches Datenspeicherung und -verarbeitung von lokalen Geräten wie PCs, Laptops, Tablets und auch Smartphones in den Bereich des Internets auslagert. Der Nutzer erfährt gar nicht mehr, wo genau seine Daten gespeichert sind. Und genau dieses unscharfe Wissen, „wo“ „was“ verarbeitet wird, prägt den Begriff der Cloud (oder auch der Wolke). Die Vorteile liegen für den Nutzer dabei auf der Hand: Er muss sich nicht um Details kümmern. So ist es normal geworden, von überall Zugang zu Mails, Kurznachrichten, Kartendiensten oder Sprachassistenten zu haben. Auch Fotos und Musikbibliotheken werden zunehmend nicht mehr auf dem Gerät, sondern in der Cloud gespeichert, damit sie von überall und auch mittels verschiedener Geräte abrufbar sind. Aber auch Unternehmen und öffentliche Stellen nutzen vermehrt Cloud-Dienste bewusst oder unbewusst.

Angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste und der Wirtschaftsspionage empfahl der TLfDI, bei der Nutzung von Cloud-Diensten generell deutsche oder europäische Cloud-Anbieter

vorzuziehen, die zudem von vertrauenswürdigen Stellen zertifiziert sind (10. Tätigkeitsbericht Pkt. 14.4).

Nachfolgend wird hier nun insbesondere die neue Entwicklung der Integration von Cloud-Funktionen in Betriebssystemen behandelt und auch auf die Änderungen der Orientierungshilfe Cloud Computing V2.0 eingegangen.

Aus der Sammlung und Aufbereitung von Datenspuren zur Bildung von Personenprofilen ist in den letzten Jahren ein großer Markt entstanden, und von diesem Markt wollen die großen Hersteller von Betriebssystemen nun auch profitieren. Bisher stellten Betriebssysteme Grundfunktionen wie Speichern und Laden von Daten, Ausführen von Programmen auf dem Gerät und die Kommunikationsmöglichkeit mit anderen Geräten zur Verfügung. Einige Betriebssystemhersteller bieten nun zum Teil auch schon Online-Funktionen wie die Internetsuche über Sprachbefehle, zentrale Terminplaner, Kartendienste oder das Speichern von Daten auf einem Speicherplatz „in der Cloud“ an. Dadurch kann das Verhalten der Benutzer von ihnen besser nachvollzogen und im Detail analysiert werden. Leider unterliegen die Betriebssystemanbieter dabei oft nicht dem deutschen oder europäischen Datenschutzrecht.

Aus datenschutzrechtlicher Sicht bergen cloud-unterstützte Betriebssysteme generell Datenschutzrisiken. Einer der Kritikpunkte sind dabei die Standardeinstellungen. Diese sind meist so gewählt, dass der Betriebssystemhersteller schon bei der ersten Inbetriebnahme sehr viele Daten erfasst. Das Datenschutzprinzip, dass die Standardeinstellungen bei der Inbetriebnahme des Systems vom Hersteller so gewählt werden, dass möglichst wenig Daten übermittelt werden (Privacy-by-Default), wird hier weitestgehend ignoriert.

Das Fenster zur Privatsphäre ist somit geöffnet. So konnte man im August 2015 der Fachpresse entnehmen, dass nach der Standardinstallation von Windows 10 Informationen wie Namen, E-Mail Adressen, Telefonnummern, Standorte, Gerätekennungen, IP-Adressen, der Browserverlauf und die Browserfavoriten sofort an Microsoft übertragen werden. Au-



ßerdem behält sich Microsoft das Recht vor, auch Inhalte von in der Cloud gespeicherten Dateien auszuwerten, falls dies als „erforderlich“ angesehen wird (siehe dazu: <http://www.microsoft.com/de-de/privacystatement/default.aspx>).

Aus diesem Grund hatte der TLfDI noch im gleichen Monat eine entsprechende Pressemitteilung veröffentlicht:



(https://www.tlfdi.de/imperia/md/content/daten-schutz/veroeffentlichungen/pmtlfdi/pressemitteilung_windows_10.pdf).

In dieser wurde auf die Notwendigkeit hingewiesen, selbst noch persönliche Einstellungen vorzunehmen, um die eigene

Privatsphäre zu schützen. Dabei wurde gleich ein entsprechender externer Link zu Tipps zur Verbesserung der Einstellungen bei Windows 10 veröffentlicht. Dadurch konnten Bürger zeitnah durch Selbsthilfe ihr Betriebssystem datenschutzgerechter einstellen.

Auch die 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder nahm sich dann im Oktober 2015 des Themas der cloud-unterstützten Betriebssysteme an und zeigte in der Entschlie-ßung „Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken“ die entsprechenden Datenschutzrisiken auf (siehe dazu Anlage 30).

So können nach Angaben der Konferenz weitreichende Datenverarbeitungs-befugnisse nicht dadurch gerechtfertigt werden, dass Nutzer auf Basis der Zustimmung zu AGB datenschutzunfreundlichen Vor-einstellungen implizit zustimmen würden. Auch das Ermöglichen einer Opt-Out-Lösung wird nicht als zielführend angesehen, d.h. das manuelle Abschalten der Dienste im Nachhinein ist keine daten-schutzfreundliche Lösung. Systeme dürfen nicht einfach Daten erfassen und im Nachhinein fragen, ob man es nicht will, sondern müssen

vorab fragen, ob man dieser Datenerfassung zustimmt (Opt-In-Lösung). Hier bedarf es technisch unterstützter Einwilligungslösungen, die vor der Inbetriebnahme greifen müssen. Für jeden Dienst muss theoretisch eine Einwilligung (und auch die Möglichkeit des Widerrufs) gegeben werden. Der Widerruf ist momentan nur durch das Finden und Nutzen der entsprechenden Einstellungen möglich und damit ein sehr mühsamer Weg. Die Konferenz fordert daher die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Weiterhin empfiehlt die Datenschutzkonferenz in der oben genannten Entschließung den Benutzern der neuen Betriebssysteme, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen.

Moderne Betriebssysteme bieten heutzutage viele Cloud-Funktionalitäten an. Dabei sind die Standardeinstellungen selten datenschutzgerecht; Privacy-by-default wird daher nicht umgesetzt. Der Nutzer muss sich momentan selber behelfen und durch Recherche die möglichen Einstellvarianten finden. Der rechtliche Mechanismus der Einwilligung und des Widerrufs ist technisch noch unzureichend umgesetzt und zu kompliziert. Damit sind viele Betriebssysteme heute Datenschleudern-by-default.

15.4 Problem: Biometrische Gesichtserkennung

Biometrische Gesichtserkennungen sind auf dem Vormarsch. Für diesen Zweck müssen vom Gesicht des Nutzers Merkmale berechnet werden, welche beim ersten Erkennungsvorgang dann einer Person zugeordnet werden. Diese erfassten biometrischen Merkmale bilden danach die Grundlage für eine spätere Wiedererkennung. Der Trend geht bspw. dahin, dass man sich mit dieser dann an Geräten anmelden kann, indem bei der jeweiligen Technik-Anmeldung das Gesicht erneut erfasst und mit den bereits gespeicherten biometrischen Merkmalen verglichen wird. Ist der Vergleich positiv, erfolgt die Anmeldung nutzerbezogen am Gerät.

Pech für den, der gerade eine Gesichts-OP hatte oder wenn eine andere Person unberechtigt vom Berechtigten, bspw. im Schlaf oder im Vollrausch, vor dem jeweiligen Gerät diese Funktion auslöst, um

den unberechtigten Zugang bspw. zum Handy und den darauf gespeicherten Mails zu bekommen.

Aber Spaß beiseite!

Die Gesichtserkennung ist unter anderem auch geeignet, Begehrlichkeiten beim Arbeitgeber zu wecken, den Zugang zu sensiblen Bereichen per Gesichtserkennung zu regeln und kontrollieren zu können. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte schon am 23. Mai 2013 in der Pressemitteilung „Nur mit dem Fingerabdruck zum Arbeitsplatz?“ darauf hingewiesen, dass die Erhebung, Speicherung und Verwendung biometrischer Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der ArbeitnehmerInnen darstellt, der datenschutzrechtlich nicht gerechtfertigt ist. Nur in besonderen Einzelfällen kann eine biometrische Zutritts- oder Zugriffskontrolle am Arbeitsplatz unter strengen Voraussetzungen zulässig sein.

Aus datenschutzrechtlicher Sicht haben alle oben genannten Beispiele gemeinsam, dass sich Nutzer überlegen sollten, ob sie diese Funktionalität wirklich selbst wollen oder lieber darauf verzichten sollten. In ihren Überlegungen sollten sie auch prüfen, ob die biometrischen Merkmale verschlüsselt abgespeichert und vor unberechtigtem Zugriff Dritter geschützt sind.

Biometrische Gesichtserkennungen werden aber auch in sozialen Netzwerken zunehmen. Schon jetzt ist es üblich, dass man bspw. bei (Gruppen-)Fotos eine Person markieren und dieser Markierung einen bestimmten Namen zuweisen kann. Es gibt auch bereits Software, die aufgrund einer Markierung auf einem Foto dann den ganzen Datenbestand durchsuchen kann, auf welchen Fotos diese Person noch zu sehen ist. Im privaten Hausgebrauch scheint dies auch eine nützliche Software. Diese Funktionalität – dann von Betreibern sozialer Netzwerke in ihren sozialen Netzwerken eingesetzt – bietet allerdings die Möglichkeit einer Komplettdurchsuchung über alle gespeicherten Fotos in der Datenbank des sozialen Netzwerkes. Sowohl für die Profilbildung, die Betreiber sozialer Netzwerke gerne für ihre eigenen Interessen optimieren wollen, als auch für jegliche Sicherheitsbehörden können solche Gesichtserkennungsprogramme hochinteressant werden.

Aus diesem Grund hatte die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2014 in einer Entschließung „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!“ auch noch

einmal auf die erforderliche Einwilligungserklärung des Betroffenen hingewiesen (siehe dazu Anlage 6). Eine der wichtigsten Forderungen ist, dass über jegliche biometrische Gesichtserkennung der Betroffene in der Regel vorher informiert wird und sie nur mit Einwilligung des Betroffenen erfolgen darf.

Eine biometrische Gesichtserkennung zur Zugangskontrolle zu Geräten und zu Räumen scheint auf den ersten Blick eine optimale Lösung, bedarf aber einer vorhergehenden Einwilligung des Betroffenen. Auch soziale Netzwerke haben die Vorteile der Gesichtserkennung für ihre Zwecke erkannt. Aber auch hier bedarf es in jedem Fall der vorhergehenden Einwilligung des Betroffenen. Weiterhin sind die gespeicherten biometrischen Merkmale verschlüsselt zu speichern und der Zugriff von Dritten ist auszuschließen.

15.5 Verschlüsselung hilft nicht immer – auf die inneren Werte kommt es an

Im Frühjahr 2014 wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) von einem Bürger darauf aufmerksam gemacht, dass beim Thüringer Landesamt für Statistik eine Webseite zur Beantragung von Wahlscheinen zwar verschlüsselt, dort jedoch nur ein veralteter Verschlüsselungsalgorithmus unterstützt würde. Da auf diesem Teil der Webseite Wahlscheine zur Kommunal- und Europawahl beantragt werden konnten, sind dort durchaus persönliche Daten erfasst worden.

Gemeinhin ist es so, dass der Nutzer beim Surfen im Internet die Nutzung von Verschlüsselung am Kürzel „https://“ oder an diversen Schlosssymbolen im Browser erkennt. Dies sagt allerdings nur aus, dass überhaupt eine Verschlüsselung stattfindet und, wenn keine weiteren Warnhinweise angezeigt werden, dass der Browser der Webseite vertraut. All das traf auch auf diesen Fall zu; aber dennoch war die Verschlüsselung nicht sicher. Warum? Dazu muss man auch wissen, dass es nicht nur einen Verschlüsselungsalgorithmus gibt, der durch HTTPS unterstützt wird, sondern mehrere. Beim Verbindungsaufbau zu einer verschlüsselten Seite schickt der Rechner des Nutzers eine Liste der unterstützten Algorithmen und welche in welcher Reihenfolge präferiert werden sollten. Der Server sucht sich dann den ersten passenden Algorithmus aus, den er unterstützen kann. Dieses Schema ist notwendig, um eine maximale Flexibilität

und Kompatibilität zu erreichen. Von diesem Prozess merkt der Nutzer für gewöhnlich nichts. Die Untersuchung des TLfDI ergab nun, dass der Webserver vom Thüringer Landesamt für Statistik ausschließlich den RC4-Algorithmus zur Verschlüsselung unterstützte. Dieser gilt durch die NSA als in Echtzeit knackbar (siehe [http://www.heise.de/security/meldung/NSA-entschluesselt-](http://www.heise.de/security/meldung/NSA-entschluesselt-Webserver-Daten-angeblich-in-Echtzeit-2041383.html)



[Webserver-Daten-angeblich-in-Echtzeit-2041383.html](http://www.heise.de/security/meldung/NSA-entschluesselt-Webserver-Daten-angeblich-in-Echtzeit-2041383.html)) und wird daher auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als unsicher eingestuft.

Auf diesen Missetand machte der TLfDI die zuständigen Behörden – das Landesamt für Statistik und das Thüringer Landesrechenzentrum – aufmerksam und es erfolgte eine Umstellung auf zurzeit als sicher geltende

Verschlüsselungsverfahren.

Nicht jede verschlüsselte Verbindung ist auch automatisch sicher. Die Sicherheit hängt maßgeblich vom verwendeten Algorithmus ab. Unglücklicherweise bemerkt man als Nutzer nicht, welcher Algorithmus verwendet wird, sodass dies eine Sicherheitslücke darstellen kann. Glücklicherweise konnte der TLfDI diese in diesem Fall beseitigen lassen. Für Hinweise zu anderen Fällen ist der TLfDI weiterhin dankbar.

15.6 Ein neues „Labor“ beim TLfDI – Prüfung von Apps

Die Welt der Informationstechnik entwickelt sich in einem schnellen Tempo weiter, und ebenso nimmt auch die Vernetzung in unterschiedlichsten Bereichen weiter zu. Vor allen Dingen Smartphones und Tablets sind heutzutage die täglichen Kommunikationswerkzeuge und als solche in der Regel dauerhaft mit dem Internet verbunden. Diese werden unter anderem zum Empfangen und Senden von Nachrichten, zum Surfen im Internet, zum Buchen von Fahrkarten oder für Online-Spiele genutzt. Dies geschieht über Apps. Viele Anwendungsbereiche erfreuen sich zunehmend solcher App-Anwendungen. So werden bspw. von Universitäten, Bibliotheken, Verkehrsbetrieben, Tourismusbranchen und Stadtwerken Apps für alle möglichen Anwendungsgebiete angeboten. Auch im Gesundheitsbereich sind zunehmend Apps im Einsatz (siehe dazu Nr. 11.8).

Aus datenschutzrechtlicher Sicht ist dabei von Interesse, welche Daten diese Apps erfassen und wohin die Daten wie versendet werden.

Die Apps dabei ausschließlich aus der verfügbaren Dokumentation heraus datenschutzrechtlich zu beurteilen, ist dabei nicht zuverlässig möglich. Oft liegen nicht einmal diesbezügliche Dokumentationen vor. Deshalb hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) 2015 ein neues „Prüflabor“ für Apps in Betrieb genommen. Vorbild ist dabei das Prüflabor beim Bayerischen Landesamt für Datenschutzaufsicht. Mit dem Prüflabor beim TLfDI, derzeit ein eigenständiger eingerichteter Arbeitsplatz, ist es nun möglich, Apps z. B. von Endgeräten wie Smartphones, Tablets, Laptops oder anderen netzwerkfähigen Geräten zu analysieren. Das Labor basiert vor allen Dingen auf frei verfügbaren Open-Source-Lösungen auf Linux-Basis und Eigenentwicklungen.

Nach der Inbetriebnahme erfolgten im Laufe des 2. Halbjahres 2015 erste technische Untersuchungen von Apps. Hierbei konzentriert sich der TLfDI entsprechend seiner Zuständigkeit auf Apps, die von Thüringer Behörden und Unternehmen eingesetzt werden. Neben der technischen App-Prüfung bedarf es allerdings auch einer rechtlichen Bewertung. Eine abschließende datenschutzrechtliche Bewertung von Apps ist besonders in den Fällen aufwendig und dauert unter Umständen einige Wochen, in denen App-Hersteller Programmteile nutzen, deren genaue Funktionsweise sie selbst nicht genau kennen.

Der TLfDI hat sich entsprechend seiner Zuständigkeit vorgenommen, Apps, die von Thüringer Behörden und Unternehmen eingesetzt werden, technisch und datenschutzrechtlich zu prüfen. Dies ist ein sehr zeit- und personalaufwändiger Prozess. Dennoch ist der TLfDI über jeden Hinweis auf solche Apps dankbar.

15.7 IT-Sicherheitsgesetz nicht ohne Datenschutz!

Seit den Terroranschlägen vom 11. September 2001 sind neben der Informationstechnik auch „kritische Infrastrukturen“ in den Mittelpunkt staatlicher Sicherheitsvorsorge gerückt. Im Jahr 2009 veröffentlichte das Bundesinnenministerium des Innern die „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“. Im Jahr 2011 folgte die „Cyber Sicherheitsstrategie für Deutschland“, in der die Bundesregierung darauf hinwies, dass u. a. die Ver-

ffügbarkeit des Cyber-Raums die existenzielle Frage des 21. Jahrhunderts geworden sei. Wirtschaft und Bevölkerung seien auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen. Der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum könnten nach Angaben der Bundesregierung zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen.

Ein nationales Cyber-Abwehrzentrum wurde geschaffen, mit dem Ziel, die operative Zusammenarbeit der relevanten staatlichen Stellen zu optimieren und die Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle zu koordinieren.

Anfang 2013 wurde dann vom Bundesministerium des Innern ein Referentenentwurf eines IT-Sicherheitsgesetzes zur Diskussion veröffentlicht, welcher eine Reihe von Kritik erfuhr.

Anfang Januar 2015 ereignete sich das Attentat auf die Redaktion „Charlie Hebdo“ in Paris. Mit dem Attentat begann nun auch wieder eine verschärfte politische Diskussion zur Sicherheit Deutschlands.

Ende Februar 2015 brachte die Bundesregierung dann den Gesetzentwurf für ein IT-Sicherheitsgesetz ein, um die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern.

Die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die ausdrücklich die Notwendigkeit von Informationssicherheit befürwortet, kritisierte in ihrem entsprechenden Entschluss im März 2015 diesen



Gesetzentwurf sehr scharf (siehe https://www.tlfdi.de/tlfdi/berichte/entschlusungen_datenschutzkonferenz/89/).

So seien beispielsweise die neuen Melde- und Benachrichtigungspflichten bei erheblichen IT-Sicherheitsvorfällen an das Bundesamt für Informationstechnik (BSI) nicht mit einer datenschutzrechtlichen Meldepflicht bei Datenpannen an die Datenschutzaufsichtsbehörden verbunden. Weiterhin kritisierte die Konferenz, dass zu unklar sei, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welchen Zweck erhoben, verarbeitet und gespeichert werden dürfen.

Wie der Zufall es so wollte: Während der Bundestag über dieses Gesetz diskutierte und dieses Gesetz dann auch verabschiedete, ereilte das Bundestagsnetzwerk selbst ein Cyberangriff. Das IT-Sicherheitsgesetz trat, nun fast logisch, dann am 25. Juli 2015 in Kraft (Bundesgesetzblatt Teil 1 Nr. 31 vom 24. Juli 2015). Es schreibt die Einhaltung eines Mindestniveaus an IT-Sicherheit und von Meldepflichten bei Betreibern so genannter kritischer Infrastrukturen vor. Als kritische Infrastrukturen werden dabei gesehen: Einrichtungen, Anlagen oder Teile, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und zugleich von hoher Bedeutung für das funktionierende Gemeinwesen sind. Nach Angaben des Gesetzes sollen Einzelheiten zum Anwendungsbereich und zum Adresskreis noch in einer Rechtsverordnung bestimmt werden.

Mit dem IT-Sicherheitsgesetz wurde auch das Telekommunikationsgesetz geändert und die rechtliche Möglichkeit geschaffen, dass Telekommunikationsdiensteanbieter die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer bei Erforderlichkeit erheben und verwenden dürfen, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.

Interessanterweise erfolgte, um ein paar Monate zeitversetzt, das parlamentarische Gesetzgebungsverfahren zum „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“, welches im Oktober 2015 vom Bundestag bestätigt wurde (siehe dazu Nr. 2.1). Man erkennt unweigerlich, dass der Bedarf, die Informationstechnik zu schützen und insbesondere Terroristen zu überwachen, offenbar zunimmt. Dies darf aber immer nur in ausgewogener Balance zum Datenschutz erfolgen. Die Datenschutzbeauftragten werden daher auch weiter darum kämpfen, dass den Bürgern ihr informationelles Selbstbestimmungsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 Grundgesetz erhalten bzw. nicht zu stark per Gesetz eingeschränkt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren. Die Datenschutzbeauftragten werden daher weiter darum kämpfen,

dass den Bürgern ihr informationelles Selbstbestimmungsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 2 Grundgesetz erhalten bzw. nicht zu stark per Gesetz eingeschränkt wird.

15.8 Happy Birthday – die elektronische Gesundheitskarte wird 10 Jahre alt

Bereits im November 2003 wurde das „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung“ (GKV-Modernisierungsgesetz – GMG) erlassen. Dies hatte zur Folge, dass auch das Sozialgesetzbuch (SGB) Fünftes Buch (V) u. a. in § 291 und § 291a geändert wurde. So wurde damals festgelegt, dass die Krankenversichertenkarte bis spätestens zum 1. Januar 2006 zu einer elektronischen Gesundheitskarte zu erweitern ist. Auch wurde festgelegt, welche Daten die elektronische Gesundheitskarte beinhalten muss und welche Daten wie verarbeitet werden sollen.

Der Thüringer Landesbeauftragte für den Datenschutz berichtete in seinen Tätigkeitsberichten mehrfach darüber.

Allerdings ist die elektronische Gesundheitskarte erst seit dem 1. Januar 2015 Pflicht und gilt seit diesem Zeitpunkt bundesweit ausschließlich als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkassen beim Arzt oder Zahnarzt. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) informierte daraufhin zum aktuellen Sachstand in einer Pressemitteilung (siehe dazu Anlage 47).

Seit dem 29. Dezember 2015 ist nun auch das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze in Kraft (E-Health-Gesetz). So soll nun mittels der elektronischen Gesundheitskarte die Verbesserung der Wirtschaftlichkeit, Qualität und Transparenz der Behandlung durch moderne Anwendungen und Informations- und Kommunikationstechnologien erzielt werden (siehe dazu Nr. 11.7).

Damit auch die kommenden Anwendungen in Thüringen datenschutzrechtskonform umgesetzt werden, hat der TLfDI seine Gesprächsbereitschaft gegenüber der Landesärztekammer Thüringen und der Landesapothekerkammer Thüringen bekundet.

Unabhängig davon wird der TLfDI den weiteren Werdegang dieser Karte aufmerksam verfolgen.

Der Einsatz der elektronischen Gesundheitskarte wird auch künftig vom TLfDI kritisch beobachtet. Der TLfDI bittet daher um Hinweise, falls datenschutzrechtliche Probleme auftauchen.

15.9 Cloud-Computing 2.0 und Safe Harbor

Zur datenschutzkonformen Gestaltung und zur Nutzung von Cloud-Computing hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits 2011 eine Entschließung veröffentlicht. Damals wurde parallel zur Entschließung auch eine entsprechende Orientierungshilfe (OH) erarbeitet (siehe 9. TB, Pkt. 14.1). Diese Orientierungshilfe richtet sich sowohl an die Anbieter von Cloud-Diensten als auch an deren Nutzer.

Aufgrund der technischen Entwicklung und aufgrund der NSA-Affäre wurde sie drei Jahre später überarbeitet und 2014 unter „Cloud-Computing 2.0“ veröffentlicht:

https://www.tlfdi.de/imperia/md/content/daten-schutz/themen/orientierungshilfen/oh_cc_2.0.pdf.



Die OH „Cloud-Computing 2.0“ geht nun neben dem grenzüberschreitenden Datenverkehr auch auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency (NSA) ein. Es wird darauf hingewiesen, dass es für die Zugriffsbefugnisse der US-Behörden nicht maßgebend ist, ob sich die Cloud innerhalb oder außerhalb der USA befindet. Es wird nach US-Recht als ausreichend angesehen, wenn der Cloud-Anbieter zumindest auch in den USA geschäftlich tätig ist.

Aus datenschutzrechtlicher Sicht steht eine entsprechende Datenübermittlung von Unternehmen mit Sitz in Europa bzw. Deutschland an US-Behörden nicht mit Art. 26 der Richtlinie 95/46/EG bzw. § 4c BDSG im Einklang. Zudem würde bei einer entsprechenden Datenübermittlung durch den Cloud-Anbieter auch der Cloud-Anwender automatisch gegen europäisches und deutsches Datenschutzrecht verstoßen, da er in seiner datenschutzrechtlichen Verantwortlichkeit bleibt. Letzteres ergibt sich aus der Tatsache, dass bei Auftragsdatenverarbeitung der Auftraggeber verantwortliche

Stelle bleibt. Die OH weist deshalb darauf hin, dass derzeit ein internationales Übereinkommen fehle, welches eine solche Datenübermittlung an US-Behörden rechtfertige.

Auch in den USA ansässige Cloud-Anbieter, die sich dem Safe-Harbor-Abkommen zwischen der EU und den USA angeschlossen hatten, waren von diesem staatlichen Eingriff durch US-Behörden nicht ausgenommen.

Das Safe-Harbor-Abkommen ist bekanntlich am 6. Oktober 2015 vom Europäischen Gerichtshof (EuGH, C-362/14) für ungültig erklärt worden, da die USA ein angemessenes Schutzniveau übermittelter personenbezogener Daten nicht gewährleisten. Dies wurde u. a. damit begründet, dass der Zugriff von Behörden, der generell auf den Inhalt elektronischer Kommunikation zielt, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzt (siehe auch Beitrag Nummer 3.1).

So ist die derzeitige Orientierungshilfe Cloud-Computing in ihrer Version 2.0 derzeit nun unter Beachtung dieses Urteils anzuwenden und die Übermittlung personenbezogener Daten in eine Cloud von Cloud-Anbietern mit Sitz in den USA zu unterlassen.

Diese Orientierungshilfe Cloud-Computing 2.0 ist nicht nur in ihrer geänderten Fassung von 2014 anzuwenden, sondern auch unter Beachtung der Entscheidung des Europäischen Gerichtshofes (EuGH) zu Safe Harbor. Die Übermittlung personenbezogener Daten in eine Cloud von Cloud-Anbietern mit Sitz in den USA ist daher bis auf Weiteres zu unterlassen.

15.10 Newsletter – immer datenschutzgerecht?

Um Informationen an eine bestimmte Zielgruppe regelmäßig oder schnell verteilen zu können, bedient man sich gerne so genannter Newsletter. Newsletter werden in der Regel einmalig versendet. Dennoch ist es nicht unüblich, die versendeten Newsletter für einen späteren Abruf noch einmal auf der entsprechenden Webseite bereitzustellen. Newsletter mit personenbezogenen Daten unterliegen dabei datenschutzrechtlichen Vorschriften. Werden sie nachträglich gespeichert, sind weitere datenschutzrechtliche Vorgaben zu beachten.

Im vorliegenden Fall hatte eine verantwortliche Stelle auf ihrer Webseite die Newsletter gespeichert, um sie für eventuelle Abrufe bereit-

zuhalten. In einem dieser Newsletter waren allerdings auch Fotos von Mitarbeitern und deren Namen veröffentlicht.

Ein ehemaliger Mitarbeiter forderte nun, sein Foto und den Namen aus dem Newsletter von der Webseite zu löschen. Alle Versuche, dies beim ehemaligen Arbeitnehmer durchzusetzen, schlugen jedoch fehl, sodass der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hinzugezogen wurde.

Nachdem der TLfDI die Sachlage geprüft und die verantwortliche Stelle kontaktiert hatte, teilte diese mit, alle Fotos des Beschwerdeführers „bei sich“ gelöscht zu haben. Der TLfDI stellte jedoch fest, dass der betroffene Newsletter nach wie vor in der Original-Version abrufbar war. Es stellte sich heraus, dass lediglich alle Links zum Newsletter auf der Webseite gelöscht worden waren. So musste der TLfDI erneut nachhaken und auf Umsetzung drängen. Dem Mangel wurde nun abgeholfen, indem der gesamte Newsletter gelöscht wurde.

Grundsätzlich sind Internetlinks nur Verweise auf Dokumente (wie Webseiten oder eben auch Newsletter), die den Ort und den Namen des Dokumentes im Internet anzeigen. Mit der Löschung des Hinweises auf ein Dokument verschwindet nicht das Dokument selber. Dieses ist unverändert vorhanden. Bei Lösungsbedarf muss also das Original-Dokument gelöscht werden und nicht (nur) alle Verweise darauf.

Die Löschung erfolgte nicht nur aufgrund von „good will“, sondern es bestand tatsächlich eine Verpflichtung hierzu. Eine konkrete Rechtsgrundlage für die Veröffentlichung von Mitarbeiterfotos ist in diesem Zusammenhang nicht ersichtlich. Daher kann die namentliche Veröffentlichung von Mitarbeitern nur mit deren Einwilligung erfolgen (§ 4 Thüringer Datenschutzgesetz).

In der Vergangenheit wurden die Mitarbeiter bei der Aufnahme der Beschäftigung lediglich darauf hingewiesen, dass für den Newsletter und im Rahmen von Veranstaltungen Fotos aufgenommen und ggf. veröffentlicht werden. Soll eine Veröffentlichung im Internet erfolgen, ist das Foto weltweit abrufbar. Eine unberechtigte Weiterverwendung oder Veränderung durch Dritte kann daher nicht generell ausgeschlossen werden. Als Mitarbeiter sollte man daher vorher immer reiflich abwägen, ob man mit der Veröffentlichung von Fotos im Internet einverstanden ist.

Eine Löschung von Links auf abrufbare Dokumente im Internet verursacht noch keine Löschung von Daten in einem Dokument selbst. Nur eine Löschung im Original-Dokument ist hier zielführend. Einwilligungserklärungen müssen zweckgebunden oder besser noch fallbezogen eingeholt werden, sonst sind sie rechtlich unwirksam.

15.11 eIDAS – was ist das?

Mit der Richtlinie 1999/93 EG des Europäischen Parlaments und des Rates der Europäischen Union wurden Regelungen zur elektronischen Signatur für die Mitgliedstaaten getroffen. So regelte nachfolgend das deutsche Signaturgesetz (SigG) die Unterschiede und den Einsatz der elektronischen Signatur, der fortgeschrittenen elektronischen Signatur und der qualifizierten elektronischen Signatur. Einige nationale Normen schreiben zudem die qualifizierte elektronische Signatur vor, wenn die eigenhändige Unterschrift durch eine elektronische Unterschrift im elektronischen Dokument ersetzt werden kann. Um den Bürgern dies zu ermöglichen, sah man auch bereits beim elektronischen Personalausweis einen festen Speicherplatz für die qualifizierte elektronische Signatur vor. So kann man auf dem elektronischen Personalausweis eine qualifizierte elektronische Signatur speichern, um mit dem Personalausweis selbst elektronische Dokumente rechtsverbindlich und fälschungssicher elektronisch zu unterschreiben. Allerdings muss es tatsächlich eine qualifizierte elektronische Signatur sein. Dies bedeutet, ein Zertifizierungsdiensteanbieter hat die Identität des Eigentümers der elektronischen Signatur eindeutig überprüft und dies mittels eines elektronischen Zertifikates belegt. Mithilfe des Zertifikates kann dann festgestellt werden, welcher Person die elektronische Signatur tatsächlich gehört.

Mit der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt vom 8. Juli 2009 wurden alle Mitgliedstaaten zudem verpflichtet, sicherzustellen, dass auch alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch abgewickelt werden können.

Dies bedeutete, auch in anderen Mitgliedstaaten ausgestellte elektronische Signaturen – hierbei insbesondere die qualifizierten elektronische Signaturen – zu prüfen und anzuerkennen.

Da aber europaweit diesbezüglich keine einheitlichen Regelungen vorhanden waren, wurde am 23. Juli 2014 die EU- „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014)“ verabschiedet. Diese Verordnung wird auch als eIDAS-Verordnung bezeichnet (**e**lectronic **i**dentification and trust services). Entsprechend dem Erwägungsgrund 3 dieser Verordnung hatte zwar die damalige EU-Richtlinie 1999/93EG Regelungen zu elektronischen Signaturen festgelegt. Dies war jedoch geschehen, ohne einen umfassenden grenz- und sektorenübergreifenden Rahmen für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen zu schaffen. Die eIDAS-Verordnung soll nun die Rechtsvorschrift jener Richtlinie stärken und erweitern.

Diese Verordnung (EU Nr. 910/2014) ist also ein weiterer Baustein, um die Nutzung grenzüberschreitender digitaler Dienste, die sichere elektronische Identifizierung und Authentifizierung und die Förderung des digitalen Binnenmarktes voranzutreiben. Sie gilt mit wenigen Ausnahmen ab dem 1. Juli 2016.

Inhaltlich unterscheidet sich die Verordnung zum Teil vom derzeit noch gültigen Signaturgesetz (SigG). Als Beispiel sei hier die elektronische Fernsignierung genannt: § 5 Abs. 6 i. V. m. § 17 Abs. 1 SigG sieht vor, dass bei der Erzeugung der qualifizierten elektronischen Signatur eine sichere Signaturerstellungseinheit einzusetzen ist und der Antragsteller auch solch eine Einheit besitzen muss. Die EU-Verordnung sieht nun allerdings auch elektronische Fernsignaturen vor, sodass Signaturen beim Vertrauensdiensteanbieter erzeugt und gespeichert werden können (siehe Erwägungsgrund 52, eIDAS-Verordnung).

Die Folgen dieser Regelungen sind aus datenschutzrechtlicher Sicht derzeit noch nicht abzuschätzen. Das hohe Datenschutzniveau in Deutschland hatte bisher sichergestellt, dass für die Signaturerstellung von qualifizierten elektronischen Signaturen bisher nur bei der Bundesnetzagentur gelistete Produkte verwendet werden durften. Mit der nun eingeführten Fernsignatur ist es dem Antragsteller nicht möglich, zu prüfen, ob seine Signatur auch gemäß dem neuesten Stand der Technik erstellt wurde. Es besteht durchaus die Gefahr,

dass der Nutzer nun unwissentlich schlechtere Verfahren auswählt, weil sie preisgünstiger sind.

Interessant für den Nutzer von qualifizierten elektronischen Signaturen könnte auch das „Aussetzen qualifizierter Zertifikate“, also das Sperren des oben genannten elektronischen Zertifikates sein. So ist es nun laut eIDAS möglich, bspw. für einen genauen Zeitraum ein qualifiziertes Zertifikat für die qualifizierte elektronische Signatur sperren zu lassen. Aus der qualifizierten elektronischen Signatur wird damit nur noch eine normale elektronische Signatur. Wie oben beschrieben, ist dann eine rechtsverbindliche elektronische Unterschrift nicht möglich, da zu der elektronischen Signatur die dazugehörige Personenüberprüfung mangels gesperrten Zertifikats nicht vorgenommen werden kann.

Denkbar ist so ein solches Szenario bspw. dann, wenn man den Datenträger mit seiner qualifizierten elektronischen Signatur verlegt hat und sicherstellen möchte, dass bis zum Wiederauffinden mit diesem Datenträger kein Missbrauch geschieht, also elektronische Dokumente nicht im eigenen Namen einfach von Dritten unterschrieben werden.

Die EU-Verordnung eIDAS regelt aber nicht nur die Anforderungen an qualifizierte Zertifikate für elektronische Signaturen, elektronische Siegel und für die Website-Authentifizierung, sondern auch Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten.

Durch die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (910/2014) wurde für alle Mitgliedstaaten die sichere elektronische Identifizierung und Authentifizierung neu festgeschrieben. Diese gilt es umzusetzen.

15.12 Kindergartengruppe 2.0 – Unvernunft der Großen zulasten der Kleinen

Eine Kindertagesstätte (Kita) teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass Eltern einer Kitagruppe über einen populären Messengerdienst eine Kontaktgruppe gegründet hätten, innerhalb deren die Erzieherinnen Informationen und Bilder von den Kindern der Kitagruppe verschicken sollten. Bei der App hat man die Möglichkeit, so ge-

nannte Kontaktgruppen einzurichten, zu denen mehrere Gruppenmitglieder gehören können und in denen diese Texte, Bilder und auch Videos austauschen können. Diese Informationen sind allen Mitgliedern der Kontaktgruppe zugänglich und können auch an andere Personen weitergeleitet werden. Laut der Kindertagesstätte lagen im konkreten Fall Einverständniserklärungen der Eltern zur Veröffentlichung von Fotos in Druckmedien und im Internet vor. Es galt nun, vom TLfDI prüfen zu lassen, ob die Einrichtung dieser Nachrichtengruppe datenschutzrechtlich zulässig war und ob die Einverständniserklärungen von den Eltern dafür ausreichend waren. Die datenschutzrechtliche Prüfung des TLfDI kam zu folgendem Ergebnis:

Für die Anmeldung bei diesem Messengerdienst muss der Nutzer zunächst die Allgemeinen Geschäftsbedingungen (AGB) akzeptieren, die leider nur auf Englisch veröffentlicht sind. In den AGB befindet sich der Hinweis, dass sich der Dienst die nötigen Rechte vorbehalte, Texte, Bilder und andere Inhalte, die ein Nutzer postet, auf weiteren Plattformen und Medienkanälen zu verbreiten. Ferner steht der Dienst immer wieder in der Kritik, das vollständige Adressbuch des Nutzers unverschlüsselt an den US-amerikanischen Server weiterzuleiten.

Der TLfDI wies darauf hin, dass die Kita-Mitarbeiterinnen und -Mitarbeiter weder im Rahmen ihrer Arbeitsverhältnisse noch im Rahmen der bestehenden Verträge zwischen den Eltern und der Kita vertraglich verpflichtet sein dürften, entsprechende Bilder über diese App einzustellen. Demnach dürften die Kita-Mitarbeiterinnen und -Mitarbeiter auch kaum verpflichtet sein, die erwünschten Fotos mit ihren Privat-Smartphones anzufertigen.

Da es sich bei dem Träger der Kindertagesstätte um eine Gemeinde als öffentliche Stelle handelte, hatte somit die Kindertagesstätte als ein Teil einer öffentlichen Stelle auch § 9 des Thüringer Datenschutzgesetzes (ThürDSG) zu beachten. Gemäß § 9 Abs. 2 Satz 1 Nr. 1 ThürDSG haben die von der öffentlichen Stelle zu treffenden technischen und organisatorischen Maßnahmen zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Aufgrund dieser Regelung war nach Prüfung des TLfDI das Übermitteln von Fotos von Kita-Kindern durch Kita-Erzieherinnen in die Kontaktgruppe unzulässig, weil die Kindertagesstätte mit ihren Kita-Mitarbeiterinnen und -Mitarbeitern gerade nicht garantieren konnte, dass die Fotos als personenbezoge-

ne Daten der Kinder von dem Dienst an andere Plattformen und Medienkanäle weitergeleitet werden. Keine Bedenken hegte dagegen der TLfDI, wenn die Kindertagesstätte nicht-personenbezogene Daten – wie z. B. den Hinweis, dass die Kita am folgenden Tag erst eine Stunde später öffnet – in die Kontaktgruppe der Eltern posten würde.

Bedenken bestanden schließlich auch gegen die Übermittlung der Fotos von Kita-Kindern in die Gruppe insoweit, dass aufgrund der oben beschriebenen Weiterleitung der Kontaktdaten an die Firmenserver in die USA auch eine Datenübermittlung in unsicherere Drittstaaten nach § 23 ThürDSG erfolgen könnte, in denen kein angemessenes Datenschutzniveau gewährleistet ist. Der Europäische Gerichtshof (EuGH) hatte in seinem Urteil vom 6. Oktober 2015 die Safe-Harbor-Entscheidung der EU-Kommission, die eine Datenübermittlung unter bestimmten Voraussetzungen in die Vereinigten Staaten von Amerika (USA) gestattete, für unzulässig erklärt. Grund dafür war, dass aus Sicht des EuGH kein angemessenes Schutzniveau für personenbezogene Daten von EU-Bürgern in den USA gewährleistet sei.

Somit wurde der Kindertagesstätte geraten, im Rahmen einer Informationsveranstaltung die Eltern ihrer betroffenen Kitagruppe über die datenschutzrechtlichen Risiken solcher Dienste zu informieren und über andere Möglichkeiten zu diskutieren, wie insbesondere Bilder der Kinder möglichst vielen Eltern auf datenschutzrechtlich sicheren Medien zugänglich gemacht werden können.

Schließlich war noch die Frage zu klären, ob die Kindertagesstätte aufgrund einer Einverständniserklärung der Eltern zur Veröffentlichung von Fotos in den Druckmedien und im Internet datenschutzrechtlich abgesichert ist. Zu beachten war dabei zunächst § 4 Abs. 1 Satz 1 ThürDSG: Danach ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Eine solche Einwilligung rechtfertigt gemäß § 4 Abs. 1 Satz 2 ThürDSG eine Datenverarbeitung aber nur dann, wenn sie zur Erfüllung anerkannter Zwecke erforderlich ist. Als anerkannte Zwecke im Sinne dieser Vorschrift kommen nach der Begründung zu § 4 Abs. 1 Satz 2 ThürDSG (Drucksache 5/3086) neben der Aufgabenerfüllung öffentlicher Stellen, die vorrangig in den §§ 19 ff. ThürDSG oder spezialgesetzlich geregelt ist, unter anderem behördeninterne Zwecke in Betracht. Somit lag ein anerkannter Zweck im

Fall der Datenerhebung in Form des Einstellens von Fotos der Kita-Kinder durch die Kindertagesstätte in eine Kontaktgruppe aus Sicht des TLfDI nicht vor. Deshalb rechtfertigte schließlich auch eine Einwilligung der Betroffenen hier nicht die Datenerhebung der Kita-Mitarbeiterinnen in Form des Einstellens von Bildern der Kita-Kinder in die Gruppe. Letztlich zu berücksichtigen waren aber auch an dieser Stelle die bereits genannten datenschutzrechtlich unbefriedigenden Zustände in den AGB der App. Aufgrund dessen war es der Kita aus der Sicht des TLfDI unmöglich, die Voraussetzungen des oben genannten § 9 Abs. 2 Nr. 1 ThürDSG zu beachten und einzuhalten, wenn sie Fotos von Kita-



Kindern auf die Kontaktgruppe der Eltern einstellen wollte. Welche Netzwerke bzw. alternativen Dienste dafür infrage kommen, stellt die Seite <http://www.youngdata.de/> ausführlich dar (siehe hierzu: www.youngdata.de/whatsapp-skype-co/whatsapp/).



In Messengerdiensten sollten nur personenbezogene Daten eingestellt werden, die auch an Ihrer Haustür hängen oder die Sie auf eine Postkarte schreiben würden. Namen und Bilder von den Kita-Kindern als personenbezogene Daten gehören – gerade wenn beide noch miteinander verknüpft werden (z. B. Bildunterschrift: „Hier sieht man Max Müller und Susi Meyer auf dem Foto.“) – hingegen grundsätzlich nicht in ungeeignete Messengerdienste. Eine öffentliche Kindertagesstätte und ihre Mitarbeiter haben nach § 9 Abs. 2 Satz 1 Nr. 1 ThürDSG die technischen Maßnahmen zu gewährleisten, dass nur befugte Personen personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Da nicht ausgeschlossen ist, dass personenbezogene Daten, die auf diese Weise versandt werden, auch „über den Ozean“ in die USA gelangen und dort von Dritten ungehindert weiterverarbeitet werden, scheidet eine Nutzung von derartigen Diensten in Kindergärten aus. Dies ergibt sich auch aus § 4 Abs. 1 Satz 2 ThürDSG, weil der Einsatz in Kindergärten nicht zur Erfüllung anerkannter Zwecke dient.

15.13 E-Government und Informationstechnik (IT) in der Thüringer Landesverwaltung

Im Mai 2014 veröffentlichte das Thüringer Finanzministerium als zuständiges Ministerium für E-Government eine „Strategie für E-Government und die IT des Freistaats Thüringen“. Dies war entsprechend dem veröffentlichten Dokument notwendig, da zur Bewältigung der vielfältigen Herausforderungen eine Strategie entwickelt werden musste, um langfristig eine gleichgerichtete Vorgehensweise innerhalb der Landesverwaltung und gegenüber den Bürgern und Unternehmen sicherzustellen.

Weiterhin wurde darin verankert, dass die ressortübergreifende Steuerung des E-Governments und der IT in der Landesverwaltung durch den IT-Beauftragten des Freistaats Thüringen (Chief Information Officer – CIO) zu erfolgen hat.

Im August 2015 veröffentlichte das Thüringer Finanzministerium dann eine „Thüringer Organisationsrichtlinie für E-Government“, in der nun die ressortübergreifende Steuerung des E-Governments und der IT in der Landesverwaltung einem im Finanzministerium angesiedelten Beauftragten des Freistaats Thüringen für E-Government und IT übertragen wurde (Thüringer Staatsanzeiger Nr. 37/2015).

Dies erscheint auch für den außenstehenden Betrachter durchaus Sinn zu haben.

War bisher E-Government ein Teilbereich der IT-Strategie, so ist nunmehr ein klares Signal gesetzt worden, dass die IT-Strategie ein Teilbereich ist, um E-Government in der Landesverwaltung durchzusetzen.

Entsprechend dieser Organisationsrichtlinie ist nun eine Koordinierungsstelle E-Government und IT ins Leben gerufen worden, bei der auch der IT-Sicherheitsbeauftragte des Freistaats Thüringen angesiedelt ist. Dessen Aufgabe ist es, den Informationssicherheitsprozess in der Landesverwaltung zu planen, zu koordinieren und zu steuern. Zudem tragen die Zentralabteilungsleiter der Staatskanzlei und der Ministerien als Ressortbeauftragte für E-Government und IT die Verantwortung für E-Government und den IT-Einsatz in ihren Geschäftsbereichen. Sie und der Landesbeauftragte für E-Government und IT bilden den so genannten Lenkungsausschuss E-Government und IT. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat in dem Zusammenhang vorgeschlagen, bei jeweils anstehenden datenschutzrechtlichen Themen

einen Vertreter des TLfDI beratend auch in den Lenkungsausschuss E-Government und IT einzuladen.

Weiterhin gibt es nun den Arbeitskreis „E-Government und IT“. Dieser Arbeitskreis setzt sich aus den für IT zuständigen Referatsleitern oder Referenten der Staatskanzlei und der Ministerien, dem IT-Sicherheitsbeauftragten des Freistaates Thüringen und dem Leiter der Koordinierungsstelle E-Government und IT zusammen. Dies ist allerdings nicht neu, denn die für IT zuständigen Referatsleiter der Staatskanzlei und der Ministerien tagten schon immer zusammen, nur der Name des Arbeitskreises änderte sich je nach Zuständigkeiten und Vorgaben.

Egal, wie dieser Arbeitskreis auch benannt ist, stets war und ist der TLfDI in diesem Arbeitskreis als beratendes Mitglied involviert. Dies hat sich aus Sicht des TLfDI auch in all den Jahren bewährt. So müssen nun beispielsweise auch die Konsequenzen des Urteils vom 06. Oktober 2015 vom Europäischen Gerichtshof (EuGH) zur Safe-Harbor-Entscheidung der EU-Kommission bezüglich der Landesverwaltung überdacht werden (siehe dazu Nummer 3.1). Denn das Urteil, welches eine Datenübermittlung von personenbezogenen Daten in die USA auf der Grundlage der Safe-Harbor-Entscheidung für rechtswidrig erklärt, gilt es umzusetzen, auch in einer Landesverwaltung.

Der TLfDI hat vorgeschlagen, ihn bei jeweils anstehenden datenschutzrechtlichen Themen im Thüringer Lenkungsausschuss E-Government und IT beratend hinzuzuziehen. Weiterhin gilt es, das Urteil des Europäischen Gerichtshofs (EuGH) zur Safe-Harbor-Entscheidung der EU-Kommission auch in der Thüringer Landesverwaltung umzusetzen.

15.14 Straßenpanoramafahrten

Neben der Google Inc. und der Microsoft Corporation erfasst nun auch die HERE Global B.V., mit Sitz in den Niederlanden, Panorama- und 3D-Ansichten von Straßenzügen in Deutschland. HERE fertigt 360-Grad-Panoramabilder, 3D-Scans über Laserscanner sowie GPS-Aufzeichnungen an. Damit können 3D-Aufnahmen von Hausfassaden, Vorgärten, Fahrzeugen und anwesenden Personen erstellt werden.

In Thüringen begannen von HERE die Erfassungen von Straßenzügen im Herbst 2014, damals im Auftrag der Firma Nokia. Der TLfDI wies im September 2014 in einer Presseerklärung „Nokia ante Portas“ frühzeitig darauf hin, dass Hausbesitzer (Behörden, Unternehmen, Privatpersonen) in den Panoramabildern ihre Hausfassaden auch gegenüber dieser Firma unkenntlich machen lassen können (https://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_zu_nokia_fahrten.pdf).

Die Frage, warum man überhaupt die Straßen befährt und filmt, ist relativ simpel. Es gibt mindestens zwei marktwirtschaftliche Gründe. Zum einen möchte man über Webseiten die virtuelle Darstellung von Straßenzügen so real wie möglich anbieten.

Zum anderen sind die derzeitigen Navigationssysteme in den Autos aus Herstellersicht zu ungenau bzw. nicht nutzerfreundlich genug. Die Idee, beim Autofahren nicht nur den Straßenverlauf einsehen zu können, sondern sich auch an den Fassaden von Gebäuden metergenau orientieren zu können, scheint vor allem von der Automobilindustrie, jedoch auch von den Autofahrern gewünscht. Zudem sollen zukünftig selbstfahrende Autos mit präziseren Navigationssystemen ausgestattet werden. Wie begehrt solche Systeme sind, kann man daran erkennen, dass Presseberichten zufolge die Automobilfirmen Audi, BMW und Daimler im Sommer 2015 den Kartendienst HERE von Nokia für 2,8 Milliarden Euro kauften.

Dem TLfDI ist es wichtig, darauf hinzuweisen, dass, egal welche Firmen gerade solche Straßenpanoramabilder erstellen, ein Widerspruchsrecht zur Veröffentlichung der Aufnahmen besteht. Der TLfDI wird Sie deshalb auch weiterhin auf dem Laufenden halten.



Bei den derzeit gängigen Straßenpanoramafahrten werden in der Regel Bilder vom Straßenverlauf und von Hausfassaden erfasst. Aber auch Vorgärten, derzeit anwesende Fahrzeuge und Personen könnten dabei zufällig erfasst werden.

Behörden, Unternehmen und Privatpersonen sollten daher die veröffentlichten Daten kritisch betrachten und bei Bedarf ihr Widerspruchsrecht gegenüber der Firma nutzen. Sollte dieses scheitern, wäre der TLfDI über eine Information dankbar.

15.15 YouNow – All know!

YouNow – eine trendige Bühne, um sein Leben mit anderen zu teilen, nicht mal eben mit ein paar hundert Freunden, sondern mit allen Internetnutzern auf dem Globus, jetzt sofort und live. Die Plattform „www.younow.com“ macht es möglich. Vor allem Jugendliche sitzen zu Hause im Kinderzimmer, schalten Handy oder PC-Kamera ein und plaudern mit Chatpartnern. So weit, so alt. Das Besondere an YouNow: Die Internetwelt ist live und ohne Anmeldung dabei. Wer mitplaudern will, kann nach einfacher Anmeldung mit seinem Facebook-, Twitter- oder Google-Account im Chat loslegen oder selbst „broadcasten“ – ganz cool, aber wo ist der Haken?

Vor allem junge Nutzer lassen häufig bewusst oder unbewusst tiefe Einblicke in ihre Privatsphäre zu. Meistens sind sie eindeutig identifizierbar. Es gibt praktisch keine Kontrolle. Das, was vom Nutzer gestreamt und gepostet wird, ist sofort in der Welt. Hinzu kommt: Entsprechend der Datenschutzrichtlinie von YouNow sind jegliche Ersuchen hinsichtlich des Datenschutzes an eine Adresse in New York, USA zu richten. Deutsche, gesetzlich vorgeschriebene Datenschutzstandards sind also kaum durchzusetzen. Zudem haben amerikanische Geheimdienste bei Bedarf den vollen Zugriff auf die Daten.



Der im Jahr 2011 von der YouNow Inc., New York, gegründete Internetdienst (<http://www.younow.com/start>) gewinnt seit Ende 2014 im deutschsprachigen Raum rasant an Bedeutung. Anlass genug für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), sich mit einem Appell an die Tee-

nager zu wenden, um auf die Besonderheiten dieser Art von Selbstdarstellung im Netz aufmerksam zu machen. Dabei ging es ihm nicht darum, den Zeigefinger zu heben und gar ein „YouNow-Verbot“ zu erteilen. Solche digitale Räume gehören selbstverständlich zu unserer Lebenswelt. Vielmehr sollten beim Streamen einige Regeln beachtet werden, um sich nicht ungewollt selbst in Gefahr zu bringen oder Persönlichkeitsrechte anderer zu verletzen. Es geht um ein Stück praktischen Selbstschutz, das ohne viel Aufwand gelebt werden kann.

Die Pressemitteilung des TLfDI vom 20. Februar 2015 (siehe dazu Anlage 53) wurde auch an alle Schulen in Thüringen versandt mit

der Bitte, die YouNow-Problematik im Unterricht aufzugreifen und die praktischen Hinweise in die Klassen zu tragen – auch ein Beitrag des TLfDI zur Medienkompetenzentwicklung der Thüringer Schülerinnen und Schüler. Es bleibt zu hoffen, dass das geschehen ist. Zeitgleich wurde vom TLfDI veranlasst, dass auf dem Thüringer Schulportal ein passendes Video für Jugendliche von einer Mainzer Anwaltskanzlei eingestellt wird. Es wird vom TLfDI für den Einsatz an Thüringer Schulen ausdrücklich empfohlen.

Die Internetplattform YouNow gewinnt seit Ende 2014 im deutschsprachigen Raum rasant an Bedeutung. Sie ermöglicht die Selbstdarstellung in Videostreams und Chats, die unmittelbar von allen Internetnutzern gesehen werden können. Gerade pubertierende Kinder und Jugendliche sollten bei der Nutzung einige Regeln beachten, um sich nicht in Gefahr zu bringen oder Persönlichkeitsrechte anderer zu verletzen.

Der TLfDI gab praktische Hinweise zu YouNow an Schulen und forderte zur aktiven Auseinandersetzung im Unterricht auf.

15.16 Daten gelöscht? – Datenschutzgerechte Entsorgung von Hardware

Seit Jahren muss der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) feststellen, dass bei der Entsorgung oder Weitergabe von PCs, Laptops und Smartphones, aber auch von Festplatten, USB-Sticks und SD-Karten es leider immer noch häufig vorkommt, dass vergessen wird, die darauf befindlichen Daten datenschutzgerecht zu löschen.

Das vollständige Formatieren einer Festplatte oder eines anderen Datenträgers – also die Wiederherstellung des Urzustandes einer Festplatte/eines Speichermediums – ist bspw. zum Löschen ungeeignet,



da nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die Zuverlässigkeit dieser Löschungsmethode keine Aussage getroffen werden kann (siehe Bundesamt für Sicherheit in der Informationstechnik (BSI):

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_cont](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02433.html)

[ent/m/m02/m02433.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02433.html)).



Aus diesem Grund informierte der TLfDI erneut im Februar 2015 per Pressemeldung über die datenschutzrechtlichen Möglichkeiten, Daten auf PCs/Laptops und insbesondere auf Smartphones zu löschen (siehe dazu Anlage 52).

Insbesondere erschien es dem TLfDI wichtig, auch die Löschung von Daten auf

Smartphones zu problematisieren. Auch hierzu gibt das BSI stets aktuelle Empfehlungen unter:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasischutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html.



Bei der Entsorgung oder Weitergabe von PCs, Laptops und Smartphones, aber auch von Festplatten, USB-Sticks und SD-Karten sind jeweils Löschverfahren nach dem neusten Stand der Technik einzusetzen. Diese werden immer aktuell vom Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/DE/Home/home_node.html) veröffentlicht.



Datenschutz – © Marco2811 / Fotolia.com

16 Technische Entwicklung in der Thüringer Landesverwaltung

16.1 Integrierte Teilhabeplanung nun als App

Das damalige Thüringer Ministerium für Soziales, Familie und Gesundheit (TMSFG) hatte in Thüringen die so genannte Integrierte Teilhabeplanung (ITP) eingeführt. Dabei ging es darum, die Ansprüche und Leistungen der Eingliederungshilfe nach § 53 ff. Sozialgesetzbuch (SGB) Zwölftes Buch (XII) für Menschen mit Behinderungen geltend machen zu können. Die Bedarfsermittlung und Hilfeplanung findet im Rahmen des Gesamtplanverfahrens nach § 58 SGB XII statt. Aufgrund der bestehenden fachlichen Anforderungen an ein einheitliches Hilfebedarfsfeststellungsverfahren einigten sich die Kostenträger und die LIGA der freien Wohlfahrtspflege e.V. Ende 2010 darauf, den ITP in Thüringen einzuführen. Gegenstand des ITP ist unter anderem ein Fragebogen zur Ermittlung der Hilfebedarfe von Menschen mit Behinderungen. Die im Fragebogen geforderten Angaben zur materiellen Situation, zu den Vermögenswerten der Hilfeempfänger, zu Familienbeziehungen, Partnerbeziehungen, Beziehungen zu Bekannten oder Freunden, Angaben zur

Religion, Spiritualität und zu Bürgerrechten begegneten aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Bedenken. Nach Aussage des TMSFG waren die geforderten Angaben Inhalt der von der Weltgesundheitsorganisation entwickelten Internationalen Klassifikation der Funktionen (ICF), die Einfluss auf den Hilfebedarf eines Antragstellers sowohl in positiver als auch in negativer Hinsicht haben können. Problematisch war, dass der ITP-Bogen als Grundlage für die Ermittlung von möglichen Teilhabebedarfen ganz verschiedener Zielgruppen dienen sollte und nicht jeder Antragsteller die gleichen Angaben zu machen hatte. Der Bogen sollte vielmehr im Rahmen einer Checkliste entweder gemeinsam mit dem Betreuer oder dem Sachbearbeiter im Sozialamt bearbeitet werden. Der ITP-Bogen sei vielmehr als eine Art Gesprächsleitfaden zu verstehen. Wenn für einen Betroffenen in einem bestimmten Bereich kein Problem und damit auch kein Leistungsanspruch vorlag, musste dieser Bereich auch nicht ausgefüllt und bearbeitet werden. Das barg allerdings Missverständnisse, die eine nicht erforderliche und damit unzulässige Datenerhebung hätten zur Folge haben können. In Abstimmung mit dem TLfDI wurde der ITP überarbeitet. An mehreren Stellen wurde ergänzt, dass bestimmte Angaben nur notwendig sind, wenn sie sich auf die mit dem Sozialarbeiter, mit dem Betroffenen und ggf. seinem Betreuer vereinbarten Ziele zur Integration und ihre Voraussetzungen beziehen. Außerdem wurde vor der Unterschriftszeile nochmals darauf hingewiesen, dass alle gemachten Angaben der Feststellung der Teilhabeleistungen dienen und solche Angaben, die keinen Bezug zu den vereinbarten Zielen haben, nicht erforderlich sind.

Im Anschluss daran wandte sich das TMSFG wiederum an den TLfDI, weil der überarbeitete ITP-Bogen als eigene App im Rahmen des Thüringer Antragsystems für Verwaltungsleistungen (ThA VEL) entwickelt werden sollte. In etlichen Sitzungen mit dem TMSFG und dem für ThA VEL zuständigen Thüringer Finanzministerium (TFM) wurden die Möglichkeiten des Betriebs von ITP als App in dem System ThA VEL beraten. Im Rahmen von ThA VEL wurde im Ergebnis eine neue App entwickelt, die die Bearbeitung des ITP-Bogens auf elektronischem Weg ermöglicht. Hierzu war insbesondere wichtig festzulegen, welche Rollen es im System gibt und welche Rechte diese Rollen jeweils haben. Nicht nur der zuständige Sozialarbeiter sollte Zugriff auf das System haben, sondern eingeschränkt auch bestimmte Leistungserbringer wie Wohnheime oder Werkstät-

ten, in denen die Betroffenen tätig waren. Keinesfalls durfte die App so gestaltet werden, dass jeder jederzeit Zugriff auf alle Daten hat; vielmehr sollten nach dem Grundsatz der Erforderlichkeit die Rechte so vergeben werden, dass immer nur derjenige Zugriff auf die Daten hat, der diese gerade für seine Aufgabenerfüllung benötigt. Die erforderlichen technischen und organisatorischen Maßnahmen wurden in Abstimmung mit dem TLfDI getroffen. Vorgesehen war, dass einige Sozialämter als Modellprojekt die ITP als App prüfen sollten. Im kommenden Berichtszeitraum wird der TLfDI die Verwendung der ITP-App vor Ort kontrollieren und prüfen, ob die schriftlich festgelegten Zugriffsrechte und sonstigen Berechtigungen in der Praxis so vorgenommen worden sind, wie sie schriftlich im Sicherheitskonzept fixiert wurden.

Der Weg der elektronischen Datenverarbeitung hat in allen Bereichen der Verwaltung Einzug gehalten. Immer mehr Antragsverfahren werden zukünftig elektronisch abgewickelt werden. Dabei ist es sehr wichtig, darauf zu achten, dass alle beteiligten Stellen nur die Zugriffsrechte auf personenbezogene Daten erhalten, die sie tatsächlich für ihre Aufgabenerfüllung benötigen. Es ist ratsam, den TLfDI im Vorfeld bei der Einführung solcher Verfahren zu beteiligen, damit alle datenschutzrechtlichen Anforderungen eingehalten werden.

16.2 Optimierung eines Beihilfe-Kontrollverfahrens oder fragwürdiger Zugriff auf personenbezogene Daten von BALVI iP?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt im Berichtszeitraum Kenntnis darüber, dass die Zahlstelle des Thüringer Landesverwaltungsamtes (TLVwA) im Zusammenhang mit Fachkontrollen der zuständigen Veterinärämter einen Abgleich auch personenbezogener Daten von Tierhaltern u. a. zu Kontrollergebnissen und festgestellten Mängeln durchführte, die in der Fachsoftware BALVI iP – diese unterstützt behördliche Kontrollen lebensmittelrechtlicher Vorschriften in überwachungspflichtigen Betrieben – gespeichert wurden. Mit diesen Zugriffen bekäme die Zahlstelle des TLVwA möglicherweise auch Kenntnis von personenbezogenen Daten von Tierhaltern, die keine EU-Fördergelder erhielten. Demgegenüber sei den Veterinärämtern bei Einführung von BALVI iP zugesagt worden, dass

keine Zugriffe anderer Behörden auf die Daten der Veterinärämter erfolgen sollte, da allein die zuständigen Fachaufsichtsbehörden, das Thüringer Landesamt für Verbraucherschutz und das Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie hierzu befugt seien.

Der TLfDI bat das TLVwA mitzuteilen, zu welchem Zweck die Zahlstelle des TLVwA einen solchen Datenabgleich durchführte und auf welcher Rechtsgrundlage dieses Vorgehen beruhte. Daraufhin teilte das TLVwA dem TLfDI mit, dass es nicht anstrebe, einen Zugriff auf die Fachsoftware BALVI iP zu erhalten. Es würde lediglich versucht, zu analysieren, wie die Vollständigkeit des Kontrollverfahrens zur Vermeidung ungerechtfertigter Agrarbeihilfen sichergestellt werden kann. Die Unvollständigkeit des Kontrollverfahrens beruhe darauf, dass nicht jeder Verstoß gegen die Cross Compliance-Anforderungen – hierbei wird die Zahlung von Agrarbeihilfen von der Einhaltung von Standards des Umwelt-, Lebensmittel-, und Verbraucherschutzes abhängig gemacht – in der Fachsoftware BALVI iP dokumentiert werde.

Abschließend stellte der TLfDI gegenüber dem TLVwA fest, dass es nicht die Aufgabe der Zahlstelle des TLVwA sein könne, die ordnungsgemäße Aufgabenerledigung der Veterinär- und Lebensmittelüberwachungsämter zu überwachen. Diese Beurteilung beruht darauf, dass die Voraussetzungen des § 4 Thüringer Datenschutzgesetz (ThürDSG), wonach die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig ist, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffenen eingewilligt hat, hier nicht vorlagen. Insofern durfte die Zahlstelle des TLVwA nicht zum Zwecke der Überwachung der ordnungsgemäßen Aufgabenerledigung der Veterinär- und Lebensmittelüberwachungsämter auf Daten der Fachsoftware BALVI iP zugreifen.

Da es sich in diesem Falle vorrangig um ein Zuständigkeits- bzw. Organisationsproblem handelte, regte der TLfDI an, in Zusammenarbeit mit Veterinärämtern und ggf. dem TLVwA eine geeignete technisch-organisatorische Lösung zu erarbeiten, die künftig unberechtigte Zahlungen von Agrarbeihilfe auszuschließen, die Verantwortlichkeiten im Kontrollverfahren klar definieren und dabei den gesetzlichen Anforderungen des Datenschutzes und der Datensicherheit Rechnung trage.

Der TLfDI ist auch „Reparaturbetrieb“ für Zuständigkeits-, Organisations- oder Softwareprobleme mit direktem Datenschutzbezug. Seine Aufgabe ist es, in solchen Fällen darüber zu wachen, dass die beteiligten Stellen beim Versuch, die genannten Mängel zu kompensieren, nicht gegen datenschutzrechtliche Bestimmungen verstoßen, und ggf. Empfehlungen zu grundlegenden Lösungsansätzen zu geben.

16.3 Oben ohne – Drohne!

Das Thüringer Innenministerium teilte zur Kleinen Anfrage der Abgeordneten König vom 11. Februar 2014 u. a. mit, dass der Freistaat Thüringen über keine eigenen Drohnen bzw. unbemannte Luftfahrzeugsysteme verfüge und dass die Landesforstverwaltung im Rahmen einzelner operativer Fernerkundungsaufgaben Drohnen von Dienstleistern einsetze (Landtagsdrucksache 5/7689).

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) recherchierte daraufhin, dass Thüringen Forst als Anstalt des öffentlichen Rechts Drohnen in verschiedenen Forstämtern zu Testflügen für folgende Zwecke eingesetzt hat:

- zur Kartierung des Borkenkäferbefalls, zur Bilderfassung für das Forsteinrichtungsverfahren, zur Kartierung der Flächenveränderungen nach dem Orkan Kyrill und für Folgemaßnahmen sowie
- zu den Forschungsprojekten Baumartenerkennung, Kronenkartierung, Biodiversitäts-Exploratorien, Kartierung von Baum- und Deichschäden am Leina-Kanal, die durch den Orkan Kyrill verursacht wurden (als Grundlage für ein entsprechendes Planungsverfahren) und zum EU-Forschungsprojekt „BioTree“ zur Dokumentation und Kontrolle von Anwuchs verschiedener Baumarten auf einer forstlichen Versuchsfläche.

Bei diesen Drohnen wurden handelsübliche digitale Kleinbildkameras eingesetzt, jedoch keine Infrarot- und Wärmebildsensoren, die jedoch für bestimmte forstliche Fragestellungen (z. B. Erkennung von Bäumen mit Vitalitätsverlust auf den Color-Infrarot-Bildern im mittleren Infrarot-Kanal oder Wildzählungen mit Thermal-Infrarot-Kameras) geeignet seien.

Programme zur Gesichtserkennung oder WiFi-Sniffer (= Programme zum Auffinden von drahtlosen Rechnernetzen) seien für die Aufga-

ben der Forstverwaltung ohne Interesse und daher weder erprobt noch eingesetzt worden. Nach weiteren Recherchen stellte der TLfDI abschließend fest, dass die von den Flugdrohnen der Landesforstverwaltung gefertigten Aufnahmen keinen Personenbezug aufwiesen. Daher bestanden aus der Sicht des TLfDI in diesem konkreten Fall auch keine datenschutzrechtlichen Bedenken.

Darüber hinaus befragte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum 25 Thüringer Städte mit einer Bevölkerungszahl von über 25.000 Einwohnern danach, ob ihre Stadtverwaltungen derzeit Flugdrohnen nutzen oder ob deren Nutzung vorgesehen sei. Sämtliche angeschriebene Stadtverwaltungen setzten den TLfDI darüber in Kenntnis, dass sie weder Flugdrohnen nutzten noch planten, diese einzusetzen.

Der TLfDI hat am 30. Januar 2015 die Pressemitteilung „TLfDI fordert: Deutschland oben ohne – Drohne!“ veröffentlicht, die auf der Internetseite des TLfDI abrufbar ist (siehe dazu Anlage 51).

Nach den Recherchen des TLfDI steht fest, dass derzeit weder von der Polizei noch von den Landesbehörden oder den Kommunen Drohnen eingesetzt werden, die personenbezogene Daten erheben. Dennoch steht das Thema „Drohneneinsatz“ angesichts des rasanten technischen Fortschritts und der hohen Aussagekraft von Luftaufnahmen unverändert auf der datenschutzrechtlichen Agenda des TLfDI.

16.4 Heimarbeit für Finanzbeamte

Bereits seit Herbst 2008 besteht für den gesamten Außendienst der Steuerverwaltung (Betriebs-, Lohnsteueraußen- und Umsatzsteuer-sonderprüfer) die Möglichkeit der Inanspruchnahme eines Heimarbeitsplatzes. Voraussetzung für die Genehmigung eines Heimarbeitsplatzes nach der „Rahmendienstvereinbarung zur Einführung von Heimarbeit im Geschäftsbereich des Thüringer Finanzministeriums“ ist neben sicherheitstechnischen Voraussetzungen auch die Einhaltung der datenschutzrechtlichen Vorschriften. Nachdem dies im Jahr 2011 an den Heimarbeitsplätzen von Beauftragten der Finanzämter überprüft worden war, keine Mängel vorlagen und die Einrichtung der Heimarbeitsplätze auch von Seiten der Heimarbeiter sehr positiv angenommen worden war, wurde die Möglichkeit zur

Heimarbeit auf die Kraftfahrttechnischen Beamten und Forstwirtschaftlichen Sachverständigen erweitert. Der eindeutige Vorteil dieser Arbeitsform ist, dass die Beamten weder vor noch nach Erledigung ihrer Aufgaben im Außendienst vor Ort die Dienststelle aufsuchen müssen. Das spart Fahrzeiten und trägt zur Effizienz bei.

Anhand der inhaltlichen Beschreibung der Tätigkeit dieses Beschäftigtenkreises ging der TLfDI davon aus, dass die Dienstposten die typischen Charakteristika der heimarbeitsauglichen Außendiensttätigkeiten in der Finanzverwaltung aufwiesen und hatte keine datenschutzrechtlichen Bedenken, zumal die erforderlichen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben nach § 9 Thüringer Datenschutzgesetz (ThürDSG) getroffen waren. Die wichtigsten Voraussetzungen aus dem datenschutzrechtlichen Blickwinkel sind, dass für unbefugte Dritte keine Möglichkeit der Kenntnis dienstlicher personenbezogener Daten bestehen darf. Das heißt, dass beispielsweise Familienangehörige, Mitbewohner und Besucher des „Heimarbeiters“ keinesfalls Zugang zu dienstlichen Angaben haben dürfen. Hierfür haben zum einen die Dienststelle und andererseits der „Heimarbeiter“ selbst zu sorgen. Hiervon hat sich die Dienststelle regelmäßig zu überzeugen. In der erforderlichen Dienstvereinbarung ist dies konkret auszuführen.

Im Jahr 2015 wurde nun dieses Arbeitsmodell der Heimarbeit auch auf die Dienstposten der Liquiditätsprüfer in den Finanzämtern ausgeweitet werden. Die Tätigkeiten des Beschäftigtenkreises bedingen nicht zwingend eine Erledigung in den Diensträumen der Beschäftigtenbehörden. Unter der Voraussetzung, dass an den Heimarbeitsplätzen die technischen und organisatorischen Maßnahmen zur Gewährleistung der Einhaltung der datenschutzrechtlichen Vorschriften nach § 9 ThürDSG getroffen sind, bestanden auch hiergegen keine Bedenken.

Auch bei Heimarbeit sind wie in der Dienststelle selbst die erforderlichen technischen und organisatorischen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften zu treffen. Insbesondere ist die Möglichkeit der Kenntnisnahme dienstlicher Daten durch unbefugte Dritte auszuschließen.

16.5 Windows XP – baufällig ...

Seit dem 8. April 2014 werden vom Hersteller Microsoft Corporation (Microsoft) für das Betriebssystem Windows XP auch keine Sicherheits-Updates mehr für den erweiterten Support geliefert. Microsoft hatte diesen Fakt bereits Ende 2002 angekündigt und grundlegende Supports schon 2009 eingestellt. Immerhin war das Betriebssystem dreizehn Jahre alt.

Dies birgt für Benutzer, die das Betriebssystem weiterhin benutzen, erhebliche Risiken. Zu vergleichen ist das mit einem alten, maroden Haus, in dem nun die immer wieder eingeworfenen Fensterscheiben nicht mehr mit neuem Sicherheitsglas ausgerüstet werden. Nur so kann ein Glaser (gemeint: der Software-Hersteller Microsoft) dem Zahn der Zeit (gemeint: dem Stand der technischen Entwicklung) trotzen und dem Verfall Einhalt gebieten.

Wo liegen die Probleme?

Aufgrund der fehlenden Sicherheits-Updates durch Microsoft sind personenbezogene Daten auf Windows-XP-Rechnern einem unverantwortlich hohen Risiko möglicher Hacker-Angriffe ausgesetzt.

Nachdem der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr, dass trotz der Abkündigung von Windows XP ein Jahr später immer noch Windows-XP-Rechner im Einsatz sein könnten, wandte sich der TLfDI an das Thüringer Innenministerium als kommunale Aufsichtsbehörde mit der Bitte, die Kommunen auf die Risiken beim Einsatz von Windows XP hinzuweisen. Dieses wurde auf wiederholtes Bitten viele Monate später umgesetzt.

Zum anderen wies der TLfDI die obersten Landesbehörden auf die entsprechenden Gefahren hin. Er bat um Rückinformationen, wie viele PCs in den Ressorts noch mit dem alten Betriebssystem arbeiteten. Wenn mit solchen Rechnern noch personenbezogene Daten verarbeitet würden, sollten diese Rechner in der Thüringer Landesverwaltung dringend umgestellt bzw. abgeschaltet werden.

Im Ergebnis teilten die Ministerien für sich und ihre jeweils nachgeordneten Bereiche mit, dass die Windows-XP-Rechner zum Großteil zeitnah abgelöst werden sollen. Allerdings werden – selbst bei Einhaltung der Zeitpläne der Ministerien – nach Redaktionsschluss des vorliegenden Tätigkeitsberichtes ca. 300 Windows-XP-Rechner in der Thüringer Landesverwaltung im Einsatz sein. Davon werden die meisten in Entwicklungs- bzw. Servicebereichen, in der Lehre oder

aber als Messplatz-PCs unter sehr speziellen Einsatzbedingungen verwendet. Hauptgrund dafür ist, dass einige Systeme wegen Software-Unverträglichkeiten (fachenglisch: Inkompatibilität) – insbesondere bei verwendeten älteren Fachverfahren oder aber in medizinischen Geräteumgebungen – nicht mit den neueren Betriebssystemen zusammenarbeiten. Hier müssen Kompromisse geschlossen und Übergangslösungen gefunden werden.

Sollen XP-Rechner weiterhin im Einsatz verbleiben, so ist es notwendig, sie in so genannten abgeschotteten Systemen zu betreiben. Das sind solche Systeme, in denen das Betriebssystem über Browserfunktionen beispielsweise keine aktive Verbindung zum Internet herstellt. Um die Funktionsfähigkeit als abgeschottete Systeme zu gewährleisten, sind explizit technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen zu treffen. Nur so können Sicherheitsrisiken minimiert werden. Eine dieser TOM ist, Einstellungen im Browser oder am Proxy so vorzunehmen, dass der PC keine Internetverbindung aufbauen kann. Aber auch organisatorische Regelungen, wie beispielsweise Dienstanweisungen, zählen zu den TOM. Darin sollte eindeutig vorgeschrieben werden, dass keine Windows-XP-Rechner mehr einen Internetzugang besitzen dürfen und zeitnah ausgetauscht werden sollten. Bei Windows-XP-Rechnern, die wegen spezieller Fachverfahren derzeit immer noch nicht einfach umgestellt werden können, bedarf es zusätzlich einer konkreten Planung mit dem Hersteller dieser Fachverfahren-Software, um die Umstellung der alten auf neuere Software zeitnah zu realisieren.

Mittelfristig bleibt im übertragenen Sinne zum Abriss des alten, maroden Hauses jedoch keine zukunftsorientierte Alternative. Das Betriebssystem Windows XP ist deshalb zeitnah und flächendeckend durch neuere Betriebssysteme zu ersetzen. Dies wurde auch von den obersten Landesbehörden erkannt und eine Umstellung mittelfristig zugesichert.

Das Client-Betriebssystem Windows XP erhält seit April 2014 im erweiterten Support keine Sicherheits-Updates mehr. Es ist daher durch neuere Client-Betriebssysteme zu ersetzen. Wo dies aus zwingenden Gründen nicht geschehen kann, müssen angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM) bei den verantwortlichen Stellen getroffen werden, um die Sicherheitsrisiken auszuschließen.

16.6 Die Telemedizinplattform Thüringen – ein Blick in die Zukunft der Patientenversorgung

An vielen Stellen werden heutzutage Patientendaten gespeichert: beim Hausarzt, bei Fachärzten, in Krankenhäusern und bei Rehabilitations- oder Pflegeeinrichtungen. Für bestimmte Krankheitsbilder müssen diese verteilten Informationen über den Patienten zusammengeführt werden, um ein korrektes Krankheits- und Therapiebild zu erhalten und eine geeignete Behandlung durchführen zu können. Dies geschieht bisher auf dem klassischen Weg des Arztbriefes, der an andere Beteiligte verschickt wird.

Das Forschungsprojekt „Telemedizinplattform Thüringen“ beschäftigt sich genau mit diesem Aufgabenfeld, nämlich wie dezentral gespeicherte Patientendaten elektronisch über eine einheitliche Oberfläche abgerufen werden können, um so zu einer besseren interdisziplinären Behandlung für zum Beispiel Demenzpatienten zu gelangen. Am Forschungsprojekt sind unter anderem das Universitätsklinikum Jena und die Technische Universität Ilmenau beteiligt.

In der letzten Phase des Forschungsprojektes wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontaktiert und darum gebeten, die vorgestellte Lösung kritisch zu hinterfragen. Kern des Projektes ist eine dezentrale Infrastruktur. Das heißt, hier werden in vielen gleichartig konstruierten Knotenpunkten Patientendaten gesammelt. Ein Knoten könnte ein Krankenhaussystem sein oder das Computersystem einer Pflegeeinrichtung. Ärzte und Hausärzte können über den Webbrowser Daten wie Diagnosen, Medikationspläne und Ähnliches in einem solchen Knoten speichern. In welchem Knoten die Daten gespeichert werden und wer auf diese Daten in welcher Form Zugriff haben darf, wird bei der Konfiguration des jeweiligen Arzt-Zugangs durch das Zugriffs- und Berechtigungskonzept der Telemedizinplattform individuell festgelegt. Zudem sind in keinem Knoten *alle* Patientendaten gespeichert – auch nicht als Kopie. Jeder Knoten funktioniert für sich als Informationsquelle und kann auch lokal genutzt werden, aber er kann von sich aus keine Patientendaten anderer Knoten anzeigen. Um dies sicherzustellen, gibt es zusätzlich ein übergeordnetes Kontrollsystem, welches die Zugriffsrechte netzwerkübergreifend regelt und kontrolliert. Anfragen von einzelnen Knotenpunkten oder den externen Rechnern der Hausärzte werden über die Kontrolleinheit

bewertet und entsprechend den Zugriffsrechten die Dateneinsichten ermöglicht. Der TLfDI bewertete innerhalb des Forschungsprojektes vor allen Dingen die Sicherheitsarchitektur und inwieweit die einzelnen Knotenpunkte als daten tragende Stellen gegeneinander vor unrechtmäßiger Kenntnisnahme gesichert waren. Außerdem wurden die Datenflüsse zum Zusammenspiel aller Knotenpunkte und der übergeordneten Kontrolleinheit analysiert sowie die Rechtevergabe für behandelnde Ärzte und das Rechtemanagement untersucht. Im Rahmen des Forschungsprojektes gab es dabei bisher keine Auffälligkeiten. Der TLfDI wird das Forschungsprojekt auch weiterhin begleiten. Allen Beteiligten ist hierbei bewusst, dass das Datenschutzrecht an Forschungsprojekte wesentlich niedrigere Anforderungen stellt als an ein marktreifes Produkt.

Auch bei Forschungsprojekten sind datenschutzrechtliche Anforderungen zu beachten. Bei solchen Neuentwicklungen ist insbesondere „Privacy-by-Design“ gleich zu Beginn zu berücksichtigen. Im vorliegenden Fall wurde dabei auf eine ausreichende Abgrenzung einzelner Teilsysteme geachtet sowie auf das Rollen- und Rechtekonzept und die technischen und organisatorischen Maßnahmen.



update – © Marco2811 / Fotolia.com

17 Vorträge – Der TLfDI ist unterwegs!

Ob Datenschutz in der Schule, bei Gericht, bei Behörden, Hochschulen, Fraktionen oder Parteien, datenschutzrechtliche Themen sind in aller Munde und bewegen die Öffentlichkeit. Indikatoren sind nicht nur die vielfältigen Eingaben von Bürgerinnen und Bürgern, sondern vor allem auch das gesteigerte Interesse der Medien an datenschutzrechtlichen Themen aller Art. Es vergeht kaum ein Tag, an dem der Schutz der persönlichen Daten nicht in den Nachrichten oder Medien auftaucht. Fast täglich kommen Anfragen über die Poststelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herein, ob der TLfDI nicht mit einem „Rundum-sorglos-Paket“ für Datenschutz an Materialien und Referenten die eine oder andere bereits geplante Veranstaltung durch seine Vorträge unterstützen kann. Der TLfDI selbst und einige seiner Mitarbeiter haben im Berichtszeitraum an mehr als **50 (!)** Diskussions- und Vortragsveranstaltungen teilgenommen und dabei über datenschutzrechtliche Themen referiert. Eine Auswahl der Vorträge im öffentlichen Bereich finden Sie ab Anlage 69.

Nicht verzagen, TLfDI fragen! Der TLfDI freut sich über das gesteigerte Interesse am Schutz der in der Tat bedrohten Privatsphäre und versucht, im Rahmen seiner Möglichkeiten, die Bürgerinnen und Bürger, die Mitarbeiter der Schulen und Unternehmen für das Thema Datenschutz in Thüringen zu sensibilisieren und über den neusten Stand seiner Erkenntnisse zu informieren.

Anlagen

Anlage 1

Entschlieung

der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 27./28. Mrz 2014 in Hamburg

Beschftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag fr die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschftigtendatenschutz bei den Verhandlungen zur Europischen Datenschutzgrundverordnung zu erhalten und darber hinausgehende Standards zu ermglichen. Falls mit einem Abschluss der Verhandlungen ber die Europische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit vllig unklar. Ohnehin ist mit einem Inkrafttreten dieser europischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterberwachung ermglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder fordert die Bundesregierung deshalb auf, ein nationales Beschftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lsst befrchten, dass der Beschftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird. Ein Beschftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewhrleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem

Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

Anlage 2

Entschlieung

der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 27./28. Mrz 2014 in Hamburg

„Gewhrleistung der Menschenrechte bei der elektronischen
Kommunikation“

Die Enthllungen des Whistleblowers Edward Snowden haben ein Ausma an geheimdienstlicher berwachung aufgezeigt, das viele zuvor nicht fr mglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte berwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in tglich wiederkehrender millionenfacher Weise. Dies beeintrchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Lnder haben daher schon im September 2013 gefordert, auf diese neue Qualitt der berwachung rechtlich und politisch zu reagieren. Darber hinaus sind aber auch technische und organisatorische Schutzmanahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integritt informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder fordert daher die Prfung und Umsetzung folgender Manahmen:

1. Sichere Verschlsslung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlsslungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlsslung in Kombination mit Verfahren zur Verbindungsverschlsslung,

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser EntschlieÙung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage 3

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

„Gewährleistung der Menschenrechte bei der elektronischen
Kommunikation“

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten

Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographische Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich. Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur

Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderen zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises. Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken

selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung

Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden. Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten

Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten

Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. Ausbau der Angebote und Förderung anonymer Kommunikation

Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. Angebot für eine Kommunikation über kontrollierte Routen

Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggfs. die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird. Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten – dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden

und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen. Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können. Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

- alle Übertragungswege – sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,
- für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgeschiffre zur Verfügung steht,
- eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und
- die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken. Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen. Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Er-

hebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud-Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik

Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist. Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung

Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern. Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik

Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsinitiative erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit

Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

Anlage 4

Entschlieung

der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 27./28. Mrz 2014 in Hamburg

„ffentlichkeitsfahndung mit Hilfe sozialer Netzwerke –
Strenge Regeln erforderlich!“

Mit zunehmender Beliebtheit sozialer Netzwerke bei Brgerinnen und Brgern steigt das Interesse von Strafverfolgungsbehrden, diese sozialen Netzwerke auch zur ffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Strafttern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder hlt es erneut fr notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur ffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Verffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdchtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet verffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu lschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren ffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeintrchtigt dies die Persnlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehrden betriebenen Angeboten weder geeignet noch erforderlich, um die behrdlichen Aufgaben zu erfllen. Die Konferenz weist darauf hin, dass ffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gem §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gem § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.
- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.
- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.
- Es ist sicherzustellen, dass
 - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert

und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Anlage 5

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

EntschlieÙung der Konferenz der Datenschutzbeauftragten des
Bundes und der Länder zur Struktur der künftigen
Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.
2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-

Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.
4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.
5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.
6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehörd-

licher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

Anlage 6

Entschlieung

der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 27./28. Mrz 2014 in Hamburg

„Biometrische Gesichtserkennung durch Internetdienste – Nur mit
Wahrung des Selbstbestimmungsrechts Betroffener!“

Die Nutzung biometrischer Daten wird zunehmend zu einem Phnomen des Alltags. Dies gilt in besonderer Weise fr die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Fr den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein spterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Ma die schutzwrdigen Interessen Betroffener berhrt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthllungen ber das berwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko fr das Persnlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausbung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es mglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darber hinaus knnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymitt des Einzelnen in der ffentlichkeit lsst sich damit zerstren, ohne dass

die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4 a BDSG rechtmäßig erfolgen.
- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4 a Abs. 3 BDSG, entspricht.
- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.
- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

Anlage 7

Forderungen

der 87. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 28. März 2014 in Hamburg

Unsere Daten sicherer machen - wir selbst haben es in der Hand!

Die bisherigen rechtlichen und politischen Reaktionen auf das massenhafte Ausspähen der Kommunikation durch Nachrichtendienste sind enttäuschend. Das zeigt exemplarisch die Diskussion um das No-Spy-Abkommen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die am 27. und 28. März 2014 in Hamburg stattfindet, fordert deshalb alle staatlichen und gesellschaftlichen Akteure dazu auf, die Grundrechte der Bürgerinnen und Bürger durch technische und organisatorische Maßnahmen wirksam zu schützen. Die Unversehrtheit der freien und geheimen Kommunikation muss wieder hergestellt werden. Dies erfordert vor allem die Bereitstellung einer von jeder Person einfach nutzbaren Verschlüsselungsinfrastruktur. Sie gilt es insbesondere bei der Kommunikation zwischen Bürger und Verwaltung vorzuhalten. Neben der standardisierten Verschlüsselung beim Transport von Daten muss auch der Einsatz von Mechanismen der Ende-zu-Ende-Verschlüsselung angeboten werden. Außerdem sollten die Angebote zur anonymen Kommunikation sowie die Vertrauenswürdigkeit von Hard- und Software durch Einsatz von Zertifizierungsverfahren ausgebaut werden. Diese Maßnahmen erfordern nicht nur eine Sensibilisierung und Aufklärung der Nutzerinnen und Nutzer durch eine Bildungsoffensive, sondern müssen auch durch eine ausreichende Finanzierung ermöglicht werden.

Hierzu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und amtierender Vorsitzender der Datenschutzkonferenz: „Wir haben es selbst in der Hand, durch die Schaffung einer sicheren IT-Infrastruktur die Hürden für eine massenhafte anlasslose Überwachung unserer Kommunikation durch die Nachrichtendienste wesentlich zu erhöhen. Gerade wenn die politische Kraft nicht ausreicht, den Schutz der Grundrechte auf internationaler Ebene wiederherzustellen, ist die Errichtung technisch organisatorischer Schutzmaßnahmen alternativlos.“

Mit einer EntschlieÙung zur biometrischen Gesichtserkennung durch Internetdienste fordern die Datenschutzbeauftragten zudem, dass die Verarbeitung biometrischer Merkmale der Gesichter der Nutzer in sozialen Medien nur mit der ausdrücklichen und informierten Einwilligung der Betroffenen erfolgen darf. Die individuellen Gesichtsbilder der Nutzerinnen und Nutzer werden bei diesen Verfahren dauerhaft und reproduzierbar millionenfach gespeichert. Das Missbrauchspotential derartiger Gesichtsdatabanken ist immens. Das informationelle Selbstbestimmungsrecht der Betroffenen muss daher bei der Erhebung und Verarbeitung dieser unveränderbaren biometrischen Daten in jedem Fall gewahrt werden.

Die polizeiliche Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke darf künftig nur unter Beachtung strenger Vorgaben erfolgen. Diese Art der Veröffentlichung von Fahndungsdaten greift nicht zuletzt wegen der größeren Reichweite deutlich intensiver in die Grundrechte ein als die herkömmliche Öffentlichkeitsfahndung. Davon sind unter Umständen nicht nur die mutmaßlichen Täter betroffen, sondern auch Zeugen. Die Datenschutzbeauftragten fordern daher unter anderem, dass eine Speicherung der Fahndungsdaten nur auf den Servern der Polizei erfolgen darf. Entscheidend ist zudem, dass die Fahndung nicht als Aufruf zu Hetzjagden und Selbstjustiz im Internet führt. Dazu muss die Kommentierungsfunktion zwingend deaktiviert sein.

Dazu Imke Sommer, die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen: „Das letzte Jahr hat uns allen die Augen dafür geöffnet, in welchem hohem Maße unser Grundrecht auf informationelle Selbstbestimmung von den großen Datensammlern und allen, die die von ihnen angehäuften Datenberge nutzen, verletzt wird. Wir dürfen jetzt nicht darin nachlassen, alle, die zum Schutz unserer Rechte handeln können, dazu zu bringen, dies auch tatsächlich zu tun.“

Die Datenschutzkonferenz hat die langjährige Forderung zur Schaffung eines nationalen Beschäftigtendatenschutzgesetzes erneut erhoben. Gesetzgeber und Regierung sind aufgefordert, angesichts des Einsatzes mannigfaltiger digitaler Technologien am Arbeitsplatz für einen hinreichenden Datenschutz der Arbeitnehmer und Arbeitnehmerinnen zu sorgen. Die immer stärkere Vermischung von Arbeit und Privatem durch die Nutzung von Handy, Laptop und Dienstwagen mit GPS, aber auch die immer weiter um sich greifende Video-

überwachung am Arbeitsplatz müssen künftig rechtssicher geregelt werden.

Schließlich begrüßt die Datenschutzkonferenz den Entwurf einer Europäischen Datenschutzgrundverordnung, fordert aber in der „Entschließung zur künftigen Struktur der Aufsichtsbehörden in Europa“ Nachbesserungen. Hierbei bekräftigt sie insbesondere den Grundsatz, dass jede Aufsichtsbehörde zur Kontrolle von datenschutzrechtlichen Verstößen befugt ist, wenn Bürgerinnen und Bürger des jeweiligen Mitgliedstaats betroffen sind. Bei grenzüberschreitender Datenverarbeitung soll die Aufsichtsbehörde am Ort der Hauptniederlassung nur federführend tätig werden und eng mit den anderen Aufsichtsbehörden kooperieren. In Streitfällen sollte der Europäische Datenschutzausschuss verbindlich entscheiden.

Andrea Voßhoff, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, unterstreicht: „Eine effiziente Datenschutzaufsicht nahe an den Bürgerinnen und Bürgern muss auch in Zukunft gesichert sein.“

Entschließungen zwischen den Konferenzen 2014

Keine Vorratsdatenspeicherung in Europa!- Neue Maßstäbe für den Datenschutz (Umlaufentschließung vom 25. April 2014)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat in einer heutigen Entschließung das Urteil des Europäischen Gerichtshofs (EuGH) zur Europäischen Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) als wegweisend für den Datenschutz in Europa gewürdigt.

Der EuGH erteilt einer anlasslosen und umfassenden Speicherung von Verkehrsdaten eine klare Absage und stützt damit das Recht auf Privatleben und den Datenschutz aller Betroffenen in der EU. Eine undifferenzierte Pflicht zur flächendeckenden Vorratsdatenspeicherung wird sich danach unionsrechtlich nicht mehr begründen lassen. Die Äußerung der Bundesregierung, gegenwärtig keinen nationalen Alleingang zu einer Regelung zur Vorratsdatenspeicherung zu unternehmen, erscheint daher konsequent und ist zu begrüßen.

Dass der EuGH im Übrigen die Pflicht zur umfassenden Verkehrsdatenspeicherung nur für zulässig hält, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen, macht aus Sicht der DSK eine Neubewertung insbesondere der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens erforderlich. Darüber hinaus setzt der Maßstab des EuGH auch der anlasslosen exzessiven Überwachung durch Nachrichtendienste Grenzen.

Dazu Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit und amtierender Vorsitzender der DSK: „Das Urteil des EuGH festigt die digitalen Grundrechte in Europa gerade zu einer Zeit, in der sie durch Nachrichtendienste systematisch außer Kraft gesetzt werden. Nun gilt es, Konsequenzen aus der Entscheidung zu ziehen. Dabei geht es nicht nur um die Vermeidung undifferenzierter Regelungen zur Vorratsdatenspeiche-

rung. Die EU-Organe wie auch die Mitgliedstaaten sollten darüber hinaus das Urteil zum Anlass nehmen, künftig der massenhaften Vorratsdatenspeicherung durch Nachrichtendienste außerhalb, aber auch innerhalb der EU mit aller Entschiedenheit entgegenzutreten. Nur so wird das Grundrecht auf Datenschutz den Platz einnehmen können, der ihm durch den EuGH gewiesen wurde.“

Anlage 9

Entschlieung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 8./9. Oktober 2014 in Hamburg

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthllungen ber die Sphaktivitten auslndischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Lnder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehrden. Die Befugnisse der Nachrichtendienste schlieen auch die berwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit auslndischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingefhrt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehrden errichtet. Die Berichte der NSU-Untersuchungsausschsse des Deutschen Bundestages und einiger Landesparlamente haben darber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzmtern offengelegt. Nach der Einschtzung der Konferenz der Datenschutzbeauftragten des Bundes und der Lnder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Fr die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehrden vorgenommene Datenverarbeitung in weitem Mae intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschrnkt. Umso wichtiger ist die Kontrolle durch unabhngige Stellen. In der Entscheidung zum Antiterrorda-

teigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Anlage 10

Entschliebung

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

Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen DoubleClick. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und

den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

Anlage 11

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

Unabhängige und effektive Datenschutzaufsicht für
Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen(siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der

Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes – und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung

- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit aus reichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.
- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

Anlage 12

Entschlieung
der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 8./9. Oktober 2014 in Hamburg

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von
Suchmaschinen

Der Europische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persnlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persnlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Eintrge ber eine unbegrenzte Zeit hinweg abrufbar. Sie knnen dann zu sozialen und wirtschaftlichen Nachteilen fr die Betroffenen fhren, die ggf. ein Leben lang mit frheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Knftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprche unmittelbar gegenber den Informationsanbietern zu verfolgen, die hufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene knnen sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen knftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu lschen oder ihre Auffindbarkeit im Internet unmglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugnglich (fr Inhalte, die regelmig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des ffentlichen Lebens handelt, hat der EuGH ausdrcklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte der Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.
- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie

auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.
- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Entschlieung

der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 8./9. Oktober 2014 in Hamburg

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Der Konferenz der Datenschutzbeauftragten des Bundes und der Lnder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten fr die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefhrdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergerten und nicht erst mit deren Auslesen oder bermitteln. Bereits diese personenbezogenen Daten geben Auskunft ber Fahrverhalten und Aufenthaltsorte und knnen zur Informationsgewinnung ber den Fahrer bzw. den Halter bis hin zur Bildung von Persnlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor berwachung zu gewhrleisten, sind Automobilhersteller, Hndler, Verkufer, Werksttten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewhrleisten.

Dazu gehrt:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote fr Kommunikations- und Teledienste die Datenschutzgrundstze von privacy-by-design bzw. privacy-by-default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.
- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.
- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.
- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Pressemitteilung

der 88. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 9. Oktober 2014 in Hamburg

Datenschutz erfordert unabhängige Kontrollbehörden

Ob private Unternehmen oder staatliche Stellen – das Recht auf informationelle Selbstbestimmung braucht handlungsmächtige Kontrollinstanzen

Personenbezogene Daten treten immer stärker in den Fokus von öffentlichen und privaten Stellen, die sie in großem Stil erfassen, speichern und verarbeiten. Dabei wird häufig die Sammelwut nur durch die technischen Möglichkeiten begrenzt; ein Ende ist nicht abzusehen. Immer schwerer wird es, der digitalen Technik und der Kapitalisierung von Daten die begrenzende Funktion der Rechte Betroffener entgegenzustellen. Folgerichtig zielen die Forderungen der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum größten Teil auf bessere Kontrollinstrumente und -möglichkeiten durch unabhängige Datenschutzbehörden ab.

Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Einzelnen folgende Entschlüsse gefasst:

Effektive Kontrolle der Nachrichtendienste herstellen!

Die Datenschutzkonferenz fordert die Gesetzgeber dazu auf, die Datenschutzbeauftragten des Bundes und der Länder sachgerecht auszustatten. Nur so können sie ihrer Kontrollfunktion, die nicht zuletzt vom Bundesverfassungsgericht im Urteil zum Antiterrordatengesetz unterstrichen wurde, nachkommen. Gleichzeitig gilt es, künftig die Datenschutzbeauftragten bei der Überwachung von Nachrichtendiensten zu beteiligen und ihre Expertise zu nutzen.

Marktmacht und informationelle Selbstbestimmung

Die deutsche Monopolkommission hat für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert. Die Datenschutzkonferenz schließt sich dem an. Zunehmende Unternehmens-

käufe vor allem in der Internetwirtschaft, die wachsende Bedeutung von Big Data sowie die Verflechtung von Internet und Smart Home fordern gemeinsame Strategien.

Unabhängige und effektive Datenschutzaufsicht ist für Grundrechtsschutz unabdingbar

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt den Gesetzesentwurf der Bundesregierung, der auf eine Stärkung der Unabhängigkeit der Bundesbeauftragten abzielt. Eine unabhängige Datenschutzaufsicht kann jedoch nur erfolgen, wenn der Behörde ausreichende Personal- und Sachmittel zur Verfügung gestellt werden. Insbesondere muss sich der stetige Aufwandszuwachs auch in der personellen Ausstattung widerspiegeln. Das gilt auch gerade für viele Datenschutzbehörden in den Ländern, die oft defizitär ausgestattet sind und damit die Grundrechte Betroffener nur unzureichend schützen können.

Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Die Datenschutzkonferenz begrüßt die Entscheidung des Europäischen Gerichtshofs zur Löschung von Treffern in der Suchmaschine von Google als „fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet“. Das in dem Urteil geprägte „Recht, schwer gefunden zu werden“ muss nun – der globalen Natur des Internet entsprechend – weltweit umgesetzt werden.

Datenschutz im Kraftfahrzeug

Moderne Kraftfahrzeuge sind längst auch zu umfassenden Datenspeichern geworden. Fahrverhalten, Aufenthaltsorte und Bewegungen des Fahrers oder der Fahrerin können problemlos ausgelesen, zu gänzlich unterschiedlichen Zwecken verwendet und zu Persönlichkeitsprofilen verknüpft werden. Die Datenschutzkonferenz fordert die Automobilindustrie sowie Händler und Werkstätten dazu auf, das Recht auf informationelle Selbstbestimmung auch im Kraftfahrzeug zu gewährleisten.

Dazu Johannes Caspar, der amtierende Vorsitzende der Konferenz: „Datenschutz ist Grundrechtsschutz. Dieser ist in der digitalen Welt immer schwerer zu gewährleisten. Datenschutzbehörden stehen öffentlichen und privaten Stellen gegenüber, die oft auf nahezu uner-

schöpfliche personelle und finanzielle Ressourcen zurückgreifen können. Ein wirksamer Grundrechtsschutz des Einzelnen gegenüber den immer tiefer in das Privatleben eingreifenden Technologien und einer Algorithmisierung unserer Lebenswelt bei der Nutzung digitaler Technologien erfordert gerade auch die Stärkung einer unabhängigen Datenschutzaufsicht in Bund und Ländern sowie eine den wachsenden Herausforderungen angemessene Ausstattung.“

Die vollständigen Entschließungstexte der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder sind unter <https://www.datenschutz-hamburg.de> abrufbar.



Anlage 15

Entschließungen zwischen den Konferenzen 2014/2015

**Keine PKW-Maut auf Kosten des Datenschutzes!
(Umlaufentschließung vom 14. November 2014)**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-) elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Entschließungen zwischen den Konferenzen 2014/2015

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern
(Umlaufentschließung vom 14. November 2014)

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebserkrankten Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können vielfältig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage 17

Entschließungen zwischen den Konferenzen 2014/2015

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern (Anlage zur Umlaufentschließung vom 14. November 2014)

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregister- und -früherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, dass dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291 a, 291 b SGB V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65 c Abs. 1 Satz 1 Nr. 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nr. 3.01 des GKV-Förderkatalog in Hinblick auf die Aufgabe der KKR gemäß § 65 c Abs. 1 Satz 1 Nr. 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65 c Abs. 1 Satz 1 Nr. 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N bzw. W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload bzw. -Download übertragen werden.

Leistungserbringer benötigen für diese Übermittlungsvariante ein Krankenhaus-Informationssystem (KIS) bzw. Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung bzw. Entschlüsselung und die Signatur der Daten bzw. die Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich.

Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau. (Szenarien 1N-4N)

2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemiologischen Krebsregist-

rierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. *Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten.*

Leistungserbringer können bei dieser Variante zwar KIS bzw. PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jedoch für den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vgl. hierzu den Beschluss des Düsseldorfer Kreises vom 04./05. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.

Ferner sind hohe (Szenarien 1-2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend. (Szenarien 1W, 2W, 4W)

3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse. Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS bzw. PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wäre Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken weitgehend denen des webbasierten Dialogverfahrens. Darüber hinaus wäre der

Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog BSI - TR 03116- 1 entnommen sein. (Szenarien 1-4)
5. Für die Identifizierung der Teilnehmer des Verfahren, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rückruf, sowie die Schlüsselspeicherung sind mindestens die Anforderungen des Schutzniveaus hoch+ gemäß Abschnitten 3 und 4 der BSI - TR 03107-1 zu erfüllen. (Szenarien 1-4)
6. (*optional*) Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291 b SGB V verwendet werden, sobald diese verfügbar sind. (Szenarien 1-4)
7. Die Wurzel der zur Zertifizierung von Teilnehmer- und KKR-Schlüsseln verwendeten PKI ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen. (Szenarien 1-4)

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsselung einzusetzen. (Szenarien 1-4)
9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann. (Szenario 1)
10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personen- oder leistungserbringerspezifische Schlüssel einzusetzen. (Szenarien 2-4)
11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich. (Szenarien 1-4)

12. Die erfolgreiche Authentisierung des KKR muss für die meldenden bzw. abrufenden Personen klar erkennbar sein. (Szenarien 1W-4W)
13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen. (Szenarien 2+4)
14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291 a Abs. 3 Satz 1 Nr. 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufsausweis ist hierfür geeignet. (Szenarien 2W+4W)
15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291 a Abs. 5 c SGB V bestimmt wurden. (Szenarien 2-4)
16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten bzw. dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt. (Szenario 2)
17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst bzw. an die Stellen übermittelt werden, bei denen sie tätig sind. (Szenario 3)
18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Bestehen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen muss das Berechtigungskonzept vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können. (Szenario 4)

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

- 19 Ambulante Leistungserbringer müssen die "Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen. (Szenarien 1-4)
- 20 Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen, die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind. (Szenarien 1-4)
- 21 Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräte dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden. (Szenarien 1-4)
- 22 Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders hohen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundsatzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundsatzkataloge, und die in der ISi-Reihe empfohlenen Maßnahmen ein. (Szenarien 1-4)
- 23 Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss (*defense in depth*). (Szenarien 1W-4W)
- 24 Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein

- autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschränkung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels TLS allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs. (Szenarien 1W-4W)
- 25 Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedürfen besonderen Integritätsschutzes. Eine direkte Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig. (Szenarien 1W-4W)
- 26 Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmöglichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden. (Szenario 4W)

Maßnahmen zur Gewährleistung der Authentizität der Daten

- 27 Da die übermittelten Daten einer folgenden Behandlung zugrundegelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind. (Szenarien 1+4)
- 28 Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel i. S. v. Artikel 3 Nr. 26 der EU-Verordnung 910/14 zu authentisieren. (Szenarien 1+4)

Maßnahmen zur Transparenz und Datenschutzkontrolle

- 29 Abrufe sind leistungserbringer- und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden. (Szenarien 2-4)
- 30 Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten. (Szenarien 2-4)
- 31 Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beaskunften. (Szenario 4)

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.

Entschließungen zwischen den Konferenzen 2014/2015

Schluss mit den datenschutzrechtlichen Missständen beim Umgang
mit Krankengeldbeziehern!
(Umlaufentschließung vom 16. Dezember 2014)

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehba-

ren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen

Anlage 19

Entschließung zwischen den Konferenzen 2014/2015

Keine Cookies ohne Einwilligung der Internetnutzer
(Umlaufentschließung vom 5. Februar 2015)

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Artikel 5 Absatz 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sogenannten Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Artikel 5 Absatz 3 der E-Privacy-

Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

Entschliebung

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

Datenschutz nach „Charlie Hebdo“ :

Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts –, „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheit-

lich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

Anlage 21

Entschlieung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 18./19. Mrz 2015 in Wiesbaden

Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europischen Innen- und Justizminister hat sich am 12. und 13. Mrz 2015 erneut mit der Reform des Europischen Datenschutzrechts befasst und dabei ber drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundstzlich geeinigt. Hierzu gehren u. a. die zentralen Vorschriften ber die Datenschutzgrundstze und die Zulssigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Lnder warnen eindringlich vor einer Aushhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundstzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebt zentrale Datenschutzgrundstze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Ma reduziert und einen Anreiz fr datenschutzfreundliche Technologien darstellt.
- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprnglichen Erhebungszweck verarbeitet werden drfen, wenn der neue Zweck mit dem ursprnglichen Zweck noch vereinbar ist. Zwecknderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein berwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Mglichkeiten und die ausdrcklich gewnschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden

Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbeugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.
- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

Anlage 22

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

Safe Harbor bietet keinen ausreichenden Schutz
für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewährleisten. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

Entschließung

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

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist¹. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

¹ Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden.“

Entschlieung

der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 18./19. Mrz 2015 in Wiesbaden

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewhrleistung der Integritt und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf fr ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes fr die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale fr Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfllen sollen dabei wichtige Bausteine einer nationalen Strategie fr mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtung vor. Bei einer Gesamtabwgung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevlkerung in die Gesetzgebung zur IT-Sicherheit zu strken, muss ein beiden Seiten gerecht werdender Abwgungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfllen.

Wenn Manahmen zur Erhhung der Informationssicherheit ergriffen werden, geht damit in vielen Fllen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in

das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o. g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldepflicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermögliche

Anlage 25

Entschlieung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 18./19. Mrz 2015 in Wiesbaden

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klrung bedrfen.

Unter anderem haftet ein Unternehmen drf, wenn ein Subunternehmer - und ggf. auch dessen Subunternehmer - den Beschftigten nicht den Mindestlohn zahlt; auerdem kann ein hohes Bugeld verhngt werden, wenn der Auftraggeber wei oder fahrlssig nicht wei, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die berprfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich - wie Industrie- und Handelskammern berichten - zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschftigendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwrdigen Interessen der Beschftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen berprfung des Mindestlohngesetzes strker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbrokratischen Lsung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklrung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, bernahme des Haftungsrisikos durch Bankbrgschaften sowie vertragliche Zustimmungsvorbehalte fr den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwrzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes,

sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Entschlieung
der 89. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 18./19. Mrz 2015 in Wiesbaden

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum
Einsatz externer Dienstleister bei Berufsgeheimnistrgern
erforderlich

Mit dem Entwurf eines Gesetzes fr sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) wrde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder den Gesetzgeber insbesondere zu folgenden Ergnzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschlielich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen ber die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden knnen. Zur Wahrung der Transparenz ist das den Betroffenen eingerumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Lschung, ermglicht. Entgegen der Gesetzeslage und entsprechender Ankndigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen knnen. Fr den Fall, dass die notwendigen Funktionalitten nicht zeitgerecht zur Verf-

gung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.
3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Anlage 27

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

Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und
Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden (“Predictive Policing“).

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien

bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertelgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten - in einem Umfang und auf eine Art und Weise - verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

Anlage 28

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

Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten
terroristischer Bedrohung!

Vor dem Hintergrund der Terroranschläge von Paris weisen die Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 89. Konferenz darauf hin, dass der Datenschutz kein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates ist. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus tatsächlich zielführend und erforderlich sind. Ließe man jeden Eingriff in dieses Grundrecht zu, hätten die Terroristen eines ihrer Ziele erreicht.

Weitere Entschließungen der Konferenz:

Datenschutzgrundverordnung darf keine Mogelpackung werden.

Die Verabschiedung der Datenschutzgrundverordnung geht auf die Zielgerade. Welche Rolle die Bundesregierung in den Verhandlungen spielt, bleibt für die Mitglieder der Datenschutzkonferenz undurchsichtig. Sie warnen eindringlich vor einer Aushöhlung des Datenschutzes. Von wesentlichen Datenschutzgrundsätzen wird durch die jetzt vorgeschlagene Fassung des Kapitels 2 der Datenschutzgrundverordnung abgewichen.

Dies betrifft insbesondere:

- Den Grundsatz der Datensparsamkeit
- Das Zweckbindungsgebot und
- Das Einwilligungsgebot

Zudem wird das Privileg, personenbezogene Daten zu Forschungszwecken zu verarbeiten, über das Recht auf informationelle Selbstbestimmung gestellt.

Damit wird nicht die angestrebte Verbesserung, sondern eine Verschlechterung des Datenschutzniveaus erreicht.

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA.

Der Nachweis, dass amerikanische Sicherheitsbehörden nicht auf personenbezogene Daten zugreifen, die deutsche Unternehmen an US-Unternehmen übermitteln, kann nach den Enthüllungen von Edward Snowden kaum erbracht werden.

Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht unmittelbar anwendbar ist, dürfen damit nach Auffassung der Konferenz nur erfolgen, wenn folgendes sichergestellt ist:

- Einhaltung der Zweckbindung
- Beschränkung staatlicher Zugriffsmöglichkeiten auf ein angemessenes und grundrechtskonformes Maß
- Sicherstellung der Betroffenenrechte (Auskunft, Berichtigung, Löschung)
- Sicherstellung des Rechtsschutzes bei Verstößen.

Verschlüsselung ohne Einschränkungen ermöglichen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Schaffung einer Infrastruktur, die eine verschlüsselte Kommunikation von Bürgern, Verwaltungen, Unternehmen mit- und untereinander ermöglichen. Durch Schaffung einer solchen Infrastruktur kann die Sicherung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet werden. Es ist nach Auffassung der Datenschutzbeauftragten des Bundes und Länder Aufgabe der Politik, dies aktiv zu unterstützen. Eine Einschränkung kryptographischer Verfahren durch staatliche Regulierungen lehnt die Konferenz ab.

Anlage 29

Entschließung zwischen den Konferenzen 2015

Gegen den Gesetzentwurf zur Vorratsspeicherung von
Telekommunikationsverkehrsdaten bestehen erhebliche
verfassungsrechtliche Bedenken
(Umlaufentschließung vom 9. Juni 2015)

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtsbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Entschliebung

der 90. Konferenz der Datenschutzbeauftragten
des Bundes und der Lnder
am 30. September/1. Oktober 2015 in Darmstadt

Cloud-untersttzte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Mae neue Versionen dieser Software an, die im Unterschied zu den herkmmlichen Betriebssystemen auf internetbasierte Cloud-Services zurckgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme fhren oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgert (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste bertragen werden. Dadurch erhlt der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatschliche und mgliche Auswirkungen auf den Umgang mit personenbezogenen Daten lngst nicht allen Anwendern, d. h. Benutzern und fr den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verndert werden. Weitreichende Datenverarbeitungsbefugnisse knnen nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch untersttzte Einwilligungslsungen zu entsprechen. Solange nicht unabhngige Dritte die Wirkung der Einstellungen auf den Datenschutz geprft haben, ist selbst nach deren nderung hufig unklar, wie weit Datenbertragungen tatschlich eingeschrnkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

Anlage 31

EntschlieÙung

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

Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem "Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes" (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer EntschlieÙung vom 4. November 2010 "Keine Volltextsuche in Dateien der Sicherheitsbehörden" hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbe-

hörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 "Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben"). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 "Effektive Kontrolle von Nachrichtendiensten herstellen!").

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

**Beschluss der obersten Aufsichtsbehörden im Datenschutz im
nicht-öffentlichen Bereich**

(Düsseldorfer Kreis am 15./16. September 2015)

Videoüberwachung in öffentlichen Verkehrsmitteln

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre 2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt.

Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit

des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z. B. Fahrerarbeitsplätze), findet neben dieser Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1 Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z. B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobachtet und dadurch im Notfall ein schnelles Eingreifen möglich wird.

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw.

dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z. B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein mildereres, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box-Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z. B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwa-

chung durch einen Notfallschalter für den Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o. Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frageankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maß-

nahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken - wie beispielsweise dem ländersübergreifenden Bahnbetrieb - eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2 Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optisch-elektronischen Einrichtungen erfasst werden (z. B. der zum Zutritt für Fahrgäste hin offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzone(n), d. h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z. B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch

in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahmefällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigten darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten technischen Personals erfolgen kann. Dies kann beispielsweise durch den Einbau diesbezüglicher Werkstatthalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z. B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetrieb-

nahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1 Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens "Videoüberwachung" mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2 Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder / Piktogramme / Displays außen die Videoüberwachung kenntlich machen (vgl. § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.

Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3 Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funktionsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4 Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Lösungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit

der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1 Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträgerspeichert und die Übrigen unverzüglich gelöscht.

4.2 Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art

der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3 Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie der Zeitpunkt der Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vgl. Anlage zu § 9 BDSG).

4.4 Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z. B. pauschal eine möglichst umfassende“ Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5 Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich z. B. nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter be-

trieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

Pressemitteilung
vom 31. Januar 2014

Das Auto – Black Box außer Kontrolle

Gestern hat der Verkehrsgerichtstag 2014 klare Regeln für Autodaten gefordert. Eine Forderung, der sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse ausdrücklich anschließt.

Die moderne technische Automobilausstattung bringt es mit sich, dass – zumindest in neueren Fahrzeugen – umfassende Daten über Fahrverhalten und Fahrroute erhoben werden können. Möglich ist sogar, in Erfahrung zu bringen, wann der Fahrer geschaltet und mit welcher Intensität er wo gebremst hat. Bereits jetzt interessieren sich die Kfz-Versicherer für diese Daten und wollen ihre Versicherten dazu bringen, eine Black Box einbauen zu lassen, die das Fahrverhalten ebenfalls beobachtet. Es ist auch nicht auszuschließen, dass derjenige, der in einen Unfall verwickelt ist, in gar nicht ferner Zukunft herangezogen werden wird, seine Fahrzeugdaten zu seiner Belastung auslesen zu lassen – ein Verstoß gegen das im Allgemeinen Persönlichkeits-Grundrecht wurzelnde Selbstbelastungsverbot! Als Gegenleistung soll dann zwar die Versicherungsprämie um etwa 5 % gesenkt werden – bei entsprechend negativem Fahrverhalten wird diese jedoch wieder erhöht werden. Ob hierin noch eine freiwillige Datenpreisgabe des Betroffenen gesehen werden kann, wird derzeit kontrovers diskutiert. Die Gefahren einer derartigen Profilbildung sowie das Wecken von Daten-Begehrlichkeiten liegen auf der Hand.

Virulent wird vor diesem Hintergrund auch die Problematik der Überwachung von Beschäftigten, die z. B. den LKW des Arbeitgebers nutzen.

Das Bundesdatenschutzgesetz hinkt der Realität wieder einmal hinterher. Es legt nicht fest, wem die erhobenen Daten gehören und wer sie zu welchen Zwecken verwenden darf. Oftmals wissen die Fahr-

zeugnutzer nicht einmal, welche Daten über sie erhoben werden und wer diese Daten zu welchen Zwecken nutzt.

„Ich werde mich im Rahmen meiner Möglichkeit dafür einsetzen, dass der Bundesgesetzgeber sich der Thematik annimmt, damit für die Autofahrer in Deutschland die Rechtssicherheit wiederhergestellt wird“, so Dr. Lutz Hasse (TLfDI).

Anlage 34

Pressemitteilung
vom 20. März 2014

§ 28 BDSG – nicht verzagen!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat einen Ratgeber zu § 28 Bundesdatenschutzgesetz (BDSG) erstellt. Bei § 28 BDSG handelt es sich um eine komplizierte, für den juristischen Laien kaum zu verstehende Norm, der jedoch im Datenschutz eine zentrale Bedeutung zukommt.

§ 28 BDSG regelt die Voraussetzungen, unter denen ein Unternehmer zu seinen Geschäftszwecken und Zwecken der Werbung personenbezogene Daten verwenden darf. Nur unter dessen kryptischen Voraussetzungen ist das Verwenden von personenbezogenen Kundendaten zulässig, es sei denn, der Betroffene willigt ein.

Die Broschüre richtet sich ausdrücklich an datenschutzrechtliche Laien und versucht, unverständlichen Gesetzestext für die Unternehmenspraxis zu übersetzen, auch und gerade anhand von Beispielen.

Die Broschüre steht Ihnen auf der Homepage des TLfDI zum freien Download bereit.

Pressemitteilung
vom 8. April 2014**EuGH kippt Richtlinie zur Vorratsdatenspeicherung –
Hasse: Ein guter Tag, auch für den Thüringer Datenschutz**

Die heutige Entscheidung des EuGH zur Vorratsdatenspeicherung bewertet Thüringens Datenschutzbeauftragter Lutz Hasse als „notwendigen Paukenschlag, der die Sammelwut staatlicher Behörden in strikte Grenzen weist. Der EuGH hat dem Datenschutz damit neues Leben eingehaucht, was auch nötig war, nachdem die Enthüllungen von Edward Snowden das Grundrecht der informationellen Selbstbestimmung ins Wanken gebracht hatten.“

Das Gericht hatte heute entschieden, dass die EU-Richtlinie 2006/24/EG aus dem Jahr 2006 in vollem Umfang nicht mit der Charta der Grundrechte vereinbar und daher ungültig sei. Daraus folgt für den EuGH, dass die verdachtslose Speicherung von Verbindungsdaten von Telefon, Internet und E-Mails „auf das absolut Notwendige“ beschränkt werden müsse.

Der Thüringer Datenschutzbeauftragte begrüßt an der EuGH-Entscheidung vor allem, dass sie den Richtervorbehalt, also die Entscheidung eines Gerichts anmahnt, bevor eine Behörde den Zugang zu den gespeicherten personenbezogenen Daten erhält. Damit werde auch auf europäischer Ebene der Richtervorbehalt zementiert. Ferner zeigt sich Lutz Hasse erfreut darüber, dass die EuGH-Richter auch eine Informationspflicht gegenüber den Inhabern der erhobenen personenbezogenen Daten gefordert haben.

Hasse: „Sowohl den Richtervorbehalt als auch die Pflicht zur Information der betroffenen Bürger habe ich bei der Novellierung des Thüringer Polizeiaufgabengesetzes mehrfach eingefordert und bin damit leider nur zum Teil auf Verständnis gestoßen.“ Der Datenschutzbeauftragte sieht deshalb in der heutigen Entscheidung auch ein „Signal für den Thüringer Verfassungsgerichtshof“, der das Polizeiaufgabengesetz derzeit erneut auf seine mögliche Verfassungswidrigkeit überprüft.

Gleichzeitig mahnt Hasse, nach der EuGH-Entscheidung nicht in „aktionistische Panik“ zu verfallen, sondern die Entscheidungsgründe genau zu studieren. „Schließlich würde es bei der Neufassung des Deutschen Telekommunikationsgesetzes wiederum um einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung gehen“, so Thüringens Datenschutzbeauftragter. „Dessen Verhältnismäßigkeit wäre nicht gegeben, wenn alle Bürgerinnen und Bürger ohne konkret definierten Anlass und weitere differenzierende Kriterien von der Vorratsdatenspeicherung erfasst würden“, so Hasse abschließend.

Die Pressemitteilung des EuGH zur heutigen Entscheidung finden Sie unter:

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf>

Anlage 36

Pressemitteilung
vom 2. Juni 2014

Arbeitskreis Datenschutz und Bildung
am 2. und 3. Juni 2014 beim Thüringer
Landesbeauftragten für den Datenschutz und die
Informationsfreiheit in Erfurt

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Herr Dr. Lutz Hasse, hat bis auf Weiteres den Vorsitz für den Arbeitskreis Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Deutschland übernommen.

Erstmals findet nun vom 2. Juni bis zum 3. Juni 2014 der Arbeitskreis Datenschutz und Bildung in den neuen Räumlichkeiten des TLfDI in Erfurt statt.

Schwerpunkthemen sind unter anderem „Young Data“, ein neues Webportal, das viele Antworten für junge Mediennutzer liefert, die Einführung von Medienkunde als eigenes Schulfach sowie die Auswertung des Koalitionsvertrages auf Bundesebene zur digitalen Bildung und zum digitalen Schutz.

Der zweite Sitzungstag beschäftigt sich mit der Überarbeitung des Moduls „Datenschutz“ bei Klicksafe sowie mit den Studien „DIVSI U25“ und „miniKIM“, die das Verhalten der nachwachsenden Generation in Hinblick auf den Medienumgang untersuchen.

Schließlich tauschen sich die Mitglieder über Initiativen in den Ländern aus, um voneinander zu lernen.

Anlage 37

Pressemitteilung
vom 4. Juni 2014

Arbeitskreis Datenschutz und Bildung
in Erfurt richtungsweisend

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Herrn Dr. Lutz Hasse, tagte der Arbeitskreis Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 2. und 3. Juni 2014 in Erfurt; in angeregt-konstruktiver Atmosphäre konnten Weichen für die Zukunft gestellt werden:

An der von Jugendlichen stark frequentierten Seite „Young Data“ des rheinland-pfälzischen Datenschutzbeauftragten wollen sich nunmehr mehrere Bundesländer mit eigenen Beiträgen beteiligen; so übernimmt der TLfDI die Themen „Video“ und „Informationsfreiheit“.

Auf große Sympathie stieß die Rede des Herrn Staatssekretärs Prof. Dr. Merten vom Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK). Prof. Dr. Merten maß dem Themenkomplex Medienkompetenz und Datenschutz sowohl an Thüringer Schulen als auch in der Lehrerbildung große Bedeutung zu. Aufgrund der rasanten Entwicklung der digitalen Medien benötigen die Schulen und Universitäten nach seiner Auffassung nachhaltige Unterstützung, um Schritt halten zu können. Die Kooperation zwischen TMBWK und dem TLfDI solle daher intensiviert werden.

In der Sitzung kristallisierte sich zudem die Bedeutung der frühkindlichen Medienbildung in Vorschulgruppen der Kindertagesstätten heraus. „In diesem Bereich werden die Datenschützer besondere Aktivitäten entfalten“, kündigte Dr. Lutz Hasse an.

Darüber hinaus hat der TLfDI die Aufgabe übernommen, das Modul „Datenschutz“ innerhalb des Internet-Auftritts der EU-Initiative für mehr Sicherheit im Netz „klicksafe.de“ zu überarbeiten und den neuen Entwicklungen anzupassen.

Alles in allem eine weiterführende Veranstaltung; Fortsetzung folgt im Dezember.

Pressemitteilung
vom 23. Juli 2014

Videogaga: Europäischer Perspektivenwechsel !

Das Problem: Nicht selten videografieren BürgerInnen ihre Mitmenschen auf der Straße oder dem Nachbargrundstück. Das kann beispielsweise mit Kameras im Auto oder in der Brille geschehen. § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) nimmt nun solche Datenerhebungen aus seinem Anwendungsbereich heraus, wenn sie ausschließlich für persönliche oder familiäre Tätigkeiten erfolgen.

Folge: Mangels Anwendbarkeit des BDSG kann der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) den aufgenommenen BürgerInnen nicht helfen; diese müssen – auf sich gestellt – beispielsweise das Unterlassen derartiger Aufnahmen vor dem Zivilgericht erstreiten (§§ 823, 1004 BGB).

Neuer Ansatz: In seinem Schlussantrag in der Rechtssache C-212/13 trifft der Generalanwalt am Europäischen Gerichtshofs zu einer auf einem Privatgrundstück fest installierten Videokamera (also – *noch* – nicht zu Handys und Camcordern), die den öffentlichen Raum sowie die Tür eines gegenüberliegenden Hauses erfasst, folgende Feststellungen:

Art. 3 Abs. 2, 2. Spiegelstrich der Europäischen Datenschutzrichtlinie 95/46/EG, der fast wortwörtlich von § 1 Abs. 2 Nr. 3 BDSG als Bundesrecht umgesetzt wird, sei *eng auszulegen*: Zur Beurteilung der Frage, ob die Videoaufnahme ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten vorgenommen werde, komme es *nicht* auf den *subjektiven Zweck* dieser Datenverarbeitung an. Entscheidend sei vielmehr in *objektiver* Hinsicht, ob auch Personen von der Videokamera erfasst würden, die in keiner persönlichen oder familiären Verbindung zum Videobetreiber stünden. Für diesen Fall fände die Europäische Datenschutzrichtlinie – und damit ihre engen Zulässigkeitsvoraussetzungen an eine Videoüberwachung - Anwendung.

Schlussfolgerungen für Thüringen: Schließt sich der Europäische Gerichtshof dem Votum des Generalanwalts an, bleibt das BDSG

immer anwendbar, wenn ein Privater Dritte videografiert, die nicht in persönlicher oder familiärer Verbindung zu ihm stehen. Mithin kann der TLfDI dem Betroffenen dann zur Seite stehen und klären, ob nach dem Maßstab des BDSG die Videoaufnahmen rechtswidrig sind. Bejahendenfalls kann der TLfDI geeignete Maßnahmen gegenüber dem Videobetreiber treffen, die die Verletzung des Grundrechts der informationellen Selbstbestimmung unterbinden.

Es würde sich ein weiteres Aufgabenfeld für den TLfDI mit einem effektiveren Grundrechtsschutz der BürgerInnen eröffnen – eine gute Entwicklung! ☺

Anlage 39

Pressemitteilung
vom 4. September 2014

EuGH-Urteil: „Recht auf Vergessen“ vs. Archive? –
Nein!

Nach dem Urteil des Europäischen Gerichtshofes (EuGH) muss die Internetsuchmaschine Google Einträge in den Suchergebnislisten mit persönlichen Daten auf Verlangen der Betroffenen streichen. Ein Formular zur Beantragung dieser Löschungen hat Google schon kurz nach dem Urteil online gestellt. Nun sind öffentliche Archive besorgt, dieses „Recht auf Vergessen“ gelte auch für sie, sodass möglicherweise auch Archivdaten zu löschen seien. Archive unterliegen indes ganz anderen rechtlichen Rahmenbedingungen als Suchmaschinen. Sie haben u. a. gerade die gesetzliche Aufgabe, Unterlagen, die aufgrund ihres rechtlichen, politischen, wirtschaftlichen, sozialen und kulturellen Wertes als Quellen für die Erforschung und das Verständnis von Geschichte und Gegenwart dienen, dauernd aufzubewahren - § 2 Abs. 2 Thüringer Archivgesetz (ThürArchivG). Zudem setzt der Zugang zu diesen Daten den Nachweis eines berechtigten Interesses sowie die Beachtung schutzwürdiger Belange Dritter voraus, worunter eben auch deren Recht auf Datenschutz fällt (§§ 15 Abs. 7, 16 Abs. 1 und 2 ThürArchivG). Dieser sicheren Datensphäre der Archive stehen Internetsuchmaschinen gegenüber, deren personenbezogene Daten überall auf der Welt mühelos zu vielfältigen Zwecken missbraucht werden können, etwa zur Profilbildung. Allein diese spezifische Internetgefahr wollte der EuGH eindämmen. Daher hat dessen Google-Urteil mangels Vergleichbarkeit keinerlei Auswirkung auf öffentliche Archive. Es bleibt zu hoffen, dass diese Zusammenhänge bei der Gestaltung der Europäischen Datenschutzgrundverordnung Berücksichtigung finden.

Anlage 40

Pressemitteilung
vom 23. September 2014

Nokia ante Portas

Die in Finnland ansässige Firma Nokia wird nun auch in Thüringen aktiv. Nokia betreibt seit einigen Jahren den Kartierungsdienst „Here“. Die Vermessung wird von der niederländischen Tochter „HERE Europe B.V.“ durchgeführt, die datenschutzrechtliche Verantwortung liegt jedoch weiterhin bei Nokia.

Die Vermessungs-Fahrzeuge sind an dem Schriftzug „here“ und den technischen Kameraaufbauten leicht zu erkennen. Sie fertigen 360 Grad Panoramabilder, 3D-Scans über LIDAR Laserscanner und GPS Aufzeichnungen an. Damit können 3D-Aufnahmen von Hausfassaden, Vorgärten, Fahrzeugen und anwesenden Personen erstellt werden. Wann und wo diese Aufnahmefahrten stattfinden, kann man erfahren unter:

→ <http://here.com/legal/driveschedule> .

Zufällig aufgenommene Personen, Gesichter oder Autokennzeichen werden laut Nokia in den aufbereiteten Kartendaten unkenntlich gemacht.

Hausbesitzer, die in den Panoramabildern ihre Hausfassade zusätzlich unkenntlich machen möchten, haben die Möglichkeit – auch auf Deutsch – sich per Mail an privacy@here.com oder per Brief an die Nokia Corporation, c/o Privacy, Karakaari 7, 02610 Espoo, Finnland, zu wenden.

Sollten sich weitere Fragen ergeben, finden Sie die Kontaktadresse des zuständigen finnischen Datenschutzbeauftragten unter:
<http://www.bfdi.bund.de/SharedDocs/Adressen/EuropaeischeDatenschutzbeauftragte/DatenschutzbeauftragterFinnland.html?nn=409072>
Führt dies nicht zum Erfolg, wenden Sie sich bitte an meine Behörde.

Anlage 41

Pressemitteilung
vom 21. Oktober 2014

Datenverschlüsselung geht zur Schule!
Ich mach's mit Safer Mail

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) und das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (Thillm) bieten gemeinsam am 23. Oktober 2014 im Erfurter KinderMedienZentrum eine Fortbildung zum Datenschutz an. Sie richtet sich an Pädagogen aller Schularten sowie an Mitarbeiter aus der Schulaufsicht und der Schulverwaltung. Im Mittelpunkt der Veranstaltung „Sicherer Datentransfer durch Verschlüsselung“ steht die Ende-zu-Ende-Verschlüsselung von E-Mails. Dies ist ein wichtiges Thema auch für die dienstliche Korrespondenz zwischen Schulleitungen, Schulverwaltung, Lehrern und Eltern, denn oft sind in alltäglichen Nachrichten auch persönliche Daten enthalten, die vor unbefugtem Zugriff zu schützen sind. Nur eine Ende-zu-Ende-Verschlüsselung bietet hier einen sicheren Schutz, der mit vertretbarem Aufwand zu erreichen ist. Das Interesse ist groß, die Anmeldungen überschreiten die mögliche Teilnehmerzahl. Als Hauptreferent konnte Herr Jens Kubieziel gewonnen werden. Der studierte Mathematiker hält Vorträge zur Kryptografie und berät Unternehmen zu IT-Sicherheitsfragen. Die genannte Fortbildung bietet den Teilnehmern breiten Raum für praktisches Ausprobieren der E-Mail-Verschlüsselung und weiterer Sicherheitsmaßnahmen am eigenen Laptop. Deshalb wird in Gruppen von ca. 12 Personen unter kompetenter Anleitung von drei weiteren Fachleuten gearbeitet. Medienvertreter sind herzlich eingeladen, sich vor Ort über den Veranstaltungsverlauf zu informieren. Näheres entnehmen Sie dem Faltblatt.

Pressemitteilung
vom 17. November 2014

Keine PKW-Maut auf Kosten des Datenschutzes!

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weisen sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die Datenschutzbeauftragten des Bundes und der Länder mahnen die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Anlage 43

Pressemitteilung
vom 27. November 2014

„Videogaga als Video“
Kurzfilm zur Videoproblematik als Modul für den
Schulunterricht

Alltägliche Erfahrung auf Spielplätzen, Sportanlagen und in Geschäften: Kameras, Kameras, Kameras ... Erfreulich, wenn sich auch Jugendliche fragen – Was soll das denn? Geht das überhaupt in Ordnung? Diese Thematik greift ein Video auf, das vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) konzipiert und von Studenten der TU Ilmenau hergestellt wurde. Gedacht ist es für den Einsatz an den Thüringer Schulen. Dort ist das Thema Datenschutz auch Gegenstand des Kurses Medienkunde in den Klassenstufen 5 bis 10. Der TLfDI verfolgt das Ziel, dass Datenschutz auch wirklichkeitsnah vermittelt werden kann. So hat seine Behörde ein Unterrichtsmodul für den Einsatz im Unterricht entwickelt, zu dem auch besagter Kurzfilm gehört. Nach Unterrichtserprobung wird das gesamte Modul, bestehend aus Video, Lehrerhandreichung und weiteren Materialien auf der Internetseite des TLfDI und im Thüringer Schulportal downloadfähig sein. Bis dahin können Neugierige ja schon mal einen Blick in das Video werfen: <http://www.tlfdi.de/tlfdi/themen/schule/>

Anlage 44

Pressemitteilung
vom 3. Dezember 2014

In's Netz gegangen – Facebook
Fortsetzung: Sachstand & Hinweise

Seit Oktober 2014 ist beim **Bundesverwaltungsgericht** eine Revision in Sachen datenschutzrechtlicher Verantwortlichkeit bei Facebook-Fanpages anhängig.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) strebt dabei eine datenschutzrechtlich grundsätzliche Klärung an, inwieweit deutsche Betreiber von Fanpages für die datenschutzwidrige Datenverarbeitung durch den Portalanbieter Facebook mit verantwortlich sind.

In der Pressemitteilung vom 14. Juni 2012 gab der TLfDI bereits einen Überblick über den damaligen Sachstand zum Betreiben von Facebook-Seiten und verwies auf die Entschließung der 82. Konferenz der Datenschutzbeauftragten 2011.

Die Datenschutzbeauftragten des Bundes und der Länder vertraten in dieser Entschließung die Auffassung, dass die öffentlichen Stellen keine Fanpages einrichten sollten.

Dies ist der Tatsache geschuldet, dass von den Besuchern der Fanpages die Nutzungsdaten (IP-Adresse, Informationen durch das Setzen von Cookies, usw.) von Facebook in nicht transparenter Weise erfasst und ohne Einfluss der Betreiber und Besucher der Fanpages verarbeitet werden. Für öffentliche Stellen, die eine Fanpage betreiben, bedeutet dies zudem, dass eine Datenübermittlung an Dritte vorliegt, wofür ggf. die Rechtsgrundlage fehlt. Bis zur endgültigen Entscheidung durch das Bundesverwaltungsgericht sieht der TLfDI das Betreiben von Fanpages weiterhin kritisch und rät daher davon ab.

Anlage 45

Pressemitteilung
vom 11. Dezember 2014

Weihnachtsgeschenk für den Datenschutz!

Etwas verfrühte Weihnachtsbescherung: Heute hat der Europäische Gerichtshof im Rahmen eines Vorabentscheidungsverfahrens über die Auslegung von Art. 3 Abs. 2 der Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bestätigt, dass auf eine privat betriebene Videoüberwachungsanlage unter bestimmten Voraussetzungen die Europäische Datenschutzrichtlinie und damit das insoweit gleichlautende Bundesdatenschutzgesetz anwendbar ist.

Bereits in der Presseerklärung vom 23. Juli 2014 „Videogaga: Europäischer Perspektivenwechsel“ hat der TLfDI auf die Rechtssache C-212/13 beim EuGH und den damit verbundenen Perspektivenwechsel hingewiesen. Gegenstand war eine privat betriebene Videoüberwachungsanlage, die zum Schutz eines Privatgrundstücks auch Teile des öffentlich zugänglichen Raums aufgezeichnet hatte.

Heute hat der EuGH klargestellt: Jede Videoüberwachung, die nicht ausschließlich auf die private Sphäre (z. B. Grundstück, Familienangehörige) des Betreibers gerichtet ist, etwa, weil sie öffentlich zugänglichen Raum erfasst, fällt in den Anwendungsbereich der Europäischen Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes; sie ist damit nur unter den dort geregelten Voraussetzungen zulässig.

Der TLfDI freut sich, dass seine bereits seit mehreren Jahren vertretene Rechtsauffassung durch den EuGH bestätigt wurde. Für Thüringen bedeutet dies, dass der TLfDI weiterhin an seiner Kontrollpraxis festhalten und die Rechtmäßigkeit von privat betriebenen Videoüberwachungsanlagen als zuständige Aufsichtsbehörde prüfen wird. Und: Der TLfDI kann damit BürgerInnen, die von solchen Videoaufnahmen betroffen sind, weiterhin unterstützen – ein guter Tag für den Datenschutz und die Privatsphäre! ☺

Anlage 46

Pressemitteilung
vom 19. Dezember 2014

Safe the Date
"Safer Internet Day"
am 10.02.2015
- Medienkunde als eigenes Schulfach -
Neuland in Sicht?

Der Umgang mit modernen Medien ist inzwischen zu einer Grundkompetenz wie Lesen, Schreiben und Rechnen geworden. Unbestritten besteht daher ein bildungspolitischer Auftrag, Kindern und Jugendlichen Medienkompetenz zu vermitteln. In Thüringen und auch in anderen Bundesländern wird der Weg gewählt, die Medienkompetenz im Rahmen des bekannten Schulfächerkanons („integrativ“) zu behandeln. Ob dies das richtige Konzept ist, in Zukunft die Herausforderungen der Mediengesellschaft angemessen zu bewältigen, ist bislang nicht ausreichend hinterfragt worden

Der TLfDI organisiert zu diesem Themenkomplex eine Fachtagung
Mit zahlreichen Experten auf diesem Gebiet am

Dienstag, dem 10.02.2015 von 10:00 Uhr bis 17:00 Uhr
im Rathausfestsaal Erfurt, Fischmarkt 1.

Pressemitteilung
vom 5. Januar 2015

Elektronische Gesundheitskarte ist nun Pflicht!

Seit dem 1. Januar 2015 gilt nunmehr ausschließlich die elektronische Gesundheitskarte (eGK) als Berechtigungsnachweis für die Inanspruchnahme von Leistungen der gesetzlichen Krankenkasse beim Arzt oder Zahnarzt.

Auf der eGK befinden sich alle Daten, die bislang auf der Krankenversichertenkarte enthalten waren sowie zusätzlich das Geschlecht und – außer in den gesetzlich vorgesehenen Ausnahmefällen – ein Lichtbild des Patienten. Hierdurch soll einem Kartenmissbrauch vorgebeugt werden.

Die eGK ist aber darauf ausgerichtet, folgende zusätzliche Funktionen zu erfüllen:

- **Online-Abgleich** der Daten der Karte beim Einlesen in der Praxis mit den bei der Krankenkasse vorliegenden aktuellen Daten des Versicherten; dabei hat die Krankenkasse keinerlei Zugriff auf die beim Arzt vorliegenden Daten;
- Speicherung ärztlicher Verordnungen (sog. **eRezept**) und des Berechtigungsnachweises für EU-Ausländer (sog. **Europäische Krankenversicherungskarte**);
- Zusätzliche Daten können **auf Wunsch des Patienten** gespeichert werden, beispielsweise Notfallversorgungsdaten, ein elektronischer Arztbrief oder persönliche Arzneimittelrisiken und -unverträglichkeiten.

Zunächst soll der Online-Abgleich ab Mitte 2015 in verschiedenen Testregionen erprobt werden, nicht aber in Thüringen. Termine für eine bundesweite Einführung des Online-Abgleichs oder für Tests der weiteren Funktionen stehen noch nicht fest. **Für die Patienten in Thüringen ändert sich also erst einmal nichts.**

Das Projekt wird durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit datenschutzrechtlich begleitet.

Die Kommunikation mit diesen sensiblen Gesundheitsinformationen zwischen Krankenversicherern, Ärzten und Apothekern ist über **ein eigens zu diesem Zweck errichtetes Gesundheitsnetz** vorgesehen, das keine Schnittstelle zum öffentlichen Internet hat. Alle Gesundheitsdaten – auch Rezeptdaten – werden verschlüsselt abgelegt. Sie werden – etwa wenn der Patient dem Arzt oder Apotheker den Zugriff auf diese Daten ermöglichen möchte – durch das gleichzeitige Stecken der eGK und des dem Arzt oder anderen Berechtigten ausgestellten Heilberufsausweises in ein spezielles Kartenlesegerät entschlüsselt.

Darüber hinaus muss der Versicherte einem **Zugriff auf medizinische Daten** durch die Eingabe einer PIN zustimmen. Eine Ausnahme bilden die freiwilligen Notfalldaten, auf die der Heilberufsausweis allein den Zugriff gewährt. Auch für das Entschlüsseln von Rezeptdaten beim Apotheker ist keine PIN erforderlich.

Die Zugriffe auf die eGK werden protokolliert, damit der Versicherte die Zugriffe auf seine Daten einsehen und verfolgen kann.

Mit der vorgesehenen elektronischen Patientenakte wird die eGK voraussichtlich eine weitere Entwicklung erfahren, die der TLfDI beobachten und gegebenenfalls beeinflussen wird.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit steht für Fragen zur eGK gern zur Verfügung und wird weiter über den Fortgang berichten.

Anlage 48

Pressemitteilung
vom 16. Januar 2015

Non vitae, sed scholae discimus?

„Nicht für das Leben, sondern für die Schule lernen wir“ kritisierte bereits der Philosoph Seneca und mahnte uns zu hinterfragen, ob die Schule junge Leute tatsächlich auf das Leben vorbereitet. Dieses Zitat gewinnt an Würze dadurch, dass sich kürzlich eine 17jährige Schülerin mittels Twitter an die Öffentlichkeit wandte und meinte, sie habe mit fast 18 keine Ahnung von Steuern, Miete und Versicherung, könne aber eine Gedichtsanalyse in vier Sprachen schreiben.

Brauchen wir also ein „Unterrichts-Update“?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) veranstaltet zum internationalen Safer Internet Day am **10. Februar 2015** im Erfurter Rathausfestsaal eine Fachtagung zum Themenkomplex **Medienkunde als eigenes Schulfach**. Besonderes Augenmerk soll dabei auf der Vermittlung von Medienkompetenz liegen. Medienkunde wird in den Schulen bisher ausschließlich integrativ vermittelt, also als Art „Anhängsel“ im Rahmen der bisherigen Schulfächer. Ob die bisherige Stoffvermittlung den gewünschten Erfolg zeigt, welche Defizite hier bestehen und was zu tun ist, soll mit Fachleuten erörtert werden.

Während einer mittäglichen Pressekonferenz wird der Startschuss für das gemeinsame Kinder- und Jugendportal der Datenschutzbeauftragten des Bundes und der Länder (www.youngdata.de) gegeben werden.

Näheres entnehmen Sie bitte dem Flyer.

Pressemitteilung
vom 28. Januar 2015

Krankenkasse als Fitnesscoach?

Der Presse waren Meldungen zu entnehmen, dass ein großer Versicherer in Europa künftig Fitnessdaten seiner Kunden sammeln will. Als Belohnung für der Gesundheit zuträgliches Verhalten winken dann Gutscheine oder Rabatte auf die zu zahlenden Beiträge zur Krankenversicherung. Die Angebote sollen demnächst auch in Deutschland erhältlich sein.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) befürchtet, dass dies erst der Anfang einer Entwicklung ist, die er sehr kritisch beurteilt. Krankenkassen haben ein zunehmendes Interesse daran, Gesundheitsdaten ihrer Versicherten zu erhalten. Dies aber nicht etwa nur, um sie möglichst effektiv bei der Gesundheitsvorsorge zu unterstützen, sondern zumindest auch, um passgenaue Angebote zu erstellen, damit ihr eigenes finanzielles Risiko so gering wie möglich bleibt.

Der TLfDI warnt: „Sicher ist es verlockend, wegen der Übermittlung von Fitnessdaten ein günstigeres Angebot der Versicherung zu erhalten. Jeder Versicherte sollte sich aber darüber klar sein, dass er seiner Krankenkasse mit diesen Daten sensible Angaben über seine Gesundheit übermittelt. Es ist nicht ausgeschlossen, dass die Krankenkasse anhand dieser Daten auch unliebsame Prognosen über die künftige gesundheitliche Entwicklung treffen kann, die sich für den Betroffenen finanziell ungünstig auswirken können.“

Das Problem stellt sich zunächst bei den privat Krankenversicherten. Nach den derzeit für gesetzliche Krankenkassen geltenden Regelungen ist eine Erhebung von Fitnessangaben unzulässig. Auch für die Erhebung im Rahmen einer Einwilligung ist nach Ansicht des TLfDI Dort nach derzeit geltender Rechtslage kein Raum.

Anlage 50

Pressemitteilung
vom 30. Januar 2015

Reminder
"Safer Internet Day" am 10.02.2015
- Medienkunde als eigenes Schulfach -
Neuland in Sicht?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) organisiert eine Fachtagung (s. Faltblatt) mit zahlreichen Experten auf dem Gebiet der Medienkompetenz am

Dienstag, dem 10.02.2015 von 10:00 Uhr bis 17:00 Uhr

im Rathausfestsaal Erfurt, Fischmarkt 1.

Da noch einige Plätze frei sind, werden Interessierte herzlich eingeladen, die Chance zu nutzen und sich anzumelden. Da der Umgang mit modernen Medien inzwischen zu einer Grundkompetenz wie Lesen, Schreiben und Rechnen geworden ist, besteht ein bildungspolitischer Auftrag, Kindern und Jugendlichen Medienkompetenz zu vermitteln. In Thüringen und auch in anderen Bundesländern wird der so genannte „integrative“ Weg gewählt, bei dem die Medienkompetenz im Rahmen des bekannten Schulfächerkanons behandelt wird. Ob dies das richtige Konzept ist, in Zukunft die Herausforderungen der Mediengesellschaft angemessen zu bewältigen, ist bislang nicht ausreichend hinterfragt worden. Der TLfDI freut sich auf eine fruchtbare Diskussion

Anlage 51

Pressemitteilung
vom 30. Januar 2015

TLfDI fordert: Deutschland oben ohne –
Drohne!

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Da können schon Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, den Nacktbadebereich am See oder in sonstige nicht einfach zugängliche Orte.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) weist darauf hin, dass eine legale Drohennutzung durch **Private** in Deutschland nur unter äußerst engen Voraussetzungen zulässig ist. Zahlreiche Rechtsvorschriften müssen beachtet werden:

Sobald mit der Kamera Menschen gefilmt und damit personenbezogene Daten erhoben werden, müssen das Recht am eigenen Bild und das Grundrecht auf informationelle Selbstbestimmung beachtet werden. Selbst wenn mögliche datenschutzrechtliche Erlaubnisnormen (§§ 6b, 28 und 32 Bundesdatenschutzgesetz) einschlägig wären, würden in aller Regel die schutzwürdigen Interessen der Betroffenen überwiegen. „**Folglich darf mit der Kamera einer Drohne grundsätzlich niemand gegen seinen Willen gefilmt werden**“, betont der TLfDI.

Leider existieren in Deutschland keine verbindlichen eindeutigen Regelungen speziell für Drohnen im zivilen Bereich. Das will die EU jetzt ändern. Sie fordert strenge Regulierung für zivile Drohnen (http://europa.eu/rapid/press-release_IP-14-384_de.htm). Der TLfDI begrüßt diese Entwicklung ausdrücklich. Da die Drohennutzung in einigen Bereichen, wie im Straßen- und Eisenbahnbrückenbau oder in der Forst- und Landwirtschaft durchaus sinnvoll sein kann, bedarf es konkreter Bestimmungen, wie der datenschutzgerechte Umgang mit Drohnen auszusehen hat.

Einen guten Überblick über die *luftverkehrsrechtlichen* Anforderungen gibt die „Kurzinformation über die Nutzung von unbemannten Luftfahrtsystemen“ (unter <http://www.bmvi.de//SharedDocs/DE/Publikationen/VerkehrUndMobilitaet/unbemannteluftfahrtsysteme.html>).

Anlage 52

Pressemitteilung
vom 6. Februar 2015

Sind sie noch da?

Bei der Entsorgung oder Weitergabe von PCs, Laptops und Smartphones, aber auch von externen Festplatten, USB-Sticks und SD-Karten kommt es leider häufig vor, dass vergessen wird, die darauf befindlichen Daten datenschutzgerecht zu löschen.

Aus gegebenem Anlass möchte der TLfDI deshalb nochmals darauf hinweisen, dass ein reiner Löschbefehl in der Regel für die Datenlöschung nicht ausreichend ist und somit die Daten mit relativem geringem Aufwand wieder herstellbar sind.

Selbst das vollständige Formatieren einer Festplatte oder eines anderen Datenträgers - also die Wiederherstellung des Urzustandes einer Festplatte/eines Speichermediums - ist zum Löschen ungeeignet, da nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die Zuverlässigkeit der Löschung der vorhandenen Daten keine Aussage getroffen werden kann (BSI: Überblick über Methoden zur Löschung und Vernichtung von Daten).

PCs, Laptops:

Auf der Webseite des BSI <https://www.bsi-fuerbueger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen.html> finden Sie entsprechende Hinweise zu derzeit vom BSI dem Stand der Technik empfohlenen Lösch-Programme für PCs und Laptops.

Die dort vom BSI empfohlenen Programme zum Überschreiben der Festplatte, die auch zum Teil kostenlos sind, sollten auf jeden Fall Anwendung finden, wenn Sie Ihr Gerät entsorgen oder veräußern möchten. Wichtig ist dabei, dass Sie genau den Anleitungen des Herstellers folgen und die Anleitungen der jeweiligen Lösch-Software genau beachten.

Nachfolgend sollen an Hand des Löschmodprogrammes DBAN die ersten Schritte erklärt werden, wenn Sie bspw. Daten auf einem Windows XP-Rechner löschen wollen. Wichtig: danach sind alle Daten (inklusive Betriebssystem) unwiderruflich gelöscht:

- Halten Sie eine CD oder einen USB-Stick bereit, worauf Sie das Löschmodprogramm speichern können.
- Gehen Sie auf die Webseite <https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen.html> und informieren Sie sich über die derzeit aktuell empfohlenen Löschmodprogramme.
- Suchen Sie sich eines der Löschmodprogramme aus und folgen Sie dem angegebenen Link.
- Beim Löschmod-Programm DBAN müssten Sie dann bspw. auf die Webseite von ComputerBild <http://www.computerbild.de/download/DBAN-Darik-s-Boot-and-Nuke-945107.html> gehen, um die Datei auf einen funktionsfähigen PC herunterzuladen.
- Starten Sie dort „Download“, um die Datei herunter zu laden.
- Diese Datei ist ein ISO-Image und kann nicht von Windows ausgeführt werden, sondern stellt ein eigenes, in sich geschlossenes Betriebssystem dar.
- Sollten Sie über einen CD-Brenner verfügen - brennen Sie diese Datei entsprechend Ihrer Brennersoftware auf die CD.
- Sollten Sie mit einem USB-Stick arbeiten, benötigen Sie noch eine entsprechende Software: (z. B. <http://www.computerbild.de/download/ISO-to-USB-6559588.html>), um das Löschmod-Programm auf den USB-Stick zu „brennen“.

- Wenn der Datenträger entsprechend vorbereitet ist, starten Sie den zu löschenden Rechner, so dass dieser Rechner mit der CD oder dem USB-Stick starten kann.
- Folgen Sie nun den Anweisungen des Programms.

Hinsichtlich der Geräte mit dem Betriebssystem Windows 8 bzw. 8.1, ist auch ein Löschen der Daten direkt möglich. Dies ist allerdings nur der Fall, wenn die Funktion von Windows 8 „Alles entfernen und Windows neu installieren“ und die Option zur gründlichen Löschung gewählt wird. Außerdem muss ebenso sichergestellt sein, dass alle Laufwerke (und nicht nur das Systemlaufwerk) durch die gründliche Löschung erfasst werden, was nur für Laufwerke gilt, die durch Windows lesbar sind. Ist dies nicht möglich, muss wie oben beschrieben verfahren werden.

Smartphones:

Dateien auf Smartphones zu Löschen ist komplizierter. Das Zurücksetzen des internen Speichers auf die Werkseinstellungen bringt meistens keine Datensicherheit.

Wie das tatsächliche Löschen bei Smartphones funktioniert und welches Programm ggf. zum Einsatz kommen sollte, ist für viele Modelle und Betriebssysteme unterschiedlich und bedarf auch hier der korrekten Anwendung der Anleitung des jeweiligen Anbieters. Um die Daten des Smartphones sicher löschen zu können, müssen Sie also die Bedienungsanleitung des Herstellers genau beachten. Einige Hersteller bieten auch auf ihren Online-Portalen spezielle Programme (Apps) zum Löschen an, die das mehrfache Überschreiben mit Zufallsdaten versprechen.

Zudem rät das BSI in seiner Empfehlung „Basisschutz für Smartphone und Co“, auch die SIM-Karte zu entfernen und – falls Sie diese nicht weiter verwenden wollen – zu vernichten.

An dieser Stelle sei nochmal darauf hingewiesen, dass Sie selbst auch zusätzlich die Sicherheit Ihrer Daten auf dem Smartphone erhöhen können:

- Installieren Sie Programme, also Apps, nur von vertrauenswürdigen Quellen.
- Schauen Sie in der Bedienungsanleitung oder im Online-Shop des Herstellers nach, ob Daten auf Ihrem Smartphone verschlüsselt werden können und nutzen sie dies.
- Lassen Sie bei Verlust Ihres Gerätes die SIM-Karte unverzüglich sperren. Manche Hersteller bieten an, dann das Gerät aus der Ferne wenigstens zurückzusetzen oder zu sperren. Ein Zugriff auf die Daten wird dadurch erschwert.

Eins ist sicher – die Frage, ob die Daten auf dem Smartphone noch vorhanden sind, also für Unbefugte wiederherstellbar sind, kann niemand beantworten.

Überlegen Sie sich daher genau, wie Sie Ihren PC, Laptop oder Ihr Smartphone vor der Weitergabe vorbereiten und ob Sie diese Geräte überhaupt in fremde Hände geben wollen.

Auch wenn Sie evtl. dafür momentan sogar einen finanziellen Gewinn erzielen, kann Sie das später teuer zu stehen kommen – Erfahrungswerte aus der täglichen Praxis des TLfDI!!!

Sollten Sie nicht selbst die Daten löschen oder das Gerät nicht physisch zerstören können, sollten Sie eine vertrauenswürdige Computerfirma mit der Löschung der Daten oder Vernichtung des Gerätes beauftragen.

Pressemitteilung
vom 20. Februar 2015

YouNow – All know!

YouNow – eine trendige Bühne um sein Leben mit anderen zu teilen, nicht mal eben mit ein paar hundert Freunden sondern mit allen Internetnutzern auf dem Globus, jetzt sofort und live. Die Plattform „www.younow.com“ macht es möglich. Vor allem Jugendliche sitzen zu Hause im Kinderzimmer, schalten Handy oder PC-Kamera ein und plaudern mit Chatpartnern. So weit, so alt. Das Besondere an YouNow: Die Internetwelt ist live und ohne Anmeldung dabei. Wer mitplaudern will, kann nach einfacher Anmeldung mit seinem Facebook-, Twitter- oder Google-Account im Chat loslegen oder selbst „broadcasten“. – Ganz cool, aber wo ist der Haken?

Entsprechend der Datenschutzrichtlinie von YouNow sind jegliche Ersuchen hinsichtlich des Datenschutzes an eine Adresse in New York, USA zu richten. Deutsche gesetzlich vorgeschriebene Datenschutzstandards sind also kaum durchzusetzen. Zudem haben amerikanische Geheimdienste bei Bedarf den vollen Zugriff auf die Daten. Beim Streamen sollten einige Regeln beachtet werden, um sich nicht ungewollt selbst in Gefahr zu bringen oder Persönlichkeitsrechte anderer zu verletzen: Seinen Klarnamen, die Wohnadresse, die Schule oder seinen Aufenthaltsort zu bestimmten Zeiten vor der Kamera auszuplaudern, kann sehr gefährlich werden, wenn sich hinter dem scheinbar netten Girl im Chat ein Pädophiler verbirgt, der einen unbedingt persönlich kennenlernen will.

Heimliche Streams aus dem Klassenzimmer mit Mitschülern und Lehrern in Wort und Bild sind zu unterlassen. Nicht nur, weil damit Persönlichkeitsrechte anderer verletzt werden, sondern auch, weil die Aufnahme und Veröffentlichung unbefugt aufgenommener Gespräche nach § 201 StGB unter Strafe steht. Ganz nebenbei: Das Handy, mit dem aufgenommen wurde, wird dabei sehr wahrscheinlich eingezogen werden.

Nicht zuletzt: Wer streamt, sollte keine Musik im Hintergrund laufen lassen, denn die würde ja mit in die Welt geschickt und es ist nicht ausgeschlossen, dass durch die Gesellschaft für musikalische Auf-

führungs- und mechanische Vervielfältigungsrechte (GEMA) Gebühren erhoben werden. Also: **Passt auf Euch auf!**

Pressemitteilung
vom 15. April 2015

Neuer Beirat beim TLfDI: Frischer Wind!

Nach der Landtagswahl fand am 13.04.2015 die erste und konstituierende Sitzung des Beirats beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) statt. Als neue Vorsitzende wurde die Abgeordnete Katharina König (Die Linke), als Stellvertreter der Abgeordnete Andreas Bühl (CDU) gewählt.

Im Anschluss an die Wahl informierte der TLfDI die Mitglieder über wichtige Projekte seiner Behörde:

Er arbeitet derzeit an Entwürfen zur Novellierung des Thüringer Datenschutzgesetzes und des Thüringer Informationsfreiheitsgesetzes - und darf dabei auch mit der vollen Unterstützung des Beirats rechnen.

Die Länder Berlin, Brandenburg, Thüringen, Sachsen und Sachsen-Anhalt planen, ein Gemeinsames Kompetenz- und Dienstleistungszentrum der Polizei zur Telekommunikationsüberwachung einzurichten. Aufgrund der Eingriffsintensität von solchen Maßnahmen kommt einer intensiven datenschutzrechtlichen Begleitung des Vorhabens ein besonderer Stellenwert zu.

Der TLfDI berichtete außerdem über seine Initiativen im Bereich der Bildung von Medienkompetenz bei Schülern. So wird beispielsweise an einem Thüringer Gymnasium eine vom TLfDI entwickelte Unterrichtseinheit zum Datenschutz mit dem Schwerpunkt „Videoüberwachung“ erprobt. Mit dem Fach/Kurs Medienkunde werden neue Wege zu gehen sein.

Die Mitglieder des Beirates nahmen sich aufgrund dieser zahlreichen aktuellen Datenschutzfragen vor, künftig häufiger als in der letzten Legislaturperiode zusammenzukommen – spannende Zeiten!!! ;-)

Anlage 55

Pressemitteilung
vom 13. Mail 2015

Bei Anruf – Betrug!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse, hat von seinem Berliner Amtskollegen Kenntnis über folgende betrügerische Maschen erhalten, die ihn zu Warnungen veranlasst: Vorgetäuscht wird zu einem der Anruf des Datenschutzbeauftragten oder eines seiner Mitarbeiter, um Kreditkarten- oder Bankdaten zu erfragen. Es wird das Vertrauen zum TLfDI missbraucht und unter dem Deckmantel einer Überprüfung eine vermeintliche Datenpanne vorgetäuscht. Es ist indes abwegig, dass sich der TLfDI mit Bürgern ohne vorherigen schriftlichen Kontakt telefonisch in Verbindung setzt, um sich nach derartigen Daten zu erkundigen. Die erwähnten verdächtigen Anrufe dienen denn auch regelmäßig missbräuchlichen Zwecken. Die Bürger, zumeist ältere Menschen, werden am Telefon aufgefordert, ihre Kartennummern von aufladbaren Kreditkarten – zum Beispiel einer Karte aus dem Supermarkt – zu nennen. Zum Teil werden sie sogar dazu aufgefordert, sich solche Prepaid-Karten im Supermarkt zu besorgen, um dann dem Anrufer – dem vermeintlichen Datenschutzbeauftragten – die Kartennummern zu nennen. Damit hat der Anrufer Zugriff auf das Prepaid-Guthaben. **bleiben Sie also wachsam!**

Damit nicht genug: Andere Betrüger geben vor, die „Euron Union d.o.o.“ aus Slowenien zu sein. Sie täuschen nach Überweisung eines dreistelligen Euro-Betrags auf ein Konto den Verkauf eines „EU-Schutzpakets“ für private Rufnummern vor, das einen Eintrag in ein „EU-Schutzregister“ beinhaltet, um ungewollte Werbung und Anrufe zu minimieren. Auch hierbei handelt es sich um Betrug, denn es kommt zu keinem Eintrag in das Schutzregister.

Der TLfDI warnt davor, persönliche Daten, insbesondere Anschrift und Kontoverbindung, an unseriöse Anrufer oder Adressaten herauszugeben. **Seien Sie vorsichtig!** Gibt es Verdachtsmomente für ein strafbares Verhalten, sollten die Strafverfolgungsbehörden (örtliche

Polizeidienststelle oder Staatsanwaltschaft) informiert werden. Hilfe bieten auch Verbraucherzentralen an – und natürlich der TLfDI :-)

Pressemitteilung
vom 12. Juni 2015

Datenschutzkonferenz verabschiedet EntschlieÙung
gegen den Gesetzentwurf zur Vorratsspeicherung
von Telekommunikationsverkehrsdaten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9. Juni 2015 eine Umlaufentschließung gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten verabschiedet. In ihrer Entschließung weisen die Datenschutzbeauftragten auf ihre erheblichen verfassungsrechtlichen Bedenken gegen den Gesetzentwurf der Bundesregierung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für die Sicherheitsbehörden hin und stellen diesen in Frage. Nachfolgend möchte ich Sie über den Inhalt der Entschließung in Kenntnis setzen:

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Juni 2015:

Gegen den Gesetzentwurf zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken.

Mit der Vorlage des "Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratspeicherung von TK-Verkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen. Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt. Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde. Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen

unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt. Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtsbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird. Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen. Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Anlage 57

Pressemitteilung
vom 3. Juli 2015

Fingerabdruckscanner in der Schule – Finger weg!

- TLfDI nimmt eingesetztes System unter die Lupe -

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist bekannt geworden, dass die Schüler einer Thüringer Grundschule ihr Mittagessen mittels ihrer Fingerabdrücke bestellen und bezahlen können. Der Essensanbieter will dadurch die Bezahlung vereinfachen und effizienter gestalten. Neben der Möglichkeit der Identifizierung des Schülers über den Fingerabdruck besteht dort auch die Möglichkeit der Nutzung eines Funk-Chips. Ob aufgrund der Schaffung dieser Alternativmöglichkeit das Verfahren prinzipiell datenschutzrechtlich zulässig ist, wird der TLfDI zeitnah in der betroffenen Schule datenschutzrechtlich prüfen. Besonderes Augenmerk wird er dabei auf die Datensicherheit der Fingerabdruckdaten und die Verhältnismäßigkeit der Datenverarbeitung legen. Fingerabdrücke sind als biometrisches Merkmal besonders kritisch, da bei einem Datenklau auch die Identität einer Person „kopiert“ werden kann. Dann sind die Folgen über ein ganzes Leben nicht absehbar.

Persönliche Daten, die gar nicht erst erhoben werden, sind am sichersten geschützt!

Unabhängig vom Prüfergebnis rät der TLfDI den betroffenen Eltern von der Nutzung des Fingerabdruckscanners durch ihre Kinder ab, da zudem nicht absehbar ist, welche Begehrlichkeiten die so erhobenen Daten wecken können.

Anlage 58

Pressemitteilung
vom 6. Juli 2015

Schutzbund der Senioren und Vorruehst ndler Th ringen e.V.

WANTED!

Gesucht werden: Maus-Liebhaber!

Der Th ringer Landesbeauftragte f r den Datenschutz und die Informationsfreiheit (TLfDI) und der Schutzbund der Senioren und Vorruehst ndler Th ringen e.V. (SBSV) sind gemeinsam auf der Suche nach Menschen f r die neue Werkstatt der Generationen. Menschen, die heute in den Ruhestand gehen, haben unter Umst nden Jahre ihres Berufslebens am Computer verbracht. Nach Dienstschluss haben sich viele privat weiter mit den spannenden M glichkeiten der Computertechnik besch ftigt und manche Geheimnisse entdeckt. Sie haben sich komfortable Techniken angeeignet und neue Anwendungen ausprobiert. Dabei sind Sch tze an Wissen entstanden. Diese Wissenssch tze sollen gemeinsam gehoben und auch anderen zug nglich gemacht werden. Wir suchen Wissende, die ihr Wissen teilen und den Kern einer Initiative bilden wollen, die Silver Surfer und Computerfreaks zusammenbringt. Das Anliegen ist es, gemeinsam zu t fteln und zu  ben, Kenntnisse zu vertiefen und Erfahrungen auszutauschen. Wir wollen mit unserer Kooperation den Erwerb von Medienkompetenz f r Seniorinnen und Senioren erm glichen und Surfer im Netz f r den notwendigen Schutz ihrer Daten im Internet sensibilisieren. Der Schutzbund der Senioren und Vorruehst ndler Th ringen e.V. stellt in seinem Kompetenz und Beratungszentrum am Juri-Gagarin-Ring diese Rahmenbedingungen zur Verf gung. Mit dem Th ringer Landesbeauftragten f r den Datenschutz und die Informationsfreiheit (TLfDI) hat der Schutzbund der Senioren einen engagierten und fachkundigen Partner an seiner Seite. Wer seine Kenntnisse und F higkeiten in die **Gr ndung eines SeniorenComputerClubs (SCC)** in Erfurt einbringen m chte, wendet sich bitte an:

Frau Marianne Schwalbe, Leiterin des Kompetenz- und Beratungszentrums, Juri-Gagarin-Ring 64, in 99084 Erfurt, Tel.: 0361-78929902, E-Mail: schwalbe@senienschutzbund.org

Anlage 59

Pressemitteilung
vom 5. August 2015

Windows 10 – Fenster zur Privatsphäre

Seit ein paar Wochen ist das Produkt Windows 10 von Microsoft auf dem Markt. Microsoft bietet sogar ein kostenloses Upgrade, also den Wechsel von alten Windows Betriebssystemen auf Windows 10 an. Zudem wirbt Microsoft damit, dass Windows 10 „voller fantastischer Innovationen“ steckt. Richtig! Denn Microsoft hat nun für sich entdeckt, dass Daten über die Nutzer und die verwendeten Geräte und deren Standorte innovativ für Microsoft selbst und für seine Geschäftspartner und Tochterunternehmen genutzt werden können.

Welche Gefahren drohen?

Wie durch die Fachpresse mitgeteilt wird, werden nach der Standardinstallation von Windows 10 Informationen wie Namen, E-Mail Adressen, Telefonnummern, Standorte, Gerätekennungen, IP-Adressen, der Browserverlauf und die Browserfavoriten an Microsoft übertragen. Außerdem behält sich Microsoft das Recht vor, auch Inhalte von in der Cloud gespeicherten Dateien auszuwerten, falls dies als „erforderlich“ angesehen wird (siehe dazu <http://www.microsoft.com/de-de/privacystatement/default.aspx>, Unterpunkt „Personifizierte Daten, die wir sammeln“ – „Mehr erfahren“ – „Inhalte“)!

Das können Sie tun:

Viele Dienste zur Datensammlung können deaktiviert werden. Dazu müssen Sie bspw. unter dem Punkt „Einstellungen -> Datenschutz“ in den 13 Kategorien Ihre persönlichen Einstellungen vornehmen. Eine ausführliche Anleitung, wie man dies bewerkstelligen kann, ist unter <http://www.computerbase.de/2015-07/windows-10-test/7/> zu finden.

!Schützen Sie Ihre Daten und Ihre Privatsphäre!

Anlage 60

Pressemitteilung
vom 12. August 2015

Aktenlager in Immelborn - Desaster mit Lerneffekt

Wie noch bekannt sein dürfte, wurden in der kleinen thüringischen Gemeinde Immelborn in einem alten, nicht hinreichend gesicherten Fabrikgebäude hunderttausende Akten unsachgemäß gelagert.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm diesen Vorfall zum Anlass, sich auch mit den dortigen tatsächlichen und rechtlichen Fehlentwicklungen näher zu befassen. Zu diesem Zweck traf er sich regelmäßig mit Unternehmern aus der Aktenarchivierungsbranche und betrieblichen Datenschutzbeauftragten. Gemeinsam entwickelten sie eine **Orientierungshilfe Aktenarchivierung**. Hiermit wird Archivierungsdienstleistern (Auftragnehmern) und Unternehmen / Privatpersonen (Auftraggebern) ein Leitfaden an die Hand gegeben, mit dem sie sich im Dschungel der Vorschriften und deren Auslegungen zurechtfinden sollen. Die Orientierungshilfe unterstützt die Praxis dabei, sich ein Urteil darüber zu bilden, welche Pflichten dem Archivierungsdienstleister obliegen und welche notwendigen Anforderungen der Auftraggeber bei Einlagerung seiner Akten zu beachten hat.

Diese Arbeiten sind nun abgeschlossen. Die Orientierungshilfe legt klar dar, was der Auftraggeber als verantwortliche Stelle bei der Einlagerung, Verwaltung und Vernichtung von Akten zu beachten hat und was ein Archivierungsunternehmen hierfür tatsächlich leisten können muss. Anhand von Checklisten kann ermittelt werden, ob ein Archivierungsunternehmen gemessen an der Brisanz der einzulagernden Akten - z. B. medizinische Akten, Personalunterlagen, geheime Geschäftsunterlagen - für die Auftragerfüllung geeignet ist oder eben nicht. Für Hilfe bei der datenschutzkonformen Vertragsgestaltung sorgen konkrete Hinweise und Muster.

Da die Orientierungshilfe einen bundesweiten Standard zur Verankerung des Datenschutzes in der Archivierungsbranche setzen soll,

wird sie zunächst den Aufsichtsbehörden der anderen Länder zur Abstimmung vorgelegt. Damit möchte der TLfDI erreichen, dass für alle Archivierungsunternehmen in Deutschland einheitliche Anforderungen gelten. Nach diesem Abstimmungsprozess wird der TLfDI die Orientierungshilfe vorstellen.

Anlage 61

Pressemitteilung
vom 18. September 2015

SeniorenComputerClub Erfurt – Start gelungen

Knapp 50 Seniorinnen und Senioren folgten dem Vorschlag, sich zur Gründung von Interessengruppen im SeniorenComputerClub (SCC) beim Schutzbund der Senioren und Vorruheständler Thüringen e. V. im Juri-Gagarin-Ring 56 a zur Auftaktveranstaltung einzufinden. Dieses überwältigende Echo zeigt, dass sich auch Menschen im fortgeschrittenen Alter intensiv mit der digitalen Technik befassen und gern gemeinsam über Neuigkeiten und Probleme diskutieren und zu neuen Erkenntnissen kommen wollen. In Anwesenheit von Dr. Lutz Hasse, dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, stellten Detlef Wagner und Marianne Schwalbe das Konzept des Clubs vor. Innerhalb des Clubs wurden vier Interessengruppen gebildet, die sich mit den Themen: Bild/Film/Musik, Internet, soziale Netzwerke und Windows 10 beschäftigen werden. Eine weitere Gruppe fand sich unter der Bezeichnung „Zum Neustart entschlossen“ zusammen, die sich – wieder – mit dem Thema Computer auseinandersetzen will. Dr. Lutz Hasse stellte in seinem Beitrag die Bedeutung des Internets als Faktor der Lebensqualität mit all seinen Fallen und den erforderlichen Vorsichtsmaßnahmen heraus. Vorträge zu Fragen der Sicherheit im Internet, zu rechtlichen Gesichtspunkten (z. B. Urheberrecht, Bildrechte usw.) und anderen relevanten Aspekten werden in eigens dafür vorgesehenen Veranstaltungen für alle Gruppen angeboten werden. Detlef Wagner, Informatiklehrer und Gründungsmitglied, der sich ehrenamtlich für die Umsetzung der Idee des SCC einsetzt, wird seine Kenntnisse und Erfahrungen in die Gruppen einbringen. „Wir sind auf die Anregungen durch die neuen Gruppen gespannt, erwarten kreative Diskussionen und bieten gern den Rahmen und Unterstützung für diese Form der Weiterbildung“, freut sich Marianne Schwalbe, Leiterin des Kompetenz- und Beratungszentrums.

Anlage 62

Pressemitteilung
vom 6. Oktober 2015

Unsafe harbor

Datenschutzbeauftragter Dr. Hasse: Der EuGH hat den „unsicheren Hafen“ endlich geschlossen

„Mit seinem Urteil zum Safe-Harbor-Abkommen (zu Deutsch: Sicherer-Hafen-Abkommen) hat der Europäische Gerichtshof (EuGH) die Rechtspositionen der Datenschutzbeauftragten des Bundes und der Länder deutlich gestärkt – dies ist ein Meilenstein für den Datenschutz in Europa, Deutschland und in Thüringen“, kommentiert Thüringens Datenschutzbeauftragter, Dr. Lutz Hasse, die Entscheidung der Luxemburger Richter. Der EuGH habe den „unsicheren Hafen“, so Hasse, heute zu Recht geschlossen und dessen Regelungen für ungültig erklärt, weil sie keinen ausreichenden Schutz vor Grundrechtseingriffen durch amerikanische Behörden geboten hätten. „Das haben die deutschen Datenschutzbehörden seit den Enthüllungen Edward Snowdens im Sommer 2013 immer wieder kritisiert“, erinnert Lutz Hasse. Seine KollegInnen und er hatten seit damals die Aussetzung einer Datenübermittlung in die USA, basierend auf dem Safe-Harbor-Abkommen, gefordert, weil dessen Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und der Zweckbindung eines behördlichen Datenzugriffs von US-amerikanischen und anderen Sicherheitsdiensten schlichtweg ignoriert wurden. Erfreut zeigte sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch über den klaren Hinweis des EuGH, dass die Kommission keine Kompetenz hatte, die Befugnisse der nationalen Datenschutzbehörden mit der Unterzeichnung des Safe-Harbor-Abkommens zu beschränken. Hasse: „Damit stärken die Luxemburger Richter erneut die Unabhängigkeit der Datenschutzbehörden.“ Zudem empfahl Hasse, die geplanten Regelungen der neuen EU-Datenschutz-Grundverordnung im Lichte dieser sehr deutlichen EuGH-Rechtsprechung zu überdenken. „Man muss sich nun die Zeit nehmen, die Auswirkungen dieses wegweisenden Urteils auf die vorgesehene Datenschutz-Grundverordnung

zu erkennen und deren Regelungen an der Entscheidung ausrichten“, so der TLfDI.

Anlage 63

Pressemitteilung
vom 3. November 2015

Kein Wildwuchs mehr bei Videoüberwachung im ÖPNV

Videoüberwachung nimmt in allen Lebensbereichen zu. Diese Entwicklung hat leider auch vor Zügen, Straßenbahnen und Bussen nicht halt gemacht. Trotz oder gerade weil in diesem Segment das Instrument der Videoüberwachung sehr geschätzt ist, wird sie oft über das zulässige Maß hinaus eingesetzt. Der Kameraeinsatz muss da enden, wo das Bundesdatenschutzgesetz die Grenzen für diese Art der Datenerhebung setzt. Zu diesem Zweck haben die Aufsichtsbehörden der Länder unter wesentlicher Beteiligung von Mitarbeitern des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine neue Orientierungshilfe für den Bereich Videoüberwachung in öffentlichen Verkehrsmitteln erarbeitet. Darin wird eine aktuelle, umfassende und klare Position der Aufsichtsbehörden für den Datenschutz zum Einsatz von Videotechnik in öffentlichen Verkehrsmitteln zum Ausdruck gebracht. Die Orientierungshilfe finden Sie auf unserer Homepage zum Download. (https://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_v_____pnv_stand_09_2015_dk.pdf)

Eine Videoüberwachung ist eine Datenerhebung, die, wie in allen anderen Bereichen auch, im Einklang mit dem Grundrecht auf informationelle Selbstbestimmung der Fahrgäste stehen muss. So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgast-raumes, der sich die Fahrgäste nicht entziehen können einen besonders intensiven Eingriff dar, der in aller Regel nicht zulässig sein dürfte. Entscheidend sind aber immer die besonderen Umstände des Einzelfalles. Daher wendet sich das Papier an Unternehmer, um Hilfestellung zu leisten, eine Videoüberwachung im Einzelfall gesetzeskonform auszurichten. Auch ausschreibenden Institutionen gibt sie eine notwendige Orientierung. Denn bei den derzeitigen Ausschreibungen für Busse und Bahnen sehen sich Unternehmer oftmals außer Stande, eine gesetzeskonforme Videoüberwachung zu installieren, die den gesetzlichen Vorgaben entspricht.

Pressemitteilung
vom 20. November 2015

NEU: Digitale Selbstverteidigung –
Youngdata hat die Tipps für Kids

Kindern und Jugendlichen stehen heute zahlreiche Möglichkeiten der Mediennutzung offen. In den meisten Fällen sind sie jedoch noch nicht in der Lage, die Vorteile und die Gefahren, die sich daraus ergeben, richtig einzuschätzen und danach zu handeln. Datenschutz als Schutz der Privatsphäre spielt dabei eine ganz wesentliche Rolle. Seit zwei Jahren gibt es ein Internet-Angebot der Datenschutzbeauftragten des Bundes und der Länder – Youngdata – ein seit dem Safer Internet Day 2015 gemeinsames Portal, das sich mit Datenschutzhinformationen gezielt an Kinder und Jugendliche richtet. Hier finden die Kids Informationen zum Datenschutz und zur Informationsfreiheit, Tipps für ein kluges Verhalten im Internet und Berichte über die digitale Zukunft unserer Gesellschaft. Youngdata enthält Informationen zum Selbstschutz bei der Nutzung von Facebook, WhatsApp, Skype & Co., YouTube, Spielekonsolen, Smartphones und anderen Anwendungen. Es klärt über die Gefahren von Cybermobbing auf und bietet Hintergrundinformationen zum Datenschutz im Allgemeinen. Zum zweijährigen Bestehen wird diese Internetseite jetzt um eine Rubrik erweitert – die „Digitale Selbstverteidigung“. Diese leider erforderlich gewordene Rubrik gibt Tipps, die helfen sollen, private Informationen zu schützen. Sie zeigt auf, welche Möglichkeiten junge User haben, durch ihr eigenes Verhalten digitale Spuren zu vermeiden und die Kontrolle über ihre Daten zu behalten. Die Pflege der Rubriken von Youngdata erfolgt im Wege einer Arbeitsteilung bei den einzelnen Landesdatenschutzbeauftragten. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat als Vorsitzender des Arbeitskreises Datenschutz und Bildung den Bereich „Informationsfreiheit“ und „Videoüberwachung“ übernommen.

Anlage 65

Pressemitteilung
vom 1. Dezember 2015

Revolution
beim 13. Arbeitskreis Datenschutz und Bildung
Wow – das ging ab:

Vom 30. November bis zum 1. Dezember tagte der 13. Arbeitskreis (AK) Datenschutz und Bildung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Erfurt unter Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Herrn Dr. Lutz Hasse. In dieser Funktion hatte der TLfDI in Berlin Kontakt zu der Ständigen Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (Kurzform: Kultusministerkonferenz, Abk. KMK) aufgenommen. Vertreter der KMK waren heute erstmals im AK anwesend – und: Sie haben intensiv eine Kooperation zwischen der KMK und den Datenschutzbeauftragten der Länder, speziell mit dem AK Datenschutz und Bildung angefragt. „Das ist revolutionär!“, so Dr. Lutz Hasse gemeinsam mit den Vertretern der KMK. Die Datenschutzbeauftragten wollen sich zusammen mit den zuständigen Gremien der KMK u. a. der drängenden Frage widmen, wie Medienkompetenz Schülern, Studenten, Lehrern und auch Eltern in attraktiver Weise nahe gebracht werden kann. Der AK Datenschutz und Bildung hatte in den letzten Jahren stets bemängelt, dass es auf diesem Gebiet nicht voran ging, obwohl die Defizite offenkundig waren. Nun aber soll es endlich losgehen; euphorisiert werden die Datenschützer versuchen, diesen Prozess möglichst zu beschleunigen. Mit von der Partie ist auch unsere Kultus-Staatssekretärin Frau Gabi Ohler, die – speziell mit Blick auf Thüringen – den Datenschutz (inklusive TLfDI) bzw. den Schutz der Privatsphäre bei der Vermittlung von Medienkompetenz umfassender einbinden will. Hasse: „War wirklich sehr angetan von der heutigen Aufbruchsstimmung und hoffe, dass wir aus dem heutigen und den künftigen Meilensteinen einen frostsicheren Medienkompetenz-Weg bauen können, für Schüler, Lehrer und Eltern!“

Pressemitteilung
vom 2. Dezember 2015

Premiere: Heilmittel für Krankenhäuser
TLfDI startet speziellen Blog zu Datenschutzproblemen im
Gesundheitsbereich

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Herr Dr. Lutz Hasse lädt Sie zum offiziellen Start des TLfDI-Blogs für Krankenhäuser auf seiner Internetstartseite www.tlfdi.de ein.

Wann: Mittwoch, 9. Dezember 2015, 10 Uhr
Wo: Behörde des TLfDI, Häbelerstraße 8, 3. Etage, 99096 Erfurt

Bei dem Blog des TLfDI ist ein geschlossener Bereich für Krankenhäuser eingerichtet. Dieser ist nur für erfolgreich registrierte und freigegebene Benutzer, sprich Thüringer Krankenhäuser, die sich über die Landeskrankengesellschaft autorisiert haben, zugänglich. Es ist eine Plattform, auf der sich Krankenhäuser anonym mit ihren Fragen zum Datenschutz an den TLfDI wenden können. Weitere Blogs sind in der Pipeline.

Ziel ist es, dass Krankenhäuser, die erfahrungsgemäß eine Fülle von Datenschutzproblemen zu bewältigen haben, ihre Fragen anonym an den TLfDI richten können, damit derartige Probleme nicht "hinter dem Berg" gehalten werden. Nur so können wir die bisweilen komplexen Schwierigkeiten erkennen, sezieren und Wege zur Genesung anbieten.

Anlage 67

Pressemitteilung
vom 9. Dezember 2015

TLfDI startet als erster Landesdatenschützer ein Internet-Forum für
Krankenhäuser!

Erfurt, 9. Dezember 2015: Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse und der Geschäftsführer der Landeskrankenhausgesellschaft Thüringen e. V. (LKHG), Michael Lorenz starteten heute mit einem offiziellen Knopfdruck das erste Internet-Forum für Krankenhäuser auf der Website eines Landesdatenschutzbeauftragten. Es handelt sich dabei um ein geschlossenes Forum, das nur für erfolgreich registrierte und freigegebene Thüringer Krankenhäuser, zugänglich ist. Die Krankenhäuser haben sich zuvor über die LKHG autorisiert. „Die Landeskrankenhausgesellschaft Thüringen e. V. unterstützt die Einrichtung dieses Forums. Die Thüringer Krankenhäuser können sich nunmehr bei datenschutzrechtlichen Fragestellungen schnell und unkompliziert an den Landesdatenschutzbeauftragten Thüringens wenden“, so Michael Lorenz. Ziel ist es, dass Krankenhäuser, die täglich mit einer Fülle von Datenschutzproblemen konfrontiert werden, ihre Fragen **anonym** an den TLfDI stellen können. „Nur so werden die bisweilen komplexen Schwierigkeiten offen angesprochen und gemeinsam auf einen guten Weg zur Heilung gebracht“, sagte Hasse. Beim Pressetermin wurde mit einer Live-Vorführung demonstriert, wie der Ablauf von der Anmeldung bis zur Antwort funktioniert. Hasse: „Ich empfangе Signale, dass Krankenhäuser auf dieses Forum warten – gut; unser Angebot ist gemacht.“

Anlage 68

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der
Datenschutz-Richtlinie im Bereich von Justiz und Inneres

29.Oktober 2015

Konferenz der unabhängigen Datenschutzbehörden des Bundes und
der Länder**I. Vorbemerkung**

Nachdem der Rat der Justiz- und Innenminister am 9. Oktober 2015 seinen Standpunkt zur Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) angenommen hat, beraten Kommission, Parlament und Rat im sogenannten Trilog über ihre verschiedenen Positionen zur JI-Richtlinie mit dem Ziel der gemeinsamen Verabschiedung von JI-Richtlinie und Datenschutz-Grundverordnung (DSGVO) im Paket zum Jahresende 2015.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Konferenz) hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012² mehrfach öffentlich zur Datenschutzreform positioniert. Am 26. August 2015 hat sie zu den Trilogverhandlungen zur DSGVO Stellung genommen³. Sie hat ferner zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben⁴. Von Anfang an hat sie das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“ und dabei auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus im Anwendungsbereich der JI-Richtlinie hingewiesen.

² Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

³ Triloggpapier der Konferenz zur DSGVO, abrufbar unter:
<https://www.datenschutz.hessen.de/entschliessungen.htm>

⁴ Stellungnahmen zur DSGVO und zur JI-Richtlinie vom 11.6.2012; Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012, jeweils abrufbar unter

<https://www.datenschutz.hessen.de/entschliessungen.htm> und
<https://www.datenschutz.hessen.de/taetigkeitsberichte.htm>

Mit dieser Richtlinie wird eine Lücke geschlossen, denn einen Rechtsakt, der die Datenverarbeitung in den Bereichen Polizei und Justiz in der EU umfassend regelt, kennt das EU-Recht bislang nicht. Dies hat die Konferenz in der Vergangenheit immer wieder kritisiert⁵.

Die Konferenz setzt sich für eine Richtlinie ein, die auf möglichst hohem Niveau eine Mindestharmonisierung innerhalb der Europäischen Union herbeiführt. Sie begrüßt insofern die Entwürfe von Rat und Europäischem Parlament, als beide eine Mindestharmonisierung festschreiben. Mit einer Richtlinie verbindet die Konferenz die Erwartung an den deutschen Gesetzgeber und die deutsche Rechtsprechung, weiterhin Impulsgeber für die Schaffung eines effektiven Datenschutzrechts zu bleiben.

Vor diesem Hintergrund bewertet die Konferenz die JI-Richtlinie als einen wichtigen Schritt zur Verbesserung des Datenschutzes in der Europäischen Union. Kernanliegen des Datenschutzes im Bereich der polizeilichen Datenverarbeitung ist es, Grenzen der Erfassung und Speicherung in polizeilichen Dateien zu setzen: Bürgerinnen und Bürgern müssen darauf vertrauen können, nicht in polizeilichen Dateien erfasst zu werden, wenn sie keinen Anlass für eine polizeiliche Speicherung gegeben haben. Rechtmäßig von der Polizei erhobene Daten dürfen nur unter besonderen Voraussetzungen auch für andere polizeiliche Zwecke verwendet werden. Wer beispielsweise Opfer oder Zeuge einer Straftat war, muss darüber hinaus darauf vertrauen können, dass seine Daten nur beschränkt und unter strengen Voraussetzungen von Polizeibehörden verarbeitet werden dürfen. Dieses sind nur einige grundsätzliche Forderungen, die in der JI-Richtlinie zu regeln sind. Dazu stellt die Konferenz mit Bedauern fest, dass die Regelungen dieser Grundanliegen insbesondere in der vom Rat vorgelegten Fassung häufig allgemein bleiben, sich im Wesentlichen in dem Verweis auf das nationale Recht erschöpfen oder gar gänzlich fehlen.

Einen ganz wesentlichen Impuls für das deutsche Datenschutzrecht im Bereich von Polizei und Justiz erwartet die Konferenz von den Regelungen zur Durchsetzung des Datenschutzrechts durch die Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Datenschutz muss effektiv durchsetzbar sein. Effektive Aufsicht

⁵ Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S.3.

muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Bei den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der JI-Richtlinie.

II. Die Vorschläge im Einzelnen

1. Keine Ausweitung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO!

Der Anwendungsbereich der JI-Richtlinie kann nicht isoliert betrachtet werden, sondern er bestimmt spiegelbildlich den Anwendungsbereich der DSGVO. Denn die DSGVO findet nach deren Art. 2 Abs. 2 lit. e keine Anwendung, soweit die JI-Richtlinie Anwendung findet. Vor diesem Hintergrund sind in der Vergangenheit verschiedene Entwürfe diskutiert worden, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-Richtlinie führen könnten. Auch die vorgelegte Version des Rates wirft insofern in Art. 1 Abs. 1 JI-Richtlinie Fragen auf, als der Anwendungsbereich der JI-Richtlinie um die Formulierung „zum Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit“ erweitert worden ist.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche der DSGVO und der JI-Richtlinie wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der Kommission enthält die JI-Richtlinie Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst sei, soweit sie nicht der Prävention einer Straftat diene. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizei unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter

einem Rechtsakt – der JI-Richtlinie – zusammenzufassen, solle der Anwendungsbereich der Richtlinie entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die Richtlinie zu fassen. Die Ordnungsverwaltung solle der JI-Richtlinie unterfallen, soweit sie Ordnungswidrigkeiten verfolgt. Damit stellt der Rat seine ursprüngliche Argumentation auf den Kopf. Denn diese Ausweitung der JI-Richtlinie führt gerade dazu, dass Ordnungsverwaltungen sodann sowohl der DSGVO als auch der JI-Richtlinie unterfielen, je nachdem welche Aufgabe sie erfüllten.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-Richtlinie für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Dies ist nach der vom Rat vorgelegten Fassung nicht der Fall. Die Datenverarbeitung anderer Behörden als der Polizeibehörden sollte weiterhin von der DSGVO geregelt werden.

Die Konferenz sieht die in der Ratsfassung hinzugefügte Erweiterung des Anwendungsbereichs der JI-Richtlinie zu Lasten der DSGVO kritisch. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte, wie im Entwurf der Kommission und des Europäischen Parlaments vorgesehen, von der DSGVO geregelt werden.

2. Die Durchbrechung der Zweckbindung darf nur in engen Grenzen erfolgen!

Die Konferenz hat in ihrer Stellungnahme vom 11. Juni 2012 die Klarstellung gefordert, dass die Regelungen über die Zweckbindung nicht so verstanden werden dürfen, „dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzung für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf“. Die Bedeutung der Zweckbindung wurde auch durch die Europäische Grundrechtecharta betont, in der sich in Art. 8 Abs. 2 die Zweckbindung als tragendes Prinzip des Datenschutzes findet. In der

Richtlinie sollte daher die Zweckbindung (Art. 4 Abs. 1 lit. b JI-Richtlinie) insgesamt strikter gefasst werden⁶.

Der Rat hat in seiner Fassung den ursprünglichen Vorschlag der Kommission in Art. 4 Abs. 2 dahingehend ergänzt, dass eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig ist, wenn es dafür nach anwendbarem (nationalen) Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhältnismäßig ist. Der Entwurf der Kommission enthielt insofern nur allgemeine Regelungen, nach der eine Weiterverarbeitung nicht „unvereinbar“ mit dem ursprünglichen Zweck der Erhebung und nicht exzessiv sein dürfe (Art. 4 Abs. 1 lit. b und c).

Die Konferenz bedauert insofern, dass der Entwurf des Rates keine ambitionierteren, strengeren Vorgaben macht. Die vorgeschlagenen Regelungen lassen nach der Auffassung der Konferenz einen zu weiten Rahmen, den auszufüllen ganz weitgehend dem nationalen Gesetzgeber überlassen wird. In Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) sollte der Begriff der Unvereinbarkeit von Datenverarbeitungen konkretisiert werden. Danach liegt eine Unvereinbarkeit vor, „wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen („hypothetischer Ersatzeingriff“)⁷.

Die Konferenz spricht sich für strenge Vorgaben an die Durchbrechung der Zweckbindung aus und regt insofern an, den Mitgliedstaaten konkrete Vorgaben für die Weiterverarbeitung zu machen. Der Begriff der Unvereinbarkeit in Art. 4 sollte bei Abs. 1 lit. b JI-Richtlinie in der Fassung des Rates wie folgt präzisiert werden: Eine Weiterverarbeitung der personenbezogenen Daten ist als unvereinbar mit dem ursprünglichen Erhebungszweck anzusehen, wenn die Daten nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.

⁶ Stellungnahme zur JI-Richtlinie vom 11. Juni 2012, S. 5.

⁷ BVerfGE 100, 313, 389; ständige Rechtsprechung.

3. Unverdächtige und andere besondere Personengruppen brauchen mehr Schutz!

Der Schutz unverdächtigter Bürgerinnen und Bürger sowie besondere Voraussetzungen für besondere Personengruppen stellen ein Kernanliegen des Datenschutzes im Bereich der Polizei und Justiz dar. Die Konferenz bedauert insofern die ersatzlose Streichung des Art. 5 in der Fassung des Rates und weist ausdrücklich auf die Fassung des Europäischen Parlaments zu Art. 5 hin, der sich an einer Stellungnahme der Art. 29-Gruppe orientiert.

Ziel der von der Art. 29-Gruppe vorgeschlagenen Regelung des Art. 5 ist es sicherzustellen, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen mit kürzeren Fristen gespeichert werden und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Die Konferenz lehnt die Streichung des Art. 5 der JI-Richtlinie in der Ratsversion ab und unterstützt Art. 5 in der Fassung des Europäischen Parlaments.

4. Datenspeicherungen sind regelmäßig auf ihre Erforderlichkeit und Verhältnismäßigkeit zu überprüfen!

Ungeachtet des Rechts auf Löschung sollten die datenverarbeitenden Stellen verpflichtet sein, die Erforderlichkeit und Verhältnismäßigkeit von Speicherungen in regelmäßigen Abständen zu überprüfen. Eine solche Verpflichtung enthält die Ratsversion im Gegensatz zu Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments nicht. Der Rat beschränkt sich in seinem Entwurf darauf, die Mitgliedstaaten zur Festlegung von Speicher- und Aussonderungsprüffristen in Verfahrensverzeichnissen („records“, Art. 23 JI-Richtlinie) zu verpflichten, wenn dies möglich ist. Dies reicht nicht aus. Vielmehr fordert die Konferenz als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

Die Konferenz fordert als eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen nach dem Vorbild von Art. 4b Abs. 2 des Entwurfs des Europäischen Parlaments, insbesondere zum Schutz bestimmter Personengruppen wie zum Beispiel Zeugen, Opfer und Kontaktpersonen.

5. Moderner Datenschutz braucht umfassende Benachrichtigungspflichten!

Benachrichtigungen gehören zu den datenschutzrechtlichen „Kernrechten“ der Betroffenen. Effektiver Rechtsschutz ist nicht möglich, wenn der von einer (heimlichen) Datenerhebung Betroffene keine Kenntnis von der Erhebung und Speicherung erlangt. Die Kontrolle dieser Datenverarbeitungen ist zwar auch Aufgabe der Datenschutzaufsichtsbehörden, doch sollte auch jede Bürgerin und jeder Bürger in die Lage versetzt werden, die sie oder ihn betreffende polizeiliche Maßnahme überprüfen zu können und überprüfen zu lassen.

Die Konferenz setzt sich daher für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

Zur Wahrung der Rechte des Einzelnen und zur Gewährung effektiven Rechtsschutzes durch Aufsichtsbehörden und Gerichte setzt sich die Konferenz für eine Stärkung der Betroffenenrechte durch Informationspflichten ein und spricht sich für die vom Europäischen Parlament vorgeschlagene Fassung des Art. 11 JI-Richtlinie aus.

6. Keine Sonderregelung der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren!

Die Konferenz spricht sich für eine möglichst weitgehende einheitliche Regelung der Rechte der Betroffenen im Anwendungsbereich der JI-Richtlinie aus. Demgegenüber enthält Art. 17 hinsichtlich personenbezogener Daten in Gerichtsbeschlüssen oder staatsanwaltlichen Verfahrensakten die Regelung, dass die Ausübung der

Betroffenenrechte „im Einklang mit dem einzelstaatlichen Recht“ erfolgt. Schon in ihrer Stellungnahme vom 11. Juni 2012 hatte die Konferenz eine Klarstellung zum Regelungsgehalt des Art. 17 II-Richtlinie gefordert. Leider tragen auch die vorgelegten Fassungen von Europäischem Parlament und Rat nicht dazu bei, die notwendige Klarstellung herbeizuführen. Die Konferenz betont daher noch einmal diese Notwendigkeit, da ansonsten Zweifel an der Anwendbarkeit der Betroffenenrechte im strafrechtlichen Ermittlungsverfahren entstehen können. Zu diesem Zweck ist die Sonderregelung des Art. 17 zu streichen und sind die Betroffenenrechte in strafrechtlichen Ermittlungen einheitlich in der II-Richtlinie zu regeln.

Die Konferenz spricht sich für eine Streichung des Art. 17 II-Richtlinie aus, und wiederholt ihre Forderung, dass die in Kapitel III gewährten Betroffenenrechte auch im Bereich des staatsanwalt-schaftlichen Ermittlungsverfahrens Anwendung finden.

7. Klarstellung - Datenverarbeitung nach dem Stand der Technik!

Die Konferenz unterstreicht die Bedeutung des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen. Die Verpflichtung, diese Grundsätze zu beachten, wird in Art. 19 II-Richtlinie jedoch in verschiedener Hinsicht erheblich beschränkt, unter anderem durch Bezugnahme auf „verfügbare Technologie“. Dies wird dem notwendigen Grundrechtsschutz nicht gerecht, denn „verfügbar“ sind auch veraltete Technologien, die nicht (mehr) die ausreichende Sicherheit bieten.

Demgegenüber stellt der „Stand der Technik“ („state of the art“) sicher, dass jeweils die modernsten vorhandenen Technologien einzusetzen sind. Der Stand der Technik ist eine im Europäischen Datenschutz handhabbare Definition. Sie findet seit längerem eine bewährte Anwendung in der Praxis und sollte auch in der II-Richtlinie verwendet werden.

Der an verschiedenen Stellen gebrauchte ungenaue und dem Schutzbedarf personenbezogener Daten nicht gerecht werdende Begriff „verfügbare“ Technik bzw. Technologie sollte konsequenter Weise

auch in der JI-Richtlinie durch „Stand der Technik“ ersetzt werden. Die Konferenz spricht sich insofern für Art. 19 in der Fassung des Europäischen Parlaments aus.

8. Datenschutz-Folgeabschätzung auch im Bereich der JI-Richtlinie!

Bei der Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden sind Datenschutz-Folgeabschätzungen äußerst wichtig, da gerade bei dieser Verarbeitung erhöhte Risiken für den Einzelnen bestehen. Das Europäische Parlament hat eine entsprechende Regelung zur Datenschutz-Folgenabschätzung vorgeschlagen, die jedoch vom Rat abgelehnt wird.

Die vom Europäischen Parlament in Art. 25a vorgeschlagene Bestimmung sieht eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitungsvorgänge aufgrund ihrer Natur, ihres Anwendungsbereichs oder ihrer Bestimmungszwecke eine konkrete Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellen können. Für die in Art. 25a (2) lit. b erwähnten „biometrischen Daten“ gibt es in Art. 3 Abs. 11 des Vorschlags des Europäischen Parlaments eine entsprechende Definition.

In Art. 33 des Entwurfs der Datenschutz-Grundverordnung (Ratsfassung) ist, anders als beim Richtlinien-Vorschlag, nach wie vor eine Datenschutz-Folgenabschätzung vorgesehen. Doch gerade im verarbeitungsintensiven Bereich der Strafverfolgung sind gründliche Sicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten von größter Wichtigkeit, weshalb sich die Konferenz für die Aufnahme einer entsprechenden Regelung in den Richtlinien-vorschlag ausspricht.

Die Konferenz setzt sich für eine Regelung der Datenschutz-Folgenabschätzung ein, die sich an Art. 25a des Richtlinien-Vorschlags des Europäischen Parlaments orientiert. In diesem Zusammenhang befürwortet die Konferenz die Wiederaufnahme der Definition der „biometrischen Daten“, wie sie vom Europäischen Parlament in Art. 3 Abs. 11 vorgesehen war.

9. Guter Datenschutz braucht behördliche Datenschutzbeauftragte!

Die Konferenz bedauert, dass der Rat es in seiner Version ablehnt, die Mitgliedstaaten zur Schaffung eines behördlichen Datenschutzbeauftragten zu verpflichten, sondern dies stattdessen in deren Ermessen stellt. Die Datenschutzbeauftragten des Bundes und der Länder haben überwiegend sehr gute Erfahrung bei der Zusammenarbeit mit den Datenschutzbeauftragten der beaufsichtigten Behörden gemacht und halten die interne Kontrolle vor Ort – neben der externen Kontrolle durch die Aufsichtsbehörden – für ein unverzichtbares Element eines flächendeckenden effektiven Datenschutzregimes.

Die Konferenz betont die Bedeutung einer verpflichtenden Bestellung eines behördlichen Datenschutzbeauftragten und spricht sich deshalb für Art. 30 des Vorschlages des Europäischen Parlaments aus.

10. Übermittlungen an Behörden und Gerichte in Drittstaaten bedürfen eines transparenten Verfahrens, der Abwägung im Einzelfall und müssen überprüfbar dokumentiert sein!

Neu an den Regelungen über die Übermittlung personenbezogener Daten in Drittstaaten ist, dass auch im JI-Bereich das Instrument des Angemessenheitsbeschlusses eingeführt werden soll. Die Konferenz ist der Auffassung, dass die geltenden Angemessenheitsbeschlüsse nicht auf den JI-Bereich übertragbar sind. Neben den Übermittlungen in Drittstaaten mit adäquatem Datenschutzniveau wird die Mehrzahl der Übermittlungen weiterhin auf der Grundlage bilateraler Abkommen und nationalen Rechts (im Einzelfall) erfolgen.

Die Konferenz fordert, in Übereinstimmung mit der Rechtsprechung des EuGH Abwägungsklauseln für alle Übermittlungen vorzusehen. Diese sollten die übermittelnde Behörde verpflichten, eine Abwägung zwischen dem Interesse an der Übermittlung und den schutzwürdigen Interessen des Betroffenen vorzunehmen. Die JI-Richtlinie sollte zugleich Dokumentationspflichten festschreiben, um die Kontrolle von Übermittlungen überprüfbar zu machen. Die Konferenz bedauert insofern die Streichung der Dokumentationspflicht in Art.

35 Abs. 2 in der Fassung des Rates. Zudem sollten die Drittstaaten über Verarbeitungsbeschränkungen (Löschfristen etc.) informiert werden.

Die Konferenz spricht sich ebenfalls für eine Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung entsprechende Regelung aus. Danach sind Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaates, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt noch vollstreckbar, wenn dies nicht in internationalen Übereinkommen zur Amts- und Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten Stellen. Die Konferenz erkennt an, dass mit der Schaffung einer solchen Regelung insbesondere die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden wird. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Die Konferenz fordert bei jeder Übermittlung in Drittstaaten eine Abwägung im Einzelfall. Des Weiteren muss die JI-Richtlinie sicherstellen, dass Übermittlungen dokumentiert und damit kontrollierbar sind. Deshalb sollte die Dokumentationspflicht gemäß Art. 35 in der Fassung der Kommission beibehalten werden. Über nationale Verarbeitungsbeschränkungen ist bei jeder Übermittlung zu informieren. Des Weiteren fordert die Konferenz eine Regelung zur Übermittlung personenbezogener Daten an Behörden und Gerichte eines Drittstaates in Anlehnung an Art. 43a der Parlamentsfassung der Datenschutz-Grundverordnung.

11. Befugnisse der Datenschutzbehörden müssen gestärkt werden!

Datenschutz muss effektiv durchsetzbar sein. Die Konferenz erwartet von der Datenschutzreform daher eine Stärkung der Befugnisse der Datenschutzbehörden. Es darf nicht länger sein, dass Datenschutzbehörden nur über stumpfe Schwerter in diesem Bereich verfügen. Art. 8 Abs. 3 der EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV ver-

langen vielmehr eine wirksame Durchsetzung der Grundrechte der Bürgerinnen und Bürger. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Datenschutz muss effektiv durchsetzbar sein. Dazu fordert die Konferenz die Stärkung der Befugnisse der Datenschutzbehörden durch die II-Richtlinie. Effektive Aufsicht muss bedeuten, dass Datenschutzbehörden Instrumente an die Hand gegeben werden, um einen Verstoß gegen das Datenschutzrecht durch eine beaufsichtigte Behörde abzustellen, notfalls mit Hilfe einer gerichtlichen Entscheidung, wenn die beaufsichtigte Behörde an einer anderen Rechtsauffassung festhält.

Anlage 69

4. Konferenz für Lehrer, Erzieher und
Sonderpädagogische Fachkräfte
14. April 2014

beim THÜRINGER MINISTERIUM FÜR BILDUNG,
WISSENSCHAFT UND KULTUR (TMBWK)

**Inhalt:**

Überblick zum Datenschutzrecht

- Datenschutz ist Grundrecht!
- Datenschutzrecht in Thüringen
- Datenschutzbestimmungen im Schulbereich

Ausgewählte Aspekte zum Datenschutz in der Schule

- Veröffentlichungen der Schule
- Kommunikation Schule – Lehrer – Schüler – Eltern

Anlage 70

Veranstaltung im Staatlichen Gymnasium Neuhaus/Rwg
15. April 2015



Inhalt:

Das Grundrecht auf informationelle Selbstbestimmung
Rechtliche Grundlagen für den Datenschutz in der Schule

Anlage 71

"Datenschutz in der verwaltungsgerichtlichen Justiz"
Thüringer Verwaltungsrichterverein
19. Juni 2014



Datenschutz in der Justiz

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz und
die Informationsfreiheit (TLfDI)

1

Inhalt:

Die Behörde des TLfDI!
Verfassungsrechtliche Grundlagen
Grundrecht auf informationelle Selbstbestimmung
Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
Abgrenzung
Brief-, Post- und Fernmeldegeheimnis
Abgrenzung öffentlicher – nicht-öffentlicher Bereich
Besonderheiten im Datenschutz für Richterinnen und Richter
Technische und organisatorische Maßnahmen (TOM)

Anlage 72

2. Tandemfortbildungsveranstaltung für Schulsozialarbeiterinnen
und Schulleitungsmitglieder“

Thematik: Erfolgreiches Agieren im Rahmen
des gesetzlichen Datenschutzes, 26. Juni 2014

und

Jahrestagung: "Schulbezogene Jugendsozialarbeit - das erste Jahr"

15. Juli 2014

Organisationsberatungsinstitut Thüringen - ORBIT –



Inhalt:

TLfDI

Rechtliche Grundlagen

Warum Datenschutz?

Datenschutz in der Schule

Datenschutz in der Schulsozialarbeit

Einzelfälle

Anlage 73

HWK Erfurt Veranstaltung,
12. November 2014

Wie kann ich vorsorgen



Datenschutz im Internet

Dipl.–Ing. Jens KeßlerMitarbeiter Referat 3
Technischer und organisatorischer Datenschutz beimThüringer Landesbeauftragten für den Datenschutz und die
Informationsfreiheit (TLfDI)**Inhalt:**

Historischer Hintergrund

IT-Sicherheit vs. Datenschutz: Gemeinsamkeiten und Unterschiede

Was ist das "Internet"?

Gefahren / Angriffsmethoden im Internet

Wie kann ich vorsorgen?

Anlage 74

Gewerkschaft Erziehung und Wissenschaft
Landesverband Thüringen (GEW)
13. November 2014

**Novelle des Thüringer Personalvertretungsgesetzes
Umsetzung der Änderungen in § 68 ThürPersVG -
Wahrung des Datenschutzes für alle Beschäftigten**



Inhalt:

Der TLfDI!

Was ist Datenschutz?

Datenschutz im Rechtssystem

Thüringer Datenschutzgesetz und die Arbeit des Personalrates

Anlage 75

Datenschutz für Personalratsmitglieder
THÜRINGER MINISTERIUM FÜR BILDUNG, WISSENSCHAFT
UND KULTUR (TMBWK)
14. November 2014

**Inhalt:**

Der TLfDI!

Was ist Datenschutz?

Datenschutz im Rechtssystem

Thüringer Datenschutzgesetz und die Arbeit des Personalrates

Speziell: Datenschutz im Schulbereich und Einzelfälle

Anlage 76

Datenschutz im Schulbereich und Einzelfälle
Datenschutz in der Erwachsenenbildung
Landesorganisation der freien Träger in der
Erwachsenenbildung e. V., LOFT
21. November 2014



Inhalt:

Der TLfDI!

Was ist Datenschutz?

Datenschutz im Rechtssystem

Welche Regelungen gelten für Bildungseinrichtungen nach BDSG?

Welche Daten darf ich erheben?

Fallstricke bei der Teilnehmerwerbung

Anlage 77

Konsequenz bei Verstößen,
Regelungen im ThürDSG
Fachhochschule Erfurt,
26. November 2014

**Inhalt:**

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?
Schlagabtausch

Anlage 78

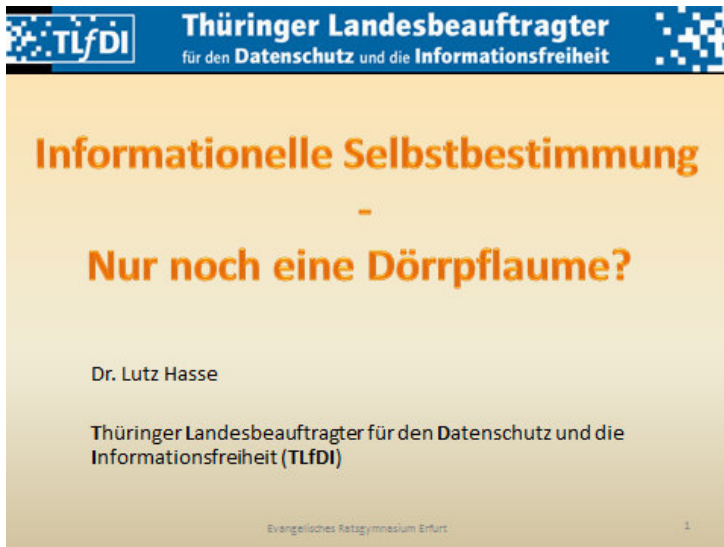
Veranstaltung der Fakultät für Mathematik und Informatik
der FSU Jena
7. Januar 2015



Inhalt:

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?
Schlagabtausch

Evangelisches Ratsgymnasium in Erfurt
25. Februar 2015



Inhalt:

Art. 6 Abs. 2 Verfassung des Freistaats Thüringen
Definition personenbezogener Daten – § 3 BDSG/ThürDSG
Art. 6 Abs. 3 Verfassung des Freistaats Thüringen
Verbot mit Erlaubnisvorbehalt – § 4 Abs. 1 BDSG/ThürDSG
Datenverarbeitung
Rechtsgrundlagen
Rechtliche Grundlagen für den Datenschutz in der Schule
Thüringer Schulgesetz
Thüringer Schulordnung
Veröffentlichungen von Stunden- und Vertretungsplänen
Veröffentlichungen im Internet
Soziale Netzwerke

1. Datenschutztag Karl-Volkmar-Stoy-Schule Jena
2. März 2015



Verschlüsselung im Internet



Inhalt:

Motivation:

Was ist das Internet?

Was wird im Internet genutzt?

Was kann passieren?

Verschlüsselung:

Gegenmaßnahmen

GPG im Detail

HTTPS

Anlage 81

Vortrag am Staatlichen Berufsschulzentrum Kyffhäuser
25. März 2015**Inhalt:**

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?
Schlagabtausch

Anlage 82

Fraktionsveranstaltung,
Bündnis 90/Die Grünen
13. Mai 2015



Inhalt:

Was ist überhaupt „E-Health“?
Vorteile und Gefahren
Rechtsgrundlagen
Aktuelle Beispiele und News
Europa

Anlage 83

FSU Jena – Institut für Politikwissenschaft
25. Juni 2015

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

**Informationelle Selbstbestimmung-
Utopie oder Realität?**

Dr. Lutz Hasse

Thüringer Landesbeauftragter für den Datenschutz und die
Informationsfreiheit (TLfDI)

25.06.2015 FSU Jena - Institut für Politikwissenschaft 1

Inhalt:

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Privatsphäre – Warum?

Anlage 84

„Grundkenntnisse im Datenschutzrecht“
Thüringer Volkshochschulverband e.V.
24. Juni 2015



Grundkenntnisse im Datenschutzrecht

Saskia Springer

Referentin i.d.M.

Thüringer Landesbeauftragten für den Datenschutz und
die Informationsfreiheit (TLfDI)

1

Inhalt:

Die Behörde des TLfDI!

Historischer Hintergrund zum Datenschutzrecht

Verfassungsrechtliche Grundlagen

Datenschutzrechtliche Grundsätze

Grundzüge des Thüringer Datenschutzgesetzes (ThürDSG)

Anlage 85

Veranstaltung der SPD Jena zur Vorratsdatenspeicherung
7. Juli 2015

**Inhalt u. a.:**

Das Grundrecht auf informationelle Selbstbestimmung

Die Vorratsdatenspeicherung – eine Beruhigungspille für das Volk?

Vorratsdatenspeicherung:

das Urteil des Bundesverfassungsgerichts vom 2. März 2010

das Urteil des Europäischen Gerichtshofs vom 8. April 2014

der Gesetzentwurf der Bundesregierung zur Einführung einer
Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten

Anlage 86

E-Mail-Verschlüsselung für GnuPG und Outlook,
Kooperationsveranstaltung des ThILLM und des TLfDI
8. September 2015

Sicherer Datentransfer durch Verschlüsselung

Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Sicherer Datentransfer durch Verschlüsselung

Beispiel: E-Mail-Verschlüsselung mit GnuPG und Thunderbird

Kooperationsveranstaltung des ThILLM und des TLfDI
am 8. September 2015

Referent: Eckhard Ludwig, TLfDI, Referat 2

© Ludwig, TLfDI, 08.09.2015

© CC-BY-NC-ND 3.0 DE

5

Inhalt:

Vorbereitung
Schlüsselerzeugung
Schlüsseltausch
Schlüsselprüfung
Schlüsselnutzung

Anlage 87

„Datenschutz in sozialen Einrichtungen“
PARITÄTISCHE Akademie Thüringen
22. September 2015



Inhalt:

Warum Datenschutz?

Historischer Hintergrund

Rechtliche Grundlagen - Systematik

Allgemeine Grundsätze des Datenschutzes

Ermächtigungsgrundlagen

nach dem SGB

nach dem BDSG

nach dem ThürDSG

Technische und organisatorische Maßnahmen

Der TLfDI!

Anlage 88

Fachtagung der Kultusministerkonferenz KMK in Berlin
29. September 2015

5 Jahre KMK-Bildung „Nationalbildung in der Schule“

Datenschutz als Zukunftskompetenz für digitale Bildung

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

**Datenschutz als Zukunftskompetenz
für digitale Bildung**

Wo stehen wir? – Wo müssen wir hin?



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

 29.09.2015

5

Inhalt:

Datenschutz - Aktuelle Situation in Deutschland und Europa

Datenschutz als Aspekt digitaler Bildung

Datenschutz als Zukunftskompetenz – Was muss passieren?

Anlage 89

Fachhochschule Erfurt,
Angewandte Informatik
26. November 2015**Inhalt:**

Das Grundrecht auf informationelle Selbstbestimmung
Fälle auf Verfassungsebene (Bestimmtheitsgrundsatz und Verhältnismäßigkeitsprinzip)
Fälle auf Gesetzesebene aus dem Arbeitsalltag des TLfDI
Bedrohungen des Grundrechts
Schutz des Grundrechts
Europa
Privatsphäre – Warum?
Schlagabtausch

Abkürzungsverzeichnis

AbfWS	Satzung über die Vermeidung, Verwertung und Entsorgung von Siedlungsabfällen
Abs.	Absatz
AfV	Amt für Verfassungsschutz
AGB	Allgemeine Geschäftsbedingungen
AgrStatG	Agrarstatistikgesetz
ALG	Arbeitslosengeld
ANBest-P	Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung
Anm.	Anmerkung
AO	Abgabenordnung
App	Application software
ARMIN	Arzneimittelinitiative Sachsen-Thüringen
Art.	Artikel
ASiG	Arbeitssicherheitsgesetz
AufbewBest	Aufbewahrungsbestimmungen
AWB	Abfallwirtschaftsbetrieb
BAföG	Bundesausbildungsförderungsgesetz
BayLDA	Bayrisches Landesamt für Datenschutzaufsicht
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BEM	betriebliches Eingliederungsmanagement
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BNotO	Bundesnotarordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
BZ	Bildungszentrum
bzw.	beziehungsweise

d. h.	das heißt
DA-DAB	Dienstanweisung zur Behandlung von Aufsichtsbeschwerden gegen Angehörige der Thüringer Polizei im Geschäftsbereich der Landespolizeidirektion
DA-Diszi	Dienstanweisung zur Behandlung von Disziplinarangelegenheiten im Geschäftsbereich der Landespolizeidirektion
DolmV TH	Thüringer Verordnung zur Regelung der allgemeinen Beeidigung von Dolmetschern und der Ermächtigung von Übersetzern
DP AG	Deutsche Post AG
DSK	Datenschutzkonferenz
DSL	Digital Subscriber Line
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EHS	Ergänzendes Hilfesystem
eIDAS	electronic identification and trust services
ESF	Europäischer Sozialfond
EStG	Einkommensteuergesetz
EuGH	Europäischer Gerichtshof
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
FBS-TH	Fallbearbeitungssystem Thüringen
GASt/Zst	Geldannahmestelle/Zahlstelle
gem.	gemäß
GewO	Gewerbeordnung
GFAW	Gesellschaft für Arbeits- und Wirtschaftsförderung
GFAW Thüringen	Gesellschaft für Arbeits- und Wirtschaftsförderung des Freistaats Thüringen
GG	Grundgesetz
ggf.	gegebenenfalls
GKDZ	Gemeinsames Kompetenz- und Dienstleistungszentrum
GKV- Modernisie- rungsgesetz	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung

– GMG

HAMASYS	Haushaltsmanagementsystem
HWK	Handwerkskammer
i. d. R.	in der Regel
i. V. m.	in Verbindung mit
ICF	Internationale Klassifikation der Funktionen
IfSG	Infektionsschutzgesetz
ITP	Integrierte Teilhabeplanung
JVA	Justizvollzugsanstalt
KAG	Kommunale Arbeitsgemeinschaft
Kita	Kindertagesstätte
KJÄD	Kinder- und Jugendärztlicher Dienst
KSJ	Kommunalservice Jena
KV	Kassenärztliche Vereinigung
LEG	Landesentwicklungsgesellschaft
LFD	Landesfinanzdirektion
LfD	Landesbeauftragte für den Datenschutz
LoD	Level of Detail
LPD	Landespolizeidirektion
LPG	Landwirtschaftliche Produktionsgenossenschaften
LPI	Landespolizeiinspektion
MiStra	Anordnung über Mitteilung in Strafsachen
NSA	National Security Agency
o. g.	oben genannte
OBG	Ordnungsbehördengesetz
OH	Orientierungshilfe
OH KIS	Orientierungshilfe „Krankenhausinformationssysteme“
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten

PÄD	Polizeiärztlicher Dienst
PAG	Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei
PAuswG	Personalausweisgesetz
PC	Personal Computer
Rn.	Randnummer
Rz.	Randziffer
SaaS	Software as a Service
SARS	SYBORG Auskunfts- und Recherche-System
SGB	Sozialgesetzbuch
SHK	Saaleholzlandkreis
SigG	Signaturgesetz
StA	Staatsanwaltschaft
StAG	Staatsangehörigkeitsgesetz
StGB	Strafgesetzbuch
StOP	Strafprozessordnung
StPO	Strafprozessordnung
StVO	Straßenverkehrsordnung
SWE	Stadtwerke Erfurt
TAB	Thüringer Aufbaubank
TB	Tätigkeitsbericht
TFM	Thüringer Finanzministerium
ThAVel	Thüringer Antragsystem für Verwaltungsleistungen
Thoska	Thüringer Hochschul- und Studentenwerkskarte
ThürAbfG	Thüringer Gesetz über die Vermeidung, Verminderung, Verwertung und Beseitigung von Abfällen
ThürAG-BMG	Thüringer Gesetz zur Ausführung des Bundesmeldegesetzes
ThürAGGVG	Thüringer Gesetz zur Ausführung des Gerichtsverfassungsgesetzes
ThürArchivG	Thüringer Archivgesetz
ThürBestG	Thüringer Bestattungsgesetz

ThürBG	Thüringer Beamten-gesetz
ThürBVVG	Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürBVVG	Thüringer Gesetz über Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürDG	Thüringer Disziplinar-gesetz
ThürDSG	Thüringer Datenschutz-gesetz
ThürFSO-SW	Thüringer Fachschulordnung für die Bildungsgänge im Sozialwesen
ThürGGO	Gemeinsame Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen
ThürGleichStatVO	Thüringer Gleichstellungsstatistikverordnung
ThürHeilBG	Thüringer Heilberufes-gesetz
ThürHG	Thüringer Hochschul-gesetz
ThürJVollzGB	Thüringer Justizvollzugsgesetzbuch
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKiStG	Thüringer Kirchensteuergesetz
ThürKO	Thüringer Kommunalordnung
ThürKWO	Thüringer Kommunalwahlordnung
ThürLWG	Thüringer Landeswahl-gesetz
ThürLWO	Thüringer Landeswahlordnung
ThürMeldeG	Thüringer Melde-gesetz
ThürMRVG	Thüringer Maßregelvollzugsgesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürPolPrüffristVO	Thüringer Verordnung über Prüffristen bei vollzugs-polizeilicher Datenspeicherung
ThürPsychKG	Thüringer Gesetz zur Hilfe und Unterbringung psychisch kranker Menschen
ThürSchFTG	Thüringer Gesetz über Schulen in freier Trägerschaft
ThürSchulG	Thüringer Schul-gesetz
ThürSchul-	Thüringer Verordnung über die Schulgesundheits-

gespflVO	pflege
ThürStAnz	Thüringer Staatsanzeiger
ThürStatG	Thüringer Statistikgesetz
ThürUIG	Thüringer Umweltinformationsgesetz
ThürVerf	Verfassung des Freistaats Thüringen
ThürVerf	Verfassung des Freistaats Thüringen
ThürVer- fGHG	Thüringer Verfassungsgerichtshof
ThürVerf- SchG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürWTG	Thüringer Wohn- und Teilhabegesetz
THVPS	Verwaltungsplattform Schulwesen
TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TKG	Telekommunikationsgesetz
TLFD	Thüringer Landesfinanzdirektion
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLKA	Thüringer Landeskriminalamt
TLS	Thüringer Landesamt für Statistik
TLVermGeo	Thüringer Landesamt für Vermessung und Geoin- formation
TLVwA	Thüringer Landesverwaltungsamt
TMASGFF	Thüringer Ministerium für Arbeit, Soziales, Gesund- heit, Frauen und Familie
TMBJS	Thüringer Ministerium für Bildung, Jugend und Sport
TMBLV	Thüringer Ministerium für Bau, Landesentwicklung und Verkehr
TMBWK	Thüringer Ministerium für Bildung, Wissenschaft und Kultur
TMG	Telemediengesetz
TMIK	Thüringer Ministerium für Inneres und Kommunales

TMIL	Thüringer Ministerium für Infrastruktur und Landwirtschaft
TMLFUN	Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz
TMMJV	Thüringer Ministerium für Migration, Justiz und Verbraucherschutz
TMSFG	Thüringer Ministerium für Soziales, Familien und Gesundheit
TMWAT	Thüringer Ministerium für Wirtschaft und Arbeit und Technologie
TMWWDG	Thüringer Ministerium für Wirtschaft, Wissenschaft und Digitale Gesellschaft
TPG	Thüringer Pressegesetz
u. a.	unter anderem
u. U.	unter Umständen
UA	Untersuchungsausschuss
UAG	Thüringer Untersuchungsausschussgesetz
UAG	Unterarbeitsgruppe
UAK	Unterarbeitskreis
UKJ	Universitätsklinikums Jena
VBS	Vorgangsbearbeitungssystem
VG	Verwaltungsgemeinschaft
vgl.	vergleiche
VoBraWeb	Software zum vorbeugenden Brandschutz
VwGO	Verwaltungsgerichtsordnung
VwV VA-StVOWi	Verwaltungsvorschrift zur Verfolgung und Ahndung von Straßenverkehrsordnungswidrigkeiten durch die Gemeinden und Polizei
WoGG	Wohngeldgesetz
ZEVIS	Zentrales Verkehrsinformationssystem
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

Sachregister

§ 203 Strafgesetzbuch	141, 310, 318, 322
§ 25a ThürDSG	37, 114, 115
§ 38 Abs. 1 Satz 2 Nr. 2 ThürDSG	106
Abfallentsorgung	74
Abgabenordnung	67, 101, 128, 414
Abgeordnete	306, 439, 497, 505, 537, 615, 664, 668
Abitur	468, 493
Ablichtung	245
Abwägung	80, 156, 219, 252, 286, 577, 604, 624, 691
Abwesenheitstage	210
Administratoren	191, 488
Adressdaten	73, 79, 93, 101, 255, 386, 394
Adresse	54, 58, 78, 98, 101, 115, 119, 125, 137, 148, 150, 158, 167, 189, 227, 254, 270, 278, 292, 311, 387, 392, 423, 435, 465, 509, 530, 550, 591, 644, 648, 662, 671
Agrarbeihilfe	536
Agrarstatistik	405
Agrarstatistikgesetz	405
AK Datenschutz und Bildung	440, 679
Akteneinsicht	65, 87, 233, 247, 283, 299, 356, 368, 378, 408, 429
Aktenplan	214
Aktenplanschlüssel	214
Aktenvernichtungsgeräte	318
Aktenvorlage	219
AlertsNet	323
Algorithmen	31, 305, 441, 496, 512, 550, 588, 611
allgemein zugängliche Quelle	436, 495
Altersgrenzen	397, 464
Amt für Ausbildungsförderung	473

Amt für Verfassungsschutz	251, 253, 355, 619
Amtsarzt	184, 295, 338, 396
Amtsblatt	46, 118
Amtsermittlungsgrundsatz	68
Amtsgeheimnis	64, 149, 175
Amtsgericht	75, 110, 138, 227, 350, 363
Amtshilfe	414
anerkannter Zweck	81, 335, 469, 525
Anerkennung	280, 386
Angehörige	57, 86, 107, 215, 220, 228, 233, 248, 328, 332, 385, 457, 497, 539, 649
angemessenes Datenschutzniveau	42, 179, 289, 305, 489, 495, 525
angemessenes Schutzniveau	519, 525
Angemessenheit	42, 101, 247, 605, 691
Anhörungsverfahren	33, 264, 288
Anlagenbetreiber	407
anonym	22, 75, 113, 138, 151, 154, 160, 177, 194, 211, 234, 314, 316, 323, 325, 337, 349, 362, 371, 393, 398, 408, 419, 423, 457, 460, 464, 480, 549, 552, 556, 564, 680, 681
Anonymisierung	71, 113, 212, 333, 338, 371, 408, 552, 605
Anonymisierungsmaßnahme	324
Anonymität	70, 195, 362, 562
Anordnung	159, 218, 451, 557, 573
Anordnung über Mitteilung in Strafsachen (MiStra)	269
Anspruch auf Löschung	180, 305, 408
Antiterrordatei	29, 252, 569, 580
Anzeigenerstatter	160, 278
Anzeigepflicht	437
AOK Plus	330
Apotheker	310, 330, 652

App	23, 31, 58, 301, 303, 308, 396, 442, 500, 513, 523, 533, 553, 571, 660, 678
Applikation	58, 396
Applikationssoftware	303
Arbeitgeber	45, 172, 189, 204, 208, 237, 288, 304, 346, 375, 499, 511, 546, 578, 626, 633
Arbeitnehmer	45, 169, 187, 193, 237, 261, 269, 304, 511, 520, 547, 565
Arbeitskreis Datenschutz und Bildung	438, 440, 445, 484, 638, 639, 679
Arbeitslosengeld (ALG) II	293, 380
Arbeitsmarkt-Dienstleistungen	390
Arbeitsplatz-PC	391
Arbeitszeit	95, 150, 174, 177, 192, 193, 266, 352, 372, 492
Archiv	272, 275, 314, 319, 391, 472, 493, 643, 672
Archivgut	90, 320
Archivierung	90, 376
Archivordnung	314
ARD	51
ARMIN	330
Arzneimittelinitiative Sachsen- Thüringen	330
Arzt	185, 216, 282, 295, 298, 303, 308, 310, 311, 312, 314, 316, 317, 322, 325, 327, 330, 337, 338, 342, 343, 395, 486, 497, 517, 542, 590, 593, 651
Ärzte	185, 217, 310, 311, 316, 317, 322, 324, 325, 326, 330, 337, 338, 340, 342, 344, 347, 485, 505, 542, 584, 589, 593, 602, 615, 652, 668

ärztliche Gutachten	208
ärztliches Attest	497
Arztpraxis	342
Arztrechnungen	312, 395
Asylbewerber	394
Aufbewahrungsfrist	221, 232, 271, 275, 279, 315, 317, 356, 376, 377, 378, 390, 472
Aufbewahrungszeiten	336
Auftragsdatenverarbeitung	96, 101, 111, 115, 128, 150, 202, 315, 318, 467, 470, 492, 518
Auftragsdatenverarbeitungsvertrag	479
Aufzeichnung	95, 155, 193, 229, 240, 246, 259, 262, 267, 286, 412, 417, 451, 528, 622, 644
Aushang	351, 457
Auskunft	36, 65, 70, 74, 82, 87, 91, 95, 106, 127, 130, 132, 147, 153, 161, 185, 195, 197, 200, 215, 218, 221, 223, 227, 243, 246, 248, 262, 279, 281, 292, 325, 332, 335, 336, 350, 356, 359, 362, 363, 371, 377, 382, 386, 391, 396, 405, 408, 420, 424, 428, 429, 450, 474, 494, 500, 578, 601, 609, 614
Auskünfte	69, 86, 143, 153, 158, 185, 189, 218, 224, 281, 282, 332, 336, 345, 354, 363, 367, 380, 385
Auskunfts- und Akteneinsichtsrecht	132
Auskunfts- und Einsichtsrecht	272, 429
Auskunftsanspruch	87, 124, 130, 197, 199, 234, 336, 350, 428
Auskunftsanspruch des Gemeinderatsmitglieds	131

Auskunftsbeschränkungen	88
Auskunftersuchen	35, 82, 88, 162, 244, 351, 382, 392
Auskunftserteilung	37, 84, 87, 133, 146, 230, 243, 283, 314, 335, 357, 388, 485
Auskunftsrecht	205, 325, 331, 337, 356
Auskunftssperre	81, 84, 91, 278
Auskunftsverweigerung	132, 248, 336
Ausländerakte	280
Ausländerbehörde	281, 355
Ausnahme	32, 66, 69, 160, 170, 173, 175, 188, 207, 213, 235, 244, 280, 298, 340, 367, 369, 397, 417, 433, 451, 469, 475, 522, 574, 575, 612, 615, 626, 651, 668
Aussage gegen Aussage	72, 121
Ausschlussgründe	219
Ausschreibung	190, 203, 390, 401, 411, 556, 592, 631, 677
Ausschreibungsverfahren	401
Austauschserver	461
Ausweis	54, 107, 243, 244, 374, 495, 521, 550, 589
Ausweiskopie	243
Authentifizierungstoken	461
Authentizität	585
Auto	58, 109, 246, 416, 421, 529, 578, 581, 633, 641
Autobahn	420, 646
Autobahnpolizei	421
automatisierte Datenverarbeitungs- anlagen	96, 491
automatisierte Verfahren	32, 192, 212, 223, 241, 436, 473, 490
Babyerstaussstattung	386
BAföG21	473
Bahnhof	411
BALVI iP	535

Bank	55, 145, 161, 245, 255, 256, 264, 297, 380, 435, 465, 546, 607, 665
Bankverbindung	161, 255
barrierefreier Bankautomat	256
Baugesetzbuch	118
Bauland	118
Baulandkataster	118
Bauprojekt	88
bDSB	152, 168, 175, 211, 242, 273, 364, 459, 490
beamtenrechtliche Untersuchungen	217
Beamter	120
beanstandet	80, 105, 108, 124, 135, 139, 167, 182, 187, 210, 221, 223, 230, 400
Beanstandung	34, 105, 147, 169, 186, 187, 226, 227, 230, 236, 271, 280, 351, 430, 437, 466, 478, 500
Bedarfsermittlung	144, 533
Befliegen	411
Beherbergungsbetriebe	85, 102
Beherbergungsstätte	85
Beherbergungsunternehmen	105
Behinderungen	257, 294, 435, 533
Behördenakten	281
Beihilfe	310, 312, 535
Beihilfestelle	309, 312
Beitragsservice	51
Belege	295, 313, 430
Benachrichtigungspflichten	515, 604, 688
Benutzer	54, 303, 376, 399, 457, 487, 508, 540, 617, 680
Benutzerkennung	399
berechtigtes Interesse	82, 84, 205, 332, 599
Berechtigungskontrolle	201
beruflich Reisenden	443
Berufsförderzentrum	391

Berufsgeheimnis	141, 302, 310, 318, 609, 615, 668
berufsrechtliche Prüfung	326
Beschäftigte	32, 38, 95, 112, 136, 152, 153, 157, 158, 173, 175, 178, 183, 189, 191, 193, 194, 197, 206, 237, 261, 286, 301, 338, 345, 352, 356, 366, 371, 375, 420, 469, 490, 499, 539, 546, 607, 621, 633, 699
Beschäftigtendaten	152, 209, 353, 546, 607
Beschäftigtendatenschutz	25, 45, 135, 193, 240, 546, 565
Beschlagnahme	72, 138, 226, 460, 610
Beschuldigte	225, 271, 278
Beschwerde	22, 35, 57, 64, 65, 72, 82, 83, 102, 106, 107, 136, 137, 143, 147, 159, 161, 188, 192, 197, 209, 220, 223, 225, 226, 227, 231, 232, 247, 258, 260, 266, 270, 278, 291, 293, 296, 298, 300, 310, 313, 315, 325, 327, 336, 350, 356, 363, 364, 368, 377, 382, 391, 405, 408, 416, 429, 431, 448, 450, 472, 477, 497, 575
Beschwerdeführer	36, 56, 65, 72, 78, 82, 83, 105, 107, 114, 118, 132, 137, 142, 146, 159, 161, 167, 173, 186, 187, 197, 207, 220, 223, 225, 226, 227, 231, 232, 248, 260, 265, 270, 293, 294, 296, 298, 300, 313, 315, 325, 336, 347, 350, 356, 363, 368, 369, 374, 378, 380, 387, 391, 406, 408, 429,

	432, 448, 450, 463, 472, 477, 520
besondere Arten von Daten	324
besondere Meldescheine	85
besonders geschützte Daten	212, 283, 381
Besteuerungsverfahren	414
Besucherkontrolle	306
Besuchsrecht	284
Betreuung	170, 210, 216, 331, 438, 448, 462, 479
Betriebliches Eingliederungs- management	345
Betriebsratswahl	172
Betriebssysteme	507, 541, 617, 660, 671
Bevollmächtigter	142
Beweis	72, 110, 128, 159, 162, 170, 218, 281, 354, 381, 384, 416, 418, 622
Beweisantrag	218
Beweisbeschluss	219
Beweisermittlung	382
Beweismittel	67, 68, 159, 219, 381
Bewerber	97, 180, 190, 202, 367, 394, 455
Bewerberdaten	180, 190, 202, 366, 547
Bewerbungsunterlagen	180, 190
Bezirksschornsteinfeger	436
BIC	347
Bietererklärung	402
bildliche Erfassung	245
Bildungsforschung	443, 456
Bildungsinstitutionen	487
Bildungsmaßnahme	391, 434
Bildungsministerium	445, 483, 490
bildungspolitisch	650, 655
Bildwiedergabe	245
Bild-Zeitung	109, 169
Binding Corporate Rules (BCR)	42
Biometrische Gesichtserkennung	510, 562
Blitzer	107, 109

Blockieren	444
Bodennutzungshaupterhebung	405
Body-Cam	239
Bonus	93
Brandschutz	115
Breitbandversorgung	144
Briefumschläge	147, 291
Browserverlauf	460, 509, 671
BSI	54, 383, 503, 513, 515, 531, 588, 604, 658
Bundesamt für Sicherheit in der Informationstechnik	55, 503, 513, 531
Bundesärztekammer	337, 342, 590
Bundesärztestatistik	337
Bundesausbildungsförderungs- gesetz (BAföG)	473
Bundesautobahnen	413, 583, 646
Bundesfernstraßen	413, 583, 646
Bundesimmissionsschutzgesetz	407, 437
Bundesmeldegesetz	32, 35, 83, 85, 88, 91, 228, 393
Bundesministerium für Gesundheit	340
Bundesnotarordnung	273
Bundespolizei	244, 417
Bundesstatistik	405
Bundestagswahl	46, 143
Bundesverfassungsgericht	28, 49, 57, 131, 219, 252, 284, 570, 580, 597, 615, 619, 667, 686, 710
Bundesverwaltungsgericht	60, 155, 175, 498
Bürger	26, 33, 43, 51, 55, 56, 60, 64, 72, 73, 78, 81, 85, 87, 88, 93, 107, 113, 115, 117, 119, 124, 125, 129, 142, 144, 148, 153, 155, 168, 177, 188, 201, 204, 216, 223, 228, 244, 260, 278, 292, 299, 325, 336, 342, 358, 362, 368, 374, 390, 392, 405, 408, 429, 445,

	449, 451, 460, 472, 494, 504, 505, 509, 512, 516, 521, 525, 527, 534, 544, 550, 556, 564, 574, 596, 597, 611, 614, 636, 641, 649, 665, 683, 693
Bürgerantrag	81
Bürgerbefragung	73, 79
Bürgerbegehren	88
Bürgerentscheid	89
Bürgermeister	64, 72, 78, 105, 114, 121, 130, 151, 152, 167, 179, 204
Bus	62, 113, 411, 419, 626, 677
Busbahnhof	411
Bußgeld	36, 92, 234, 367, 574, 607
Chipkarten	496
Cloud	55, 116, 305, 444, 470, 483, 489, 507, 518, 549, 554, 617, 671
Community-Plattform	467
Cookies	61, 167, 595, 648
CPT	282
Cross Compliance-Anforderungen	536
Cyber-Raum	515
das Thüringer Landesverwaltungsamt	352
Daten der Personalplanung	461
Daten Dritter	88, 198, 208, 219, 301, 356, 465
Datenabfrage	220, 227, 234
Datenabgleich	52, 66, 222, 296, 536
Datenaustausch	67, 388, 569
Datenbanken	231, 236, 325, 389, 435, 444, 511, 552, 562, 565, 591
Datenerhebung	59, 74, 79, 103, 108, 111, 146, 158, 164, 188, 196, 200, 211, 246, 253, 262, 326, 330, 334, 339, 358,

	360, 361, 370, 386, 389, 395, 413, 415, 435, 436, 449, 465, 480, 486, 497, 499, 526, 534, 583, 629, 641, 646, 677, 688
Datenerhebung beim Betroffenen	69, 311
Datengeheimnis	70, 422, 424
Datenhehlerei	30
Datenlöschung	309, 376, 658
Datenschutzaudit	96
Datenschutzbeauftragte	97, 116, 134, 135, 150, 151, 155, 166, 168, 174, 191, 198, 211, 221, 239, 242, 253, 254, 256, 264, 273, 274, 293, 302, 330, 384, 385, 407, 413, 414, 417, 438, 441, 445, 447, 459, 462, 464, 478, 487, 490, 500, 504, 506, 509, 511, 515, 518, 546, 548, 550, 556, 559, 560, 562, 564, 567, 569, 571, 573, 575, 578, 580, 583, 593, 595, 597, 599, 601, 602, 604, 607, 609, 611, 613, 615, 617, 619, 621, 628, 636, 637, 638, 639, 644, 646, 648, 653, 665, 667, 672, 675, 678, 679, 681, 691
Datenschutzbeauftragter	<i>Siehe</i> Datenschutzbeauftragte
Datenschutzgrundverordnung	22, 24, 28, 43, 47, 306, 546, 566, 572, 599, 613, 643
Datenschutzhinweis	73, 144
Datensicherheit	238, 272, 309, 365, 403, 444, 445, 446, 462, 491, 536, 579, 590, 660, 669

Datensparsamkeit	45, 61, 113, 129, 193, 241, 280, 325, 341, 413, 460, 552, 579, 583, 599, 605, 613, 629, 646
Datenspeicherung	187, 231, 309, 398, 505, 507, 687
Datenübermittlung	25, 28, 33, 42, 52, 61, 72, 93, 99, 109, 112, 122, 126, 137, 159, 167, 168, 180, 182, 189, 202, 211, 239, 263, 269, 283, 290, 316, 326, 342, 345, 354, 355, 388, 424, 429, 433, 444, 466, 479, 486, 495, 503, 505, 518, 525, 528, 579, 584, 585, 601, 648, 675
Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes	98, 289
Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs	64
Datenübermittlung durch die Gemeinde an die Öffentlichkeit	73
Datenverarbeitung im Auftrag	74, 111, 126, 149
Datenvermeidung	413, 460, 579, 583, 629, 646
De-Mail	149, 504, 603
der Verfassung des Freistaats Thüringen	222
Deutschlandradio	51
Diagnosen	140, 185, 208, 302, 308, 324, 326, 374, 395
Dialog21	473
Diebstahl	55, 94, 183, 504
Dienstanschrift	271
Dienstanweisung	66, 73, 113, 114, 136, 169, 178, 184, 221, 240, 248, 327, 383, 479, 541, 628
Dienstleister	101, 149, 159, 302, 318, 468, 537, 609, 672

dienstliche Dateien	240
dienstlicher Bezug	198
Dienstvereinbarung	136, 182, 184, 287, 345, 538
Dienstversammlung	230, 261
Digitale Agenda 2014-2017	505
DIN-Norm 32757	318
DIN-Norm 663399-1	318
Direkterhebung	201
Diskothek	66
Dissertation	494
Disziplinarmaßnahme	205, 218
Disziplinarverfahren	168, 249
DNA-Intern-Datei	236
Doktorand	494
Dokumentenmanagementsystem	21, 191, 547
Dolmetscher	288
Dozenten	429, 460
Drittanbieter	467
Drogenscreening	306
Drohnen	537, 656
DSGVO	28, 43, 47, 599, 682
DSL	144, 145
Durchsuchung	226, 284, 366, 511
Durchsuchungs- und Beschlagnahme- beschluss	226
technische und organisatorische Maßnahmen	629
E-Government	527, 555, 603
Ehe	86, 107, 159, 161, 260, 280, 299, 378, 485
eHealth	301, 609
E-Health-Gesetz	302, 344, 517
eIDAS	521
Eigenbetrieb	130, 134, 172
Eilbedürftigkeit	370
Eilverfahren	369
Einbürgerungsbewerber	354

Einkommen	147, 150, 158, 260, 263, 295, 296, 297, 354, 358, 381, 448
Einkommensnachweise	158, 361
Einkommenssteuer	260
Einkommensteuergesetz	263
Einschulungsuntersuchung	334, 376
Einsichtnahme	107, 118, 140, 180, 281, 282, 301, 314, 332, 431, 472
Einsichtsfähigkeit	389, 397, 464
Einsichtsrecht	106, 117, 132, 180, 209, 274, 376, 429, 607
Einstellungsbescheid	270
Einverständnis	160, 230, 260, 300, 367, 398, 429, 524
Einwilligung	42, 44, 59, 60, 66, 70, 78, 93, 103, 125, 141, 144, 145, 162, 175, 178, 182, 194, 216, 229, 233, 237, 257, 267, 282, 288, 304, 307, 316, 324, 326, 330, 338, 339, 346, 350, 354, 360, 363, 365, 367, 385, 388, 389, 395, 396, 403, 411, 429, 436, 443, 458, 460, 463, 467, 468, 472, 477, 479, 480, 485, 488, 499, 510, 512, 520, 525, 563, 565, 579, 594, 595, 600, 613, 617, 654
Einwilligungserklärung	71, 94, 140, 179, 230, 237, 258, 283, 308, 324, 331, 354, 398, 464, 479, 485, 499, 512, 521
Einwohnermeldedaten	148
Einzelfunktion	245
Eisfeld	161
elektronische Aktenhaltung	286
elektronische Arztbriefe	344, 651

elektronische Gesundheitskarte	302, 343, 517, 609, 651
elektronische Patientenakte	322, 344, 652
elektronische Personalakte	191
elektronisches Klassebuch	470
Eltern	31, 70, 158, 208, 334, 339, 356, 389, 397, 442, 448, 457, 464, 465, 469, 471, 475, 477, 480, 483, 488, 489, 490, 501, 523, 645, 669, 679, 694
E-Mail	25, 54, 58, 83, 99, 102, 122, 125, 143, 145, 158, 177, 189, 197, 200, 202, 204, 278, 298, 322, 350, 389, 461, 483, 509, 547, 552, 636, 645, 670, 671, 711
Emissions- und Immissionsschutz	406
Empfangstresen	432
Ende-zu-Ende-Verschlüsselung	26, 33, 149, 484, 507, 548, 551, 564, 602, 645
Ende-zu-Ende-Verschlüsselung	588
Energieeffizienz	422
Entfernen von Suchergebnissen	54
Entschlüsselung	190, 391, 550, 586
Entsorgungsunternehmen	77, 97
E-POSTBUSINESS-BOX	149
Erforderlichkeitsprüfung	499
Erfurter Lösung	155
Erhebung beim Betroffenen	164, 312, 362, 369
Erhebung von Kurbeiträgen	87
Erhebungsbogen	158, 334, 392, 435, 448
Erhebungswelle	481
Ermäßigungstatbestand	448
Ermittlungen	69, 109, 222, 224, 232, 234, 248, 269, 270, 366, 689
Ermittlungsakte	224, 225, 226, 234, 271, 278
Ermittlungsführer	168, 248

Ermittlungsverfahren	120, 140, 221, 223, 225, 233, 249, 270, 278, 689
erweiterte Melderegisterauskunft	85
erweitertes Führungszeugnis	474
Erzieherbedarf	449
Erziehungsberechtigte	388, 390, 396, 448, 469, 476, 481, 485
ESF	430, 434
EuGH	25, 29, 41, 61, 238, 274, 433, 467, 519, 525, 528, 567, 575, 636, 643, 649, 675, 691
EU-Kommission	42
EU-Richtlinie „INSPIRE“	411
Europaausschuss	305
Europäische Gerichtshof	43, 49, 53, 60, 525, 575, 641, 649, 675
Europäische Kommission	43, 304, 559, 571, 600
Europäischer Datenschutzausschuss	46, 559, 560, 566
EU-Standardvertragsklauseln	42
Evaluierung	439, 616, 668
Existenzgründerpasses	430
extern	32, 55, 111, 128, 135, 168, 183, 302, 331, 440, 468, 488, 542, 609, 658, 691
externe	204
Facebook	59, 66, 92, 163, 467, 484, 530, 556, 571, 648, 662, 678
Fachschule	210, 455, 493
Fachsoftware	535
Fahrerlaubnisbehörde	269, 414
Fahrzeug	92, 107, 111, 136, 182, 186, 247, 412, 413, 416, 419, 528, 578, 583, 627, 633, 644, 646
Fahrzeugdaten	184, 633
Fahrzeughalter	92, 107, 416
Fahrzeuginnenräume	416
Familiengerichte	281, 350, 363

Familiensachen	281
Familienstand	281, 379
Fanpages	59, 648
Fax	312
FBS-TH	241
Fehltage	210, 476
Feinkonzept	191
Festplatte	25, 169, 423, 489, 503, 531, 658
Feuerstättenmangel	437
Feuerungsanlage	436
Feuerwehr	421
Finanzamt	146, 260, 414
Finanzkassen	255
Fingerabdruckscanner	193, 669
Firewall	384
Flughafen	417
Förderleistung	431, 473
Forderung	33, 44, 48, 77, 135, 163, 254, 259, 260, 276, 287, 295, 313, 315, 352, 382, 390, 411, 435, 440, 452, 465, 474, 494, 506, 512, 552, 564, 580, 603, 620, 633, 683
Forderungseintreibung	254
Formatieren	531, 658
Formularschreiben	297
Forschung	25, 70, 332, 386, 423, 456, 495
Forschungsinstitut	70, 386, 393, 456, 480
Forschungsprojekt	324, 404, 422, 537, 542
Forschungsstelle	481
Forschungsvorhaben	332, 385, 424, 480
Forstverwaltung	538
Fortbildungszertifikat	342
Foto	60, 72, 107, 109, 138, 180, 244, 258, 413, 415, 469, 507, 511, 520, 524, 562
Fotobeweis	416

Fotografien	178, 562
Fotografieren	245, 416
Fragebogen	70, 144, 151, 195, 294, 334, 362, 392, 393, 435, 480, 533
Fraud-Management	434
Freigabe	133, 212, 474, 479, 490
freiwillig	74, 78, 86, 158, 159, 179, 194, 196, 229, 237, 280, 294, 303, 308, 331, 335, 359, 393, 403, 435, 442, 448, 469, 476, 480, 485, 487, 497, 609, 633, 652
Fremdenverkehrsstatistik	86
Friedhofsamt	148
fristgerecht	118
Führerschein	268, 294
Funktionsübertragung	111
Fürsorge- und Erziehungspflichten	474
Fürsorgepflicht des Dienstherrn	122
Gebäude	200, 267, 286, 410, 422, 450, 529
Gebäudemodelle	410
Gebot der Datensparsamkeit	129, 243, 280
Geburtsdatum	86, 91, 117, 148, 225, 255, 324, 414
Geburtsort	225, 275
Geburtstag	376
gefährdete Schutzpersonen	200
Gefährdung der Sicherheit	285
Gefährdungsstufe	200
Gefahrenabwehr	166, 201, 222, 223, 421, 605, 611, 615, 667, 684
Gefangene	274, 283
Gefangenendaten	282
Gefangenepersonalakte	275
Gehaltshöhe	130
Geheimhaltungsinteresse	332, 385
Geheimnisverrat	309
Geldautomat	258

Geldbörsenfunktion	495
Geldinstitut	383
Gemeinderat	72, 130, 154, 155, 205
Gemeinsames Kompetenz- und Dienstleistungszentrum	238, 664
Geobasisdaten	410, 422
Geoproxy	410
Geoproxyserver	423
Gera	169, 278, 341
Gericht	29, 52, 53, 61, 83, 101, 110, 131, 172, 206, 225, 227, 266, 269, 271, 279, 280, 289, 355, 363, 416, 434, 498, 519, 528, 544, 573, 577, 581, 615, 636, 641, 643, 667, 688, 710
Gerichtsakten	265
Gerichtsvollzieher	162
Gesamtplanverfahren	533
Gesamtrechtsnachfolger	260
Gesamtschuldner	260
Geschäftsfähigkeit	397
Geschäftsordnung	33, 157, 380, 492
Geschlechtsverkehr unter Alkoholeinfluss	121
Geschwindigkeitsüberwachung	111
Gesetz zur Einführung einer Speicher- pflicht und einer Höchstspeicherfrist für Verkehrsdaten	516
Gesetzgebungsverfahren	44, 62, 213, 274, 341, 516
Gesichtserkennung	510, 537, 562, 565
Gesundheit	26, 46, 83, 91, 169, 256, 257, 268, 282, 284, 291, 295, 298, 300, 301, 303, 322, 332, 338, 341, 374, 379, 381, 385, 388, 392, 435, 485, 497, 513, 516, 533, 536, 585, 654, 680
gesundheitliche Einschränkungen	295
Gesundheitsamt	334, 338, 376, 476

Gesundheitsämter	334, 339, 376, 386, 477
Gesundheitsbehörde	332, 385
Gesundheitsdaten	31, 140, 208, 274, 283, 304, 310, 323, 324, 326, 339, 341, 394, 475, 610, 652, 654
Gesundheitskarte	301, 343, 517, 609, 651
Gesundheitswesen	302, 333, 344, 385, 517, 609
Gewerbedaten	432
GewO	432
Girokonten	297, 464, 465
Global Positioning System	135, 186
Google	30, 52, 489, 528, 530, 571, 575, 581, 617, 643, 662
GPS (Global Positioning System)	135
Grabstelle	148
Grenzmarken	409
Grundgesetz	28, 57, 98, 130, 179, 222, 273, 289, 329, 348, 407, 516
Grundrecht	28, 46, 49, 52, 131, 156, 201, 218, 220, 223, 277, 286, 340, 389, 407, 506, 519, 547, 556, 564, 567, 573, 576, 581, 597, 601, 602, 606, 613, 615, 619, 624, 633, 636, 642, 667, 668, 685, 693, 694, 702, 703, 706, 708, 714
Grundrecht auf informationelle Selbstbestimmung	28, 42, 52, 131, 193, 202, 219, 222, 226, 275, 284, 329, 339, 396, 445, 511, 516, 565, 604, 613, 636, 642, 656, 677, 695, 696, 702, 703, 706, 708, 710, 714
Grundrechte-Charta der EU	49, 692

Grundrechtseingriff	222, 285, 340, 421, 616, 668, 675
Grundsatz der Datenerhebung beim Betroffenen	69, 311
Grundsatz der Erforderlichkeit	122, 535
Grundsicherungsträger	387
Grundsteuerdaten	100
Grundstücke	75, 118, 128, 268, 408, 410, 423, 450, 649
Grundstücksangaben	75
Grundstückseigentümer	101, 118, 127, 408, 482
Grundstücksgrenzen	408
Gutachten	186, 208, 294, 392, 414, 461, 484, 616, 668
Gutachter	340, 414
Hafteinrichtungen	282
Haftraumtüren	274
HAMASYS	255
Handelsregister	433
Handwerkskammer	428
Handy	226, 245, 342, 389, 530, 547, 565, 641, 662
Hartz IV	380
Hausarzt	315, 542
Hausdurchsuchung	226
Hausrecht	114, 267, 412, 417, 427, 483, 622
Hausverwalter	35
Hebamme	392
Heilfürsorge	216
Heimarbeit	266, 538
Heimarbeitsplatz	538
Heimaufsicht	299, 352
HERE	528, 644
Hilfebedarfsfeststellungsverfahren	533
Hilfeplankonferenz	349
Hinweis nach § 19 Abs. 3 ThürDSG	145
Hirndiagnostik	329
Hochschulbibliothek	495

Hochschule	445, 457, 459, 460, 494, 495, 497, 544
Hochschulstandorte	473
Homepage	38, 61, 157, 193, 194, 221, 232, 389, 412, 635, 677
Hörsaal	229
Hortgebühren	149, 158, 450
Hunde	127, 398
Hundesteuern	128
Hundesteuersatzung	127
IBAN	347
Identität des Fahrers	107
Identitätsfeststellung	244
illegaler Datenhandel	366
individuelle Hilfeplanung	140
Infektionsschutzgesetz	476
informationelle Selbstbestimmung	28, 42, 52, 80, 95, 105, 124, 131, 156, 166, 193, 202, 219, 222, 225, 226, 232, 247, 259, 268, 272, 275, 284, 329, 339, 381, 413, 445, 511, 516, 547, 565, 571, 578, 580, 598, 599, 604, 611, 613, 620, 625, 636, 642, 656, 677, 695, 696, 702, 703, 706, 708, 710, 714
informationelles Selbstbestimmungs- recht	259, 275, 307, 563, 565, 623
Inkrafttreten	22, 36, 191, 252, 288, 306, 546
INPOL	220
Institution des Landes	499
Integrierte Teilhabeplanung	533
Integrität	100, 123, 272, 461, 505, 516, 548, 579, 585, 602, 604, 614, 696
Interamt	202
Interessenskollision	216

Internet	25, 30, 52, 55, 61, 67, 97, 118, 121, 125, 141, 142, 143, 144, 156, 167, 177, 179, 273, 288, 293, 384, 396, 406, 411, 423, 433, 442, 444, 457, 465, 467, 479, 487, 490, 494, 507, 511, 512, 513, 515, 520, 524, 530, 538, 541, 547, 549, 551, 556, 562, 565, 571, 575, 578, 581, 590, 595, 610, 611, 617, 636, 643, 647, 650, 652, 653, 655, 662, 670, 674, 678, 680, 698, 704, 705
Internetauftritt	438, 458, 462, 468, 469, 639
Internet-Forum	681
Internetportal	55, 56, 121, 463
Internetveröffentlichung	98, 466
Intranet	182, 215
ITP	349, 533
IT-Sicherheitsgesetz	26, 515, 604
IT-Sicherheitskonzept	383, 492
Jagdbehörde	66
JII-Richtlinie	24, 28, 47, 682, 683
Jobcenter	291, 293, 294, 296, 297, 353, 380, 386, 390
Journalist	30, 56, 156, 505, 615, 668
Jugendamt	350, 356, 363, 367
Jugendberufsagentur	387, 444
Jugendhilfe	387, 452, 474
Jugendliche	69, 231, 363, 389, 445, 452, 462, 474, 480, 530, 639, 647, 650, 655, 662, 678
Jugendstudie	69
Justizministerium	98, 276, 281, 288
Justizvollzugsanstalt	274, 277, 283, 287

Kamera	23, 38, 72, 94, 113, 114, 157, 229, 239, 245, 258, 416, 417, 419, 420, 450, 481, 530, 537, 622, 641, 644, 647, 656, 662, 677
Kameraattrappe	94, 114
Kammermitglied	428
Karnevalswagen	72
Kassenärztliche Vereinigung	308, 317, 326, 590
Kassenärztlicher Notfalldienst	308
Kassenzahnärztliche Vereinigung	336
Kassenzeichen	254
Katasterbereich	408
Katasterunterlagen	409
Katasterverwaltung	410
Kfz-Kennzeichen	76, 199, 246, 421, 583, 646
Kfz-Kennzeichnen	413
Kinder- und Jugendärztlicher Dienst	334, 376
Kindertagesstätte	335, 523, 639
Kirchensteuer	263
Klagerecht	42
Klasse	389, 446, 463, 465, 466, 468, 471, 475, 480, 482, 484, 531, 647, 662
Klassenbuch	470, 472, 493
Klassenfoto	469
Kleine Anfrage	404
klinisches Krebsregister	340, 584, 585
Klötzchenmodell	410
Kohärenzverfahren	46, 559
Kommunalaufsicht	77, 105, 168
kommunaler Betrieb	130
Kommunalwahl	97, 117
Kommunalwahlgesetz	99, 117
Kommunalwahlordnung	89
Kommunen	25, 59, 65, 71, 74, 78, 100, 104, 112, 134, 143, 146, 156, 178, 182, 292, 293,

	294, 361, 366, 414, 415, 423, 499, 538, 540
Kommunikation	25, 29, 54, 60, 61, 100, 102, 157, 202, 302, 344, 417, 423, 433, 442, 447, 467, 483, 487, 505, 508, 513, 515, 517, 519, 548, 550, 558, 564, 567, 569, 573, 578, 584, 587, 595, 597, 602, 604, 609, 614, 615, 637, 652, 668, 694
Kommunikationsplattform	478, 484, 609
Konto	158, 161, 162, 254, 255, 293, 297, 364, 380, 382, 430, 457, 465, 665
Kontopfändung	161
Kontrolle	22, 34, 39, 73, 80, 109, 133, 134, 136, 147, 168, 176, 187, 207, 222, 227, 235, 238, 243, 246, 252, 256, 261, 264, 265, 273, 274, 285, 287, 300, 317, 322, 353, 365, 398, 407, 412, 413, 417, 490, 530, 535, 537, 542, 552, 562, 566, 567, 569, 577, 580, 583, 592, 607, 612, 620, 627, 633, 646, 678, 688
Kontrollpunkt	413, 583, 646
Kopie	52, 64, 83, 169, 172, 185, 207, 218, 234, 243, 245, 293, 298, 301, 368, 374, 384, 391, 409, 431, 495, 669
Kopplungsverbot	93
Kosten der Unterkunft	101, 369
Kostenschuldner	163
Krankendaten	283

Krankenhaus	311, 314, 316, 319, 322, 324, 398, 542, 586, 593, 680, 681
Krankenhauskeime	323
Krankenhausversorgung	319
Krankenkasse	306, 326, 330, 343, 517, 593, 651, 654
Krankenversichertenkarte	344, 517, 651
Krankenversicherung	304, 331, 344, 458, 517, 593, 651, 654
Krankheitsgründe	475
Krankheitstage	211, 345
Krankmeldung	192, 475
Krebsfrüherkennung	340
Krebsregister	340, 584, 585
Kreditwirtschaft	257
Kryptoalgorithmen	496
kryptografische Verfahren	551, 588
kryptographische Verfahren	506, 614
kryptographischen Verfahren	602
Kultusbereich	454, 466
Kultusministerkonferenz	31, 439, 445, 454, 679, 713
Kundendaten	93, 116, 256, 635
Kündigungsgrund	300
Kündigungsschutzprozesses	300
Kunsturhebergesetz	180
Labor	324, 513
Landesapothekerkammer Thüringen	344, 517
Landesärztekammer	216, 311, 325, 337, 342, 347, 517
Landesärztekammer Thüringen	344
Landesaufnahmeeinrichtung für Flüchtlinge	267
Landeskrankenhausgesellschaft Thüringen e. V.	399, 681
Landespolizeidirektion	49, 220, 228, 233, 235, 240, 245, 248
Landeswahlgesetz	91, 98
Landeswahlleiter	98

Landfahrer	214
Landratsamt	66, 89, 100, 125, 132, 138, 143, 149, 159, 167, 180, 268, 350, 363, 364, 374, 383, 433
Landtagswahl	97, 109, 664
Landwirtschaftlichen Produktions- genossenschaft	404
Laptop	241, 301, 504, 507, 514, 531, 547, 565, 617, 645, 658
Laserscanning	411
Lebenslauf	495
Lehr- und Unterrichtsbetrieb	487
Lehrende	440
Lehrer	31, 210, 442, 444, 446, 447, 457, 460, 461, 468, 483, 487, 489, 490, 500, 645, 647, 662, 674, 679, 694
Lehrerausbildung	439, 441, 445, 467, 639
Lehrerdaten	210, 442, 471, 478, 487, 501
Lehrkraft	211, 396, 441, 442, 446, 452, 460, 461, 463, 464, 466, 468, 469, 471, 475, 477, 478, 487, 500
Lehrpläne	439
Leistungs- und Verhaltenskontrolle	136, 152, 183, 184, 186, 261, 288
Leistungserbringer	340, 362, 433, 534, 584, 585
Leistungskontrolle	235, 261
Leistungsmissbrauch	382
Lernen	440, 442, 638, 653
Lernerfolg	441, 454
Lernkontrolle	487
Lernmanagementsystem	447
Lernplattform	442, 484, 487
Lernprozesse	441

Level of Detail	410
Lichtbildabgleich	107
Liegenschaftskataster	408
Live-Stream	155
Login	457, 467, 471
Löschantrag	53
Löschfristen	188, 231, 314, 323, 479, 692
Löschung	30, 33, 44, 52, 56, 74, 96, 105, 146, 170, 192, 199, 214, 230, 239, 263, 283, 308, 335, 351, 356, 376, 377, 388, 390, 479, 483, 485, 520, 532, 581, 601, 609, 614, 630, 643, 658, 687
Löschung von Daten	521
LPD	233, 235, 240, 248
Mandantenfähigkeit	384
Maßregelvollzug	284, 306
Medienbildung	439
Mediendatenbank	444
Medienkompetenz	31, 439, 445, 446, 639, 650, 653, 655, 664, 670, 679
Medienkompetenzentwicklung	446, 531
Medienkunde	439, 444, 447, 462, 638, 647, 650, 653, 655, 664
Medienprivileg	56
Medienschule	446
Medienunternehmen	157
Medienzentrum	478, 645
Medikationsplan	330, 344
Meldeamt	52, 82, 83, 89, 228
Meldebehörde	33, 35, 51, 82, 84, 87, 107, 227, 232, 355, 393
Meldepflicht	37, 85, 212, 312, 515
melderechtliche Auskunftssperre	280
Melderegisterauskunft	82, 85, 228, 312, 387
Melderegisterdaten	51, 393

Meldewesen 83, 85, 87, 393
Menschen mit Behinderung 533
Messengerdienst 523
mHealth 301, 303
Mieter 35
Mietobjekt 101
Mietwerterhebung 101
Migranten 454
Migrationshintergrund 334, 435
Minderjährige 389, 396
Misshandlungen 474
Mitarbeiter 22, 25, 38, 66, 70, 79, 87, 92, 103, 110, 127, 135, 136,
138, 141, 143, 148, 151,
152, 163, 169, 176, 177,
178, 182, 188, 191, 195,
197, 199, 221, 232, 236,
242, 255, 258, 262, 266,
268, 269, 271, 273, 288,
304, 312, 315, 318, 327,
350, 352, 356, 363, 366,
370, 376, 384, 391, 401,
403, 408, 415, 418, 430,
431, 459, 479, 496, 520,
524, 544, 546, 593, 645,
665, 677
Mitarbeiterbefragung 194
Mitarbeitern 371
Mitwirkungspflicht 36, 159, 328, 359, 363, 381
Mobbing 182, 678
Mobile-Health-Dienste 303
Mobilfunk 429, 444, 553
Mobilfunknummer 429
Mobilgeräte 304, 501, 553
Mobiltelefone 245, 304
Monitoring 418, 426, 622
Moratorium 78
MPU-Gutachten 414
Mütterbefragung 392
Mystery-Check 102
Nachweisführung 460, 497

Name	36, 92, 101, 129, 234, 300, 352, 369, 406, 414, 458, 472, 475, 528, 631
Namenskennung	236
namentliche Nennung	160
Nationaler Krebsplan	340
natürliche Person	57, 75, 188, 407
Naturschutz	407, 425
netzwerkfähig	514
Newsletter	397, 519
nicht-öffentliche Stelle	38, 162, 179, 205, 213, 397, 426, 451
nicht-öffentliche Stelle	551
nicht-öffentlicher Sitzung	131, 154
Notar	271
Notenbekanntgabe	464
Notfalldaten	344, 652
Notfallversorgungsdaten	344, 651
Notfallzugriff	322
Novellierung	118, 236, 289, 474, 607, 636, 664
NSA-Untersuchungsausschuss	29
Nutzungsbeschränkung	264, 379
Oberbürgermeister	78, 120, 135, 151, 167
obersten Landesbehörden	60, 189, 540
OBG	163
öffentlich bestellter Vermessungs- ingenieur	409
öffentlich zugängliche Räume	417, 482, 622, 649
öffentliche Stelle	24, 32, 37, 56, 59, 72, 93, 99, 101, 104, 112, 117, 125, 127, 134, 144, 150, 166, 170, 178, 179, 190, 204, 206, 213, 244, 259, 269, 299, 321, 364, 395, 397, 410, 417, 421, 423, 426, 430, 436, 451, 461, 484, 507, 524, 555, 557, 648
öffentlichen Sitzung	131, 157, 168, 363

öffentliches Interesse	213, 332, 385
Öffentlichkeit	47, 61, 72, 98, 121, 131, 140, 156, 251, 406, 426, 477, 482, 501, 544, 552, 556, 562, 565, 576, 616, 653, 668
Öffentlichkeitsarbeit	251
Öffentlichkeitsgrundsatz	155
öffentlich-rechtliches Unternehmen	320
Öffnungszeit	448, 451
OH KIS	321, 323
Ohnhänder	257
One-Stop-Shop-Verfahren	44
Onlineabgleich	344
Onlinebewerbung	203
Online-Lernplattformen	442
Online-Medien	58
Online-Plattform	467
Opferzeugin	120
ÖPNV	411, 621, 677
Opt-In-Lösung	510
Optionskommunen	292, 293, 294
Opt-Out-Lösung	509
Ordnungsamt	58, 59, 64, 99, 137, 163, 177, 416
Ordnungsämter	<i>Siehe</i> Ordnungsamt
Ordnungsbehörde	163, 355, 415
Ordnungsgeld	311
Ordnungswidrigkeit	92, 99, 108, 137, 139, 166, 173, 222, 685
Ordnungswidrigkeitenverfahren	110, 173, 182
Organspende	328, 344
Orientierungshilfe	37, 116, 232, 321, 384, 412, 420, 442, 487, 508, 518, 621, 672, 677
Orientierungshilfe Krankenhaus- informationssysteme	323
Originalbelege	313, 431
Originaldokumente	384
pädagogische Fachkräfte	441, 694

PAG	200, 222, 231, 240, 244, 246
Parkhaus	417
Parkplätze	418
Parkscheibe	415
Parkschein	415, 418
Parkverstöße	415
Parlament	44, 600, 682, 688
Passwort	55, 187, 192, 322, 458, 479, 481
Patient	25, 284, 302, 303, 308, 314, 316, 318, 319, 322, 323, 326, 330, 332, 340, 342, 344, 376, 542, 589, 593, 651
Patientenakten	314, 317, 319, 322, 344
Patientendaten	309, 312, 314, 315, 317, 322, 376, 542, 584, 587, 609
PC	166, 169, 240, 308, 391, 480, 487, 501, 507, 530, 531, 540, 658, 662
Personalakte	153, 175, 185, 190, 191, 206, 218, 275, 282, 315, 366, 371, 375
Personalaktendaten	152, 175, 192, 207, 345, 375
Personalaktenführung	191, 207
Personalaktenführungsrichtlinie	192, 207
Personalausweis	54, 86, 107, 245, 504, 521, 550
Personalausweisgesetz	26
Personalausweisgesetz (PAuswG)	107
Personalausweiskopie	243
Personalausweisregister	107
Personaldaten	97, 153, 172, 315, 367
Personaldatenschutz	367
Personalnummern	371

Personalrat	95, 174, 180, 198, 237, 262, 287, 346, 375, 699, 700
Personalratsmitglied	175, 180, 256, 700
Personalunterlagen	207, 219, 672
Personalverwaltung	152, 153, 175, 178, 185, 191, 198, 207, 345, 366
personenbeziehbare Daten	402, 403
Personenbeziehbarkeit	70, 112, 480
Personenbezug	167, 188, 262, 325, 435, 538
Personenkonten	254
Personennotrufanlage	287
Persönlichkeitsprofile	487, 578, 581
Pfändungs- und Einziehungsverfügung	161
Pflegedienste	371
Pflegeheim	68, 299, 351, 364
Pflegeheimträger	371
Pflegepersonal	303, 322
Pflicht	45, 73, 77, 124, 126, 164, 174, 241, 273, 295, 322, 407, 432, 435, 476, 494, 517, 567, 578, 604, 624, 636, 651, 672
PKW-Maut	413, 583, 646
Planungsbüro	112
Plausibilität	327, 358, 373, 473
Polizei	24, 49, 107, 136, 137, 188, 200, 214, 216, 220, 222, 223, 227, 229, 231, 232, 233, 234, 236, 238, 239, 240, 241, 243, 244, 246, 247, 252, 270, 312, 355, 422, 538, 556, 565, 569, 611, 619, 631, 636, 664, 666, 683
Polizeiarzt	216
polizeiärztlicher Dienst	216
Polizeiaufgabengesetz	200, 221, 223, 240, 243, 246, 422, 636

Polizeibeamte	138, 227, 233, 234, 240, 244, 247
polizeiliche Auskunft- und Recherchesysteme	221
Positionspapier	24, 42
Postfachadresse	278, 292
Postgeheimnis	347
Postweg	100, 149, 298
Postzustellung	147
praktische Konkordanz	131
Pressemitteilung	55, 60, 103, 120, 241, 343, 414, 484, 509, 511, 517, 530, 538, 580, 613, 633, 635, 636, 638, 639, 641, 643, 644, 645, 646, 647, 648, 649, 650, 651, 653, 654, 655, 656, 658, 662, 664, 665, 667, 669, 670, 671, 672, 674, 675, 677, 678, 679, 680, 681
Presserat	57
Privacy-by-Default	508, 560, 578
Privacy-by-Design	543, 560, 578
Privatadresse	270, 311
Privatanschrift	271, 278, 311
private Datenverarbeitungsgeräte	442
private Wohnanschrift	280
privates Forschungsinstitut	393
Privatkonten	465
Profilbildung	511, 633
Profilingbogen	294
Promotion	494
Promovend	494
Prostitution	163, 212, 214
Protokoll	33, 105, 151, 186, 220, 229, 232, 253, 300, 308, 322, 479, 592
Protokollierung	152, 253
Prüfeinrichtung	326
Prüffrist	48, 221, 231, 687

Prüfpflicht	271, 395
Prüfungsamt	459, 497
Prüfungsergebnisse	457, 496
Prüfungskompetenz des TLfDI	273
Prüfungslisten	468
Prüfungsordnungen	460
Prüfungsunfähigkeit	497
Prüfungszwecke	373
Prüfverfahren	327, 443, 456
Pseudonyme	92, 556
Pseudonymisierung	113, 333, 605
qualifizierte elektronische Signatur	27, 397, 521, 523
qualifizierten elektronischen Signatur	26, 230, 384, 469, 521
Qualitätsmanagement	194, 324
Qualitätssicherung	323, 340
Rasterfahndung	222, 612
Ratsinformationssystem	142
Räumfahrzeug	188
RC4	513
Reanonymisierung	71, 362, 373
Recherche	30, 65, 76, 106, 107, 120, 125, 145, 148, 161, 163, 220, 223, 227, 385, 444, 510, 538, 619
Rechnungsprüfung	153, 208
Recht auf informationelle Selbst- bestimmung	28, 42, 52, 95, 105, 124, 131, 156, 166, 193, 202, 219, 223, 225, 226, 232, 247, 259, 268, 275, 286, 339, 381, 413, 445, 511, 547, 580, 600, 605, 614, 625, 637, 656, 677
Recht auf körperliche Unversehrtheit	329
Recht auf Vergessenwerden	30, 44
Rechtsanwalt	87, 132, 167, 247, 325, 347
Rechtsgeschäfte	397
Regelschule	446, 485, 493

Registrierung	203, 278, 311, 341, 399, 484, 587
Rehabilitation und Teilhabe	348
Reihenuntersuchungen	338
Religionsgemeinschaft	263, 298, 381
religiöse Überzeugungen	45, 125, 264
Rezept	309, 312, 344, 651
RFID-Technologie	496
richterliche Unabhängigkeit	227
Risikoanalyse	384, 587
Rollen- und Rechtekonzept	543
Rollenkonzept	191
Saale-Holzland	74
Sachverhalt	36, 56, 64, 66, 67, 68, 72, 79, 87, 98, 103, 106, 107, 109, 114, 116, 120, 129, 139, 145, 146, 151, 159, 165, 167, 170, 177, 199, 207, 214, 220, 224, 225, 228, 230, 231, 233, 237, 246, 249, 261, 278, 281, 297, 298, 299, 316, 320, 356, 363, 369, 373, 379, 382, 387, 390, 402, 405, 409, 411, 429, 431, 449, 456, 459, 464, 465, 466, 471, 477
Safe Harbor	29, 41, 61, 238, 518, 528, 601, 614, 675
Safe-Harbor-Abkommen	41, 519, 567, 675
Safer Internet Day	439, 462, 678
SARS	223
Schöffenvwahl	142
Schornsteinfegerinnung	436
Schreddern	318
Schriftform	141, 179, 230, 257, 260, 283, 324, 331, 397, 469
Schriftgut	96, 221, 232, 271, 279, 401
Schufa	465

Schulamt	70, 446, 449, 461, 466, 470, 478, 490
Schulämter	449, 461, 469, 479, 483, 491
schulärztlicher Dienst	338
Schulaufsicht	211, 488, 645
Schulaufsichtsbehörde	212, 470, 488
Schulbehörden	484, 490
Schulbetrieb	470, 481
Schulden	260, 294
Schule	31, 32, 70, 210, 352, 387, 439, 441, 444, 446, 447, 449, 450, 452, 455, 456, 457, 459, 461, 464, 465, 468, 470, 472, 474, 475, 477, 478, 480, 481, 483, 485, 486, 490, 494, 496, 497, 501, 530, 544, 639, 645, 647, 653, 662, 669, 694, 695, 697, 704, 705
Schulen in freier Trägerschaft	446, 474
Schüler	31, 70, 338, 388, 396, 440, 442, 444, 446, 447, 450, 453, 454, 460, 461, 463, 465, 468, 471, 472, 473, 477, 478, 480, 483, 485, 487, 489, 490, 501, 531, 653, 662, 664, 669, 679, 694
Schüler- und Elterndaten	466, 470
Schüler- und Lehrerdaten	444, 457, 487, 501
Schülerdaten	388, 443, 461, 465, 501
Schülerliste	466
Schulgebäude	481
Schulgesundheitspflege	334, 339
Schulhomepage	468, 492
Schulhort	448
Schulkind	448, 463, 475
Schulleistungsuntersuchungen	456
Schulnoten	463

Schulportal	444, 466, 478, 531, 647
Schulstoff	487
Schulsystem	454
Schulträger	449, 465, 470, 490
Schulverwaltungsamt	471
Schulverwaltungsprogramme	493
Schulverwaltungssoftware	493
schulzahnärztlicher Dienst	339
Schutzbereich	405
Schutzstufe	384
schutzwürdige Belange	286, 333
schutzwürdige Interessen	83, 95, 268, 370, 392, 426, 483, 622
schutzwürdige Interessen des Betroffenen	91, 104, 114, 259, 267, 370, 371, 392, 412, 418, 426, 482, 624
Schwärzen	59, 244, 298, 381, 395, 431
schwarzes Brett	457
Schwärzung	198, 219, 260, 293, 298, 301, 374, 381
Schweigepflicht	141, 186, 216, 302, 322, 328, 486, 610
Schweigepflichtentbindung	141, 186, 314, 363, 485
Schweigepflichtentbindungserklärung	318
Schwerbehindertenausweis	374
Schwerbehindertenrecht	383
Schwerbehindertenvertretung	346
Sektionsschein	332, 385
Selbstdatenschutz	462, 530, 678
SEPA-Zahlungsverkehr	347
Serverräume	384
Sexueller Kindesmissbrauch	498
Sexueller Missbrauch	474, 499
sichere Passwörter	56
Sicherheitsbehörden	222, 252, 268, 355, 413, 505, 511, 569, 570, 601, 614, 616, 619, 667

Sicherheitskonzept	99, 169, 473, 479, 491, 535
Sicherheitsstufe	97, 318
SIM-Karte	553, 660
Skimming	258
smartes Heizsystem	403
Smartphone	13, 58, 241, 244, 301, 303, 309, 460, 463, 487, 501, 507, 513, 524, 531, 617, 658, 678
Software	23, 55, 115, 125, 191, 239, 240, 302, 322, 325, 331, 415, 441, 442, 470, 479, 487, 490, 504, 510, 511, 536, 540, 550, 564, 586, 617, 658
Software as a Service	116
Softwarefirma	115, 125
Softwareunternehmen	126
Sorgeberechtigte	70, 216, 356, 452, 465
Sozialamt	140, 298, 348, 359, 361, 364, 378, 394, 534
Sozialarbeit	444, 452, 485, 534, 697
Sozialdaten	69, 141, 256, 291, 294, 336, 348, 353, 357, 359, 368, 369, 374, 377, 383, 391, 414
soziale Netzwerke	61, 443, 467, 484, 512, 557, 674, 704
soziales Netzwerk	483
Sozialgeheimnis	292, 383, 414
Sozialhilfe	348, 359, 361, 364
Sozialhilfeträger	349, 361, 371, 388
Sozialleistungen	293, 297, 299, 381
Sozialleistungsträger	292, 381
Sparkasse	255, 258, 259, 382
Speicher- und Aussonderungsprüffristen	48, 687
Speicherdauer	258, 336, 417

Speichern	67, 80, 137, 188, 240, 296, 305, 377, 471, 475, 482, 508, 512, 521, 542, 580, 581, 583, 592, 619, 646, 659
Speicherplatz	471, 508, 521
Speicherung	24, 29, 43, 57, 61, 116, 133, 136, 146, 180, 184, 187, 193, 202, 230, 231, 243, 245, 255, 262, 283, 302, 307, 335, 336, 357, 378, 382, 388, 389, 418, 476, 482, 485, 511, 548, 550, 554, 562, 565, 567, 583, 588, 595, 609, 611, 616, 629, 636, 646, 651, 667, 683, 710
Speicherungsfrist	188, 231, 237
Spender-Anamnesebogen	329
Spenderorgan	329
Sperrung	30, 53, 201, 245, 275, 379, 391, 408, 575, 581
Sportunterricht	476
Staatsanwaltschaft	65, 106, 109, 120, 139, 173, 225, 226, 232, 233, 258, 268, 270, 278, 289, 557, 631, 666, 688
Staatsvertrag	52, 238
Stadtentwicklung	112, 422
Stadtentwicklungskonzept	112
Stadtrat	25, 77, 79, 142, 152, 155, 177, 204
Stadtratsbeschlüsse	142
Stadtratssitzung	142, 155, 204
Stadtverwaltung	67, 68, 70, 73, 77, 83, 92, 96, 99, 101, 107, 109, 112, 115, 117, 119, 121, 130, 135, 141, 142, 145, 148, 150, 153, 157, 158, 161,

	164, 167, 177, 178, 182, 204, 358, 370, 448, 538
Stadtwerke	93, 169, 186, 513
Stasi-Unterlagen-Gesetz	77
statistische Auswertung	262, 323
statistische Erhebung	454
Stellenausschreibung	189, 203
Stellenplattform	202
Stellenzeichen	262, 373
Steuerfahndungsstelle	414
Steuergeheimnis	102, 128
Steuerkonto	255
Steuerprüfer	66
Stichproben	34, 148, 189, 322, 327, 392, 435, 607
Störhaftung	62
StPO	166, 222, 223, 226, 233, 242, 557
Strafantrag	139, 172
Strafanzeige	138, 232, 249, 270, 278, 623
Strafbefehl	225
Strafmaß	140
Strafprozessordnung	120, 221, 222, 223, 226, 233, 557
Straftat 3	0, 46, 47, 139, 173, 186, 222, 223, 225, 231, 242, 250, 267, 269, 348, 420, 474, 557, 611, 622, 683
Straftatbestand	30, 110, 140
Strafverfahren	72, 138, 173, 233, 269, 294
Strafverfolgungsbehörde	54, 224, 226, 268, 355, 556, 665, 690
Straßen	58, 74, 77, 107, 112, 163, 410, 414, 416, 419, 421, 422, 529, 656
Straßenbahnen	62, 411, 677
Straßenpanoramafahrten	528

Student	459, 460, 473, 496, 647, 679
Studentenausweis	495
Studentenwerk	473, 495
Studienprojekte	456
Studierende	457, 459, 460, 497
Stundenpläne	468, 478
Suchtmittelmissbrauch	285
Suchtprobleme	294
Tablets	23, 309, 480, 501, 507, 513
Täter	110, 140, 200, 222, 224, 234, 247, 258, 499, 556, 565
Täternamen	498
Technik	25, 61, 113, 116, 136, 183, 204, 238, 257, 260, 302, 309, 384, 419, 479, 496, 505, 510, 513, 514, 522, 527, 532, 549, 550, 557, 562, 580, 590, 604, 610, 621, 658, 670, 674, 677, 689
technische und organisatorische Maßnahmen	26, 71, 73, 74, 96, 99, 116, 170, 173, 174, 185, 190, 191, 203, 211, 242, 253, 271, 272, 286, 292, 305, 314, 316, 325, 331, 345, 347, 353, 383, 394, 417, 459, 461, 466, 468, 479, 481, 489, 491, 501, 524, 535, 539, 541, 543, 548, 564, 579, 712
Teilnehmerzahl	67, 645
Telefon	102, 143, 245, 271, 275, 304, 358, 636, 665
Telefongespräch	276
Telefonnummer	115, 137, 143, 158, 224, 465, 509, 671

Telekommunikation	26, 51, 224, 238, 245, 516, 552, 567, 569, 573, 605, 615, 667
Telekommunikationsgesetz	62, 224, 516, 637
Telekommunikationsüberwachung	238, 570, 664
Telemediengesetz	61, 126, 390, 556
Telemedizinplattform	542
ThA VEL	534
thoska	495
Thüringer Landeskriminalamt	220, 232, 236, 253
Thüringer Landesrechenzentrum	74, 399, 473, 513
Thüringer Landesverwaltungsamt	117, 267, 299, 334, 371, 394, 535
Thüringer Landtag	33, 109, 156, 218, 305, 306, 315, 440
Thüringer Liegenschaftsmanagement	401
Thüringer Ministerium für Bau, Landesentwicklung und Verkehr	402, 411
Thüringer Ministerium für Infra- struktur und Landwirtschaft	402, 412
Thüringer Ministerium für Migration, Justiz und Verbraucherschutz	272, 277, 282
Thüringer Schulportal	<i>Siehe Schulportal</i>
Tiefgarage	199
TIM	107, 117, 214, 235, 239, 241, 354, 392
TMBJS	388, 455, 465, 471, 500
TMIK	33, 99, 217, 244, 252, 421
Todesursachen	332, 385
Tonaufzeichnung	155
Totenschein	332, 385
Transparenz für die Betroffenen	136, 185, 262, 355
Transplantation	329
Transplantationsbeauftragter	328
Tresen-Lösung	459
Trilog-Verfahren	44
TrueCrypt	503
Übermittlungsbefugnis	184, 213, 300, 318, 328, 368, 423
Überschreitung von Verordnungs-	

summendaten	327
Übersetzer	288
Übersetzerdatenbank	289
Überwachung der Mitarbeiter	189, 418
Überwachungsberichte	406
Überweisung	255, 298, 364, 381, 665
Umfrage	59, 125, 144, 155, 195, 354
Umzugskosten	369
unbefugte Kenntnis	173, 190, 211
unberechtigter Zugriff	256, 306
Universität	316, 320, 324, 332, 422, 489, 513, 542, 639
Universitätsklinikum	316, 324, 332
Universitätsklinikum Jena	315, 319, 324, 542
unsichere Drittstaaten	432
Unterarbeitskreis Datenschutz und Schule	441, 486
Unterhaltspflicht	387, 458
Unterhaltssache	367
Unternehmensgründer	430
Unterricht	202, 210, 222, 251, 396, 439, 442, 444, 463, 470, 475, 477, 482, 484, 486, 489, 493, 531, 630, 647, 653, 664
Unterrichtskonzepte	441
Unterrichtsmaterialien	444, 466, 478
Unterrichtszeiten	481
Unterrichtungspflicht	202, 222, 630
Unterschriften	78, 88, 117
Unterschriftensammlung	25, 78, 88
Unterstützerliste	33, 118
Unterstützungs- und Auskunftspflicht	147
Unterstützungspflicht	187, 227, 402, 500
Untersuchungsausschuss	29, 218, 620
unzulässige Übermittlung	368
Urin-, Blut- oder Speichelprobe	307
Urkunde	135, 192, 272, 281, 312, 342

Urkundenarchiv	271
Urteil des Thüringer Oberverwaltungs- gerichts (OVG)	130
USA	25, 41, 53, 60, 239, 467, 518, 525, 528, 530, 567, 571, 601, 614, 662, 675
USB	504, 531, 658, 659
Veranstaltung	67, 164, 179, 200, 229, 246, 267, 439, 462, 520, 544, 640, 645, 674, 695, 698, 703, 710
Verfahrensverzeichnis	95, 202, 211, 237, 266, 474, 479, 488, 492, 687
Verfassung des Freistaats Thüringen	130, 227, 704
Verfassungsschutzbericht	252
Verhältnismäßigkeit	29, 48, 185, 193, 219, 247, 286, 497, 551, 557, 570, 597, 615, 637, 668, 669, 675, 687, 702, 703, 706, 714
Verkehrsleistungen	411
Verkehrsordnungswidrigkeit	92, 107
Vermieter	39, 101, 369
Vernichtung von Daten	170, 658
Verschlüsselung	26, 150, 190, 192, 317, 479, 496, 503, 505, 512, 548, 550, 564, 586, 602, 614, 645, 705, 711
Verschlüsselungsverfahren	26, 100, 204, 384, 462, 505, 513
Verschreibung	310
Verschwiegenheitspflicht	414, 505, 602
Versetzung in den Ruhestand	153, 241
Versichertendaten	327
Versicherungsunternehmen	366
versiegelte Umverpackungen	319
Verstorbene	57, 260, 329, 332, 385
Verteidiger	277

vertraulich	168, 172, 175, 198, 204, 207, 219, 270, 431, 459, 505
Vertraulichkeit	100, 110, 190, 272, 292, 302, 347, 431, 459, 461, 505, 516, 524, 548, 553, 585, 602, 604, 609, 614, 696
Vertraulichkeitsgrad	318
Vertretungspläne	468, 478, 704
Verwaltungsangelegenheiten	227, 266
Verwaltungsplattform	461
Verwargelder	235
Verwargeld-Vorverfahren	92
Veterinärämter	535
Video	37, 62, 94, 113, 114, 229, 239, 258, 267, 411, 417, 419, 420, 425, 444, 450, 462, 481, 524, 531, 562, 619, 621, 639, 641, 647, 649, 677
Videoaufzeichnung	267, 418, 452
Videotechnik	113, 229, 419, 677
Videoüberwachung	25, 37, 95, 113, 114, 258, 267, 286, 411, 416, 419, 425, 444, 450, 462, 481, 547, 566, 621, 641, 649, 664, 677, 678
Vignette	413, 583, 646
Volksbegehren	81, 90
Volksentscheid	81, 90
Volljährigkeit	396
Vorabkontrolle	412, 417, 490, 628
Vorlage von Kontoauszügen	299, 382
Vor-Ort-Kontrolle	188
Vorratsdatenspeicherung	29, 197, 567, 597, 615, 636, 667, 710
Vorsorgeuntersuchung	335
Waffenbehörde	34, 138
Waffenbesitzkarte	138

Waffengesetz	35, 138
Waffenregister	33
Wahlberechtigte	91, 117
Wahlbüro	143
Wahlen	33, 97, 172, 228
Wahlscheine	91, 512
Wahlstatistik	98
Wahlunterlagen	89, 172
Waldgebiete	426
Wasserverbrauch	422
websta	278
Wegeheld	58
Weiterbildung	441, 492, 674
Weiterbildungsmaßnahmen	492
Werbeeinwilligung	398
Werkstoffhof	169
Wettbewerb	32, 37, 170, 173, 195, 259, 316, 319, 324, 417, 451, 571, 580
Widerspruch	51, 53, 83, 118, 159, 208, 289, 321, 327, 364, 474, 529, 576
Widerspruchsrecht	62, 118, 529
Wildkamera	425
Wildkameras	425
Windows 10	509, 671, 674
Wissenschaft	321, 332, 403, 424, 425, 427, 428, 433, 439, 443, 446, 448, 454, 456, 461, 467, 469, 471, 473, 474, 490, 495, 498, 552, 616, 639, 668, 694, 699, 700, 708
wissenschaftliche Forschung	386, 423
wissenschaftliches Monitoring	427
WLAN	62
Wohnanschrift	36, 97, 232, 233, 280
Wohngeld	68, 355, 358
Wohnort	81, 233, 278, 332, 385, 389

Wohnung	35, 87, 91, 137, 138, 226, 369
Wohnungsverwaltung	137
Wolfsbeobachtung	425
Wolke	185, 489, 507
Young Data	438, 638, 639
Zahlstelle	235, 535
ZDF	51
Zeitkontingent	492
Zeitung	58, 66, 109, 157, 169, 177, 178, 266
Zeitungsartikel	266, 314
Zensuren	463
Zentrales Verkehrsinformationssystem	228
Zentralkartei	376
Zentralrat der Sinti und Roma	215
Zertifikate	96, 342, 521, 551, 561
Zeugnis	464, 475, 476, 484
Zugangsbeschränkung	410
Züge	62, 336, 411, 677
Zugriffs- und Berechtigungskonzept	377, 384
Zugriffsrechte	25, 192, 305, 322, 341, 376, 481, 535, 542
Zugriffsregelungen	471
Zuweiserportal	316
Zuwendungsempfänger	431
Zwangsbehandlung	284
Zweckbindungsgrundsatz	305

Notizen:

Notizen:

Notizen:

