10. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 1. Januar 2012 bis 31. Dezember 2013
Zitiervorschlag: 10. TB LfDI Thüringen

Der 10. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Mai 2014

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

Inhaltsverzeichnis

A. Öffentlicher Bereich

Vorwort **15**

1 Schwerpunkte im Berichtszeitraum 17

2 Allgemeine Entwicklungen im Datenschutz 19
2.1 Das neue Thüringer Datenschutzgesetz 19
2.2 Snowden, NSA, PRISM, Tempora und Antiterrordatei - das Jahr 2013 als „datenschutzrechtlicher Durchlauferhitzer“ 20
2.3 Schutzfristenverkürzung gemäß § 17 Abs. 5 Thüringer Archivgesetz bei herauszugebenden Unterlagen an den Untersuchungsausschuss des Landtags 27
2.4 E-Government-Gesetz des Bundes 28
2.5 Zensus 2011 reloaded 29
2.6 Senioren im Netz des Mikrozensus 30
2.7 Bundesweites Schuldnerverzeichnis im Internet - Schuldnerverzeichnisverordnung – erst nach Intervention der Datenschutzbeauftragten datenschutzgemäß 31
2.8 Gesetz zur Optimierung der Geldwäscheprävention - auf Kosten des Datenschutzes bei E-Geld-Transaktionen! .. 33
2.9 Nationales Waffenregister - Schuss in den Ofen? 35
2.10 Der bewegte Weg des Gesetzes zur Fortentwicklung des Meldewesens 36

3 Europäischer und Internationaler Datenschutz 40
3.1 Gesamtkonzept für den Datenschutz in der Europäischen Union – KOM(2010)609 – Allgemeine Datenschutzverordnung 40
3.2 Einführung des interoperablen EU-weiten eCall-Dienstes – Mehr Verkehrssicherheit auf Kosten des Datenschutzes? 40
3.3 Ausschreibung im Schengener Informations-system (SIS) 43

4 Neue Medien – Rundfunk – Telekommunikation 45
4.1 Bekommt Deutschland den Cooki gebacken? 45

4.2 Leitplanken für soziale Netzwerke 47
4.3 In's Netz gegangen - Facebook 48
4.4 Notruf 51
4.5 Überwachung der Telekommunikation gem. § 100 a StPO und Erhebung von Verkehrsdaten nach § 100 g StPO im Jahr 2010 – auch mittels Eilanordnung erfolgt? 52

5 Kommunales 54
5.1 Datenschutzrechtliche Kommunalkontrollen allgemein – Steter Tropfen höhlt den Stein 54
5.2 Arbeitskreis Kommunaler Datenschutz 56
5.3 Videoüberwachung über und unter Wasser: Videogaga 1 56
5.4 Zensus 2011 - Kontrolle der Statistikstelle der Stadtverwaltung Pößneck 58
5.5 Rettungsleitstelle: Privates für den Vorgesetzten 60
5.6 Videoüberwachung im Schloss: Videogaga 2 61
5.7 Wer ist der „amtliche" Vater – zur Weitergabe sensibler Daten durch das Standesamt 64
5.8 Heirat mit Nachteilen – Datenweitergabe des Standesamts Lauscha an das Jobcenter Suhl 65
5.9 Kaffeekränzchen mit Neubürgern: Bitter bei Datenschutzverstoß 66
5.10 Kommunen als „verlängerter Arm" von Steuerbehörden? 67
5.11 Der Status "Soldat im Auslandseinsatz" schützt nicht vor berechtigten Forderungen eines Gläubigers 70
5.12 Schutz vor gefährlichen Tieren contra Datenschutz 71
5.13 Meldescheinkopien nehmen kein gutes Ende 73
5.14 1000 Greizer 75
5.15 Bitte keine zwangsweise Familienzusammenführung! Zu den Voraussetzungen der Einwilligung in die Verarbeitung und Nutzung personenbezogener Daten ... 77
5.16 Innenminister versus Antikorruptionsbeauftragter 79
5.17 Lieferung von Obdachlosen-Gesundheitsdaten frei Haus? 80
5.18 Videoüberwachung der Beschäftigten durch die Suhler Stadtwirtschaft GmbH: Videogaga 3 81
5.19 Keine Drohnen im Rechtsstaat: Videogaga 4 82

5.20 Fremdenverkehrssatzung – „Die Dritte“ 84
5.21 Übermittlung von Grundstückseigentümerdaten an Dritte 86
5.22 Erfurter Streetview 87
5.23 Rechtmäßige Befragung der Nachbarn? 89
5.24 Datenübermittlung: Für Eltern zu viel des Guten 90
5.25 Kaufvertragsabschluss nur mit „Bürgerentscheid“ 92
5.26 Bleibt der Informant anonym? 92
5.27 Liveübertragung von Sitzungen des Stadtrates im Internet: Video 5 95
5.28 Zuviel Information für Fraktionsvorsitzende in Suhl 98
5.29 Vorsicht beim Versand von Unterlagen für Stadtratssitzungen 99
5.30 „Hunger“ auf Gewerbedaten – innerhalb der Behörde erlaubt? 100
5.31 Bürgerbefragung ist Datenerhebung 102
5.32 Übermittlung gaststättenbezogener Außenbewirtschaftungszeiten von der Bauaufsichtsbehörde an die Gewerbebehörde 103
5.33 Widerspruchsmöglichkeit des Bürgers gegen Weitergabe seiner Daten durch die Meldebehörde 104

6 Personaldaten 106
6.1 Verwaltungsschule veröffentlicht Beschäftigtenfotos 106
6.2 Ist die moderne Verwaltung in allen obersten Landesbehörden angekommen? 108
6.3 Kein Datenschutz am Sonntag 109
6.4 Alkoholabhängigkeit eines Bediensteten 110
6.5 Datenschutz-(Bei-)Hilfe 112
6.6 Erkennungsdienstliche Maßnahmen des Arbeitgebers? 113
6.7 Manchmal müssen Zeiterfassungsdaten auch länger aufbewahrt werden 114
6.8 Darf der Dienstherr den behandelnden Arzt kennen? 115

7 Polizei 117
7.1 „Datenleck" und andere Datenschutzpannen im Bildungszentrum der Thüringer Polizei in Meiningen 117

7.2 Wem gehören die Dateien auf dem Dienst-Computer? 119
7.3 Polizei auf Abwegen 122
7.4 Die Polizei auf Abwegen - Teil 2 124
7.5 Auch Bilder und Videos können Träger personenbezogener Daten sein 126
7.6 Videoüberwachung von Gewahrsamsräumen – in Thüringen ohne gesetzliche Grundlage unzulässig: Videogaga 6 127
7.7 "Betäubungsmittel-Konsument" - eine Jugendsünde fürs Leben? 128
7.8 „Jungbrunnen" für Prüf- und Löschfristen 130
7.9 Moratorium gegen die Vernichtung von Akten mit Bezügen zum Nationalsozialistischen Unter-grund (NSU) 132
7.10 Videoüberwachung aus dem Blumentopf – zur Aufklärung von Einbrüchen erlaubt!: Videogaga 7 135
7.11 Mitteilung der Staatsanwaltschaften an Ausländerbehörden: Unterrichtung, statt Aktenübersendung 137
7.12 Erkennungsdienstliche Erfassung in den Polizeidienststellen 138
7.13 Die Novellierung des Thüringer Polizeiaufgabengesetzes – auf die „lange Bank“ geschoben und am Ende wenig erreicht 139
7.14 IGVP und Findus 143
7.15 Vernichtung von Ermittlungsakten des TLKA nach der Ablauf der Aufbewahrungsbestimmungen - Leitfaden 146
7.16 Löschung personenbezogener Daten in INPOL sowie bei der zuständigen Landespolizeidirektion 149
7.17 Anmeldeverfahren zum Tag der Deutschen Einheit 2012 149
7.18 Klopapier: Thüringer Landeskriminalamt von der Datenschutz-Rolle - Videogaga 8 152
7.19 Bestandsdatenabfrage nach § 113 Abs. 1 Telekommunikationsgesetz (TKG) - auch in Übergangszeiten kein rechtsfreier Raum 154
7.20 Abgeordnete des Thüringer Landtags zu Unrecht im Fokus der Polizei 157

7.21 Polizei vs. Journalisten 160
7.22 Papstbesuch in Thüringen – nicht nur der Himmel schaute zu: Video 9 163
7.23 Unbemerktes Mithören und GPS-Daten-Übertragung beim digitalen Polizeifunk – Überwachung der Polizisten durch die Polizei? 164

8 Verfassungsschutz 168
8.1 Unkenntnis und Raummangel sind kein „Freibrief“ zur Aktenvernichtung – Nichtanbietung von Schriftgut des Thüringer Landesamtes für Verfassungsschutz an das Thüringer Staatsarchiv 168
8.2 Das Thüringer Landesamt für Verfassungsschutz schweigt - zu Recht? 170

9 Finanzwesen 173
9.1 Spezielle Probleme mit der Steuer-Identifikationsnummer 173
9.2 Pflicht zur Online-Steuererklärung auch für Land- und Forstwirte, Gewerbetreibende und Selbstständige 174
9.3 Datensparsamkeit auch beim Glücksspiel 177
9.4 Großes Interesse an Steuerdaten 178
9.5 Verarbeitung von Steuerdaten durch Privatfirmen? 180
9.6 Beschwerde über die Information der Finanzämter zum SEPA- Verfahren 181

10 Justiz 183
10.1 Datenschutz hinter Gittern – auch in einer Justizvollzugsanstalt gilt das Grundrecht auf informationelle Selbstbestimmung 183
10.2 Todeserklärung nach dem Verschollenheitsgesetz: Welche Daten dürfen in der Zeitung veröffentlicht werden? 185
10.3 Das Thüringer Justizvollzugsgesetzbuch - alles in Einem - alles gut? 187

10.4 Schutz des Erbrechts und der Verfahrensbeteiligungsrechte nichtehelicher und einzeladoptierter Kinder im Nachlassverfahren ("weiße Karteikarten") 190
10.5 Aktenklau 192

11 Gesundheits- und Sozialdatenschutz 195
11.1 OH KIS reloaded 195
11.2 Kooperation zwischen Jugendamt und Jobcenter 196
11.3 Emergency Room auf Rädern: Videogaga 10 197
11.4 Datenerhebung im Jobcenter des Landkreises Eichsfeld 199

12 Wirtschaft, Arbeit, Bau und Verkehr 201
12.1 Unklarheiten nicht nur beim Landesamt für Statistik – für welche Umsätze ist eine Steuerberaterin auskunftspflichtig? 201
12.2 Fahrerlaubnis nur mit Gutachten? 203
12.3 Alles smart oder was ? 205
12.4 Section Control – Abschnittsgeschwindigkeits-Kontrolle auf Autobahnabschnitten bald auch in Thüringen?: Videogaga 11 207
12.5 Unzulässige Übermittlung von Daten durch die Industrie- und Handelskammer (IHK) an den Arbeitgeber 208
12.6 Datenschutz in Internetportalen des Deutschen Industrie- und Handelskammertags 210
12.7 Darf eine kommunale Stelle beliebige Daten aus den Datenbanken des amtlichen Vermessungswesens erhalten? 211
12.8 Digitales Portemonnaie – oder bar? 211
12.9 Bargeldlose Bezahlfunktion nur mit ausreichender Information der Kunden 213
12.10 Meldungen zu Datenpannen 214
12.11 Skimming-Attacken sind zu melden! 216

13 Bildung, Wissenschaft und Forschung 218
13.1 AK Datenschutz und Bildung/ AG Datenschutz und Schule 218
13.2 Behördliche Datenschutzbeauftragte an Schulen – ein Fall für die Nachhilfe 219

13.3 Modellprojekt „Grundschulen“ – Wer zahlt, will wissen wofür 222
13.4 Der Datenschutz geht auf die Schule zu 224
13.5 Vertretungspläne für die Welt: Anforderungen an die Veröffentlichung von Vertretungsplänen im Internet durch Schulen 226
13.6 Toilettenszenen: Videogaga 12 228
13.7 Datenschutz geht zur Schule 229

14 Entwicklungen der automatisierten Datenverarbeitung 231
14.1 IPv4 goes to IPv6 – muss mein Kühlschrank das können? 231
14.2 Sind Sie mandantenfähig ? 232
14.3 Wie sicher ist mein Passwort? 233
14.4 Clouds – schwere Wetter 235
14.5 Ende-zu-Ende ist der Anfang! 237
14.6 Datenübermittlung Meldedaten an Kirchen und GEZ über Internet 239
14.7 Das Multifunktionsgerät – ein unbekanntes Speichermedium 241

15 Technische Entwicklung in der Thüringer Landesverwaltung 242
15.1 Babyphone im Dienstzimmer: Wozu? 242
15.2 Unterrichtung über regelmäßige Datenübermittlungen infolge der Neuregelung von § 7 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) 245
15.3 Einrichtung eines barrierefreien Notrufs für Menschen mit Behinderungen 246
15.4 Haushaltmanagementsystem - HAMASYS 247
15.5 Projekt "Digitales Magazin des Freistaats Thüringen" 248

16 Parlamentarische Anfragen gem. § 112 a Geschäftsordnung des Thüringer Landtags 251
16.1 Parlamentarische Anfragen gem. § 112 a Geschäftsordnung des Thüringer Landtags (Anfragen an den Datenschutzbeauftragten) 251

Anlagen

Entschließung zwischen den Konferenzen 2011/2012

Anlage 1 Schuldnerverzeichnis im Internet:
Anzeige von Schuldnerberatern nur im Rahmen der gesetzlich legitimierten Zwecke 252

Entschließungen der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam

Anlage 2 Ein hohes Datenschutzniveau für ganz Europa! 254
Anlage 3 Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln 258
Anlage 4 Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum - nicht ohne Datenschutz 259

Entschließungen zwischen den Konferenzen 2012

Anlage 5 „Patientenrechte müssen umfassend gestärkt werden“ Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf! ... 261
Anlage 6 Orientierungshilfe zum datenschutzgerechten Smart Metering 263
Anlage 7 Melderecht datenschutzkonform gestalten! 265

Entschließungen der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder)

Anlage 8 Europäische Datenschutzreform konstruktiv und zügig voranbringen! 268
Anlage 9 Einführung von IPv6 - Hinweise für Provider im Privatkundengeschäft und Hersteller 270
Anlage 10 Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten 273

Anlage 11 Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben 275

Entschließung zwischen den Konferenzen 2013

Anlage 12 Beschäftigtendatenschutz nicht abbauen, sondern stärken! 277

Entschließungen der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven

Anlage 13 Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten 279
Anlage 14 Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor .. 280
Anlage 15 Europa muss den Datenschutz stärken 282
Anlage 16 Erläuterungen zur Entschließung „Europa muss den Datenschutz stärken“ 285
Anlage 17 Pseudonymisierung von Krebsregisterdaten verbessern 290
Anlage 18 Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen 292

Entschließung zwischen den Konferenzen 2013

Anlage 19 Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen 294

Entschließungen der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./2. Oktober 2013 in Bremen

Anlage 20 Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln 297
Anlage 21 Stärkung des Datenschutzes im Sozial- und Gesundheitswesen 299

Anlage 22 Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages.....301
Anlage 23 Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken! 303

Parlamentarische Anfragen an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Anlage 24 Anfrage 1 des Abgeordneten Bergner (FDP).....305
Anlage 25 Anfrage 2 des Abgeordneten Meyer (BÜNDNIS 90/DIE GRÜNEN 310
Anlage 26 Anfrage 3 des Abgeordneten Meyer (BÜNDNIS 90/DIE GRÜNEN).....314
Anlage 27 Anfrage 4 des Abgeordneten Bergner (FDP).....321
Anlage 28 Anfrage 5 der Abgeordneten König (DIE LINKE).....324
Anlage 29 Anfrage 6 des Abgeordneten Bergner (FDP).....328
Anlage 30 Anfrage 7 der Abgeordneten König (DIE LINKE).....331
Anlage 31 Anfrage 8 der Abgeordneten Leukefeld (DIE LINKE) 337
Anlage 32 Anfrage 9 des Abgeordneten Fiedler (CDU) 345

Pressemitteilungen 2012

Anlage 33 Nutzung der LKA-Akten zur Aufklärung der Neonazi-Morde nicht bestritten 353
Anlage 34 Konferenz der Datenschutzbeauftragten in Potsdam fordert ein modernes Datenschutzrecht für Europa.....354
Anlage 35 Warnung vor fingierten Anrufen einer „Datenschutzzentrale“.....356
Anlage 36 Der Thüringer Landesbeauftragte für den Datenschutz und die Landeskrankenhausgesellschaft Thüringen e. V. treffen sich am 22. Mai 2012 mit Vertretern der Krankenhäuser zum Informationsaustausch „Umsetzung der Orientierungshilfe Krankenhausinformationssysteme“ 358
Anlage 37 Vorstellung des 9. Tätigkeitsberichts des TLfD.....360
Anlage 38 In’s Netz gegangen – Facebook Sachstand & Hinweise 364
Anlage 39 Orientierungshilfe zum datenschutzgerechten Smart Metering.....365

Anlage 40 Missachtung des Datenschutzes im "Gesetz zur Fortentwicklung des Meldewesens" stoppen 367
Anlage 41 Patrick Kurth (FDP) und das neue Bundesmeldegesetz.....368
Anlage 42 Gemeinsame Presseerklärung des Bundestagsabgeordneten Patrick Kurth (FDP) und des Thüringer Landesdatenschutzbeauftragten Dr. Lutz Hasse zum neuen Melderecht 370
Anlage 43 TLfD meets Facebook.....371
Anlage 44 Grünes Licht für Solarkataster in Erfurt.....372
Anlage 45 Sicherheitshinweis des BSI !!! „Kritische Schwachstelle im Internet Explorer“ 374
Anlage 46 Sicherheitsupdate für kritische Schwachstelle im Internet Explorer für Freitagabend, den 21. September 2012, angekündigt.....376
Anlage 47 Besseres Datenschutzbewusstsein bei Schülern Kooperation TLfD - Thillm 377
Anlage 48 Thüringer Landesamt für Verfassungsschutz: Datenlöschung rechtswidrig.....379
Anlage 49 Datenschutztagung zu sozialen Netzwerken 383
Anlage 50 Unabhängigkeit des Thüringer Landesbeauftragten für den Datenschutz (TLfD) wird vom Thüringer Generalstaatsanwalt in Frage gestellt.....385
Anlage 51 „Soziale“ Netzwerke?Meine Daten! Mein Leben! – Dein Geschäft! 388
Anlage 52 Volles Haus!.....390
Anlage 53 Nicht jedes Mittel ist Recht! 391

Pressemitteilungen 2013

Anlage 54 BIG BROTHER - STANDARD 393
Anlage 55 Toilettenpapier endlos – Fehlende Unterstützung durch das Thüringer Landeskriminalamt (TLKA) 395
Anlage 56 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 396
Anlage 57 Cyber-Attacke: gefälschte Rechnungsmahnungen.....398
Anlage 58 Staatsanwaltschaft Meiningen nicht gehindert, unzulässig erhobene und gespeicherte Daten zu löschen.....399
Anlage 59 Neue Homepage – Datenschutz in Bewegung 401
Anlage 60 Datenschutz im Klassenzimmer gestärkt! 402

Anlage 61 Gefahr für Steuergeheimnis und Sozialdaten 403
Anlage 62 Multifunktionsgerät: Das unbekannte Speicher-medium! 406
Anlage 63 Gefällt Dir mein Spiel? 409
Anlage 64 Nur mit Fingerabdruck zum Arbeitsplatz ? 411
Anlage 65 Polizei, Staatsanwaltschaften, Verfassungsschutz: Aufbewahrungsfristen von personenbezogenen Daten & dienstlichem Schriftgut 412
Anlage 66 Bundesgerichtshof: Überwachung mit GPS-Empfängern durch Private grundsätzlich strafbar.....413
Anlage 67 PRISM + TEMPORA Was Sie tun können, um Ihre Individualität und Privatsphäre vor Geheimdienstattacken besser schützen zu können: 414
Anlage 68 SPRENGSÄTZE.....416
Anlage 69 Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten 418
Anlage 70 prism: Miteinander reden – nicht übereinander.....421
Anlage 71 Lehrer in facebook & Co.? NEIN! 422
Anlage 72 Persönlichkeitsrechte– auch im Internet – keine Frage …des Alters! 424
Anlage 73 Keine umfassende und anlasslose Überwachung durch Nachrichtendienste – Zeit für Konsequenzen.....425
Anlage 74 PRISM + TEMPORA + XKEYSCORE Teil II 427
Anlage 75 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1. und 2. Oktober 2013 in Bremen.....428
Anlage 76 IT-Systeme der Landesverwaltung sicher? 431
Anlage 77 Sitzung des Deutschen Bundestags zu den Abhöraktivitäten der NSA: Bundesdatenschutzbeauftragter legt Bericht vor.....433
Anlage 78 Datenschutzbeauftragter hat Anspruch auf Amtshilfe .435

A Öffentlicher Bereich

Vorwort

Dr. Lutz Hasse

Nachdem der Thüringer Landtag seinen neuen Datenschutzbeauftragten gewählt hatte, konnte Dr. Lutz Hasse am 1. März 2012 seine Amtsgeschäfte aufnehmen. Dies war für ihn kein Schritt in berufliches Neuland, da er von 2006 bis Anfang 2011 bereits Rechtsreferatsleiter beim Thüringer Datenschutzbeauftragten gewesen war. Mit Blick auf das Datenschutzrecht sowie die personelle Zusammensetzung der Behörde waren die Vorkenntnisse des neuen Datenschutzbeauftragten hilfreich bei der Umsetzung des seit dem 9. Dezember 2011 geltenden neuen Thüringer Datenschutzgesetzes. Denn gemäß § 42 Abs. 1 dieses Gesetzes darf der Thüringer Landesbeauftragte für den Datenschutz auch die Funktion der Aufsichtsbehörde nach § 38 Abs. 6 Bundesdatenschutzgesetz im nichtöffentlichen Bereich wahrnehmen. Diese Aufgabenübertragung war ein wichtiger Schritt, um die Datenschutzaufsicht nunmehr auch im Bereich der Unternehmen zu etablieren. Denn bis zu dieser Aufgabenübertragung auf den Thüringer Landesbeauftragten für den Datenschutz wurde die Aufgabe der Datenschutzaufsicht vom Landesverwaltungsamt wahrgenommen, allerdings nur von sogenannten 0,85 Vollbeschäftigen-Einheiten. Dieser prekäre Umstand hatte zur Folge, dass der Datenschutz im unternehmerischen Bereich seit den letzten 20 Jahren am Boden lag – eine Situation, die mit Nachdruck aufzuarbeiten ist! Der hieraus resultierende stark erhöhte Arbeitsanfall zog einen entsprechenden Personalbedarf nach sich, auf den im Vorwort zum nichtöffentlichen Bereich näher eingegangen wird. Mit Inkrafttreten des Thüringer Informationsfreiheitsgesetzes vom 29. Dezember 2012 hat der neue Datenschutzbeauftragte - wie von diesem stets gefordert - auch die Aufgabe des Informationsfreiheitsbeauftragten übernehmen können. Einblick in dieses Tätigkeitsfeld wird ein gesonderter Bericht verschaffen. Die steigenden qualitati-

ven, insbesondere aber auch quantitativen Anforderungen an die Behörde des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) - so die neue Bezeichnung - sind nur mit hoch motiviertem Personal zu bewältigen. Voraussetzung hierfür ist ein Klima nicht nur des Forderns, sondern gerade auch des Förderns; unabdingbar ist zudem die Atmosphäre der Offenheit und des Vertrauens. Aufgrund dieser Gegebenheiten darf es gestattet sein, die Behörde des TLfDI als hoch effizient zu bezeichnen. Gleichwohl liegt es auf der Hand, dass sich die Personaldichte an der Dichte der Aufgaben orientieren muss; daher darf ich an dieser Stelle für die Unterstützung der Landtagsfraktionen, der Landtagspräsidentin sowie des Personalrats der Thüringer Landtagsverwaltung für die tatkräftige Unterstützung danken, in der Hoffnung, dass diese anhalten möge.

1 Schwerpunkte im Berichtszeitraum

Datenschutz
© Coloures Pic – Fotolia.com

Der Bereich der Polizei beschäftigte den Thüringer Landesbeauftragten für der Datenschutz und die Informationsfreiheit (TLfDI) im Berichtszeitraum in besonders starkem Maße. Zu nennen ist zunächst die datenschutzrechtliche Begleitung des Papstbesuches, da mit diesem Ereignis zahlreiche Datenerhebungen im Vorfeld und während der Veranstaltung verbunden waren (Punkt 7.22). Im sogenannten „Toilettenpapierfall“ musste der TLfDI eingreifen, weil die Beschäftigten des Landeskriminalamtes aufgrund des Verdachts des Abhandenkommens von Toilettenpapier videoüberwacht wurden (Punkt 7.18). Auch gab es Fälle, in denen Polizeibeamte durch ihre Kollegen „ausspioniert“ wurden (Punkt 7.3; 7.4). Schließlich kontrollierte der TLfDI das Bildungszentrum der Polizei in Meiningen aufgrund von eingegangenen Hinweisen und beanstandete die dort festgestellten zahlreichen datenschutzrechtlichen Verstöße (Punkt 7.1).

Da den TLfDI in der Vergangenheit die vielfach komplexen und mitunter recht unebenen „Regelungslandschaften“ der Aufbewahrungs- und Prüffristen bei den öffentlichen Stellen beschäftigten, erarbeitete er den umfangreichen Leitfaden „Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut beim Thüringer Landesamt für Verfassungsschutz, in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei sowie in den Thüringer Staatsanwaltschaften“. Hierbei wurden alle einschlägigen Regelungsmaterien im Zusammenhang dargestellt und erläutert (Punkt 7.15).

Ein weiterer Schwerpunkt war die Fortführung der Kommunalkontrollen. Hierüber hatte der TLfDI bereits im 9. Tätigkeitsbericht (dort unter Punkt 5.1) berichtet. Noch nicht alle Kontrollen waren abgeschlossen. Hier bedurften die kontrollierten Kommunen einer weite-

ren Begleitung. Außerdem kontrollierte der TLfDI im Berichtszeitraum weitere Kommunen (Punkt 5.1).
Aufgrund von Meldungen aus der Presse bestand der Verdacht, dass die in der Thüringer Landesverwaltung verwendeten Telefonanlagen über eine sogenannte „Babyphone-Funktion“ verfügen, die es technisch ermöglicht, einen Raum zu überwachen. Um dies abzuklären, veranlasste der TLfDI eine Abfrage bei allen Landesbehörden (Punkt 15.1).

2 Allgemeine Entwicklungen im Datenschutz

Cloud computing and computer networking concept
© Scanrail – Fotolia.com

2.1 Das neue Thüringer Datenschutzgesetz

Am 9. Dezember 2011 trat das neue Thüringer Datenschutzgesetz in Kraft. Damit der Thüringer Landesbeauftragte für den Datenschutz in zeitgemäßer Weise enger an das Parlament gebunden wird, hat das neue Thüringer Datenschutzgesetz (ThürDSG) dem Thüringer Landtag nicht nur die Wahl des Datenschutzbeauftragten, sondern auch das Recht eingeräumt, die zur Wahl stehenden Kandidaten vorzuschlagen. Korrespondierend damit wurde die Dienstaufsicht über den Thüringer Landesbeauftragten für den Datenschutz weiterhin reduziert (§ 36 ThürDSG). Zudem wird der Austausch zwischen Parlament und Datenschutzbeauftragtem dadurch intensiviert, dass er im Rahmen seines Zuständigkeitsbereichs parlamentarische Anfragen beantwortet. Der neue § 42 ThürDSG überträgt für den nicht-öffentlichen Bereich die Funktion der Aufsichtsbehörde nach § 38 Abs. 6 Bundesdatenschutzgesetz nunmehr auch auf den Thüringer Landesbeauftragten für den Datenschutz. Diese Novellierung entsprach dem eindeutigen Votum des Europäischen Gerichtshofs, dass eine *unabhängige* Stelle die Datenschutzaufsicht gegenüber nicht-öffentlichen Stellen auszuüben hat – vgl. dazu B. Nicht-öffentlicher Bereich, Vorwort. Positiv hervorzuheben ist die Einfügung des neuen § 4 Abs. 1 Satz 2 ThürDSG, nach dem auch im Falle der Einwilligung die Verarbeitung oder Nutzung personenbezogener Daten nur zulässig ist, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist; eine Kompetenzerweiterung im Wege der Einwilligung wird hierdurch ausgeschlossen. Ein weiteres Novum sind die Regelungen in § 21 Abs. 6 und § 22 Abs. 3 ThürDSG, nach denen der Betroffene bei Datenübermittlungen zu informieren ist. Leider ist die Novellierung des Thüringischen Datenschutzrechts an nicht wenigen Stellen hinter den Anforderungen an ein modernes Daten-

schutzrecht zurück geblieben: beispielhaft sei hier nur genannt, dass behördliche Datenschutzbeauftragte gemäß § 10 a ThürDSG nur noch für die Dauer von vier Jahren bestellt werden können. Weitere Bestellungen sind zwar möglich, nach Ablauf der Bestellungsfrist wird sich jedem bzw. jeder behördlichen Datenschutzbeauftragten jedoch der Gedanke auf-drängen müssen, ob er bzw. sie sich zwecks Wiederbestellung behördenleitungskonform verhalten oder weiterhin offensiv die Interessen des Datenschutzes vertreten soll. Denn mit der Bestellung zum behördlichen Datenschutzbeauftragten ist ein verstärkter Kündigungsschutz verbunden, der natürlich eine gewisse Attraktivität dieser Funktion mit sich bringt. Kündigungsschutz und Datenschutz sollten jedoch nicht gegeneinander ausgespielt werden, sodass diese neue für den Datenschutz kontraproduktive Fristenregelung bei nächster Gelegenheit abzuschaffen ist. Nicht genutzt wurde auch die Möglichkeit, externe Sachverständige als behördliche Datenschutzbeauftragte einzubinden. Als unzureichend erweist sich in der Praxis auch, dass im schulischen Bereich ein behördlicher Datenschutzbeauftragter pro Aufsichtsbehörde – und nicht pro Schule - genügen soll; hier muss an der Verbesserung der datenschutzrechtlichen Aufsicht noch gearbeitet werden. Defizitär ist auch die Regelung des § 25 a ThürDSG geraten, die Regelungen zur Videoüberwachung enthält. Anders als in der bayerischen Parallelregelung ist hier nur die Videoüberwachung zur Wahrnehmung des Hausrechts geregelt, nicht aber zur Aufgabenerfüllung der Behörden in konkret definierten Grenzen. Schließlich fehlen im neuen ThürDSG moderne Regelungen zur Veröffentlichung personenbezogener Daten in Telemedien sowie etwa zum Cloud Computing. Die nächste Novellierung des ThürDSG sollte daher nicht allzu lange auf sich warten lassen.

Das ThürDSG muss mit der Zeit Schritt halten. Novellierungen sind daher unabdingbar und liegen in der Natur der Sache.

2.2 Snowden, NSA, PRISM, Tempora und Antiterrordatei - das Jahr 2013 als „datenschutzrechtlicher Durchlauferhitzer“

Wenn die Datenschutzbeauftragten des Bundes und der Länder gefragt werden sollten, welches Jahr aus datenschutzrechtlicher Sicht in den vergangenen 20 Jahren besonders spannend gewesen ist, so

könnte die Antwort spontan und mit Recht lauten: Das Jahr 2013. Warum ist diese Antwort zutreffend? Rückblick:
Am Donnerstag, 6. Juni 2013 berichtet erstmals die britische Zeitung „The Guardian“ darüber, dass der US-Telefonkonzern Verizon der National Security Agency, kurz NSA – der größte Auslandsgeheimdienst der Vereinigten Staaten, der für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig ist – detaillierte Verbindungsdaten zur Verfügung stellen müsse: Es gehe um Rufnummern, Dauer- und Uhrzeit. Einen Tag später, am Freitag, 7. Juni 2013 berichten wiederum „The Guardian“ und die Zeitung „Washington Post“ über einen direkten Zugriff der NSA auf die Server (= Netzwerkcomputer) von neun Internetfirmen: NSA-Fahnder überwachten Audios, Videos, Fotos und E-Mails, Dokumente und Verbindungsdaten, um Kontakte und Bewegungen einer Person nachvollziehen zu können. Das dafür zur Anwendung kommende Programm heiße PRISM (= „Planning Tool for Resource Integration Synchronization and Management“, zu deutsch: Planungswerkzeug für Quellenintegration, -synchronisierung und -management), sei im Jahr 2007 unter der Bush-Regierung aufgelegt worden und habe sich seitdem stark ausgeweitet. Beide Zeitungen berufen sich darauf, dass sie als Quelle für ihre Information Unterlagen eines NSA-Beschäftigten besäßen. Nur zwei Tage später, am Sonntag, 9. Juni 2013, enttarnt sich der 29-jährige Edward Snowden in einem Interview mit „The Guardian“ als Ex-NSA-Beschäftigter, der zuletzt für die Beratungsfirma Booz Allen Hamilton auf Hawaii gearbeitet habe. Als Beschäftigter dieser Beratungsfirma könne er jeden Menschen überwachen, sogar den US-Präsidenten. Denkwürdig sind folgende Äußerungen Snowdens: „ Du musst nichts Falsches getan haben, aber du kannst durch jemanden in Verdacht geraten. Dann durchleuchten sie alles, was du jemals getan hast, jeden Freund, mit dem du diskutiert hast.“
Aber nicht nur die NSA gerät im Sommer 2013 durch die Enthüllungen Edward Snowdens in die Kritik. Auch der Britische Geheimdienst GCHQ (=The Government Communications Headquarters) gerät am 21. Juni - wiederum durch einen Artikel im „The Guardian“ - in den öffentlichen Fokus: Laut „The Guardian“ führe der GCHQ eine Internetüberwachung durch, die noch schlimmer als PRISM sei. Das Programm dafür heiße „Tempora“ und habe es auf die Daten aus den Seekabeln abgesehen. Durch diese Glasfaserverbindungen fließe der überwiegende Teil der globalen Telefon- und Internetkommuni-

kation. „Tempora“ erlaube es demnach, den Datenverkehr in Pufferspeichern zu sammeln und E-Mails, Telefonate und Videochats zu rekonstruieren.

Die Reaktionen auf die Veröffentlichungen Edward Snowdens fielen, je nachdem, aus welcher Perspektive man sie beobachtete, unterschiedlich aus: Während die damalige Bundesjustizministerin Leutheusser-Schnarrenberger von einem „Alptraum à la Hollywood“ sprach, ging der Thüringer Datenschutzbeauftragte Dr. Lutz Hasse bereits am 28. Juni 2013 noch einen Schritt weiter und bewertete Snowdens Enthüllungen „als schon heldenhaft, sich gegen solche Organisationen aufzulehnen.“ Wenn es solche Leute wie Snowden nicht gäbe, würden wir auf „solche Parallelwelten“ der Geheimdienste nicht gestoßen werden, so das erste Fazit von Dr. Hasse.

Welche Reaktionen folgten diesen Enthüllungen? Der damalige Innenminister Friedrich reiste nach der Aufdeckung der NSA-Spähoperation im Juli 2013 nach Washington. Das Fazit der Zeitung „Die Zeit“ fiel dazu wie folgt aus: „Reisen bildet, heißt es. Aber dass die Dienstreise von Innenminister Hans-Peter Friedrich nach Washington ihn oder gar uns Bürger über die Überwachungsaktivitäten des US-Geheimdienstes zufriedenstellend aufklären würde, war von vornherein nicht zu erwarten. Es war vermutlich auch gar nicht die Absicht der Stippvisite.“ Um die Menschen in Thüringen nicht im datenschutzrechtlichen Dauerregen des Sommers 2013 stehen zu lassen, veröffentlichte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) am 10. Juli 2013 eine „Neun-Punkte-Liste“, wie man seine Individualität und Privatsphäre vor Geheimdienstattacken besser schützen kann: Unter anderem empfahl der TLfDI, beim Surfen im Internet Anonymisierungsdienste zu verwenden und gleichzeitig mehrere Browser, mehrere E-Mail-Accounts oder mehrere sonstige Identitäten zu verwenden. Denn damit würden so genannte Profilbildungen erheblich erschwert. Ferner sprachen der Thüringer Datenschutzbeauftragte Dr. Lutz Hasse und die datenschutzpolitische Sprecherin der SPD-Fraktion im Thüringer Landtag Dorothea Marx am 25. Juli 2013 mit dem amerikanischen Generalkonsul Mark J. Powell über die NSA-Affäre und die PRISM-Problematik. Bereits einen Tag vorher, am 24. Juli 2013 reagierte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf die NSA-Affäre mit einer Pressemitteilung. Darin forderte die Konferenz die Bundesregierung dazu auf, plausibel darzulegen, dass der unbeschränkte Zugriff ausländischer Nachrich-

tendienste auf die personenbezogenen Daten Menschen in Deutschland effektiv im Sinne des Safe-Harbour-Abkommens begrenzt wird. Safe-Harbour ist ein Abkommen der Europäischen Kommission, das Unternehmen in Europa ermöglicht, personenbezogene Daten „legal“ in die USA zu übermitteln. Bevor die Einhaltung der Save-Harbour-Grundsätze nicht sichergestellt sei, würden, so die Pressemitteilung der Datenschutzkonferenz weiter, die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten erteilen und prüfen, ob solche Datenübermittlungen auf Grundlage des Safe-Harbour-Abkommens auszusetzen seien.

So weit zu den Aufklärungsbemühungen gegenüber den ausländischen Geheimdiensten. Aber wie stand es im Jahr 2013 um die „Helfer der US-Spione“? Unter diesem Titel veröffentliche die „Süddeutsche Zeitung“ im Juli 2013 einen höchst interessanten Artikel, der sich kritisch mit der Rolle des Bundesamts für Informationssicherheit (BSI) auseinandersetzte. Vorgängerin des BSI, das erst 1991 gegründet wurde, war keine geringere als die Zentralstelle für das Chiffrierwesen, eine geheime Dienststelle des Bundesnachrichtendienstes. Und es kommt noch „besser“: In den Dokumenten der NSA, die Edward Snowden verschiedenen Medien zugespielt habe, wird laut „Süddeutscher Zeitung“ die Hilfe des BSI ausdrücklich erwähnt. Mehr noch: Das BSI war nach Aussage der „Süddeutschen Zeitung“ ein „Schlüsselpartner“ der NSA. Dies ergebe sich unter anderem aus der Aufgabe des BSI, nämlich vor Sicherheitslücken in Internet-Browsern zu warnen oder Produkte der Informationstechnik zu zertifizieren. IT-Unternehmen würden, so die „Süddeutsche Zeitung“ weiter, den BSI-Experten dabei in das Innerste ihrer Produkte Einblick gewähren - und damit auch die Schwachstellen an die Analysten des BSI verraten. Ein Zertifikat des BSI besäße auch der weltweit größte Internetknotenpunkt, der „De-Cix“ in Frankfurt. In Sicherheitskreisen kursierte nach Informationen der „Süddeutschen Zeitung“ schon länger das Gerücht, dass die NSA an diesem Knotenpunkt Daten abgreife, sodass dies die Frage aufwerfe, ob das BSI dabei geholfen habe. Dass der Bundesnachrichtendienst (BND) am „De-Cix“ Daten abgreife, sei nach Recherche der „Süddeutschen Zeitung“ kein echtes Geheimnis mehr, denn die Betreiber seien gesetzlich verpflichtet, dem BND Zugang zu gewähren.

Zurück nach Thüringen: Nachdem im „Summer of Snowden“ das Nachrichtenmagazin „Der Spiegel“ Anfang September 2013 berich-

tet hatte, dass Deutsche Nachrichtendienste und die CIA jahrelang eine geheime Anti-Terror-Datei mit dem Namen „Projekt 6“ in Neuss betrieben hatten, war das dem TLfDI eine Nachfrage beim Thüringer Landesamt für Verfassungsschutz (TLfV) wert. Entsprechend wortkarg fiel daher das Antwortschreiben des TLfV Ende September 2013 aus: Ihm, dem Landesamt, sei das „Projekt 6“ bisher nicht bekannt gewesen. „Wissentlich“, so das TLfV, habe es daher auch keine Daten aus der Datenbank „Projekt 6“ erhoben, gespeichert, verändert oder genutzt bzw. personenbezogene Daten in die genannte Datenbank übermittelt. Ferner lägen dem TLfV auch keine Erkenntnisse vor, dass die von ihm genutzten Verbunddateien Schnittstellen zum „Projekt 6“ enthielten. Bei diesem Projekt handele es sich jedenfalls nach Kenntnis des TLfV nicht um eine Verbunddatei im Sinne von § 6 Satz 1 Bundesverfassungsschutzgesetz, sondern allenfalls eine vom Bundesamt für Verfassungsschutz genutzte Datei. Mit anderen Worten: Wir haben jedenfalls nicht wissentlich Informationen ins „Projekt 6“ „gefüttert“, aber eine Bedienung aus oder ein Einpflegen in die Datei können wir nicht ausschließen!

Themenwechsel: Eine andere Datei, die vom Bundesverfassungsgericht (BVerfG) im April 2013 als im Grundsatz rechtmäßig beurteilt worden ist, ist die so genannte Antiterrordatei. Darin gebündelt sind die Erkenntnisse aller 38 deutschen Polizei- und Geheimdienstbehörden über mutmaßliche Terroristen des internationalen Terrorismus und deren Kontaktpersonen. Gegen diese Datei hatte ein pensionierter Richter vor dem BVerfG geklagt. Ins Stammbuch des Gesetzgebers geschrieben wurden vom BVerfG folgende Nachbesserungen:

- Nach den Maßstäben des Bestimmtheitsgebotes müssen die an der Antiterrordatei beteiligten Behörden entweder unmittelbar durch Gesetz oder aufgrund eines Gesetzes durch Rechtsverordnung bestimmt werden. Weder § 1 Abs. 2 Antiterrordateigesetz (ATDG) allein noch in Verbindung mit der Errichtungsanordnung gemäß § 12 Nr. 2 ATDG genüge diesen Anforderungen.
- Eine Speicherung von Unterstützern einer Gruppierung, die ihrerseits eine Vereinigung nach § 2 Satz 1 Nr. 1 Buchstabe a ATDG unterstützen, ist gemäß dem Gebot der Normenklarheit und dem Übermaßverbot nur dann zulässig, wenn „tatsächliche Anhaltspunkte für die wissentliche Förderung

> einer solchen Gruppierung bestehen.“ Eine solche Einschränkung vermisste das BVerfG aber in § 2 Satz 1 Nr. 1 Buchstabe b ATDG. Dieses Fehlen hatte bisher zur Folge, dass Menschen in die Datei aufgenommen werden, die „ohne Wissen von einem Terrorismusbezug eine in ihren Augen unverdächtige Vereinigung“ unterstützten.

Das BVerfG forderte den Gesetzgeber deshalb auf, bis zum 31. Dezember 2014 die notwendigen Änderungen im ATDG vorzunehmen.

Zurück zu den Affären über nachrichtendienstliche Überwachungen: Was bleibt als Zwischenfazit aus den Enthüllungen von Edward Snowden, den immer neuen Berichten über verdeckte Datenerhebungen der Geheimdienste und dem mangelhaften Aufklärungswillen der Deutschen Bundesregierung zu ziehen? Ein NSA-Untersuchungsausschuss des Deutschen Bundestags, der vor allem die Verzahnungen zwischen deutschen und US-amerikanischen sowie britischen Ausspähaktionen beleuchtet, mag das „notwendige Sauerstoffzelt“ für das stark angegriffene Grundrecht auf informationelle Selbstbestimmung sein. Es dient dabei aber nur dazu, die Verletzungen der Vergangenheit aufzudecken. Künftige Eingriffe lassen sich nur durch ein Mehr an Schutz im Netz erreichen, ausgeübt vom einzelnen, aufgeklärten Konsumenten und unterstützt von einer Bundesregierung, der Bürgerrechte wieder mehr bedeuten als ein „Supergrundrecht auf Sicherheit“. Erst dann sieht die „Privatsphäre“ nicht mehr aus „wie eine Dörrpflaume“ (so Heribert Prantl in seinem hervorragenden und bewegenden Vortag zum 8. Europäischen Datenschutztag am 28. Januar 2014).

Wir müssen weiterhin aufmerksam bleiben: Mit der informationellen Selbstbestimmung ist die Privatsphäre zwar grundrechtlich geschützt und Gesetze wie das Thüringer Datenschutzgesetz und das Bundesdatenschutzgesetz formen diesen Schutz näher aus. Damit hat es jedoch nicht sein Bewenden. Die NSA-Affäre führt deutlich vor Augen, dass Datenschutzgesetze umgesetzt und befolgt werden müssen und dass diese Umsetzung der umfassenden und eingehenden Kontrolle bedarf. Der schleichende Verlust der Privatsphäre nimmt dem Individuum die Selbstbestimmung, degradiert es zum Datenschatten und gibt totalitären Big-Data-Mechanismen Raum. Mensch

sein ist allerdings mehr, als eine Datenhülle gefüllt mit Verhaltensalgorithmen. Eigenwert und Eigenständigkeit prägen die Würde des Menschen, einschließlich seiner Geheimnisse. Diese Menschenwürde darf nicht zum bloßen Gegenstand staatlichen oder unternehmerischen Handelns verkommen. Bestrebungen, das Zusammengehen von Staat und Wirtschaft gerade auch in der Datennutzung zu intensivieren, bergen die Gefahr einer ungehemmten Zerstörung der Privatsphäre, es droht uns Big-Data-2.0. Dem gilt es, zu wehren. Privatheit und personenbezogene Daten schützen sich indes nicht von selbst. Fehlentwicklungen im behördlichen und unternehmerischen Schutz der persönlichen Datensphäre bedürfen dringend der Korrektur. Darüber hinaus müssen die Bürger und Bürgerinnen in die Lage versetzt werden, sich ungehinderter als bisher vom Staat Informationen beschaffen zu können, um informiert an der demokratischen Meinungs- und Willensbildung teilhaben zu können. Datenschutz und Informationsfreiheit müssen auf eine zeitgemäße gesetzliche Grundlage gestellt werden. Dazu gehört auch, dass den Bürgerinnen und Bürgern mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit ein starker Partner an die Seite gestellt wird.

Ein „Patentrezept“, wie den immer neuen Tricks der Nachrichtendienste zur Erlangung personenbezogener Daten beizukommen ist, hat auch der TLfDI nicht in seinem Instrumentenkoffer: Schützen kann man sich und seine personenbezogenen Daten aber, wenn man bei Dateien und E-Mails Verschlüsselungsmechanismen anwendet und beim Surfen im Internet Anonymisierungsdienste verwendet (nähere Infos dazu unter http://tu-dresden.de). Verzichten sollten Sie auch auf die Verwendung von Cloud-Computing. Weitere Infos finden Sie dazu auf der Homepage des TLfDI (http://www.tlfdi.de/tlfdi). Erst die Kopplung all dieser und weiterer Instrumente, von Millionen Usern tagtäglich praktiziert, macht die Auswertung der Daten für die Geheimdienste damit so aufwändig und unerschwinglich, dass hinreichender Datenschutz „im Kleinen“ wieder gewährleistet scheint. „Im Großen“ bleibt die Bundesregierung gefordert, auf politische Lösungen hinzuwirken.

2.3 Schutzfristenverkürzung gemäß § 17 Abs. 5 Thüringer Archivgesetz bei herauszugebenden Unterlagen an den Untersuchungsausschuss des Landtags

Das Thüringer Staatsarchiv Weimar trat mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran, ob bei der Herausgabe von Akten an den Untersuchungsausschuss des Landtags „Rechtsterrorismus und Behördenhandeln“ die Schutzfrist nach § 17 Abs. 5 Thüringer Archivgesetz (ThürArchivG) zu verkürzen sei. Als Schutzfrist wird dabei der Zeitraum definiert, in dem die entsprechenden Archivunterlagen durch die Allgemeinheit noch nicht benutzt werden dürfen. Im Regelfall wird das Archivgut, sofern keine Verkürzung der Schutzfrist vorliegt, erst 30 Jahre nach Schließung der Unterlagen für die Benutzung freigegeben.
In § 17 Abs. 5 ThürArchivG sind für Schutzfristenverkürzungen Einzelfälle vorgesehen, die die Aktennutzung zu einem beantragten Zweck und nur durch den beantragenden Benutzer zulassen, ohne damit im Anschluss eine automatische Freistellung der Akten für die Allgemeinheit nach einer individuellen Nutzung zu implizieren. Bei der Aufgabenstellung des Untersuchungsausschusses handelt es sich im Ergebnis um eine nach § 17 Abs. 5 Satz 2 Nr. 2 ThürArchivG vorgesehene „Aufklärung von Verwaltungsakten".
Um eine Entscheidungshilfe hinsichtlich der Schutzfristverkürzung zu liefern, wurde ein entsprechendes Antragsformular entwickelt. Dies dient zusammen mit einer Stellungnahme des Archivs als Entscheidungsgrundlage für das dafür zuständige Thüringer Ministerium für Bildung, Wissenschaft und Kultur zur Entscheidung.
Dem TLfDI wurde durch das Thüringer Staatsarchiv darüber hinaus auch mitgeteilt, dass die Beachtung des Datenschutzes und die sorgfältige Aufbewahrung wie auch die vollständige Rückgabe der Akten in einem Übergabeprotokoll verpflichtend Erwähnung finden würden.
Der TLfDI hielt die Herausgabe der in Rede stehenden Akten an den Untersuchungsausschuss des Landtages „Rechtsterrorismus und Behördenhandeln“ nach erfolgter Einzelfallprüfung für datenschutzrechtlich zulässig.

Als öffentliches Archivgut des Landes werden gemäß § 3 ThürArchivG alle archivwürdigen Unterlagen bestimmt, die bei

den Verfassungsorganen, Behörden, Gerichten und sonstigen Stellen des Landes Thüringen, bei deren Funktions- und Rechtsvorgängern sowie bei sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen entstanden sind und von den thüringischen Staatsarchiven nach Maßgabe dieses Gesetzes archiviert werden.
Die öffentlichen Archive haben gemäß § 7 Abs. 1 Satz 1 ThürArchivG die Aufgabe, das Archivgut der im Gesetz genannten öffentlichen Stellen zu übernehmen. Sie erfassen, verwahren, erhalten und erschließen das von ihnen übernommene Archivgut und stellen es zur Benutzung bereit (Archivierung). § 17 ThürArchivG regelt dabei die Fristen, wann das Archivgut für die Benutzung freigegeben wird.

2.4 E-Government-Gesetz des Bundes

Das am 3. Mai 2011 in Kraft getretene De-Mail-Gesetz regelt, dass mit sogenannten De-Mail-Diensten ein sicherer, vertraulicher und nachweisbarer Geschäftsverkehr für jedermann im Internet gewährleistet werden soll. Ermöglicht wird beispielsweise das Versenden von De-Mails oder das Ablegen von wichtigen Dokumenten in einem sogenannten De-Safe.
Allerdings sind die teilnehmenden akkreditierten Diensteanbieter nach dem Gesetz gezwungen, nach Eingang einer Nachricht diese unmittelbar auf Schadsoftware zu prüfen. Damit diese Prüfung durchgeführt werden kann, muss die Nachricht - wenn auch nur für einen kurzen Zeitpunkt - geöffnet werden. Dies bedeutet, dass keine Ende-zu-Ende-Verschlüsselung erfolgt, sondern der Staat per Gesetz bewusst eine offene Schnittstelle bei der Übertragung vorsieht. Es stellt sich die Frage, ob dieses „offene Scheunentor“ das Einfallstor für inländische und ausländische Geheimdienste ist!
Mit dem Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (Bundesgesetzblatt 2013 Teil 1 Nr. 43) wird nun zudem geregelt, dass auch sensible Daten, wie beispielsweise Sozialdaten und Steuerdaten durch staatliche Stellen per De-Mail übertragen werden können. Die Folge ist, dass der bisher vorgeschriebene Einsatz von Verschlüsselungsverfahren, die dem Stand der Technik entsprechend einzusetzen sind, ausgehebelt wird und bei der Datenübermittlung von Sozialdaten und Steuerdaten mittels De-Mail keine Ende-zu-Ende-Verschlüsselung mehr

erfolgen muss. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte auf die geplante Änderung des § 67 Abs. 6 Satz 2 Nr. 3 Zehntes Buch Sozialgesetzbuch (SGB X) und § 30 und § 87 Abgabenordnung in seiner Pressemitteilung vom 26. April 2013 hingewiesen (siehe Anlage 61), und leider erfolglos die Thüringer Staatskanzlei gebeten, dem Gesetz nicht zuzustimmen.
Ungeachtet der grundsätzlichen Zulässigkeit des Einsatzes von De-Mail im Bereich des Steuer- und Sozialgeheimnisses ohne zusätzliche Sicherheitsmaßnahmen kann es entsprechend der Begründung zum E-Government-Gesetz gleichwohl in bestimmten Konstellationen erforderlich werden, von der zusätzlichen Verschlüsselung nach § 5 Absatz 3 Satz 3 des De-Mail-Gesetzes Gebrauch zu machen. Insoweit sind, entsprechend der Gesetzesbegründung, die Empfehlungen der Beauftragten für den Datenschutz des Bundes und der Länder zu beachten (Bundestagsdrucksache 17/11473, Seite 47).
So hat der TLfDI auch in seiner Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Thüringer Verwaltungsverfahrensgesetzes und anderer verwaltungs-rechtlicher Vorschriften - leider erfolglos - gefordert, dass durch eine entsprechende Änderung des § 3 a Abs. 2 Satz 4 Nr. 2 ThürVwVfG-E sicherzustellen ist, dass bei Verfahren, in denen personenbezogene Daten verarbeitet werden, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch bei der Nutzung von De-Mail zusätzlich eine Ende-zu-Ende-Verschlüsselung einzusetzen ist.

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

2.5 Zensus 2011 reloaded

Im Hinblick auf eine voraussichtlich im Jahr 2021 erneut stattfindende statistische Erhebung hat der Arbeitskreis Statistik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe gebildet, die eine Zusammenstellung von Aspekten für die weitere Diskussion über eine Novellierung des Bundesstatistikgesetzes und die Durchführung statistischer Erhebungen – insbesondere des nächsten Zensus – erörtern sollte.

Im Kreis der Datenschutzbeauftragten wurde der vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erarbeitete Entwurf eines Eckpunktepapiers zur datenschutzgerechten Durchführung von Volkszählungen beraten. Insbesondere galt es, die seitens der Datenschutzbeauftragten in Bund und Ländern gewonnenen Erkenntnisse bei der Vorbereitung und Durchführung des Zensus 2011 einzubeziehen.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat Ende Mai 2013 ein eigenes Eckpunktepapier herausgeben:
(http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/EckpunktepapierZensus2021.html?nn=408908).

Nach dem Zensus ist vor dem Zensus.

2.6 Senioren im Netz des Mikrozensus

Ein – nach eigenen Angaben – Altersrentner betrachtete die Maßnahmen im Zusammenhang mit dem Mikrozensus als Eingriff in seine Privatsphäre und fühlte sich im Recht, die Angaben dazu zu verweigern. Bei dem Mikrozensus handelt es sich um eine jährliche repräsentative Haushaltsbefragung in Deutschland.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat ihn zunächst auf das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts verwiesen, in dem festgestellt wird, dass das Recht auf informationelle Selbstbestimmung nicht schrankenlos gilt, sondern im überwiegenden Allgemeininteresse auf der Grundlage eines normenklaren Gesetzes unter Beachtung der Verhältnismäßigkeit beschränkt werden darf. Geregelt ist dies auch in § 4 Abs. 1 Thüringer Datenschutzgesetz, wonach die Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen des Freistaates Thüringen dann zulässig ist, wenn dies eine Rechtsvorschrift erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.
Weiter hat der TLfDI dem Betroffenen mitgeteilt, dass die Rechtsgrundlage für die Datenerhebungen zum Mikrozensus das Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte (Mikrozensusgesetz [MZG]) ist. Im Rahmen einer Stichprobe werden danach jährlich von einem Prozent der Bevölkerung nach einem be-

stimmten Auswahlverfahren Daten erhoben. Die vom Gesetzgeber zur Auskunftspflicht bestimmten Personen sind in § 7 MZG sowie die vorgesehenen Erhebungsmerkmale in § 4 MZG eindeutig benannt. Die Auswahl der Auskunftspflichtigen erfolgt durch ein mathematisches Zufallsverfahren gemäß § 2 MZG. Es liegt weder im Ermessen eines einzelnen Beschäftigten des Statistischen Landesamtes (TLS), Auskunftspflichtige zu bestimmen, noch einzelner Einwohner, sich an dieser Erhebung zu beteiligen. Der TLfDI hat den Betroffenen abschließend darüber informiert, dass er während der Zeit der Einbeziehung in die Stichprobe gegenüber dem TLS gemäß § 7 MZG auskunftspflichtig ist. Diese Angaben unterfallen aber besonderen Geheimhaltungsvorschriften, dem Statistikgeheimnis, und dürfen nicht personenbezogen ausgewertet oder der Verwaltung, z. B. für Datenabgleiche, zur Verfügung gestellt werden.

Auch für Altersrentner gilt das Recht auf informationelle Selbstbestimmung nicht schrankenlos.

2.7 Bundesweites Schuldnerverzeichnis im Internet – Schuldnerverzeichnisverordnung – erst nach Intervention der Datenschutzbeauftragten datenschutzgemäß

Der Gesetzentwurf zur Reform der Sachaufklärung in der Zwangsvollstreckung auf Initiative der Bundesländer Baden-Württemberg, Bayern, Hessen, Niedersachsen und Sachsen aus dem Jahr 2008 sah für alle Bundesländer unter anderem die Einrichtung eines gemeinsamen Vollstreckungsportals der Länder vor. Darin sollten die bundesweiten Daten aus den Schuldnerverzeichnissen nach §§ 882 b ff. Zivilprozessordnung zum kostenpflichtigen Abruf bereitgestellt werden. Das bundesweite Schuldnerverzeichnis beinhaltet z. B. Eintragungen von Personen, die der Gerichtsvollzieher angeordnet hat, weil sie ihrer Pflicht zur Abgabe einer Vermögensauskunft nicht nachgekommen sind. Personenbezogene Daten eines solchen Schuldners, wie z. B. Name und Geburtsname des Schuldners, sein Geburtsdatum und sein Geburtsort sowie sein Wohnsitz werden in das Schuldnerverzeichnis aufgenommen. Das Gesetz ist teilweise zum 1. August 2009 und ferner zum 1. Januar 2013 in Kraft getreten.
Im Rahmen des sich daran anschließenden Gesetzgebungsverfahrens zur Schuldnerverzeichnisführungsverordnung (SchuFV-E) – ‚die die

Einzelheiten der Führung des Verzeichnis inklusive Eintragung und Einsichtnahme regelt – waren auch die Datenschutzbeauftragten des Bundes und der Länder um Stellungnahme gebeten worden. Aus Sicht des Landesbeauftragten für den Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI) gab es dabei einige Kritikpunkte am Verordnungsentwurf:

- Aus Sicht des LDI war eine Registrierung der Nutzungsberechtigten (jeder, der ein berechtigtes Interesse darlegt, z. B. zum Zwecke der Zwangsvollstreckung oder um wirtschaftliche Nachteile abzuwenden) mittels Kreditkarte nicht zu erwägen, weil dadurch einerseits die Gefahr des Missbrauchs fremder Kreditkarten bestehe. Andererseits ergebe sich ein grundsätzliches Problem, wenn staatliche Stellen zur Identifizierung abfrageberechtigter Personen auf Karten zurückgreifen, die von nicht-öffentlichen Stellen ausgegeben werden. Ein geeigneteres Identifizierungsinstrument sei demgegenüber der neue elektronische Personalausweis.
- Nach dem dem LDI vorliegenden Verordnungsentwurf waren die Voraussetzungen zur Einsichtnahme Dritter in das Schuldnerverzeichnis insoweit datenschutzrechtlich unbefriedigend geregelt, weil die Regelung in § 9 SchuFV-E keine konkreten Parameter zur Abfrage beinhaltete. Die Stellungnahme des LDI wies deshalb darauf hin, dass es zur Identifikation einer natürlichen Person durch Dritte notwendig sei, neben dem Vor- und Nachnamen auch das Geburtsdatum und den Geburtsort im Schuldnerverzeichnis einzugeben.

Im weiteren Gesetzgebungsverfahren wurde die aufgezeigte Identifizierung per Kreditkarte dann als Form der Registrierung nicht weiter verfolgt. Durch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Februar 2012 lenkte schließlich auch das Bundesministerium der Justiz (BMJ) in der Streitfrage ein, welche Parameter bei der Abfrage im Schuldnerverzeichnis einzugeben sind. Nunmehr hat der private Gläubiger mindestens Vor- und Nachnamen sowie den Wohn- bzw. Aufenthaltsort oder das zuständige zentrale Vollstreckungsgericht anzugeben. Sind nach Eingabe dieser Daten mehrere Treffer vorhanden, erfolgt noch keine Übermittlung, sondern der Gläubiger hat ferner das Geburtsdatum und gegebenenfalls auch den Geburtsort einzugeben. Erst wenn

nach Eingabe dieser Daten immer noch mehrere Treffer vorliegen, werden diese an den Gläubiger übermittelt. Die Bemühungen der Datenschutzbeauftragten, bei der Ausgestaltung des Schuldnerverzeichnisses dem Datenschutz weitest gehende Beachtung zukommen zu lassen, hatten also Erfolg.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung wollte der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht deshalb vor, dass der Inhalt des Schuldnerverzeichnisses seit dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Damit können z. B. Vermieter unter bestimmten Voraussetzungen prüfen, ob ihr in Frage kommender Mieter keine Zahlungsschwierigkeiten besitzt.

2.8 Gesetz zur Optimierung der Geldwäscheprävention – auf Kosten des Datenschutzes bei E-Geld-Transaktionen!

Im Mai 2011 brachte die Bundesregierung den Entwurf eines Gesetzes zur Optimierung der Geldwäscheprävention in Bundestag und Bundesrat ein. Kern dieses Artikel-Gesetzentwurfs war unter anderem, eine Regelung in § 2 des Geldwäschegesetzes aufzunehmen, wonach Unternehmen und Personen in den Kreis der Verpflichteten aufgenommen werden sollen, die E-Geld vertreiben oder rücktauschen. E-Geld ist jeder elektronisch – auch magnetisch – gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, die gegen Zahlung eines Geldbetrages ausgestellt wird. Die wesentliche Sorgfaltspflicht sollte für die Unternehmen und Personen darin bestehen, gem. § 3 Abs. 1 Nr. 1 des Geldwäschegesetzes die Identifizierung des Vertragspartners vorzunehmen. Folglich war es der Zweck des Gesetzentwurfs, künftig jede Tankstelle, die z. B. Prepaid-Tankkarten vertreibt, zu verpflichten, die personenbezogenen Daten des Käufers zu erheben und mindestens fünf Jahre aufzubewahren.
Gegen diese beabsichtigte Vorgehensweise richtete sich selbstverständlich der Argwohn von Wertkartenunternehmen, die Prepaidkarten für Zahlungen im Internet vertreiben. Diese wandten sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und trugen ihre Bedenken gegen die geplanten Neuregelungen des Geldwäschegesetzes vor. Der TLfDI war sich

mit den Prepaidkarten-Unternehmen einig, dass auch weiterhin eine *anonyme* Zahlungsweise in den genannten Fallkonstellationen aus datenschutzrechtlichen Gründen möglich sein muss.
Um dieses Ziel zu erreichen, fasste auch die 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. und 29. September 2011 in München die Entschließung „Anonymes elektronisches Bezahlen muss möglich bleiben!“ Darin forderten die Datenschützer vom Bundesgesetzgeber, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Kritik übte die Entschließung an dem bereits genannten Gesetzentwurf, weil dieser einerseits zu weit gehe, indem er sämtliches anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausschließe. Andererseits verkenne die Bundesregierung, dass gerade anonyme Bezahlsysteme ihren Nutzern die Möglichkeit böten, Angriffe von Hackern auf Finanzdaten zu minimieren. Abschließend wiesen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass die verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung auch europarechtlich nicht geboten sei. Denn die dritte Geldwäscherichtlinie (2005/60/EG) erlaube den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteige.
Und das „Ende vom Lied“? Die berechtigten Bedenken der Datenschützer sind leider unberücksichtigt geblieben. Das Gesetz zur Optimierung der Geldwäscheprävention ist inklusive der kritisierten Änderungen am 1. März 2012 in Kraft getreten.

Aufgrund der Tatsache, dass ein anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen mit dem Inkrafttreten des Gesetzes zur Optimierung des Geldwäschegesetzes zu Nichte gemacht worden ist, empfiehlt der TLfDI, Prepaidkarten zur Bezahlung nur noch im absoluten Ausnahmefall einzusetzen. Als Beispiele sind hier Prepaid-Tankkarten, bei denen man einen Geldbetrag der Tankstelle bezahlt und im Gegenzug dann eine Tankkarte in Höhe des einbezahlten Geldbetrages erhält, oder aber Prepaid-Karten zur Bestellung von Waren im Internet zu nennen. Stattdessen sollte grundsätzlich auf die Bezahlung in bar oder per Überweisung ausgewichen werden.

2.9 Nationales Waffenregister - Schuss in den Ofen?

Gemäß Artikel 4 Absatz 4 EU-Waffenrichtlinie (2008/51/EG) müssen die Mitgliedstaaten dafür Sorge tragen, dass spätestens bis 31. Dezember 2014 ein computergestütztes, zentral oder dezentral eingerichtetes Waffenregister eingeführt und stets auf aktuellem Stand gehalten wird. Ziel ist es, für mindestens 20 Jahre Typ, Modell, Fabrikat, Kaliber, Seriennummer von Waffen sowie Namen und Anschriften von Lieferanten und der Person, die die Waffe erworben hat oder besitzt, zu registrieren und zu speichern.
Die Umsetzung in nationales Recht erfolgte gemäß § 43 a Waffengesetz (WaffG), wonach bis zum 31. Dezember 2012 ein Nationales Waffenregister (NWR) zu errichten war. Entsprechend dem Nationalen Waffenregistergesetz (NWRG) wird das NWR beim Bundesverwaltungsamt geführt. Die Datenübermittlung durch die zuständigen Waffenbehörden hat unverzüglich nach Erfassung oder Änderung der zu führenden Daten zu erfolgen.
Nach Recherchen der Gewerkschaft der Polizei (GdP) droht dies zu einem „Schuss in den Ofen“ zu werden, denn die gespeicherten Daten aus den bundesweit über 500 Waffenbehörden an das NWR seien zum Teil fehlerhaft.
Aus datenschutzrechtlicher Sicht haben öffentliche Stellen, die personenbezogene Daten verarbeiten, zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (§ 9 Abs. 2 Nr. 2 Thüringer Datenschutzgesetz (ThürDSG)). Dies bedeutet für die Waffenbehörden, dass sie nur dann einen Datenbestand in das Waffenregister übermitteln dürfen, wenn er den aktuellen Gegebenheiten entspricht. Dies wird der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit bei Thüringer Waffenbehörden stichprobenartig 2014 überprüfen. Unbeschadet dessen können auch Waffenbesitzer sich selbst an ihre zuständige Waffenbehörde wenden und die ordnungsgemäße Speicherung ihrer Daten überprüfen lassen. Eine Überprüfung einer Thüringer Waffenbehörde im Jahr 2013 ergab bereits, dass entsprechende Akten nicht ordnungsgemäß vor unbefugtem Zugriff aufbewahrt wurden.
Die GdP befürchtet zudem, dass bei einer Datenübermittlung aus dem NWR auch jemand, der beispielsweise eine bestimmte Waffe schon vor Jahren verkauft hat, in den Fokus einer Ermittlung geraten

kann, indem er als amtlich registrierter Besitzer der gesuchten Waffe verdächtig erscheinen kann.
Die Datenübermittlung aus dem NWR ist für die Waffenbehörden, Polizeien des Bundes und der Länder, Justiz- und Zollbehörden, Steuerfahndung sowie Nachrichtendienste in § 10 NWRG geregelt. Stellen die genannten Stellen sogar einen Antrag zum Datenabruf im automatisierten Verfahren, so wird gemäß § 13 Abs. 3 NWRG der für die Kontrolle der Einhaltung der Vorschriften zum Schutz personenbezogener Daten zuständige Datenschutzbeauftragte des Bundes oder des Landes vom Bundesverwaltungsamt unterrichtet. Entsprechend dieser Unterrichtung nehmen derzeit 29 Thüringer Behörden am Datenabruf im automatisierten Verfahren teil; dies sind neben dem Thüringer Landesamt für Verfassungsschutz und dem Thüringer Landeskriminalamt drei Landespolizeiinspektionen, die Landespolizeidirektion sowie 23 Behörden aus dem kommunalen Bereich.

Gemäß § 9 ThürDSG ist unter anderem auch in den Thüringer Waffenbehörden sicherzustellen, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Dies gilt es sowohl lokal bei der Datenverarbeitung in den Waffenbehörden, als auch bei der Datenübermittlung an das nationale Waffenregister zu beachten. Dem Vernehmen nach wird hieran intensiv gearbeitet.

2.10 Der bewegte Weg des Gesetzes zur Fortentwicklung des Meldewesens

Die Föderalismusreform I hatte das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Mit der Vorlage des Gesetzes zur Fortentwicklung des Meldewesens im November 2011 hat der Bund diese Gesetzgebungskompetenz ausgefüllt, indem er das Melderechtsrahmengesetz aus dem Jahr 1980 mit den Landesmeldegesetzen in einem Gesetzentwurf zur Fortentwicklung des Meldewesens zusammengeführt hat. Bundestag und Bundesrat haben diesen Gesetzentwurf im letzten Jahr beschlossen; das Gesetz tritt zum 1. Mai 2015 in Kraft. In diesem Gesetz sind zwar Forderungen der Datenschutzbeauftragten teilweise unberücksichtigt geblieben, wie z. B. der Verzicht auf die Mitwirkung des Wohnungsgebers bei der Anmeldung, allerdings sah der ursprüngliche Regierungsentwurf zu den einfachen Melderegisterauskünften daten-

schutzfreundliche Regelungen vor. So sollten nach § 44 Abs. 3 Nr. 2 des Entwurfs Melderegisterauskünfte zu Werbezwecken sowie für den Adresshandel nur bei entsprechender Einwilligung des Betroffenen erteilt werden dürfen.
Derzeit darf nach § 31 Thüringer Meldegesetz (ThürMeldeG) die Meldebehörde Personen Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Einwohner zwar erteilen (einfache Melderegisterauskunft). Weiter ist in § 7 ThürMeldeG aber geregelt, dass schutzwürdige Interessen der Betroffenen durch die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nicht beeinträchtigt werden dürfen. Schutzwürdige Interessen werden insbesondere beeinträchtigt, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, den Betroffenen unverhältnismäßig belastet. Die Prüfung, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden, entfällt, wenn die Erhebung, Verarbeitung oder Nutzung durch Rechtsvorschrift vorgeschrieben ist (Mussvorschrift). Eine solche Vorschrift ist nach dem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 21. Juni 2006 (6C 05.05) nicht § 31 ThürMeldeG, denn diese Norm wird vom Gericht als Ermessensnorm und nicht als Mussvorschrift qualifiziert (die Entscheidung des BVerwG bezieht sich auf die hamburgische Rechtslage, die jedoch der thüringischen Rechtslage entspricht). Aus der Entscheidung des BVerwG ergibt sich damit, dass § 31 und § 7 ThürMeldeG im Kontext zu lesen sind. Diese Vorschriften verlangen daher eine Interessenabwägung, bei der das Interesse des Betroffenen an der Geheimhaltung seiner Daten gegen das Interesse der Meldebehörde oder eines Dritten an der Erhebung, Verarbeitung oder Nutzung abzuwägen ist. Mithin darf – so das Gericht präzisierend – eine Meldebehörde eine einfache Melderegisterauskunft nicht erteilen, wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird und der Betroffene einer Weitergabe seiner Daten für solche Zwecke zuvor ausdrücklich widersprochen hat. Dieses Widerspruchsrecht ergibt sich aus den erwähnten §§ 31, 7 ThürMeldeG. Jeder Bürger und jede Bürgerin in Thüringen kann somit derzeit bei der Meldebehörde Widerspruch gegen die Preisgabe der Daten für Zwecke der Direktwerbung einlegen. Ein entsprechendes Formular „Widerspruch gegen die Übermittlung meiner Daten durch die Meldebehörde“ ist auf der Internetseite des

Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI)
(http://www.tlfdi.de/tlfdi/wir/info/mustervordrucke/) zu finden.
Der oben genannte Bundesgesetzentwurf hat allerdings im Lauf der parlamentarischen Beratungen eine signifikante Verschlechterung in Sachen Datenschutz erfahren. Aus der vormals vorgesehenen Einwilligungslösung wurde eine Widerspruchslösung mit zusätzlichen Einschränkungen. Nunmehr hätten nach der vom Bundestag in zweiter Lesung beschlossenen Regelung Melderegisterauskünfte für Zwecke der Werbung oder des Adresshandels an Firmen auch erteilt werden können, wenn die betroffene Person gegen die Übermittlung für jeweils diesen Zweck Widerspruch eingelegt hätte und zwar dann, wenn die Daten ausschließlich zur Bestätigung oder Berichtigung bereits vorhandener Daten verwendet worden wären. Die Einführung dieser Ausnahme vom Verbot der Übermittlung bei Widerspruch hätte damit gravierende Auswirkungen für die betroffenen Bürgerinnen und Bürger sowie die Meldebehörden zur Folge gehabt.
Diese Änderung war aus Sicht des TLfDI nicht akzeptabel, da damit den Bürgerinnen und Bürgern alle Rechte aus der Hand genommen worden wären, selbstbestimmt zu entscheiden, ob Firmen für Zwecke der Werbung und des Adresshandels ihre personenbezogenen Daten erhalten dürfen. Um diese den Datenschutz missachtende Regelung im Gesetzentwurf zu stoppen, hat sich der TLfDI an die Fraktionen des Thüringer Landtags mit der Bitte um Unterstützung seines datenschutzrechtlichen Anliegens gewandt. Zudem verständigten sich die Datenschutzbeauftragten des Bundes und der Länder auf eine gemeinsame Position und verabschiedeten eine Entschließung „Melderecht datenschutzkonform gestalten!“, die einerseits die Rückgängigmachung der Auskünfte zu Werbezwecken und zu Zwecken des Adresshandels, andererseits auch noch andere offene Forderungen der Datenschutzbeauftragten zum Inhalt hatte.
Im Ergebnis wurde das Verfahren einem datenschutzrechtskonformen Ausgang zugeführt. Auch wenn nicht alle Forderungen der Datenschutzbeauftragten in Gänze umgesetzt wurden, so enthält das Gesetz nunmehr wieder die datenschutzfreundliche Einwilligungslösung als Voraussetzung für Melderegisterauskünfte zu Werbezwecken sowie für den Adresshandel.

Die Wachsamkeit und das Engagement der Datenschutzbeauftragten des Bundes und der Länder haben im Laufe des Gesetzgebungsver-

fahrens doch noch zu einem guten Ende geführt und ein weitgehend datenschutzfreundliches Gesetz zur Fortentwicklung des Meldewesens ermöglicht.

3 Europäischer und Internationaler Datenschutz

media global technology
© Edelweiss – Fotolia.com

3.1 Gesamtkonzept für den Datenschutz in der Europäischen Union – KOM(2010)609 – Allgemeine Datenschutzverordnung

Die Europäische Datenschutzrichtlinie 95/46 sollte von der Europäischen Datenschutzgrundverordnung abgelöst werden. Mit dieser für die Mitgliedsstaaten unmittelbar geltenden Vorschrift sollte das europäische Datenschutzniveau auf einen höheren Standard gehoben werden – indes ist dieses Unterfangen jedenfalls beim ersten Anlauf gescheitert. Tausende von Änderungsanträgen sowie eine rekordverdächtige Lobbyarbeit erwecken den Eindruck, dass die tragenden datenschutzrechtlichen Grundsätze noch besser heraus gearbeitet werden können und müssen. Eine Orientierung an den ausgeprägten Datenschutzstandards des Bundesdatenschutzgesetzes erscheint hier zielführend. Bis zur Verabschiedung neuer europäischer Datenschutzregelungen bleibt das belastbare Geflecht von hohem Datenschutzstandard und moderner verfassungsgerichtlicher Rechtsprechung in Deutschland in Kraft.

Die Europäische Datenschutzgrundverordnung muss sich vielen Herausforderungen stellen. Es bleibt abzuwarten, ob sie Antworten auf unzählige drängende Fragestellungen geben kann.

3.2 Einführung des interoperablen EU-weiten eCall-Dienstes – Mehr Verkehrssicherheit auf Kosten des Datenschutzes?

Ein „heißes Eisen angepackt “ aus datenschutzrechtlicher Sicht hatten das Europäische Parlament und der Europäische Rat im Jahr 2013 mit dem Vorschlag für eine Verordnung über Anforderun-

gen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge. Was verbirgt sich hinter diesem Begriff? eCall ist ein Notrufsystem für Fahrzeuge. Bei einem Unfall des Kraftfahrzeuges wird ein Notruf (eCall) ausgelöst, sobald Sensoren einen schweren Zusammenstoß registrieren. Das aktivierte System wählt die europäische Notrufnummer 112 an, stellt eine Telefonverbindung zur nächsten Notrufzentrale her und übermittelt den Notdiensten Daten zum Unfall, wie z. B. den Unfallzeitpunkt, den genauen Standort des Unfallfahrzeugs und die Fahrtrichtung. ECall kann ferner, und das ist aus datenschutzrechtlicher Sicht relevant, auch manuell, etwa durch Zeugen eines schweren Unfalls, ausgelöst werden, indem ein Knopf im Auto betätigt wird. Denn dadurch hätte der Nutzende des Systems letztendlich selbst die Entscheidung in der Hand, ob er eCall aktivieren will oder nicht.

So weit, so gut. Die datenschutzrechtliche „Kehrseite der Medaille“ beim eCall-Dienst ist jedoch in der zweiten Ausbaustufe des Dienstes zu sehen: Diese sieht vor, dass zu den ausgetauschten, bereits genannten Basisdaten zusätzliche Angaben hinzukommen, die im Besitz eines Dritten sind – z. B. Versicherungsgesellschaften, Kraftfahrzeug-Callcenter, Gesundheitsdienste, Rechtsanwälte oder Automobilclubs. Es ist also naheliegend, dass Kfz-Fahrer aufgrund dieser zweiten Ausbaustufe in vertragliche oder ökonomische Zwänge gebracht werden können, etwa dadurch, dass sie Versicherungssondertarife („Pay-As-You-Drive“-Versicherungsverträge) nur gegen Aktivierung der in der zweiten Ausbaustufe vorgesehenen Übermittlung von Zusatzdaten erhalten. Diese Zusatzdaten könnten z. B. Angaben über die Zahl der Insassen, ob Sicherheitsgurte zum Zeitpunkt des Unfalls angelegt waren oder wie viel Kilometer das Fahrzeug zu welchen Orten zurückgelegt hat, beinhalten.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat im Rahmen des sogenannten Subsidiaritäts-Frühwarnsystems im europäischen Rechtssetzungsprozess gegenüber dem Europaausschuss des Thüringer Landtags im Juli 2013 eine Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung von Richtlinie 2007/46/EG, KOM (203) 316 abgegeben. Darin weist der TLfDI – neben der oben genannten, datenschutzrechtlich bedenklichen zweiten Ausbaustufe - insbesondere auf Folgendes hin:

- Eines der zentralen Kriterien für die Zulässigkeit der Verarbeitung von Daten ist nach Artikel 7 Buchstabe a) der Datenschutzrichtlinie 95/46/EG, dass die Verarbeitung von Daten dann erfolgen darf, wenn die betroffene Person ohne jeden Zweifel ihre Einwilligung zu der Verarbeitung gegeben hat. Eine solche Einwilligung muss nach Auffassung der Artikel 29-Datenschutzgruppe – einem unabhängigen Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes – „ohne Zwang“ gegeben worden sein und sollte der betroffenen Person auch die Möglichkeit geben, die Einwilligung widerrufen zu können.
- Im Rahmen der Einführung des eCall-Dienstes sieht die Artikel 29-Datenschutzgruppe gerade dann eine Einwilligung nicht als „ohne Zwang gegeben“ an, wenn der Fahrzeugkäufer im Rahmen eines Fahrzeugkaufvertrages mit nicht verhandelbaren Klauseln eine solche Klausel zur obligatorischen Aktivierung des eCall-Systems zu akzeptieren hat (was Artikel 5 Nr. 2 des Verordnungsvorschlags von den Autoherstellern auch verlangt).
- Artikel 5 Satz 1 Nr. 2 Satz 1 des genannten Verordnungsentwurfs enthält die (weitergehende) Nachweispflicht für Kfz-Hersteller, dass ihre neuen Fahrzeugtypen so konstruiert sind, dass bei einem „schweren Unfall […] automatisch ein eCall-Notruf über die europaweite Notrufnummer 112 ausgelöst wird.“ Nach Auffassung des TLfDI wird mit dieser Regelung die „Einwilligungsregelung“ von Artikel 7 Buchstabe a) der Datenschutzrichtlinie 95/46/EG vollkommen konterkariert.

Aufgrund dieser beachtlichen Bedenken kam der TLDI in seiner Stellungnahme zu dem Ergebnis, dass der Verhältnismäßigkeitsgrundsatz im genannten Verordnungsentwurf nicht hinreichend beachtet worden sei. Vorzugswürdig erscheint dem TLfDI deshalb nach wie vor die freiwillige Basis des eCall-Dienstes, durch die ein Kfz-Nutzender bzw. Halter nicht rechtlich gezwungen wird, das eCall-System in Betrieb zu nehmen bzw. ihm dadurch eine Wahlmöglichkeit verbleibt.

Nicht zuletzt aufgrund der Stellungnahme des TLfDI fasste der Europaausschuss des Thüringer Landtags in seiner 23. Sitzung am 5. Juli 2013 einen Beschluss (siehe dazu die Drucksache 5/6323), in dem er die Bedenken des TLfDI aufgriff und ferner darauf hinwies,

dass die Mindestinformationen im Mindestdatensatz des eCall-Systems aufgrund ihrer Sensibilität einer genauen Definition in der Verordnung bedürfen. Auch sollten nach Auffassung des Europaausschusses die Grenzen des zulässigerweise übermittelten Datensatzes festgelegt und Regelungen getroffen werden, welche erweiterten Daten an welche privaten Dienstanbieter übersandt werden dürfen. Der Thüringer Landtag hat den genannten Beschluss direkt an die Europäische Kommission übermittelt.
Kritik und Bedenken signalisierte auch der Bundesrat an der Einführung des eCall-Dienstes. In seinem Beschluss vom 20. September 2013 (Drucksache 519/13) hat der Bundesrat deshalb angeregt, den Termin zur Einführung des eCalls bei den Notrufabfragestellen um ein Jahr auf den 1. Oktober 2016 zu verschieben.

Angesichts ungeklärter Sachfragen, z. B. zur Definition des Mindestdatensatzes beim eCall-System und möglicher ökonomischer Zwänge im Rahmen der zweiten Ausbaustufe des eCall-Systems, insbesondere im Bereich der Versicherungswirtschaft, ist die Forderung des Bundesrats, die Einführung des eCall-Systems zu verschieben, mehr als berechtigt und notwendig.

3.3 Ausschreibung im Schengener Informationssystem (SIS)

Um ein reibungsloses Funktionieren des Schengener Informationssystems (SIS) zu gewährleisten, verfügt jeder Mitgliedstaat über eine nationale Zentralstelle, eine sogenannte SIRENE (Supplementary Information Request at the National Entry). Sie ist zuständig für den nationalen und internationalen Nachrichtenaustausch (Informationsbeschaffung und -steuerung sowie Koordinierungsmaßnahmen) in Zusammenhang mit Schengener-Informationssystem-Fahndungen. Die SIRENE Deutschland ist beim Bundeskriminalamt in Wiesbaden angesiedelt.

Im Berichtszeitraum hatte sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewandt und mittgeteilt, dass er durch die SIRENE Deutschland darüber informiert wurde, dass ein Betroffener gemäß Art. 96 Schenger Durchführungsübereinkommen (SDÜ) zur Einreiseverweigerung im Schengener Informationssystem (SIS) erfasst ist. Die Erfassung

(sogenannte Ausschreibung) im SIS erfolgte durch die Stadtverwaltung Erfurt – Bürgeramt / Ausländer- und Asylangelegenheiten. Die Stadtverwaltung Erfurt hatte den Betroffenen 2003 gemäß § 47 Abs. 1 Satz 2 Ausländergesetz (AuslG; jetzt § 53 Aufenthaltsgesetz (AufenthG)) aus dem Bundesgebiet ausgewiesen und in sein Heimatland abgeschoben.

Gemäß § 50 Abs. 6 Satz 2 AufenthG kann ein ausgewiesener, zurückgeschobener oder abgeschobener Ausländer zum Zweck der Einreiseverweigerung zur Zurückweisung und für den Fall des Antreffens im Bundesgebiet zur Festnahme ausgeschrieben werden. Gegen den Betroffenen erging eine unbefristete Wiedereinreisesperre nach § 11 Abs. 1 Satz 1 AufenthG für die Bundesrepublik Deutschland sowie das gesamte Schengengebiet. Dabei handelte es sich – nach Auskunft der Stadtverwaltung Erfurt – um eine Maßnahme zur Gefahrenabwehr, da der Betroffene wegen einer Straftat verurteilt wurde (Art. 96 Abs. 2 und Abs. 3 SDÜ).

Diese Erfassung in SIS bleibt so lange bestehen, wie die Wiedereinreisesperre gegen den Betroffenen aufrechterhalten wird. Für ihn besteht lediglich die Möglichkeit, einen Antrag nach § 11 Abs. 1 Satz 3 AufenthG auf nachträgliche Befristung der Wiedereinreisesperre bei der Stadtverwaltung Erfurt zu stellen.

Die Erfassung eines ausgewiesenen, zurückgeschobenen oder abgeschobenen Ausländers im Schengener Informationssystem (SIS) entspricht den gesetzlichen Regelungen und ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

4 Neue Medien – Rundfunk – Telekommunikation

social network touchsreen – connectivi
© Torbz – Fotolia.com

4.1 Bekommt Deutschland den Cookie gebacken?

Am 25. November 2009 beschlossen das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG unter anderem Änderungen über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Diese E-Privacy-Richtlinie, auch unter „Cookie-Richtlinie“ bekannt, regelt im Wesentlichen in Artikel 5 Absatz 3 die Verwendung von Cookies. Dem Erwägungsgrund Nr. 66 der Cookie-Richtlinie ist zu entnehmen:

> „Es ist denkbar, dass Dritte aus einer Reihe von Gründen Informationen auf der Endeinrichtung eines Nutzers speichern oder auf bereits gespeicherte Informationen zugreifen wollen, die von legitimen Gründen (wie manchen Arten von Cookies) bis hin zum unberechtigten Eindringen in die Privatsphäre (z. B. über Spähsoftware oder Viren) reichen. Daher ist es von größter Wichtigkeit, dass den Nutzern eine klare und verständliche Information bereitgestellt wird, wenn sie irgendeine Tätigkeit ausführen, die zu einer solchen Speicherung oder einem solchen Zugriff führen könnte. Die Methoden der Information und die Einräumung des Rechts, diese abzulehnen, sollten so benutzerfreundlich wie möglich gestaltet werden. Ausnahmen von der Informationspflicht und der Einräumung des Rechts auf Ablehnung sollten auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen. Wenn es technisch durchführbar und wirksam ist, kann die *Einwilligung* des Nutzers zur Verarbeitung im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG über die Handhabung der

entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden. Die Umsetzung dieser Voraussetzungen sollte durch die Stärkung der Befugnisse der zuständigen nationalen Behörden wirksamer gestaltet werden."

Der Erwägungsgrund 66, der praktisch die Absichten von Rat und Parlament hinsichtlich Art. 5 Abs. 3 erläutert, verunsicherte in ihrer Umsetzung eher. Denn die Mitgliedstaaten und auch die Anwender hätten schon gerne ein Rezept vorgegeben bekommen, wie Cookies zu backen sind, damit sie nicht zu schwerverdaulich für die Nutzer werden.
Für Deutschland bedeutet dies, dass das Opt-in (Einwilligung) dem § 15 Abs. 3 Satz 1 Telemediengesetz (TMG) widerspricht, wonach Internetseitenbetreiber z. B. für Zwecke der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen dürfen, sofern der Nutzer dem nicht *widerspricht*. Diese Widerspruchsmöglichkeit (Opt-out) scheint mit der EU-Regelung der Einwilligung vorab (Opt-in) unvereinbar.
Inwieweit die Vorgaben aus der Richtlinie in Deutschland umgesetzt sind oder welches Recht wann wie Anwendung findet, wurde dementsprechend in den letzten Jahren diskutiert. So kann man einer Antwort der Bundesregierung auf eine kleine Anfrage im Juli 2011 entnehmen, dass die Bundesregierung prüft, wie durch eine Regelung im Telemediengesetz Artikel 5 Absatz 3 der E-Privacy-Richtlinie umgesetzt werden kann. Dem Deutschen Bundestag würde hierzu kurzfristig – im Rahmen der Novellierung des TKG – Vorschläge unterbreitet werden (BT DS 17/6689).
Aber die Novellierung des Telekommunikationsgesetzes regelte diesbezüglich nichts und der Bundesbeauftragte für den Datenschutz, Peter Schaar, kritisierte die weiterhin fehlende zwingende umzusetzende europäische Vorgabe (http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/35_NovellierungTKG.html).
Am 24. Januar 2012 lag ein Gesetzentwurf zur Umsetzung der Cookie-Richtlinie dem Deutschen Bundestag vor (BT DS 17/8454), der aber am 1. März 2013 vom Ausschuss für Wirtschaft und Technologie abgelehnt wurde (BT DS 17/8814). Da die konkrete Umsetzung der Cookie-Richtlinie in deutsches Recht weiter ausblieb, stellte sich dann die Frage, ob bei Nichtumsetzung der Richtlinie diese dann in

Deutschland direkt gelte, denn sie sei „hinreichend bestimmt“. Diese Meinung vertrat beispielsweise der Bundesbeauftragte für Datenschutz, Peter Schaar, im Mai 2012.
Um endlich Anwendungsrezepte für Cookies zu kreieren und zu verteilen, veröffentlichte die Artikel-29 – Datenschutzgruppe der EU-Mitgliedstaaten im Juni 2012 einen Leitfaden zur rechtskonformen Nutzung von Cookies nach der E-Privacy-Richtlinie. Insbesondere beleuchtet er Szenarien, wann nach der Richtlinie keine Einwilligung zum Setzen eines Cookies erforderlich erscheint. Dieses Arbeitspapier ist für alle Anwender ein gutes Arbeitspapier und wurde mittlerweile im Oktober 2013 nochmals konkretisiert (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf).
Derzeit wird im Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder diskutiert, wie man die Umsetzung der Cookie-Richtlinie bei Internetseitenbetreibern effektiv prüfen kann. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit wird davon berichten. Wir kriegen das schon gebacken!

Die Datenschutzbeauftragten des Bundes und der Länder werden weiterhin die Umsetzung der E-Privacy-Richtlinie begleiten. Für Programmierer und Anwender von Cookies ist der Leitfaden der Art. 29 Datenschutzgruppe ein wichtiges Arbeitsdokument.

4.2 Leitplanken für soziale Netzwerke

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnerte die 85. Datenschutzkonferenz des Bundes und der Länder am 13. März 2013 in der Entschließung „Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor“ deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen (siehe Anlage 14).
Es zeichnete sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke –insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber –den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und priva-

ten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen.
Zudem forderten die Datenschutzbeauftragten die europäischen und nationalen Gesetzgeber auf, für die notwendige Klarheit in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht zu sorgen.
Sowohl die Entschließung als auch die entsprechende Orientierungshilfe können unter
http://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/82_nutzerdaten.pdf bzw. unter
http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_soziale_netzwerke.pdf abgerufen werden.
Auch wird die Frage der polizeilichen Fahndung in Facebook unter den Datenschutzbeauftragten des Bundes und der Länder streitig diskutiert. So lehnt z. B. der nordrhein-westfälische Datenschutzbeauftragte eine polizeiliche Fahndung mit Hilfe Sozialer Netzwerke ab, weil gerade bei privaten Plattformen nicht bekannt sei, wer wie mit den Daten umgehe, die dort eingestellt werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit teilt diese Auffassung unter Hinweis darauf, dass nicht beinflussbar sei, wie lange die Daten im Netz erhalten bleiben.

Die Orientierungshilfe richtet sich an Betreiber sozialer Netzwerke. Sie richtet sich auch an Behörden und Unternehmen die mit sozialen Netzwerken ihre Aufgaben erfüllen (wollen) oder ihre Geschäftszwecke verfolgen. Eine Fahndung durch die Polizei per Facebook ist aus datenschutzrechtlicher Sicht grundsätzlich abzulehnen.

4.3 In’s Netz gegangen – Facebook

Öffentliche und nicht-öffentliche Stellen bedienen sich zunehmend globaler sozialer Netzwerke, um sich dort mittels sogenannter Fanpages (Internetseite-Seiten beim Betreiber des Sozialen Netzwerkes) darzustellen und um interaktiv mit dem Bürger zu kommunizieren (siehe Punkt 4.2) .Aber auch eigene Webseiten, die nicht beim Betreiber solcher sozialen Netzwerke gespeichert sind, sind zum Teil mit sogenannten „Social Plugins“ von den Webseitenbetreibern selbst erweitert worden. Eines solcher „Social Plugin“ ist beispiels-

weise der von Facebook bereitgestellte „Gefällt mir“ - Button (Like-Button).
Bei der datenschutzrechtlichen Bewertung ist zwischen Like-Button und Betreiben einer Fanpage zu unterscheiden: Mit Hilfe eines Like-Buttons ist es Facebook möglich, Daten über die Vorlieben der Nutzer zu sammeln, wenn der Button angeklickt wird. Dies geschieht mit Hilfe von Cookies (kleine Dateien), die dann auf dem Gerät platziert werden und Informationen an Facebook senden. Wenn der Nutzer gleichzeitig Facebook-Mitglied ist, ist er dadurch eindeutig identifizierbar. Durch das Setzen von Cookies können aber auch Daten von Nicht-Facebook-Mitgliedern durch Facebook erfasst werden. Registriert sich ein Nutzer später, können die gespeicherten Daten rückwirkend zugeordnet werden. Die aktive Einbindung eines Like-Buttons (Social-Plugin) auf einer Internetseite stellt dabei einen Telemediendienst nach dem Telemediengesetz (TMG) dar.
Gemäß § 13 Abs. 2 TMG dürfen Like-Buttons nur dann eingebunden werden, wenn der Nutzer gegenüber dem Internetseitenbetreiber in die mit der Einbindung von Social-Plugins verbundene Übertragung personenbezogener Daten bewusst und eindeutig eingewilligt hat. Diese erforderliche Einwilligung könnte über die sogenannte „Doppel-Klick“-Lösung erlangt werden. Dies kann zum Beispiel realisiert werden, indem an der Stelle, an der das Social-Plugin auf der Internetseite erscheint, zunächst eine vom Internetseitenbetreiber selbst bereitgestellte Grafik mit einer Datenschutzerklärung eingebunden wird. Nach einem Klick auf diese Grafik muss die Nutzerin oder der Nutzer dann über die mit der Anzeige des Social-Plugins verbundene Übertragung personenbezogener Daten an Facebook informiert werden. Willigt die Nutzerin oder der Nutzer ausreichend informiert und aktiv ein, so kann darauffolgend das Social-Plugin von Facebook geladen werden. Auch wenn es an der ausreichenden Information fehlen dürfte, weil unklar ist, welche Daten genau von Facebook erfasst und in welcher Weise weiter verarbeitet werden, ist aus datenschutzrechtlicher Sicht die Doppel-Klick-Lösung ein Weg, Nutzerinnen und Nutzer informativ auf das Risiko hinzuweisen und nicht Social-Plugins von vornherein zu verbieten.
Die Datenschutzbeauftragten des Bundes und der Länder vertraten mit der Entschließung der 82. DSK im September 2011 die Auffassung, dass die öffentlichen Stellen keine Fanpages einrichten sollten, da derzeit keine Möglichkeit bekannt ist, Fanpages datenschutzkon-

form zu gestalten. Hierzu wird auf die im Anhang beigefügte Pressemitteilung verwiesen:
(http://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/82_nutzerdaten.pdf).
Nutzen Schulen globale soziale Netzwerke, wie beispielsweise Facebook, werden die Daten nicht unter der alleinigen Kontrolle der Schule verarbeitet. Die Schulen und somit auch die Lehrer können derzeit nicht dafür Sorge tragen, dass sowohl die Verkehrs- und Inhaltsdaten der Lehrer und der Schüler vertraulich bleiben. Hinsichtlich der Nutzung von Fanpages durch Schulen muss man zudem unterscheiden, ob Lehrer den Schülern den sachkundigen Umgang mit sozialen Netzwerken vermitteln (siehe Anlage 14) oder ob sie als Lehrer mit Schülern in sozialen Netzwerken kommunizieren, etwa Hausaufgaben verteilen, Ergebnisse von Arbeiten, Unterrichtsausfälle, Lob und Tadel mitteilen. Im Ergebnis stellt jegliche dienstliche Kommunikation, die personenbezogene Daten beinhaltet, mittels solcher sozialen Netzwerke sowohl zwischen Lehrkräften und Schülern als auch der Lehrkräfte untereinander einen Verstoß gegen das Thüringer Datenschutzgesetz dar. Irrelevant ist dabei, ob der Lehrer dabei von der Schule oder von zu Hause aus tätig wird.
Datenschutzrechtliche Alternativen bilden Netzwerke, die dezentral bei den Schulen selbst eingerichtet oder deren Server ausschließlich in Deutschland betrieben werden; sie sind im Internet zu finden. Zudem ist zu bedenken, dass Schüler, die bislang auf die Nutzung sozialer Netzwerke wie Facebook verzichtet haben, faktisch gezwungen werden könnten, sich hieran zu beteiligen, um keine Nachteile infolge verspäteter oder unvollständiger schulischer Informationen zu erleiden. Schulen und Lehrer sollten angesichts der dargelegten Argumente keinen derartigen Druck ausüben:
(http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/pm_lehrer_in_facebook___co.pdf).

Da derzeit keine Möglichkeit bekannt ist, Fanpages bei Facebook datenschutzkonform zu gestalten, ist weiterhin von deren Betreiben abzuraten. Zudem stellt insbesondere die Kommunikation zwischen Lehrkräften und Schülern mittels globaler sozialer Netzwerke als auch der Lehrkräfte untereinander einen Verstoß gegen das Thüringer Datenschutzgesetz dar. Bei der Nutzung von Social-Plugins (wie beispielsweise dem Like-Button) ist vorab die Einwilligung – beispielsweise durch die Doppel-Klick-Lösung einzuholen.

4.4 Notruf

Im 9. Tätigkeitsbericht Punkt 4.4 berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit bereits von der technischen Richtlinie Notruf (TR Notruf). Diese dient dem Ziel, dass beim Absetzen eines Notrufes mit einem Mobil- oder Festnetztelefon stets die Rufnummer und der Standort bzw. die Adresse des Anrufers an den Empfänger des Notrufs mit übermittelt werden. Zudem dürfen ab 1. Januar 2014 nur noch die öffentlichen Münz- und Kartentelefone betrieben werden, die ebenfalls die Notrufverbindung mit der Nummer 112 und 110 aufbauen können.
Zuständig für die Umsetzung der TR Notruf ist die Bundesnetzagentur. Dem Tätigkeitsbericht 2012/2013 der Bundesnetzagentur ist zu entnehmen, dass bei Notrufen aus dem Mobilfunknetz die Informationen zu der Mobilfunkzelle, in der sich der Notrufende befindet, ordnungsgemäß übermittelt werden. Jedoch gäbe es Defizite bei der Übermittlung von Standortdaten bei einigen Festnetzanbietern. Erste Maßnahmen wurden im Herbst 2013 von der Bundesnetzagentur eingeleitet.
Auch wenn nach der TR Notruf, der Verordnung über Notrufverbindungen – NotrufV (zuletzt geändert 2012) und § 108 Telekommunikationsgesetz die Netzbetreiber und Mobilfunkanbieter beim Notruf verpflichtet sind, die Rufnummer des Anschlusses und die Standortdaten des Hilfesuchenden schon im Verbindungsaufbau zu übermitteln, so bedarf es noch der technischen Ausstattung der Notrufanschlüsse in den Notrufabfragestellen, also bei den Stellen, die die Notrufe entgegen nehmen. Diese müssen ihre bestehende Technik bis zum 31. Dezember 2014 so anpassen, dass sie die empfangenen Standortdaten auch verarbeiten bzw. nutzen und damit sichtbar machen können.
Entsprechend einer Pressemeldung wurde beispielsweise das thüringenweit erste Pilotprojekt zur automatisierten Ortung von Handynotrufen erfolgreich in der Rettungsleitstelle Gotha abgeschlossen. Seit 1. Juli 2013 kann nun die Rettungsleitstelle Gotha den Umkreis, aus dem der Notruf kommt, ermitteln und schneller helfen. Es ist davon auszugehen, dass die anderen Rettungsleitstellen 2014 nachrüsten.
Aus datenschutzrechtlicher Sicht sind Standortdaten sehr sensible Daten, eine Ortung ohne einen aktiven Notruf ist daher unzulässig und wurde gemäß § 4 Abs. 6 NotrufV untersagt.

Auch beim Absetzen eines Notrufes muss der Datenschutz gewährleistet sein. So ist gemäß § 4 Abs. 6 Verordnung über Notrufverbindungen das automatische Herstellen einer Notrufverbindung ohne unmittelbares Tätigwerden eines Menschen unzulässig. Abweichendes gilt für in Kraftfahrzeugen installierte Einrichtungen für E-Call (siehe dazu den Beitrag „Einführung eines EU-weiten eCall-Dienstes – Mehr Verkehrssicherheit auf Kosten des Datenschutzes?“).

4.5 Überwachung der Telekommunikation gem. § 100 a StPO und Erhebung von Verkehrsdaten nach § 100 g StPO im Jahr 2010 – auch mittels Eilanordnung erfolgt?

Mit Schreiben vom Juni 2011 informierte das Thüringer Justizministerium (TJM) den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über die im Freistaat Thüringen im Jahr 2010 getroffenen Maßnahmen zur Überwachung der Telekommunikation nach § 100 a Strafprozessordnung (StPO) und zur Erhebung von Verkehrsdaten nach § 100 g StPO. Der übersandten Aufstellung des TJMs war jedoch nicht zu entnehmen, wie viele Eilanordnungen es von den zuständigen Staatsanwaltschaften für die besagten Überwachungsmaßnahmen nach § 100 b Abs. 1 Satz 2 StPO gegeben hat. Dieses Fehlen hatte seine Ursache darin, dass die Zahl der Eilanordnungen nicht von den Berichtspflichten umfasst ist. Gemäß § 100 b Abs. 1 Satz 2 StPO ist für die Anordnung von Maßnahmen nach § 100 a StPO und auch für die Erhebung von Verkehrsdaten gem. § 100 g Abs. 2 Satz 1 StPO die Staatsanwaltschaft bei Gefahr im Verzug zuständig.
Der TLfDI bat daher mit Schreiben vom Juli 2011 das TJM um Mitteilung, in wie vielen Fällen eine Eilanordnung durch die Staatsanwaltschaft getroffen wurde, und in wie vielen Fällen diese nicht gemäß § 100b Abs. 1 Satz 3 StPO aus welchen Gründen vom Gericht bestätigt wurde.
Das TJM teilte daraufhin Folgendes mit: Bei den Staatsanwaltschaften Meiningen und Mühlhausen habe es im Jahr 2010 keine entsprechenden Eilanordnungen gegeben. Bei der Staatsanwaltschaft Gera seien für das Jahr 2010 ebenfalls keine Eilanordnungen bekannt. Im Bereich der Staatsanwaltschaft Erfurt sollen für das Jahr 2010 Eilanordnungen allenfalls in ganz seltenen Ausnahmefällen getroffen

worden sein. Soweit diese Eilanordnungen zu verzeichnen gewesen seien, seien diese auch richterlich bestätigt worden.

Gemäß § 100 b Abs. 5 StPO sind die Bundesländer und der Generalbundesanwalt sowohl für Maßnahmen nach § 100 a Abs. 1 StPO als auch für Maßnahmen nach § 100 g Abs. 1 StPO verpflichtet, dem Bundesamt für Justiz kalenderjährlich bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über die in ihrem Zuständigkeitsbereich angeordneten Maßnahmen zu berichten. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet. Soweit danach noch Klärungs- oder Nachfragebedarf existiert, ist der TLfDI hier der richtige Ansprechpartner.

5 Kommunales

Rathaus
© Doce Rabe Media 5 – Fotolia.com

5.1 Datenschutzrechtliche Kommunalkontrollen allgemein – Steter Tropfen höhlt den Stein

In seinem 8. und 9. Tätigkeitsbericht (jeweils Punkt 5.1) berichtete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über die Kontrollen des Grunddatenschutzes in 40 Kommunalverwaltungen. Zum 31. Dezember 2013 waren insgesamt 33 der damaligen Kontrollverfahren abgeschlossen. Nachdem sich die Verwaltungsgemeinschaft „Goldene Aue“ am 30. November 2010 aufgelöst hatte, hat der TLfDI, anknüpfend an die Kontrolle der Verwaltungsgemeinschaft „Goldene Aue“, auch deren Rechtsnachfolgerin, die Landgemeinde Stadt Heringen/Helme, kontrolliert.
Bislang sind Gera, Weimar, Ruhla, Eisfeld, Stadtilm, Artern und Heringen/Helme der Forderung, ein IT-Sicherheitskonzept gemäß § 9 Thüringer Datenschutzgesetz (ThürDSG) vorzulegen, noch nicht nachgekommen. In diesem Zusammenhang hat der TLfDI wegen mangelnder Unterstützung bei der Erledigung der datenschutzrechtlichen Forderungen eine Beanstandung gemäß § 39 ThürDSG gegenüber der Stadt Weimar ausgesprochen.
Von Oktober 2012 bis November 2013 hat der TLfDI 11 weitere Kommunalverwaltungen unter die Lupe genommen. Da erfahrungsgemäß meist kleine Kommunen datenschutzrechtliche Defizite aufweisen, wurden neben einem Landratsamt, vier Verwaltungen von Städten unter 20.000 Einwohnern, zwei Gemeindeverwaltungen, drei Verwaltungsgemeinschaften und eine Landgemeinde, verteilt auf mehrere Thüringer Regionen, geprüft. Im Fokus der Kontrollen standen neben dem Grunddatenschutz die potenziellen und tatsächlich aktivierten Leistungsmerkmale der jeweiligen Telefonanlagen, insbesondere im Hinblick auf die besonders missbrauchsanfälligen

Funktionen Raumüberwachung, Speicherung von Telefongesprächen und die so genannte Gesprächsaufschaltung.
Dass die Kontrollen des TLfDI der Jahre 2008 und 2009 nicht ohne Wirkung geblieben sind, zeigte sich in einer vielfach gesetzeskonformen Gestaltung der vorgelegten Verträge für die Datenverarbeitung im Auftrag. Trotz dieses teilweisen Lichtblicks hat der TLfDI im Landratsamt des Ilm-Kreises, in den Stadtverwaltungen Heilbad Heiligenstadt, Bleicherode und Auma-Weidental, den Verwaltungsgemeinschaften Rennsteig und Wasungen-Amt Sand sowie in der Landgemeinde Hörsel schwerwiegende datenschutzrechtliche Verstöße festgestellt und daher gegenüber diesen sieben verantwortlichen Stellen Beanstandungen ausgesprochen.
Im Einzelnen gab es auch dieses Mal erhebliche Mängel beim IT-Sicherheitskonzept und den erforderlichen Regelungen zu Datenschutz und Datensicherheit. So konnte nur in einem Fall ein vollständiges IT-Sicherheitskonzept vorgelegt werden. Leider zeigen die hohe Beanstandungsquote von fast 64 % und die auch in größeren Verwaltungen, wie dem Landratsamt des Ilm-Kreises und der Stadtverwaltung Heilbad Heiligenstadt vorgefundenen Defizite, dass auch künftig große Anstrengungen den Verantwortlichen von Nöten sein werden, um den kommunalen Datenschutz auf ein befriedigendes Niveau zu heben.
Der TLfDI steht im Rahmen seiner gesetzlichen Verpflichtung nach § 40 Abs. 7 ThürDSG auch künftig zur Verfügung, um öffentliche Stellen zu beraten und Empfehlungen zu Verbesserungen des Datenschutzes zu geben. In diesem Zusammenhang hat der TLfDI auf seiner Internetseite unter den Menüpunkten „Themen“ – „Kommunales“ das Dokument „Datenschutzrechtliche Anforderungen an Kommunen“ veröffentlicht. Neben den Schulungsangeboten der Kommunalen Spitzenverbände und der privaten Anbieter zu Fragen des Datenschutzes und der Datensicherheit bietet der Arbeitskreis Kommunaler Datenschutz die Möglichkeit des Erfahrungsaustausches zu datenschutzrechtlichen Themen. Es kommt nun darauf an, diese vielfältigen Informationsangebote zu nutzen. Ein Blog zu kommunalen Datenschutzfragestellungen ist angedacht.

Die Herstellung datenschutzgerechter Zustände in der Kommunalverwaltung ist gerade im Hinblick auf aktuelle Bedrohungsszenarien eine unabweisbare Aufgabe, die Beharrlichkeit erfordert. Hierbei kommt es insbesondere darauf an, dass die verantwortlichen Leiter

und engagierten Datenschutzbeauftragten vor Ort in Zusammenarbeit mit den Fachabteilungen und den EDV-Fachleuten klare Regeln schaffen, und alle Beschäftigte durch Schulung und Aufklärung in Fragen des Datenschutzes sensibilisiert werden.

5.2 Arbeitskreis Kommunaler Datenschutz

Traditionell treffen sich zweimal im Jahr kommunale behördliche Datenschutzbeauftragte der Landkreise und kreisfreien Städte mit Vertretern des Thüringer Landkreistages, des Gemeinde- und Städtebundes Thüringen, des Thüringer Landesrechenzentrums und des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zum Arbeitskreis Kommunaler Datenschutz.
Der Arbeitskreis dient dem Erfahrungsaustausch zu aktuellen rechtlichen, organisatorischen und technischen Fragen des Datenschutzes im kommunalen Bereich und findet im Wechsel immer bei einer anderen teilnehmenden Stelle statt. Der TLfDI nutzt den Rahmen des Arbeitskreises Datenschutz für den öffentlichen Bereich, um seiner Beratungspflicht nach § 40 Abs. 7 ThürDSG nachzukommen.
In einzelnen Beiträgen dieses Tätigkeitsberichts findet sich eine Reihe von Themen, die im Berichtszeitraum im Rahmen des Arbeitskreises erörtert wurden. Insofern wird auf den Gliederungspunkt Kommunales verwiesen.

Der Arbeitskreis Datenschutz für den öffentlichen Bereich ist ein bewährtes Forum des Erfahrungsaustausches und der Beratungstätigkeit des TLfDI.

5.3 Videoüberwachung über und unter Wasser: Videogaga 1

Die Videoüberwachung im Schwimmbad war bereits im 9. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) unter Nummer 5.5 ein Thema. Bei der Durchführung von elf datenschutzrechtlichen Kontrollen in Frei- und Hallenbädern hatte der TLfDI seinerzeit festgestellt, dass viele Bäder in Thüringen eine Videoüberwachung durchführen, die nicht den gesetzlichen Anforderungen entspricht. Insbesondere zwei Probleme sind dabei in den rechtlichen Auseinandersetzungen mit den Bädern bisher noch offen geblieben: Zum einen ist fraglich, ob eine Videoüberwachung aufgrund des Haus-

rechts gerechtfertigt sein kann, wenn es in dem Bad bislang keine konkreten Anhaltspunkte für eine Sachbeschädigung oder einen Diebstahl in bestimmten Bereichen gegeben hat. Zum anderen ist die Frage der Zulässigkeit der Videoaufzeichnung an sogenannten gefährlichen Stellen problematisch. Letzteres deswegen, weil durch die *Aufzeichnung* kein Unfall im Bad verhindert werden kann. Zulässig ist nach Auffassung des TLfDI eine Video*beobachtung* (Monitoring) an gefährlichen Stellen, damit im Gefahrenfall eingegriffen werden kann. Die Aufzeichnung der Bilder dient demgegenüber der *nachträglichen* Klärung von Haftungsfragen und ist von der gesetzlichen Ermächtigung des § 6 b Bundesdatenschutzgesetz nicht gedeckt. Der TLfDI versuchte, sich mit der Deutschen Gesellschaft für das Bäderwesen e. V. auf eine einheitliche Linie zu verständigen und Grundsätze für die zulässige Videoüberwachung in Schwimmbädern zu entwickeln. Leider konnte in Bezug auf die zwei vorgenannten Punkte bisher keine Einigung erzielt werden. Der TLfDI hat daraufhin das Thema Videoüberwachung in Schwimmbädern in der Ad-hoc-AG Videoüberwachung des Düsseldorfer Kreises der Datenschutzkonferenz thematisiert. Es wurde eine gemeinsame Auffassung der Teilnehmer erarbeitet, die sich mit der vom TLfDI vertretenen Auffassung deckt, und der Gesellschaft für das Bäderwesen e. V. schriftlich dargelegt. Eine Reaktion hierauf ist bislang nicht erfolgt. Thüringen unterbreitete daher zunächst dem Düsseldorfer Kreis (siehe 1. Tätigkeitsbericht für den nicht-öffentlichen Bereich Punkt 2) einen Beschlussvorschlag für die zulässige Videoüberwachung in Schwimmbädern. Dieser wurde jedoch zurückgestellt, da die Ad-hoc-AG zunächst eine „Orientierungshilfe Videoüberwachung“ erarbeiten sollte, die die grundsätzlichen Anforderungen an eine zulässige Videoüberwachung festlegt. Nachdem diese Orientierungshilfe unter maßgeblicher Mitarbeit Thüringens fertiggestellt und in der Sitzung des Düsseldorfer Kreises vom 25./26. Februar 2014 zustimmend zur Kenntnis genommen wurde (vgl.
http://www.tlfdi.de/imperia/md/content/datenschutz/themen/videoueberwachung/oh-v__-durch-nicht-__ffentliche-stellen.pdf), wird Thüringen das Thema erneut in die Ad-hoc-AG Videoüberwachung einbringen und sich dafür einsetzen, dass als Ergänzung zur OH Videoüberwachung eine Handreichung zur Videoüberwachung in Schwimmbädern erarbeitet wird. Da bereits die in der OH Videoüberwachung gemachten Feststellungen allgemeiner Art die Rechts-

auffassung des TLfDI zur Videoüberwachung in Schwimmbädern stützen, wird sich dieser im kommenden Berichtszeitraum weiter mit den Schwimmbadbetreibern auseinandersetzen, um zu einer datenschutzkonformen Lösung in den Thüringer Schwimmbädern zu kommen.

Die Deutsche Gesellschaft für das Bäderwesen e. V. und der TLfDI vertreten unterschiedliche Auffassungen an die Anforderungen zulässiger Videoüberwachung in Schwimmbädern. Die Auffassung des TLfDI wurde durch die „Orientierungshilfe Videoüberwachung“ des Düsseldorfer Kreises gestützt. Der TLfDI wird sich daher gegenüber den Thüringer Schwimmbadbetreibern weiterhin verstärkt für eine datenschutzgerechte Nutzung von Videoüberwachungstechnik in Schwimmbädern einsetzen.

5.4 Zensus 2011 – Kontrolle der Statistikstelle der Stadtverwaltung Pößneck

Im Berichtszeitraum führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Sommer 2013 eine Kontrolle der Statistikstelle der Stadtverwaltung Pößneck durch. Die Kontrolle hatte zum Ziel, die Einhaltung der Vorschriften des Thüringer Datenschutzgesetzes (ThürDSG) sowie anderer Vorschriften über den Datenschutz bei der Statistikstelle zu kontrollieren (§ 37 ThürDSG). Insbesondere galt es zu prüfen, ob in der Statistikstelle die erforderlichen Voraussetzungen einer abgeschotteten Statistikstelle für den Zugang der Gemeinden zu Einzelangaben der amtlichen Statistik gemäß § 16 Abs. 5 Bundesstatistikgesetz (BStatG) vorliegen.
Gemäß § 22 Abs. 2 Zensusgesetz 2011 (ZensG 2011) dürfen die statistischen Ämter des Bundes und der Länder den für statistische Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände (Statistikstellen) für ausschließlich kommunalstatistische Zwecke auf Ersuchen für deren Zuständigkeitsbereich Einzelangaben zu den Erhebungsmerkmalen sowie zu den Hilfsmerkmalen „Straße“ und „Hausnummer“ oder nach Blockseiten zusammengefasste Einzelangaben übermitteln. Die Übermittlung ist dabei nur zulässig, wenn das Statistikgeheimnis durch gesetzlich vorgeschriebene Maßnahmen (§ 16 Abs. 5 BStatG i. V. m. § 20 Thüringer Statistikgesetz(ThürStatG)), insbesondere zur räumlichen, organisatorischen

und personellen Trennung der Statistikstellen von den für nichtstatistische Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände, gewährleistet ist.
Im Ergebnis der Kontrolle wurde seitens des TLfDI festgestellt, dass in der Statistikstelle Pößneck die organisatorischen Voraussetzungen einer abgeschotteten Statistikstelle (§ 16 Abs. 5 BstatG i. V. m. § 20 ThürStatG) für den Zugang zu den Einzelangaben der amtlichen Statistik vorliegen. Ein Kritikpunkt des TLfDI war allerdings, dass die nach den Angaben der Ansprechpartner bestehende Schlüsselverfügungsgewalt zur Statistikstelle nicht nur der zuständigen Statistikstellenleiterin, sondern auch den vier Fachbereichsleitern der Stadtverwaltung zustand. Bereits vor Ort wurde dem TLfDI zugesichert, die Statistikstelle mit separatem Schloss mit alleiniger Schlüsselhoheit durch die zuständige Statistikstellenleiterin auszustatten. Telefonisch wurde dem TLfDI seitens der Ansprechpartner mitgeteilt, dass entsprechende Maßnahmen bereits in die Wege geleitet wurden.
Der TLfDI hat zudem empfohlen, die organisatorische Trennung von Stadtverwaltung und Statistikstelle bzw. die eigenständige organisatorische Einheit „Statistikstelle“ auch im Organigramm / in Arbeitsverteilungsplänen oder ähnlichem der Stadtverwaltung abzubilden.
Das gemäß § 9 Abs. 2 ThürDSG zu erstellende IT-Sicherheitskonzept (IT-SiKo) wird in Zusammenarbeit mit der Kommunalen Informationsverarbeitung Thüringen GmbH (KIV Thüringen GmbH) überarbeitet. Dabei geht es insbesondere darum, die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionsfähigkeit zu gewährleisten.
Regelungen zu Datenschutz und Datensicherheit gibt es bereits in der Dienstanweisung „Nutzung der Informationstechnik“. Diese Regelungen sollten auch Bestandteil des neuen IT-SiKo sein. Insbesondere sind verbindliche Festlegungen für alle Beschäftigten in Bezug zu den Gefährdungen durch Nutzung der IT darzustellen, um ihnen wirksam zu begegnen.
In den zum IT-SiKo gehörenden Dokumentationen sind weiterhin solche Schutzmaßnahmen aufzunehmen, die der Absicherung des internen lokalen Netzes (z. B. Firewall, Schutzsoftware vor Schaden stiftenden Programmen, sicherheitstechnische Einstellungen der Software etc.) dienen. Weiterhin sind Aussagen zu Protokollierungen, zur Datensicherung oder Analysen und Festlegungen zur Wartung und Fernwartung von Fremdfirmen erforderlich.

Das Konzept sollte so gestaltet sein, dass es den aktuellen Gegebenheiten zeitnah angepasst werden kann. Dies trifft bei Änderungen und Weiterentwicklungen der IT-Infrastruktur sowie der Anpassung der Fachverfahren an den Stand der Technik zu.

Datenschutzkonforme Zustände waren in Vorbereitung des Zensus 2011 zu schaffen, bei der Durchführung des Zensus 2011 erforderlich und sind auch nunmehr bei der Nutzung der Statistikdaten zu gewährleisten. Das IT-Sicherheitskonzept ist entsprechend den Vorgaben des § 9 ThürDSG zu gestalten.

5.5 Rettungsleitstelle: Privates für den Vorgesetzten

Ein Rettungsassistent der Leitstelle/Rettungsdienst des Landratsamtes Saalfeld-Rudolstadt wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), weil ein Telefongespräch zwischen ihm und dem Fachdienstleiter der Leitstelle zu Angelegenheiten und Aufrechterhaltung des Dienstbetriebes aufgezeichnet und an Dritte, seinen Vorgesetzten übermittelt und dann ausgewertet worden sei. Hierzu wurde die Rettungsleitstelle Saalfeld um Stellungnahme gebeten. Der Datenschutzbeauftragte des Landratsamtes Saalfeld-Rudolstadt teilte mit, dass nach Punkt 9.2 des Landesrettungsplans für den Freistaat Thüringen zur Aufgabenerledigung eine Ton- und Schriftdokumentation erfolge. Über diese Dokumentationspflicht der Zentralen Leitstelle seien die Rettungswachen aktenkundig belehrt worden. Der Datenschutz in den Leitstellen bestimme sich nach § 30 Thüringer Rettungsdienstgesetz (ThürRettG). Die Benutzung der zentralen Telefonanlage der Leitstelle mit der angeschlossenen Langzeitdokumentation schließe jede Vertraulichkeit der Äußerung im Hinblick auf den Arbeitgeber aus. Die Beschäftigten seien ausdrücklich belehrt, dass keine privaten Telefongespräche zu führen sind und die zentrale Rettungsleitstelle eine Dokumentation der Gespräche vornimmt. Der Betroffene musste damit rechnen, dass Äußerungen gegenüber dem Leiter der Leitstelle keine Vertraulichkeit genießen und keinen privaten Charakter haben. Im Rahmen der Dienstaufsicht über die Rettungswachen obliege es dem Leiter der Zentralen Rettungsleitstelle, Äußerungen die die Arbeit der Leitstelle und des Rettungsdienstes als solche gefährden, verantwortlichen Personen zur Verfügung zu stellen.

Nach rechtlicher Prüfung durch den TLfDI wurde diese Rechtsauffassung des Datenschutzbeauftragten des Landratsamtes Saalfeld-Rudolstadt nicht geteilt. Gemäß § 31 ThürRettG sind die am Rettungsdienst Beteiligten „verpflichtet, die Einsätze in der Notfallrettung und im Krankentransport … im erforderlichen Umfang zu dokumentieren.“ Nur zu diesen Zwecken ergibt sich aus § 30 ThürRettG die Erlaubnis zur Einsatzdokumentation. Somit ist eine Auswertung nur zulässig, soweit diese im Zusammenhang mit einer Notfallrettung, einem Krankentransport usw. steht. Falls ein Telefongespräch ohne Einsatzbezug unter einer Telefonnummer erfolgt, unter der üblicherweise Notrufe eingehen und die Abwicklung von Einsätzen erfolgt, so wird dieses technisch bedingt ebenfalls aufgezeichnet. Ein solches Gespräch darf aber keinesfalls inhaltlich ausgewertet werden.
Im Ergebnis liegt ein Verstoß gegen § 4 ThürDSG i. V. m. § 30 Abs. 2 – 4 ThürRettG vor, den der TLfDI beanstandet hatte. Um einige ungeklärte Fragen im Zusammenhang mit der Funktionsweise der Telefonanlage der Leitstelle zu analysieren, wurde von Seiten des TLfDI eine Vor-Ort-Kontrolle durchgeführt. Bis auf drei konnten alle Fragen während der Kontrolle beantwortet werden. Zu den drei offenen Fragen antwortet die Leitstelle Rettungsdienst im Nachgang. Gegen die technischen Einrichtungen, die Räume incl. Festlegungen zur Sicherung des Zugangs sowie Maßnahmen zur Einschränkung des Zugriffs auf die Software-Anwendungen gab es keine Einwände.

Auch wenn nach geltendem Recht zur Aufgabenerledigung der Rettungsleitstellen eine Ton- und Schriftdokumentation aller eingehenden Anrufe erfolgt, darf ein Telefongespräch ohne Einsatzbezug nicht inhaltlich ausgewertet werden. Eine Auswertung ist nur zulässig, soweit diese im Zusammenhang mit einer Notfallrettung, einem Krankentransport usw. steht.

5.6 Videoüberwachung im Schloss: Videogaga 2

Die Stiftung Schloss Friedenstein Gotha trat an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) heran und bat um datenschutzrechtliche Bewertung der Videoüberwachung, die von ihr in allen zur Stiftung gehörenden Museen betrieben werde. Zum Schloss Friedenstein gehören das

Schloss- und das Herzogliche Museum, die Schlosskirche und das Ekhof-Theater, die kunst- und naturwissenschaftliche Sammlung, das Thüringische Staatsarchiv Gotha, die Universitäts- und Forschungsbibliothek Erfurt / Gotha sowie der Park- und Orangeriegarten.

Da Träger der Stiftung Schloss Friedenstein Gotha (Stiftung) laut der Stiftungssatzung die Stadt Gotha und das Land Thüringen sind und eine Aufgabe der öffentlichen Verwaltung wahrgenommen wird, ist die Stiftung zwar als öffentliche Stelle im Sinne von § 2 Abs. 2 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) anzusehen. Allerdings ist davon auszugehen, dass ein öffentliches Museum im Wettbewerb mit privaten Museen und Kunstsammlungen steht. Gemäß § 26 ThürDSG sind daher im Wesentlichen die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) heranzuziehen.

Der TLfDI stattete Schloss Friedenstein einen Kontrollbesuch ab und machte folgende Feststellungen: Die Videoüberwachung wird durch eine private Sicherheitsfirma durchgeführt. Mit der Sicherheitsfirma existierte kein den gesetzlichen Anforderungen entsprechender Vertrag über die Datenverarbeitung im Auftrag. Zum Zeitpunkt der Kontrolle wurden insgesamt 40 Videokameras betrieben, bei denen es sich um höchst unterschiedliche Modelle handelte. 26 Kameras befinden sich im Schlossmuseum, 6 im Bereich der Orangerie und weitere Kameras sind vorübergehend auf Baustellen an dem Schlossbau zur Objektüberwachung installiert. Letztere werden nach Fertigstellung der Baumaßnahmen wieder entfernt. 20 Kameras haben dabei lediglich die Aufgabe, als „verlängertes Auge“ Livebilder in den Wachraum der privaten Sicherheitsfirma zu übertragen, ohne dass eine Aufzeichnung der Bilder erfolgt. Hiermit werden die Zugänge zu den Treppenhäusern, den Fluren, einigen Türen, dem Parkplatz und zum Innenhof überwacht. Die Kameras an der Fahrzeugzufahrt zum Schlossgelände und am Zugang zum Innenhof, werden zur Durchfahrtsüberwachung genutzt. Regelungen zur Durchführung der Videoüberwachung in Form von Dienst- bzw. Arbeitsanweisungen waren nicht dokumentiert. Es gab nur einen Hinweis auf die Videoüberwachung im Eingangsbereich.

Die Zulässigkeit des Einsatzes einer Videoüberwachung des Schlosses Friedenstein und des Schlossgeländes bestimmt sich nach den Regelungen des § 6 b BDSG. Der videoüberwachte Bereich ist als öffentlich zugänglicher Raum anzusehen. Die Videoüberwachung muss zur Wahrnehmung berechtigter Interessen für konkret festge-

legte Zwecke, § 6 b Abs. 1 Nr. 3 BDSG, erforderlich sein. Im Museumsbereich kann man davon ausgehen, dass wertvolle Kulturdenkmäler und Kunstwerke gesichert werden müssen. Die Stiftung hat ein berechtigtes Interesse daran, Gefahren für die Kulturdenkmäler und Kunstwerke abzuwenden und gegebenenfalls auch einen Nachweis für den Ersatz von entstandenen Schäden führen zu können (§ 6 b Abs. 1 Nr. 3 BDSG). Die Videoüberwachung muss jedoch für die Wahrnehmung berechtigter Interessen erforderlich sein. Hier ist zu differenzieren. Die Videoüberwachung lässt sich in technischer Hinsicht auf unterschiedliche Weise realisieren. Vom so genannten Monitoring spricht man, wenn die aufgenommenen Bilder nur auf einen Monitor übertragen werden. In dieser Fallkonstellation stellt der Monitor nur ein „verlängertes Auge“ des Betrachters dar. Deshalb greift diese Form der Videoüberwachung weniger intensiv in die Rechte des Betroffenen ein als dies bei der Speicherung von Bilddaten der Fall ist. Unter Zugrundlegung der dargelegten Grundsätze erschien die Videoüberwachung im Kassenraum bedenklich, da das dort beschäftigte Personal einer ständigen Überwachung ausgesetzt war.

Nach der Begehung des Objektes stellte der TLfDI folgende Forderungen auf: Die Stiftung musste kurzfristig schriftlich einen Beauftragten für den Datenschutz bestellen. Dieser muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen und ist dem Leiter der Stiftung unmittelbar zu unterstellen. Da eine Videoüberwachung besondere Risiken für die Rechte und Freiheiten der überwachten Personen aufweist, muss der Beauftragte für den Datenschutz eine Vorabkontrolle nach § 4 d Abs. 6 BDSG unter Prüfung der Angaben gemäß § 4 e Satz 1 BDSG und der nach § 9 BDSG getroffenen technischen und organisatorischen Maßnahmen vornehmen. Jede Stelle, die personenbezogene Daten verarbeitet, muss nach dem Gesetz den Umgang mit diesen Daten dokumentieren. § 4 e BDSG legt fest, welche Angaben zu machen sind.

Mit der Sicherheitsfirma ist ein Vertrag über die Auftragsdatenverarbeitung zu schließen. Nach § 11 BDSG muss hierzu ein schriftlicher Vertrag mit Regelungen zum Umfang der Datenverarbeitung, den verwendeten Programmen, Datenschutz- und Datensicherheitsmaßnahmen und der Weisungsbefugnis des Auftraggebers geschlossen werden.

Es ist an mehreren Stellen auf den Umstand der Videoüberwachung hinzuweisen. Die Stiftung erfüllte mittlerweile die an sie gestellten

Forderungen. Im Hinblick auf die Kamera im Kassenbereich wurde eine Betriebsvereinbarung geschlossen, nach der sichergestellt wird, dass eine Verhaltens- und Leistungskontrolle der Beschäftigten nicht stattfindet.

In einem Museum müssen oft wertvolle Kulturdenkmäler und Kunstwerke gesichert werden. Grundsätzlich ist daher eine Videoüberwachung zur Abwehr von Gefahren für die Kulturdenkmäler und Kunstwerke denkbar. Die Videoüberwachung muss jedoch für die Wahrnehmung berechtigter Interessen erforderlich sein und schutzwürdige Interessen der Betroffenen dürfen nicht überwiegen.

5.7 Wer ist der „amtliche“ Vater – zur Weitergabe sensibler Daten durch das Standesamt

Ein Student hat dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, dass unrichtige personenbezogene Daten seiner Person seitens des für ihn zuständigen Standesamtes Jena an das Jobcenter übermittelt worden seien, wohl zur Klärung von Unterhaltsfragen, und hat um Überprüfung der datenschutzrechtlichen Zulässigkeit der Übermittlung gebeten. Im Einzelnen handele es sich dabei um die Übermittlung von Angaben zu seinem angeblichen Vater sowie dem (dann auch angeblichen) Vaterschaftsverhältnis zu ihm. Er teilte weiter mit, er kenne diesen „angeblichen Vater“ nicht und dieser sei auch nicht sein leiblicher Vater. Dies sei nach seinen Angaben insbesondere für ihn ärgerlich, weil er wegen (angeblicher) Unterhaltszahlungen nunmehr Rückforderungen vom Jobcenter erhalten habe.
Das Standesamt, das zur datenschutzrechtlichen Bewertung der Angelegenheit vom TLfDI zur Stellungnahme aufgefordert wurde, teilte Folgendes mit:
Herr X habe vor ca. 28 Jahren (wohl im Geburtsjahr des Beschwerdeführers) beim Jugendamt die Vaterschaft zum Beschwerdeführer anerkannt. Die leibliche Mutter des Beschwerdeführers habe dieser Vaterschaftsanerkennung zeitnah zugestimmt, sodass die Vaterschaftsanerkennung als Randvermerk im Geburtenregister des Beschwerdeführers beigeschrieben wurde. In der Folge erscheine nach standesrechtlichen Vorschriften (§ 91 a Abs. 4 i. V. m. § 285 Abs. 1 Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden) Herr X als „amtlicher“ Vater auf der Geburtsur-

kunde des Beschwerdeführers. Im Wege der Amtshilfe wurden in einem Sozialverwaltungsverfahren die Angaben zum Vater des Beschwerdeführers (entsprechend der Geburtsurkunde) durch das Standesamt an das Jobcenter übersandt.
Diese Datenübermittlung hat der TLfDI gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz i. V. m. § 65 Personenstandsgesetz und § 20 Sozialgesetzbuch X für datenschutzrechtlich zulässig angesehen.

Der TLfDI ist nur zuständig für die Klärung der datenschutzrechtlichen Zulässigkeit der Datenübermittlung vom Standesamt an das Jobcenter. Die inhaltliche Prüfung, wer der „richtige“ Vater ist, wer wem in welcher Höhe Unterhalt zu zahlen hat, liegt nicht in seinem Zuständigkeitsbereich.

5.8 Heirat mit Nachteilen – Datenweitergabe des Standesamts Lauscha an das Jobcenter Suhl

Ein Bürger hat sich mit einer Beschwerde über sein Standesamt an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt. Nach seinen Angaben hat er vor seiner Hochzeit per E-Mail die für die Eheschließung erforderlichen Unterlagen (Abstammungsnachweise für sich und seine zukünftige Ehefrau) bei dem zuständigen Standesamt angefordert. Zu diesem Zeitpunkt war er nach seinen Angaben Hartz IV - Empfänger. Seine Ehefrau wohnte bis über den Termin der Eheschließung hinaus in einer eigenen Wohnung. Im Zusammenhang mit einem Widerspruchsverfahren (Widerspruch wegen der Höhe der bewilligten Kosten für Unterkunft und Heizung) hat er Kenntnis von der Weitergabe seiner Daten seitens des Standesamtes an das Jobcenter erlangt und bat den TLfDI um Unterstützung hinsichtlich der datenschutzrechtlichen Klärung der Angelegenheit.
Nach Angaben des Standesamtes wurde dem Jobcenter auf dessen Amtshilfeersuchen – dies wurde dem TLfDI vorgelegt – aber lediglich mitgeteilt, an welchem Tag der Beschwerdeführer die erforderlichen Unterlagen für seine Eheschließung beantragt hatte und auf welchem Weg dies geschehen ist. Demnach benötigte das Jobcenter im Rahmen seines Amtsermittlungsgrundsatzes im Widerspruchsverfahren die Information „Termin der Anforderung und der Ausstellung der zur Anmeldung der Eheschließung erforderlichen Unterla-

gen“, und zwar zur Prüfung, ob und gegebenenfalls nach welchem Zeitablauf den zukünftigen Eheleuten die Vermeidung einer Doppelmiete möglich und subjektiv zumutbar war.
Nach datenschutzrechtlicher Bewertung des Vorgangs hat der TLfDI dem Beschwerdeführer Folgendes mitgeteilt:
Die Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) nur zulässig, soweit das ThürDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Gemäß § 65 Abs. 1 Personenstandsgesetz aber sind Behörden auf Ersuchen Auskunft oder Einsicht in einen Registerauszug zu gewähren, soweit dies zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. Die Kenntnis des oben genannten Datums für das Jobcenter – nämlich zur Ermittlung der Anspruchsgrundlagen für Leistungen zur Sicherung des Lebensunterhaltes im Widerspruchsverfahren – hat auch der TLfDI als erforderlich und damit die Einhaltung der datenschutzrechtlichen Bestimmungen in der vom Beschwerdeführer vorgetragenen Angelegenheit als gegeben angesehen.

Angehende Eheleute, die Empfänger von Leistungen nach dem SGB II sind, müssen damit rechnen, dass Standesamtsdaten dem Jobcenter zur Kenntnis gegeben werden dürfen.

5.9 Kaffeekränzchen mit Neubürgern: Bitter bei Datenschutzverstoß

Der Bürgermeister einer Gemeinde wollte sich aus dem Melderegister eine namentliche Liste mit Bürgern, die im vergangenen Jahr in die Gemeinde zugezogen waren, erstellen lassen und diese Bürger zu einer Begrüßungsveranstaltung einladen.

Eine Verarbeitung – diese umfasst auch die Erhebung, Übermittlung und Nutzung personenbezogener Daten – ist aber nur zulässig, soweit das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Zulässigkeit der Datenübermittlung könnte sich zwar aus § 28 Abs. 8 Thüringer Meldegesetz (ThürMeldeG) ergeben. Danach dürfen innerhalb einer Gemeinde oder Verwaltungsgemeinschaft die in § 3 Abs. 1 ThürMeldeG aufgeführten Daten weitergegeben oder zur Einsichtnahme bereitgehalten werden, soweit dies zur

Aufgabenerfüllung der Meldebehörde oder des Empfängers erforderlich ist. Die Einladung der „Neubürger“ der Gemeinde zu einer Begrüßungsveranstaltung zählt aber nach Meinung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nicht zu den Aufgaben des Bürgermeisters, jedenfalls nicht gemäß den Bestimmungen der Thüringer Kommunalordnung.
Als datenschutzfreundliche Lösung wurde seitens des TLfDI eine entsprechende Information für alle „Neubürger“ im Internet, Amtsblatt und/oder der örtlichen Presse empfohlen. Für die folgenden Jahre wurde zudem vorgeschlagen, ein Informationsschreiben des Bürgermeisters jedem zur Neuanmeldung im Meldeamt erscheinenden Einwohner zu übergeben oder im Meldeamt auszulegen und die „Neubürger“ in diesem Schreiben bei Interesse an einer derartigen Veranstaltung um Rückäußerung an den Bürgermeister zu bitten. Davon abgesehen könnten „Neubürger“ bei der Anmeldung auch um ihre Einwilligung nach § 4 Abs. 3 ThürDSG zur Weitergabe ihrer Daten zu dem genannten Zweck gebeten werden.
Datenschutzrechtlich unbedenklich ist auch ein sogenanntes Adressmittlungsverfahren, das die Betroffenen weniger belastet. Der Bürgermeister müsste dafür der Meldebehörde die Anschreiben für die „Neubürger“ der Gemeinde übergeben. Die Adressierung und den Versand (bei entsprechender Kostenübernahme durch den Bürgermeister) würde die Meldebehörde übernehmen. Soweit die Betreffenden an Kaffee und Kuchen mit dem Bürgermeister interessiert wären, könnten sie dies dann selbstbestimmt durch eine entsprechende Rückinformation an den Bürgermeister zum Ausdruck bringen.

Ein Treffen von „Neubürgern“ der Gemeinde mit dem Bürgermeister muss nicht aus Datenschutzgründen ausfallen. Eine Übergabe von Melderegisterabfragen an den Bürgermeister bzw. dessen Datenerhebung ist für diesen Zweck allerdings datenschutzrechtlich unzulässig.

5.10 Kommunen als „verlängerter Arm“ von Steuerbehörden?

Die Kassen der Kommunen sind bekanntermaßen nicht besonders gut gefüllt. Sie sind daher immer auf der Suche nach weiteren Einnahmequellen. Eine solche ist die so genannte Bettensteuer, wie die Kulturförderabgabe umgangssprachlich genannt wird. Etliche Städte

in ganz Deutschland verlangten von den Hotels einen gewissen Prozentsatz des Übernachtungspreises als Abgabe. Das Bundesverwaltungsgericht stellte in seinem Urteil vom 11. November 2012, (Az. 9 CN 1/11, 9 CN 2/11) unter anderem klar, dass beruflich veranlasste Übernachtungen von einer Besteuerung auszunehmen sind. Damit war durch die Gemeinden, die Bettensteuer erheben, die Aufgabe zu lösen, wie festzustellen ist, ob ein Gast aus privaten oder beruflichen Gründen in einem Hotel übernachtet. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat die Erhebung von Daten zur Bestimmung einer solchen Steuer in Erfurt, Weimar, Eisenach, Suhl und Gera geprüft.

Einige der kommunalen Satzungen verpflichteten die Gäste, die beruflich zwingend in einem Beherbergungsbetrieb entgeltlich übernachten, dem Betreiber des Beherbergungsbetriebs zum Nachweis der zwingend beruflich erforderlichen Übernachtungen geeignete Unterlagen vorzulegen oder bei ihm eine Eigenbestätigung nach einem amtlich vorgeschriebenen Vordruck abzugeben.

Nach § 4 Thüringer Datenschutzgesetz (ThürDSG) ist die Verarbeitung – sie beinhaltet auch die Datenerhebung – personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine anderer Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Im Falle der Einwilligung (siehe dazu Hinweis unter Punkt 5.12) ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist (§ 4 Abs. 1 Satz 2 ThürDSG).

Gemäß § 6 Thüringer Kommunalabgabengesetz (ThürKAG) kann die Steuersatzung Dritte, die zwar selbst nicht Steuerschuldner sind, aber in engen rechtlichen oder wirtschaftlichen Beziehungen zum Steuergegenstand oder zu einem Sachverhalt stehen, an den die Steuerpflicht oder der Steuergegenstand anknüpft, verpflichten, die Steuer zu kassieren, abzuführen und Nachweis darüber zu führen, und ferner bestimmen, dass sie für die Steuer neben dem Steuerschuldner haften.

Jedoch darf die Steuer nur kassiert und abgeführt und über diese beiden Tätigkeiten ein Nachweis geführt werden. Unzulässig ist hingegen eine Prüfung, ob ein Betroffener der Steuerpflicht unterfällt oder nicht. Erkundigungen oder Nachforschungen seitens des Beherbergungsbetriebes bei Gästen oder gar Dritten sind unzulässig, da diese als "verlängerter Arm" der Steuerbehörde fungieren würden. In diesem Fall würde der Betreiber des Beherbergungsbetriebes als

Verarbeiter von Steuerdaten im Sinne des § 30 Abgabenordnung tätig werden. Hierfür fehlt es an der erforderlichen steuerrechtlichen Regelung, die dieses Vorgehen gestatten würde. Daher sind auch eine Erhebung und Speicherung der Daten des Arbeitgebers des Gastes oder sonstige weitere Einzelheiten nicht von § 6 ThürKAG gedeckt. Die Prüfung der Steuerpflicht an sich muss Aufgabe der Steuerbehörde bleiben. Zur Feststellung der Steuerpflicht reicht es aus, wenn der Gast lediglich Angaben dazu machen muss, ob er aus dienstlichem oder privatem Anlass in der Beherbergungsstätte übernachtet. Die Prüfung des Vorliegens der Tatbestandsvoraussetzungen obliegt dann der jeweiligen Stadt.
Im Ergebnis der datenschutzrechtlichen Prüfung wurde festgestellt, dass die satzungsrechtlichen Regelungen von Erfurt und Weimar den gesetzlichen Vorgaben entsprachen. Jedoch erfolgte in beiden Fällen die Information des Gastes zur Datenerhebung und den Folgen einer Auskunftsverweigerung nicht mit der gebotenen Transparenz.
Demgegenüber waren in Eisenach, Suhl und Gera Satzungsregelungen in Kraft, wonach die Gäste gezwungen waren, ohne Rechtsgrundlage oder qualifizierte Einwilligung personenbezogene Daten gegenüber den Beherbergungsbetrieben preiszugeben. Der TLfDI hat die festgestellten Datenschutzverstöße gemäß § 39 ThürDSG gegenüber den Stadtverwaltungen Eisenach, Suhl und Gera beanstandet und gefordert, die Beherbergungsbetriebe umgehend darüber in Kenntnis zu setzen, dass die beanstandete Datenerhebung bis auf weiteres zu unterbleiben hat. In der Folge sind die rechtswidrigen Satzungen des Städte Suhl und Gera außer Kraft gesetzt worden. Die Stadt Eisenach hat ihre Satzung datenschutzkonform gestaltet, und die Städte Erfurt und Weimar haben ihre Gästeinformation entsprechend den Hinweisen des TLfDI überarbeitet.

Eine Prüfung durch den Beherbergungsbetrieb, ob ein Gast der Steuerpflicht unterfällt, ist unzulässig. Erkundigungen oder Nachforschungen seitens des Beherbergungsbetriebes bei Gästen oder gar Dritten sind rechtswidrig, da der Beherbergungsbetrieb als "verlängerter Arm" der Steuerbehörde in Erscheinung treten würde.

5.11 Der Status "Soldat im Auslandseinsatz" schützt nicht vor berechtigten Forderungen eines Gläubigers

Ein Beschwerdeführer teilte dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit, dass bei seinem für ihn zuständigen Meldeamt wegen seines Status „Soldat im Auslandseinsatz“ eine Auskunftssperre zu seinen Meldedaten nach § 31 Abs. 7 Thüringer Meldegesetz (ThürMeldeG) eingetragen sei. Das Meldeamt hatte nach seiner Kenntnis die Anfrage eines Inkassounternehmens erhalten, das zu Zwecken der Eintreibung einer Forderung gegen ihn seine Anschrift erhalten wollte. Nach Angaben des Beschwerdeführers hatte er sich über dieses Inkassounternehmen informiert und befürchtete nun, dass seine Daten nicht nur zum Forderungseinzug, sondern auch für Werbezwecke verwendet werden könnten. Der Beschwerdeführer gab weiter zu bedenken, dass er infolge des „Eintrages seiner Daten“ bei diesem Inkassounternehmen „Briefe und Anrufe von diversen Firmen“ erhalten werde.
Grundsätzlich darf die Meldebehörde gemäß § 31 ThürMeldeG anfragenden Personen Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Einwohner erteilen (einfache Melderegisterauskunft). Hat die Meldebehörde auf Antrag oder von Amts wegen gemäß § 31 Abs. 7 Satz 1 ThürMeldeG eine Auskunftssperre für den Betroffenen im Melderegister eingetragen, ist eine Melderegisterauskunft unzulässig, es sei denn, dass nach Anhörung des Betroffenen eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen ausgeschlossen werden kann. Eine aus einem konkreten Anlass eingetragene Auskunftssperre (hier: Soldat im Auslandseinsatz) führt dabei nicht zwingend zu einer Verweigerung jedweder Melderegisterauskunft (so Medert/Süßmuth/Dette-Koch, Kommentar zum Melderecht des Bundes und der Länder, Erläuterung zu § 21 MRRG, Rn. 70a). Vielmehr greift danach eine im Hinblick auf eine konkrete Gefährdungslage bewilligte Auskunftssperre dann nicht mehr, wenn nach Anhörung des Betroffenen ausgeschlossen werden kann, dass das Auskunftsersuchen in Zusammenhang mit dem der Auskunftssperre zugrunde liegenden Sachverhalt steht. Die Anhörung des Betroffenen ist nach der genannten Kommentierung entbehrlich, wenn die Meldebehörde aufgrund der ihr vorliegenden Informationen ausschließen kann, dass eine Auskunft im konkreten Fall schutzwürdige Interessen des Betroffenen gefährden kann; dies wird insbesondere

bei glaubhaften Anfragen von Gläubigern oder Inkassounternehmen der Fall sein.
Nach Prüfung des Beschwerdesachverhaltes hat der TLfDI die Vorgehensweise des Meldeamtes – die Melderegisterauskunftserteilung trotz Vorliegens einer Auskunftssperre – für datenschutzrechtlich zulässig erklärt, wenn es sich beim Auskunftsbegehrenden um Gläubiger oder Inkassounternehmen handelt und eine Anhörung des Betroffenen wegen der genannten Gründe entbehrlich war (dem besagten Inkassounternehmen lagen nachweislich offene Geldforderungen vor, welche zur Klärung gebracht werden sollten).

Eingetragene Auskunftssperren im Melderegister sollen die Betroffenen schützen vor Gefahren für das Leben, für die Gesundheit und für ähnliche schutzwürdige Interessen. Wenn diese Gefahren aber ausgeschlossen werden können, darf ein Schuldner zur Begleichung seiner Schulden mit Unterstützung des Meldeamtes vom Gläubiger gefunden werden.

5.12 Schutz vor gefährlichen Tieren contra Datenschutz

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Eingabe eines Bürgers, mit der er bestimmte Angaben nach dem Thüringer Gesetz zum Schutz der Bevölkerung vor Tiergefahren hinterfragte. In diesem Zusammenhang teilte er dem TLfDI mit, dass von dem zuständigen Ordnungsamt der Verwaltungsgemeinschaft Mittleres Schwarzatal Formulare mit dem Titel „Angaben über die Haltung eines Hundes“ versandt würden, in denen unter anderem die Kennzeichnung des Hundes mit einem Mikro-Chip, die entsprechende Mikro-Chip-Nummer, das Datum der Markierung sowie die Anschrift und der Name des Tierarztes angegeben werden müsse. Außerdem werde eine Kopie des Versicherungsscheins als Nachweis einer Haftpflichtversicherung verlangt, welche bei dem Ordnungsamt verbleiben soll.
Auf Nachfrage des TLfDI berief sich die Ordnungsbehörde Mittleres Schwarzatal auf § 2 Abs. 4 des Thüringer Gesetzes zum Schutz der Bevölkerung vor Tiergefahren (TierGefG). Demnach ist der Halter eines Hundes verpflichtet, den Hund auf seine Kosten dauerhaft und unverwechselbar mit einem fälschungssicheren lesbaren Transponder nach ISO-Standard (Mikrochip) durch einen Tierarzt kennzeich-

nen zu lassen. Der Halter hat der zuständigen Behörde die Kennzeichnung anzuzeigen. Die zuständige Behörde darf die gespeicherten Daten im Rahmen der Erfüllung ihrer Aufgaben nach diesem Gesetz zur Feststellung der Person des Halters nutzen. Außerdem ist vorgesehen, dass das für das Ordnungsrecht zuständige Ministerium im Einvernehmen mit dem für Tierschutz und Tiergesundheit zuständigen Ministerium durch Rechtsverordnung die Art und Weise der Kennzeichnung sowie die Verwendung der personenbezogenen Daten des Hundehalters regelt.

Eine solche Regelung durch Rechtsverordnung ist bislang nicht getroffen worden. Insoweit musste ergänzend auf die Rechtsvorschriften des Thüringer Datenschutzgesetzes (ThürDSG) zurückgegriffen werden, denn die das Tier betreffenden Angaben in Verbindung mit den Angaben zum Hundehalter sind insgesamt als personenbezogene Daten des Hundehalters anzusehen.

Nach § 4 ThürDSG ist die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn eine Rechtsvorschrift dies konkret regelt oder der Betroffene eingewilligt hat. Eine konkrete Regelung, welche Daten durch die Ordnungsbehörde verarbeitet werden dürfen, ist allerdings im Thüringer Gesetz zum Schutz der Bevölkerung vor Tiergefahren nicht enthalten. Daher besteht das Problem, dass die Aufgaben zwar durch die kommunalen Stellen zu erfüllen sind, aber nur die ganz konkret hierfür erforderlichen Daten verarbeitet werden dürfen.

Gemäß § 19 Abs. 1 in Verbindung mit § 20 Abs. 1 ThürDSG ist die Verarbeitung personenbezogener Daten zulässig, wenn dies zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle (hier: des Ordnungsamtes) liegenden Aufgabe erforderlich ist.

Die Angaben zur Mikrochip-Nummer und das Datum der Markierung wurden seitens des TLfDI, um dem Nachweis aus § 2 Abs. 4 TierGefG gerecht zu werden, für erforderlich erachtet.

Datenschutzrechtlich problematisch ist jedoch der Verbleib des Versicherungsnachweises bei dem zuständigen Ordnungsamt. Zu den Angaben zur Versicherung ist in § 2 Abs. 5 TierGefG lediglich der Abschluss einer entsprechenden Versicherung anzuzeigen. Dies bedeutet, dass eine Kopie des Versicherungsscheins zum Verbleib bei der Behörde nicht verlangt werden kann. Der TLfDI hat daher darauf hingewirkt, dass kein Nachweis als Anlage beizufügen ist, sondern ein Nachweis nur zur Einsicht vorgelegt werden kann.

Auch wenn das Gesetz vorschreibt, dass die Kennzeichnung durch einen Tierarzt zu erfolgen hat, hält der TLfDI die unfreiwillige Angabe zum behandelnden Tierarzt für unzulässig. Probleme ergeben sich hierbei auch dann, wenn das Tier vor Inkrafttreten des oben genannten Gesetzes bereits mit einem Mikrochip versehen wurde und der vornehmende Tierarzt unter Umständen nicht (mehr) bekannt ist.
Die Ordnungsbehörde Mittleres Schwarzatal ist dem Vorschlag des TLfDI gefolgt und hat die Angabe zum durchführenden Tierarzt als eine freiwillige Angabe in das Formular „Angaben über die Haltung eines Hundes“ aufgenommen. Außerdem wird es künftig seitens des Ordnungsamtes als ausreichend erachtet, wenn der Nachweis der Versicherung dem Ordnungsamt zu Einsicht vorgelegt wird.

Allgemeiner Hinweis zu Einwilligungserklärungen:

Eine Einwilligungserklärung muss den Vorgaben des § 4 Abs. 3 ThürDSG entsprechen.
Die Einwilligung ist als Zulässigkeitsvoraussetzung für die Verarbeitung und Nutzung personenbezogener Daten nur solange tauglich, wie der Betroffene auch tatsächlich die Möglichkeit hat, selbst darüber zu bestimmen, ob und unter welchen Bedingungen seine personenbezogenen Daten verarbeitet und genutzt werden. Sein Selbstbestimmungsrecht tatsächlich ausüben kann der Betroffene jedoch nur, wenn er über den vorgesehenen Zweck der Verarbeitung oder Nutzung informiert ist.
Außerdem muss er darüber informiert werden, ob die Verweigerung seiner Einwilligung für ihn nachteilige Folgen hat und gegebenenfalls welche Folgen eintreten können. Die Einwilligung bedarf der Schriftform oder der elektronischen Form mit einer qualifizierten elektronischen Signatur. Soweit die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt wird, muss sie im äußeren Erscheinungsbild der Erklärung hervorgehoben werden.

5.13 Meldescheinkopien nehmen kein gutes Ende

Ein Betreiber einer Pension in der Kurstadt Bad Salzungen hat dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mitgeteilt, dass er auf Verlangen der Stadtverwaltung Bad Salzungen quartalsweise sämtliche in seiner Obhut

befindliche Meldescheine in Kopie (die unter anderem auch die Privatadressen von Dienstreisenden enthalten) zur Überprüfung des Kurbeitrages an die Stadtverwaltung auszuhändigen habe. Der Pensionsbetreiber bat den TLfDI um datenschutzrechtliche Überprüfung der Angelegenheit.
Der TLfDI forderte daraufhin zunächst bei der Stadtverwaltung die für eine Prüfung erforderlichen Unterlagen an. Dies waren unter anderem der aktuelle Meldeschein, die Satzung für die Erhebung des Kurbeitrages, Hinweis- bzw. Merkblätter der Stadtverwaltung für die Leiter der Beherbergungsstätten sowie Vordrucke für die Beherbergungsstätten zur Abrechnung des Kurbeitrages. Nach seiner datenschutzrechtlichen Prüfung teilte der TLfDI der Stadtverwaltung Folgendes mit:
Personen, die in einer Beherbergungsstätte für nicht länger als zwei Monate aufgenommen werden, haben gemäß § 24 Abs. 2 Thüringer Meldegesetz (ThürMeldeG) am Tag ihrer Ankunft einen besonderen Meldeschein nach § 25 Abs. 2 ThürMeldeG handschriftlich auszufüllen und zu unterschreiben. Für Zwecke der Erhebung des Kurbeitrags nach § 9 Thüringer Kommunalabgabengesetz (ThürKAG) dürfen gemäß § 25 Abs. 3 ThürMeldeG die erforderlichen Angaben erhoben und verarbeitet sowie Durchschriften der besonderen Meldescheine gefertigt werden. Nach § 38 Abs. 1 Nr. 3 ThürMeldeG ist das für das Meldewesen zuständige Ministerium ermächtigt, durch Rechtsverordnung die Muster dieser Meldescheine zu bestimmen. Die Vordrucksmuster (vergleiche dazu § 26 Anlagen 9, 10, 10 a und 10 b ThürMeldeVO) erfüllen die datenschutzrechtlichen Bestimmungen dahingehend, dass mit ihnen nur solche Daten erhoben und insbesondere auch an die jeweilige Kommune übermittelt werden, die zur Aufgabenerfüllung in den Kommunen (Abrechnung der Kurbeiträge) erforderlich sind. Da die Vordrucke zur Vereinfachung im Durchschreibeverfahren gestaltet sind, wurden in diesen die für die Abführung des Kurbeitrages nicht notwendigen Angaben jeweils geschwärzt.

Eine Gemeinde, in der Kurbeiträge erhoben werden, kann entscheiden, ob bei ihr unter Verwendung der genannten Muster (§ 26 Anlagen 10, 10 a und 10 b ThürMeldeVO) mit dem Meldeschein auch die Kurbeiträge abgerechnet werden sollen oder, ob alternativ Anlage 9 als Meldeschein verwendet und zur Erhebung des Kurbeitrages ein gesondertes Verfahren genutzt wird. Im letzt-

genannten Fall ist darauf zu achten, dass die Datenerhebung und -verarbeitung auf das zur Aufgabenerfüllung erforderliche Maß beschränkt bleibt. Zudem bedarf es als Ermächtigungsgrundlage einer Satzung (§ 9 i. V. m. § 2 Abs. 1 ThürKAG).
Diese für alle Kommunen durch Rechtsvorschrift verbindlich geregelte Verfahrensweise wurde aber von der Stadtverwaltung nicht eingehalten. Weder die verwendeten Meldescheine noch die in der Satzung enthaltenen Formulierungen (z. B., dass die vollständig ausgefüllten Meldeformulare bei der Stadtverwaltung abzugeben sind) entsprachen den gesetzlichen Vorgaben im ThürMeldeG und der ThürMeldeVO.
Der TLfDI hat die Stadtverwaltung aufgefordert, das Verfahren und die Satzung kurzfristig den geltenden Rechtsvorschriften anzupassen – insbesondere auch auf die Verarbeitung der unzulässig erhobenen Daten zu verzichten und diese zu löschen.
Die Stadtverwaltung hat daraufhin den TLfDI informiert, dass die Gestaltung des Meldescheines neu und datenschutzgerecht veranlasst worden sei und dem TLfDI einen Entwurf des neuen Meldescheines sowie den Entwurf einer entsprechend den Forderungen des TLfDI abgeänderten Kurbeitragssatzung zur Verfügung gestellt.
Nachdem der TLfDI diese Änderungen dem Pensionsbetreiber mitgeteilt hatte, konnte er diese Angelegenheit zur datenschutzrechtlichen Zufriedenheit aller Beteiligten abschließen.

Möchte eine Kommune bei der Erhebung von Kurbeiträgen das „Rad nicht (datenschutzgerecht) neu erfinden“, bietet sich an, von geprüften Vordruckmustern (§ 26 Anlagen 9, 10, 10 a und 10 b ThürMeldeVO) Gebrauch zu machen.

5.14 1000 Greizer

Im Berichtszeitraum hat sich ein Greizer Bürger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt und darüber beschwert, dass er (und – seinen Angaben nach – „1000 ausgewählte Greizer Bürger“) einen Fragebogen vom Stadtmarketing Greiz e. V. zugesandt bekommen haben. Laut Veröffentlichung in der „Ostthüringer Zeitung“ habe der Vorsitzende des Vereins mehrfach mitgeteilt, dass diese Bürger per Zufallsgenerator ausgewählt worden seien. Der Beschwerdeführer fragte sich nun, wie der Verein an die Adressen der Bürger gelangt war, ob

diese Adressdaten noch gespeichert sind und wer die Aufbewahrung / Vernichtung der Adressdatensätze überwacht.
Der mit der Befragung beauftragte Verein hatte die Adressen der mittels Zufallsgenerator ausgewählten Bürger als Adressaufkleber von der Stadtverwaltung Greiz erhalten. Diese Adressaufkleber in Papierform enthielten die Namen, Vornamen sowie die postalischen Anschriften der Bürger. Nach Mitteilung der Stadtverwaltung Greiz wurde der Stadtmarketing Greiz e. V. mit Stadtratsbeschluss beauftragt, ein Tourismus- und Marketingkonzept für die Stadt Greiz zu erarbeiten. Die besagte Bürgerbefragung sei Teil dieses Konzeptes und somit im öffentlichen Auftrag erfolgt und liege im öffentlichen Interesse. Die Stadtverwaltung habe dem Stadtmarketing Greiz e V. im Rahmen einer Gruppenauskunft aus dem Melderegister 1000 Datensätze mit dem Inhalt „Vorname; Familienname. Anschrift“ als Adressaufkleber mit der Maßgabe zur Verfügung gestellt, die übermittelten Daten (Adressaufkleber) ausschließlich und einmalig für die Bürgerbefragung im Rahmen des Tourismus- und Marketingkonzeptes zu verwenden und nicht an Dritte weiter zu geben. Nach Angaben der Stadtverwaltung wurde durch entsprechende Filter im Melderegister programmtechnisch sichergestellt, dass im Verfahren keine Meldedaten Minderjähriger zur Verfügung gestellt sowie die im Melderegister eingetragenen Widersprüche gegen eine Melderegisterauskunft bei der Abfrage der 1000 Datensätze berücksichtigt wurden.
Eine Verarbeitung, diese umfasst auch die Übermittlung, und Nutzung personenbezogener Daten ist nur zulässig, soweit das Thüringer Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat, § 4 Abs. 1 Thüringer Datenschutzgesetz. Gemäß § 31 Abs. 5 Thüringer Meldegesetz (ThürMeldeG) darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) erteilt werden, wenn sie im öffentlichen Interesse liegt. Unter anderem dürfen Familiennamen, Vornamen, Doktorgrad und Anschriften mitgeteilt werden. Der TLfDI hat die Übermittlung der 1000 Datensätze gemäß § 31 Abs. 5 ThürMeldeG für datenschutzrechtlich zulässig angesehen. Er hat aber die Stadtverwaltung aufgefordert, in zukünftigen Fällen das sogenannte Adressmittlungsverfahren zu wählen, das die Betroffenen datenschutzrechtlich weniger belastet. Der Verein müsste dafür der Meldebehörde die Anschreiben für die 1000 Bürgerin-

nen und Bürger der Gemeinde übergeben. Die Adressierung und den Versand (bei entsprechender Kostenübernahme durch den Verein) würde die Meldebehörde übernehmen. Soweit die Betreffenden an der Teilnahme an der Befragung durch den Stadtmarketing Greiz e. V. interessiert wären, könnten sie dies dann selbstbestimmt durch eine entsprechende Rückinformation an den Verein zum Ausdruck bringen.

Über das Ergebnis der datenschutzrechtlichen Prüfung hat der TLfDI gleichlautend auch den Beschwerdeführer informiert.
Melderegisterauskünfte sind gemäß den Bestimmungen des Thüringer Meldegesetzes in einer Vielzahl von Fällen möglich und damit datenschutzrechtlich grundsätzlich nicht zu beanstanden. Im Sinne des Datenschutzes ist allerdings ein Adressmittlungsverfahren vorzugswürdig.

5.15 Bitte keine zwangsweise Familienzusammenführung! Zu den Voraussetzungen der Einwilligung in die Verarbeitung und Nutzung personenbezogener Daten

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde über das Stadtarchiv Erfurt.
Ein Beschwerdeführer hatte sich mit Fragen zu seiner Abstammung (Daten seiner lebenden und verstorbenen Halbgeschwister unter anderem Personen und deren Namen und Geburts- bzw. Sterbedaten) an das Stadtarchiv gewandt, eine Weitergabe seiner Adresse und Telefonnummer dem Stadtarchiv aber ausdrücklich untersagt. Im Anschluss daran ist er jedoch von einer weiblichen Person angerufen worden, die sich als seine Halbschwester ausgegeben und über personenbezogene Daten von ihm verfügt hat, sodass der Beschwerdeführer einen nicht datenschutzgerechten Umgang mit seinen Daten im Stadtarchiv Erfurt vermutete.
Nach Angaben des Stadtarchivs hatte der Beschwerdeführer erst telefonisch, später per Post um Auskunft gebeten, insbesondere über seine Halbgeschwister. Nachdem eine Beschäftigte des Stadtarchivs Angaben zur Familie und auch zu den Halbgeschwistern ermittelt hatte, teilte sie dem Beschwerdeführer telefonisch mit, dass Halbgeschwister zwar ermittelt worden seien, ihm über diese aus datenschutzrechtlichen Gründen aber keine Auskunft erteilt werden kön-

ne. Um in solchen Fällen überhaupt eine Verbindungsaufnahme zu ermöglichen, trete das Stadtarchiv Erfurt jeweils mit dem ermittelten Halbbruder bzw. der Halbschwester in Verbindung und teile die Erreichbarkeit der suchenden Person mit, damit sich der Halbbruder bzw. die Halbschwester bei Interesse mit der suchenden Person in Verbindung setzen könne. Dagegen hätte der Beschwerdeführer am Telefon keinen Einwand erhoben. Diese Vorgehensweise sei ihm dann auch zusätzlich schriftlich dargestellt worden. Nachdem die Beschäftigte des Stadtarchivs Erfurt mit einer Halbschwester des Beschwerdeführers telefoniert hatte, sprach diese Halbschwester selbst im Stadtarchiv vor, um Genaueres über die verwandtschaftlichen Verhältnisse zu erfahren. Am Tag darauf ging im Stadtarchiv Erfurt ein zweites Schreiben des Beschwerdeführers ein, in dem er in einer Fußnote ausdrücklich untersagt hatte, die aus seinem oben genannten Schreiben an das Stadtarchiv hervorgehenden Daten weiterzugeben. Zu diesem Zeitpunkt war, wie dargestellt, die Kontaktaufnahme jedoch bereits erfolgt.
Eine Einwilligung des Betroffenen zur Verarbeitung seiner personenbezogenen Daten bedarf gemäß § 4 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG) der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Hier wurde dem TLfDI von Seiten des Stadtarchivs aber schlüssig dargelegt, dass das Stadtarchiv von einer – wenn auch nur auf der Grundlage eines mündlich erteilten Einverständnisses – Rechtmäßigkeit der Übermittlung der Kontaktdaten des Beschwerdeführers an seine Halbschwester ausgegangen ist. Im Ergebnis hat der TLfDI das Stadtarchiv Erfurt aufgefordert, zur Vermeidung derartiger Fälle zukünftig noch sorgsamer mit den personenbezogenen Daten der Betroffenen umzugehen und zum Nachvollzug der Einwilligungen diese nur in Schriftform einzuholen. Das Stadtarchiv hat in Auswertung dieses Vorfalls für die Beschäftigten des Stadtarchivs Erfurt verfügt, dass bei künftigen Suchen nach nahen Verwandten erforderliche Einverständniserklärungen zur Weitergabe personenbezogener Daten nur noch schriftlich erfolgen dürfen.

Die Vermittlung von Familienzusammenführungen muss sich innerhalb der durch den Datenschutz festgelegten Grenzen bewegen. Einwilligungserklärungen bedürfen grundsätzlich der Schriftform.

5.16 Innenminister versus Antikorruptionsbeauftragter

Einer Pressemeldung vom 11. Januar 2013 war zu entnehmen, dass der Antikorruptionsbeauftragte im Thüringer Innenministerium (TIM) (dort im Bereich Leitstelle Innenrevision der Landesregierung) einen Bericht über mögliche Unregelmäßigkeiten im Zusammenhang mit der Übernahme der E.ON-Anteile erstellt hatte. Dieser wurde der Pressemitteilung zufolge dem Thüringer Landesverwaltungsamt als zuständige Rechtsaufsichtsbehörde für die E.ON-Übernahme übergeben. Der Antikorruptionsbeauftragte des TIMs ist zugleich der Leiter der Leitstelle Innenrevision. Da im Rahmen der Korruptionsbekämpfung in der Regel auch personenbezogene Daten von Bediensteten verarbeitet werden, ging der TLfDI davon aus, dass der Bericht Personenbezug aufwies. Da auch Presseanfragen beim TLfDI hierzu eingegangen waren, bat der TLfDI das TIM um kurzfristige Stellungnahme, auf welcher Rechtsgrundlage der angesprochene Bericht angefertigt und dem Thüringer Landesverwaltungsamt übermittelt worden sei.
Als mögliche Rechtsgrundlage für die Übermittlungsbefugnis des Antikorruptionsbeauftragten wurde Ziffer 3 Abs. 3 der Richtlinie zur Korruptionsbekämpfung durch das TIM angeführt. Demnach ist die Leitstelle nicht nur eine Ansprechstelle für Behördenbeschäftigten, sondern auch für Bürgerinnen und Bürger bei Korruptionshinweisen. Sie prüft die Hinweise auf Stichhaltigkeit und leitet sie, soweit sie nicht offensichtlich unbegründet sind, an den Antikorruptionsbeauftragten in dem jeweiligen Geschäftsbereich weiter.
Zuvor hatte der Thüringer Innenminister aber in diversen Presseartikeln die Auffassung vertreten, dass der Antikorruptionsbeauftragte des TIMs ohne Rechtsgrundlage gehandelt habe.
Aufgrund der gegensätzlichen Aussagen bat der TLfDI das TIM um erneute Stellungnahme. Außerdem forderte der TLfDI das TIM in einer weiteren Anfrage dazu auf, den in Rede stehenden Bericht an den TLfDI zu übersenden.
Nach abschließender datenschutzrechtlicher Prüfung dieses Berichts hat der TLfDI festgestellt, dass die Regelungen der Richtlinie zur Korruptionsbekämpfung eingehalten wurden. Aus datenschutzrechtlicher Sicht hat der TLfDI daher den Vorgang nicht beanstandet.

Der Antikorruptionsbeauftrage wird gemäß Ziffer 5 der Richtlinie zur Korruptionsbekämpfung vom jeweiligen Behördenleiter bestellt

und abberufen. Seine Aufgabe ist die Unterstützung der Behördenleitung in ihrer Steuerungs- und Entscheidungsfunktion sowie die Verhütung und Aufdeckung von Korruptionsfällen. Seine Prüfungen haben neben einer kontrollierenden vornehmlich eine unterstützende, beratende sowie präventive Funktion. Bei der Prüfung und Wertung von Sachverhalten ist der Antikorruptionsbeauftragte unabhängig und unterliegt hinsichtlich Art und Umfang der Prüfungsaufgaben unmittelbar den Weisungen des Behördenleiters.
Der Antikorruptionsbeauftragte ist gemäß Ziffer 3 Abs. 3 der Richtlinie zur Korruptionsbekämpfung befugt, Korruptionshinweise, die nicht offensichtlich unbegründet sind, an den Antikorruptionsbeauftragten des jeweiligen Geschäftsbereiches weiterzuleiten.

5.17 Lieferung von Obdachlosen-Gesundheitsdaten frei Haus?

Aufgrund eines Hinweises erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis, dass die Stadt Arnstadt personenbezogene Daten der Bewohner einer Obdachloseneinrichtung in Arnstadt unzulässigerweise an Dritte übermittelt hat. Die Stadt Arnstadt hatte geplant, die Obdachloseneinrichtung in eine andere Trägerschaft zu überführen und hierzu ein Interessenbekundungsverfahren durchgeführt. Nach Abschluss dieses Verfahrens hatte nur eine Einrichtung Interesse zur Übernahme der Trägerschaft signalisiert. Um sich einen Überblick über die Obdachloseneinrichtung zu verschaffen, forderte der potenzielle Träger Gesundheitsdaten bzw. Krankenbilder der Bewohner an. Obwohl der behördliche Datenschutzbeauftragte empfohlen hatte, die geforderten Daten zu anonymisieren oder zumindest zu pseudonymisieren, hatte die Stadt sich auf Drängen des potenziellen Trägers entschlossen, eine namentliche Aufstellung an diesen weiterzuleiten. Übermittelt wurde eine Tabelle mit Daten der Einwohner, in der sich auch Angaben über ihren Gesundheitszustand befanden. Bei den übermittelten Daten handelt es sich um Gesundheitsdaten und damit um nach § 4 Abs. 5 Thüringer Datenschutzgesetz (ThürDSG) besonders geschützte Daten. Das Verarbeiten und Nutzen derartiger Daten ist nur unter sehr strengen Voraussetzungen zulässig. Keine der waren im vorliegenden Fall gegeben. Der TLfDI beanstandete daher nach § 39 Abs. 1 Satz 1 ThürDSG die Übermittlung an den potenziellen künftigen Träger der Obdachloseneinrichtung und forderte die Stadt auf, den Empfänger dieser Daten unver-

züglich darüber zu informieren, dass die Übermittlung widerrechtlich erfolgte. Dieser sollte durch die Stadt aufgefordert werden, die Daten unverzüglich zu löschen. Außerdem sollten die Beschäftigten der Stadt Arnstadt in geeigneter Weise informiert werden. Die Stadt hat zwischenzeitlich die Forderungen des TLfDI umgesetzt.

An die Übermittlung von besonderen Arten von Daten, unter die auch Gesundheitsdaten fallen, sind erhöhte Anforderungen zu stellen. Auch wenn ein Dritter nachvollziehbare Gründe dafür darlegt, warum er diese Daten benötigt, dürfen sie nur unter den in § 4 Abs. 5 ThürDSG genannten engen Voraussetzungen übermittelt werden.

5.18 Videoüberwachung der Beschäftigten durch die Suhler Stadtwirtschaft GmbH: Videogaga 3

Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ging eine Beschwerde über die Suhler Stadtbetrieb GmbH ein. Vorgetragen wurde, dass das Unternehmen Videokameras ohne Wissen der Beschäftigten betreibt, um die Beschäftigten auszuspionieren. Der Geschäftsführer habe in einer Betriebsversammlung Videoaufzeichnungen von den Beschäftigten vorgeführt und ausgewertet. Daraufhin führte der TLfDI eine Vor-Ort-Kontrolle der Videoüberwachung auf dem Betriebsgelände durch.
Zwar handelt es sich bei der Suhler Stadtbetrieb GmbH um eine öffentliche Stelle nach dem Thüringer Datenschutzgesetz (ThürDSG). Da sie jedoch mit anderen Unternehmen im Wettbewerb steht, sind auf sie weitestgehend die Vorschriften des Bundesdatenschutzgesetzes (BDSG) anwendbar, § 26 ThürDSG. Die datenschutzrechtliche Zulässigkeit der Videoüberwachung richtet sich daher nach § 6 b BDSG. Bei dem Betriebsgelände handelt es sich um öffentlich-zugänglichen Raum, da das Gelände während der Betriebszeiten von Kunden betreten und befahren werden kann, die Abfall anliefern.
Bei der Kontrolle wurde festgestellt, dass auf dem Betriebsgelände acht Videokameras installiert waren, von denen lediglich fünf betriebsbereit waren. Die Kunden fahren mit dem gelieferten Abfall zunächst auf eine große Waage. Eine Kamera, die lediglich Lifebilder lieferte und nicht aufzeichnete, diente dazu, dem Waagepersonal

die Sichtbewertung von angelieferten Materialien vorzunehmen. Die übrigen Kameras sind nur außerhalb der Öffnungszeiten des Betriebes eingeschaltet und zeichnen auf. Als Grund hierfür wurde angegeben, dass es immer wieder zu Diebstählen und Sachbeschädigungen auf dem Gelände gekommen sei. Es existiert eine Dienstanweisung zum Umgang mit der Videoüberwachung, die allerdings die tatsächlichen Gegebenheiten in dem Betrieb nicht ganz korrekt wiederspiegelte. Sie enthält Löschfristen sowie Festlegungen dazu, wer die Bilddaten in welchem Fall auswerten darf. Bei den Videoaufzeichnungen, die bei einer Betriebsversammlung gezeigt worden seien, habe es sich um eine Videoaufnahme auf einer DVD gehandelt, die dem Betrieb durch eine Privatperson zugespielt worden sei. Diese Person habe wahrscheinlich von einem Balkon aus in der Nähe des Betriebshofes gefilmt und die Aufnahmen dem Betrieb unter Hinweis auf die Untätigkeit der dort Beschäftigten anonym zugesandt.
Die Verhältnisse, die der TLfDI vor Ort vorfand, waren datenschutzrechtlich nicht zu beanstanden. Während der Öffnungszeiten des Geländes wurde lediglich eine Videobeobachtung durchgeführt, die der Sicherung der Betriebsabläufe diente. Die Aufzeichnung außerhalb der Öffnungszeiten des Betriebsgeländes begegnete keinen datenschutzrechtlichen Bedenken, da durch sie keine Beschäftigten an ihrem Arbeitsplatz überwacht werden. Nicht zulässig war das Auswerten der übersandten Video-DVD in der Betriebsversammlung. Die von dem unbekannten Dritten erstellten Videoaufnahmen wurden personenbezogen durch die verantwortliche Stelle ausgewertet und Dritten zur Kenntnis gegeben, ohne dass es hierfür eine Rechtsgrundlage gegeben hätte. Die DVD hätte unverzüglich vernichtet werden müssen. Dies wurde dem Betrieb mitgeteilt. Auf Verlangen des TLfDI wurde zudem die Dienstanweisung nochmals überarbeitet und an die tatsächlichen Verhältnisse vor Ort angepasst.

Videoaufzeichnungen dürfen nicht zur Leistungskontrolle der Beschäftigten heran gezogen werden. Dies gilt auch für solche Aufzeichnungen, die dem Arbeitgeber durch Dritte übermittelt werden.

5.19 Keine Drohnen im Rechtsstaat: Videogaga 4

Aufgrund einer Beschwerde eines Bürgers der Stadt Heilbad Heiligenstadt recherchierte der Thüringer Landesbeauftrage für den Da-

tenschutz und die Informationsfreiheit (TLfDI) im Amtsblatt Nr. 13/2013 vom 27. Juni 2013 der Stadt Heilbad Heiligenstadt. Dem Amtsblatt war zu entnehmen, dass die Stadtverwaltung beabsichtigte, eine ferngesteuerte Drohne mit acht Propellerarmen (Oktokopter) einzusetzen, die während eines Fluges Videos mit einer Auflösung von 36 Megapixeln aufnehmen oder fotografieren könne. Die Drohne sollte vielfältig genutzt werden, so z. B. auch zur Inspektion für Neubaugebiete und der Fertigung von Aufnahmen bei Veranstaltungen.

Daraufhin forderte der TLfDI die Stadtverwaltung auf, mitzuteilen, zu welchem Zweck die drohnengestützten Bildaufnahmen insbesondere von Neubaugebieten und Veranstaltungen durchgeführt werden sollten und auf welcher Rechtsgrundlage diese Maßnahmen beruhten. Zugleich bat der TLfDI um Auskunft darüber, welche technisch-organisatorischen Maßnahmen in diesem Zusammenhang vorgesehen sind, um bei den geplanten Einsatzszenarien datenschutzrechtliche Bestimmungen einzuhalten. In diesem Zusammenhang forderte der TLfDI auch die zu Grunde zu legenden Regelungen (Dienstanweisungen) an.

Daraufhin warnte der TLfDI in einer Presseerklärung vor einem massiven Eingriff in die Privatsphäre der Bürgerinnen und Bürger im Zusammenhang mit Flugdrohnen, deren Einsatz aus datenschutzrechtlicher Sicht grundsätzlich unzulässig ist. Insbesondere ist es durch derartige Luftbildaufnahmen nicht ausgeschlossen, dass auch private Gärten, Balkone, Wohnsiedlungen und Schwimmbäder in das Visier der Drohne gelangen und so personenbezogene Daten gesammelt werden. Dies erweckt den Anschein, als würde eine Kommune „Geheimdienstmethoden“ anwenden, gegen die sich die Bürgerinnen und Bürger nur schwer zur Wehr setzen können. Eine solche Überwachung über den Dächern Thüringens muss daher bereits in ihren Anfängen gestoppt werden. Die grundsätzliche Unzulässigkeit des Einsatzes von Flugdrohnen ergibt sich aus § 4 Abs. 1 Thüringer Datenschutzgesetz, wonach die Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig ist, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene hierin eingewilligt hat. Keine dieser Voraussetzungen liegt im Falle einer Datenerhebung mittels solcher Flugdrohnen vor.

Daraufhin teilte der Bürgermeister der Stadt Heilbad Heiligenstadt schließlich mit, dass die Stadt noch keine Kameradrohne besitze und

auch nicht beabsichtige, eine solche anzuschaffen. Ebenso wenig solle eine Kameradrohne angemietet werden.

Der Einsatz von Kameradrohnen zur Inspektion von Wohngebieten stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger ohne Rechtsgrundlage dar und wäre gemäß § 39 Thüringer Datenschutzgesetz zu beanstanden.

5.20 Fremdenverkehrssatzung – „Die Dritte“

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte die Unzulässigkeit der an einen Unternehmer gerichteten Forderung der Verwaltungsgemeinschaft Rennsteig, den Jahresumsatz seines Produktionsunternehmens zur Berechnung der Fremdenverkehrsabgabe anzugeben, festgestellt und zweimal beanstandet, 8. (Punkt 5.7) und 9. (Punkt 5.8) Tätigkeitsbericht des TLfD. In der Folge hatte die Kommunalaufsicht des Landratsamtes Ilm-Kreis erklärt, dass sie ein rechtsaufsichtliches Vorgehen dahingehend, der Verwaltungsgemeinschaft Rennsteig eine Anwendung der Fremdenverkehrsbeitragssatzung der Gemeinde Schmiedefeld am Rennsteig gegenüber dem Beschwerdeführer zu untersagen, für nicht durchsetzbar ansehe. Das daraufhin eingeschaltete Thüringer Landesverwaltungsamt teilte zwar die rechtliche Wertung des TLfDI, allerdings habe sich die Kommunalaufsicht bei vertretbaren Entscheidungen der Gemeinde mit Aufsichtsmitteln zurückzuhalten, da dem Betroffenen grundsätzlich der Rechtsweg nach Art. 19 Grundgesetz offen stehe und die Möglichkeiten zur Klage Vorrang vor einem aufsichtlichen Eingreifen gebühre.
Das Thüringer Datenschutzgesetz (ThürDSG) sieht in § 39 Abs. 2 vor, dass der TLfDI, wenn die Beanstandung nicht behoben wird, von der für die Sicherstellung des Datenschutzes nach § 34 ThürDSG verantwortlichen Stelle und der Aufsichtsbehörde binnen angemessener Frist geeignete Maßnahmen fordert. Diese Bestimmung würde ins Leere laufen, wenn die Aufsichtsbehörde, zumal wenn sie die Rechtsauffassung des TLfDI teilt, nicht Maßnahmen zu Beseitigung der rechtswidrigen Zustände trifft. Im vorliegenden Fall hätte dies bedeutet, der Verwaltungsgemeinschaft Rennsteig zu untersagen, Umsätze des fraglichen Unternehmens aufgrund der Fremdenverkehrssatzung weiterhin zu erheben.

Daher hatte sich der TLfDI an das Thüringer Innenministerium (TIM) als oberste Aufsichtsbehörde gewandt, um die weitere Zusammenarbeit mit den Kommunalaufsichtsbehörden in Thüringen gesetzeskonform auszurichten. Wie das TIM hierzu unter anderem mitteilte, beschränke sich die staatliche Aufsicht in den Angelegenheiten des eigenen Wirkungskreises, wie im Falle der Erhebung der Fremdenverkehrsabgabe, auf die reine Rechtskontrolle; Eingriffe in das Verwaltungsermessen ständen ihr nicht zu. Nach Auffassung Kommunalaufsicht des Landratsamtes Ilm-Kreis sei die maßgebliche abgaberechtliche Frage, ob dem Produktionsbetrieb des Beschwerdeführers durch den Fremdenverkehr im Gemeindegebiet mittelbare wirtschaftliche Vorteile in Sinne der Fremdenverkehrsbeitragssatzung erwachsen, nicht eindeutig zu beantworten. Da der Beschwerdeführer von seinem Klagerecht gegen den Abgabenbescheid keinen Gebrauch gemacht habe und keine Thüringer Rechtsprechung zur Definition des „Vorteils" nach der Fremdenverkehrsbeitragssatzung bekannt sei, lägen auch keine eindeutigen Anhaltspunkte dafür vor, dass die Rechtsauffassung der zuständigen Behörden nicht vertretbar wäre. Lediglich ein verwaltungsgerichtliches Verfahren hätte in diesem Fall Klarheit ergeben. Da nach der Bewertung der zuständigen Behörden der Anwendungsbereich der Fremdenverkehrsbeitragssatzung eröffnet sei, habe auch die nach § 4 ThürDSG erforderliche Rechtsvorschrift vorgelegen, die eine Datenverarbeitung und -nutzung erlaubte. Schließlich habe die Kommunalaufsicht des Landratsamtes Ilm-Kreis mitgeteilt, dass der Betrieb des Beschwerdeführers im Jahre 2009 für das Jahr 2008 mit Null Euro letztmalig veranlagt worden sei. Gleichwohl zeigt dieser Fall einen datenschutzrechtlich bedenklichen Werdegang auf. Wirkliche Abhilfe würde nur eine Anordnungsbefugnis des TLfDI gegenüber Behörden im ThürDSG oder im Rahmen der vorgesehenen EU-Datenschutzgrundverordnung schaffen.

Es ist zu hoffen, dass das Datenschutzrecht um weitere aufsichtsrechtliche Befugnisse ergänzt wird, die geeignet sind, dass Datenschutzbehörden eine Aufsichtsfunktion künftig auch gegenüber öffentlichen Stellen wahrnehmen können.

5.21 Übermittlung von Grundstückseigentümerdaten an Dritte

Insbesondere Firmen, die sich für bestimmte private Grundstücke interessieren, erhalten auf Anfrage aus dem Thüringer Landesamt für Vermessung und Geoinformation (TLVermGeo) bzw. einer der acht Außenstellen der Behörde personenbezogene Daten zu den jeweiligen Grundstückseigentümern. Hin und wieder fragen betroffene Grundstückseigentümer beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob diese Datenübermittlungen aus datenschutzrechtlicher Sicht zulässig sind.
Die Grundstückeigentümer werden dann auf die Regelungen des § 18 Abs. 2 Thüringer Vermessungs- und Geoinformationsgesetz verwiesen, wonach *„die Einsicht in die Namen, die Geburtsdaten und die Anschriften sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zustehen, die ein berechtigtes Interesse an der Kenntnis der Daten haben und soweit überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Entsprechendes gilt für Daten der Bevollmächtigten. Das berechtigte Interesse ist darzulegen. Die Empfänger dürfen diese Daten nur für den Zweck nutzen, der das berechtigte Interesse begründet und zu dessen Erfüllung die betreffenden Daten übermittelt wurden.“*
Aufgrund dieser Rechtsvorschrift muss das TLVermGeo zunächst prüfen, ob ein berechtigtes Interesse bei der anfragenden Stelle bzw. Person vorliegt. Das „berechtigte Interesse“ ist ein unbestimmter Rechtsbegriff. Hierunter wird im allgemeinen jedes Interesse verstanden, dass *„sich aus vernünftigen Überlegungen ergibt und die vorgesehene Datenverwendung und der damit verfolgte Zweck im Einklang mit der Rechtsordnung stehen. In diesem Rahmen kommen sowohl ideelle als auch wirtschaftliche Interessen in Betracht.“* (Dammann, in: Simitis, Bundesdatenschutzgesetz, zu § 16, Rdnr. 17 f.) Darüber hinaus ist aber auch das schutzwürdige Interesse des Grundstückseigentümers am Ausschluss der Übermittlung zu prüfen. Die Belästigung durch die Zusendung von Werbeschriften oder Kaufinteressen wird als geringfügige Beeinträchtigungen bei der Betrachtung des schutzwürdigen Interesses angesehen (Dammann aaO., Rdnr. 22). Im Ergebnis sind deshalb solche Übermittlungen erlaubt.
Allerdings prüft das TLVermGeo das berechtigte Interesse für jedes einzelne der Daten, die grundsätzlich übermittelt werden dürfen. Bei

einem Kauf- oder einem Werbeinteresse werden daher lediglich der Name und die Anschrift des Eigentümers übermittelt.

Es ist dem TLVermGeo erlaubt, bestimmte Daten des Grundstückseigentümers an Dritte zu übermitteln, wenn diese ein berechtigtes Interesse glaubhaft machen und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Dabei ist der Umfang der zulässigen Datenübermittlung festzulegen.

5.22 Erfurter Streetview

Mit diesem Titel lassen sich die Beschwerden auf den Punkt bringen, die den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten. Hintergrund war, dass die Stadt Erfurt den Zustand ihrer Straßen erfassen wollte. Aufgrund der Größe der Stadt schied nach deren Mitteilung eine Begehung durch Personen aus, sodass die Straßenzustandserfassung durch einen mit moderner Technik ausgestatteten Kamerawagen erfolgen sollte. Dabei sollten Fotos gefertigt werden, die den Zustand der Straßenverkehrsanlagen dokumentieren. Das Verfahren war für die Vermögensbewertung im Rahmen der für den Jahresanfang 2013 geplanten Einführung der doppelten Buchführung notwendig. Zum anderen wurden die Angaben auch für die fachliche Arbeit der Erhaltung der Verkehrssicherheit der öffentlichen Straßen benötigt. Die Stadt Erfurt beauftragte nach Ausschreibung eine private Firma mit der Befahrung der Straßen. Dabei sind auf einem Transporter verschiedene Kameras fest installiert. Solange der Übertragungswagen durch normal breite Straßen fuhr, wurden nur Fotos von der Straße und den Gehwegen aufgenommen. In schmaleren Straßen war jedoch auch die Aufnahme von Privatgrundstücken möglich. Zusätzlich ist das Fahrzeug mit so genannten Laserscannern ausgestattet, die die Längsebenheit und die Querebenheit der Straße erfassen. Bei diesem Verfahren werden keine personenbezogenen Daten erhoben.
Anders jedoch bei den Bildern, die die Kamera macht. Hier werden auf den Fotos unter Umständen auch Fahrzeuge, die auf den Straßen fahren, abgebildet sowie Personen, die sich auf dem Gehweg befinden. Außerdem werden möglicherweise Vorgärten und darin befindliche Personen erfasst. Nach § 19 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden

Stellen erforderlich ist. Vorliegend lag die Problematik darin, dass alle Erkenntnisse außerhalb des Straßenraums für die Aufgabenwahrnehmung der Stadt nicht erforderlich waren.
Die Stadt teilte mit, dass die Bilder nach Abschluss der Befahrung durch die private Firma der Stadtverwaltung Erfurt übergeben und dann dort für weitere Zwecke gespeichert würden. Aufgrund der Vielzahl der erstellten Fotos (520.000 Bilder) sei der Aufwand einer manuellen Nachbearbeitung sämtlicher gespeicherten Fotos unangemessen hoch und nicht leistbar. Die Fotos würden durch die private Firma vollständig an die Stadtverwaltung übergeben und dürfen nur durch die Stadt verwendet werden.
Das zuständige Amt hat auf Anregung des TLfDI durch Dienstanweisung geregelt, dass die Übermittlung von Bildaufnahmen oder Bildausdrucken an Dritte, das heißt andere Stellen innerhalb der Stadtverwaltung bzw. die Veröffentlichung nur zulässig ist, wenn die auf den Bildaufnahmen enthaltenen personenbezogenen Daten durch geeignete Maßnahmen unkenntlich gemacht worden sind, z. B. durch das Auspixeln oder Radieren der entsprechenden Stellen mit einem Fotobearbeitungsprogramm. Auch innerhalb der Stadtverwaltung dürfen die auf den Fotos befindlichen personenbezogenen Daten nicht genutzt werden. Weiterhin wurden alle Aufnahmen, in denen von einem überwiegenden Interesse der betroffenen Grundstückseigentümer auszugehen ist, etwa weil überwiegend kein öffentlicher Verkehrsgrund abgebildet ist, gelöscht. Bei Straßen, deren Verkehrsraumbreite sechs Meter unterschritt, wurden die Seitenkameras deaktiviert und mit einem Magnetschild an beiden Seiten des Messfahrzeugs darauf hingewiesen, dass die Seitenkameras außer Betrieb genommen sind und tatsächlich nicht aufzeichnen.
Die betroffenen Grundstückseigentümer wurden im Amtsblatt der Landeshauptstadt Erfurt darüber informiert, dass sie ein Widerspruchsrecht in Bezug auf Fotografien von ihrem Grundstück haben. Im Falle eines Widerspruchs sind die betreffenden Fotos so zu bearbeiten, dass ausschließlich Verkehrsanlagen erkennbar sind.

Bei der Erstellung von Fotos durch oder im Auftrag von öffentlichen Stellen können immer auch personenbezogene Daten erhoben werden. Dies ist in aller Regel nicht zur Aufgabenerfüllung erforderlich und damit unzulässig. Die öffentliche Stelle hat Vorkehrungen zu veranlassen, dass solche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung unterbleiben.

5.23 Rechtmäßige Befragung der Nachbarn?

Wie eine Beschwerdeführerin den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) informierte, waren ohne ihre Einwilligung und ihre vorherige Kenntnis ihre Nachbarn von Beschäftigten der Stadtverwaltung Bad Sulza zu ihren Lebensgewohnheiten befragt worden.
Die Stadtverwaltung teilte auf entsprechende Anfrage des TLfDI mit, dass eine örtliche Ermittlung erforderlich gewesen sei, da gegenteilige Informationen bezüglich des Datums „Anschrift der Beschwerdeführerin“ vorgelegen hätten. Bei der örtlichen Ermittlung sei es nicht um die Erforschung der Lebensgewohnheiten der Betroffenen, sondern um die Klärung des Meldeverhältnisses der Beschwerdeführerin gegangen.
Gemäß § 10 Abs. 2 Thüringer Meldegesetz (ThürMeldeG) ist die Meldebehörde verpflichtet, bei konkreten Anhaltspunkten für die Unrichtigkeit oder Unvollständigkeit des Melderegisters bezüglich namentlich bekannter Einwohner den Sachverhalt von Amts wegen zu ermitteln. Mit dieser Regelung ist es den Meldebehörden möglich, auf eindeutiger Rechtsgrundlage namentlich benannte Einwohner und deren Meldeverhältnisse zu überprüfen. Ob Meldedaten unrichtig sind, bestimmt sich dabei aber ausschließlich nach objektiven Kriterien. Nach der einschlägigen Kommentarliteratur reichen jedenfalls Vermutungen oder bloße Hinweise, dass Daten unrichtig sein könnten, als „konkrete Anhaltspunkte“ für die Unrichtigkeit des Melderegisters nicht aus. Im vorliegenden Fall lagen der Meldebehörde der Stadtverwaltung mündliche und mehrmalige schriftliche Hinweise der Gemeinde vor, nach denen sich die Beschwerdeführerin nicht mehr in der Gemeinde aufhalten sollte und der Bürgermeister der betreffenden Gemeinde Berichtigung des Melderegisters bezüglich des Datums „Anschrift der Beschwerdeführerin“ verlangte. Nach mündlichem und erstmaligem schriftlichen Hinweis der Gemeinde hinsichtlich der vermeintlichen – die Beschwerdeführerin betreffende – Unrichtigkeit des Melderegisters wurde seitens der Meldebehörde lediglich telefonisch bei der Beschwerdeführerin zum Sachverhalt nachgefragt. Nach erneutem schriftlichem Hinweis der Gemeinde wurde die Beschwerdeführerin in der Meldebehörde in einem persönlichen Gespräch zum Sachstand befragt. In diesem konnte die Angelegenheit nicht zweifelsfrei geklärt werden, zudem

lag in Folge ein nochmaliger Hinweis der Gemeinde vor, sodass Anhaltspunkte für die Unrichtigkeit des Melderegisters vorlagen und seitens der Meldebehörde eine Ermittlung (Prüfung der Beschriftung des Briefkastens sowie des Klingelschildes der Beschwerdeführerin und Nachbarbefragung) vor Ort in der Gemeinde erfolgte.
Obwohl der TLfDI bei konkreter Annahme der Unrichtigkeit des Melderegisters eine Überprüfung der Zustellmöglichkeit an den betroffenen Meldepflichtigen zur Bestätigung der Richtigkeit des Melderegisters für ausreichend erachtet, wurde die hier stattgefundene Befragung von Nachbarn seitens der Meldebehörde wegen der wiederholten Hinweise der Gemeinde mit der steten Bitte um jeweils erneute Prüfung des Melderegisters als datenschutzrechtlich zulässig angesehen. Der TLfDI hat der Meldebehörde aber für zukünftige derartige Fälle empfohlen, auf Nachbarbefragungen zu verzichten und zur Bestätigung der Richtigkeit des Melderegisters lediglich auf die Prüfung der Zustellmöglichkeit an den betroffenen Meldepflichtigen abzustellen.
Das Ergebnis der datenschutzrechtlichen Prüfung der Beschwerde teilte der TLfDI der Beschwerdeführerin mit. Der seitens der Beschwerdeführerin geäußerten Bitte zur Übersendung des Schriftverkehrs des TLfDI mit der Stadtverwaltung Bad Sulza ist der TLfDI mangels Rechtsgrundlage aber nicht nachgekommen. Gemäß § 13 Abs. 1 Thüringer Datenschutzgesetz hat die Daten verarbeitende Stelle (TLfDI) dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung sowie die Herkunft der Daten zu erteilen. Dies gilt aber nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle gespeichert sind.

Eine Meldebehörde hat erst bei konkreten Anhaltspunkten für die Unrichtigkeit oder Unvollständigkeit des Melderegisters den Sachverhalt von Amts wegen zu ermitteln.

5.24 Datenübermittlung: Für Eltern zu viel des Guten

Im Amtsblatt einer Verwaltungsgemeinschaft wurde über den Umbau des Kindergartens in einer Mitgliedsgemeinde berichtet. Da diese Darstellung aus Sicht eines Elternpaares unzutreffende Aussagen enthielt, erstellten sie ihren eigenen Bericht und übermittelten ihn der Verwaltungsgemeinschaft mit der Bitte um Veröffentlichung

im Amtsblatt. Dies wurde von der Verwaltungsgemeinschaft abgelehnt. In einem Elternabend des Kindergartens, zu dem die Verfasser des Berichts nicht geladen waren, verlas die Bürgermeisterin der betroffenen Gemeinde den Bericht unter Nennung der Namen der Verfasser.

Die Betroffenen fragten daraufhin beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an, ob die Weitergabe des Berichts von der Verwaltungsgemeinschaft an die Bürgermeisterin und deren Verhalten auf dem Elternabend rechtens gewesen sei.

Der TLfDI bat die Bürgermeisterin um Stellungnahme und wies darauf hin, dass bei der Nennung der Verfasser personenbezogene Daten der Betroffenen an Dritte übermittelt wurden. Dies ist nach § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift das erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Bürgermeisterin teilte mit, dass ihr der Bericht vom Verwaltungsleiter zur Kenntnis übergeben wurde. In der Annahme, dass der Verfasser den Artikel im Amtsblatt öffentlich bekannt machen wollte, habe sie im besagten Elternabend diesen den Eltern zur Kenntnis gegeben. Sie war davon ausgegangen, dass die Übermittlung an den Bürgermeister zur Aufgabenerfüllung der Verwaltungsgemeinschaft erforderlich war. Für die Weitergabe an die Eltern liegt aber keine Rechtsgrundlage vor. Diese Weitergabe ist zur Aufgabenerfüllung nicht erforderlich. Auch fehlte es an der Einwilligung der Verfasser zum Offenbaren der Daten. Das Vorgehen ist daher ein Verstoß gegen datenschutzrechtliche Bestimmungen.

Die Bürgermeisterin bedauerte ihre Vorgehensweise und den Verstoß gegen datenschutzrechtliche Bestimmungen. Sie war davon ausgegangen, dass der Bericht veröffentlicht werden sollte und hat ihn somit den anderen Eltern an dem besagten Elternabend zur Kenntnis gegeben. Der TLfDI teilte der Bürgermeisterin mit, dass sie sich künftig in ähnlichen Fällen ausdrücklich bei den Betroffenen zu versichern hat, ob diese die Offenbarung ihrer personenbezogenen bzw. personenbeziehbaren Daten wünschen.

Personenbezogene Daten dürfen von der Verwaltung an Dritte außerhalb der öffentlichen Verwaltung nur mit Rechtsgrundlage oder mit ausdrücklicher Einwilligung der Betroffenen bei Vorliegen der

Voraussetzungen des § 4 Abs. 1 Satz 2 ThürDSG übermittelt werden.

5.25 Kaufvertragsabschluss nur mit „Bürgerentscheid“

Der Bürgermeister der Stadt Bad Sulza wollte beim Verkauf eines gemeindlichen Grundstücks auf Nummer sicher gehen. Er teilte die Namen der Kaufinteressenten und die Vorgeschichte des jeweiligen Kaufantrages mit personenbezogenen Daten ohne Einwilligung der Betroffenen in Form eines Rundbriefs an die Einwohner des Ortsteils Sonnendorf mit. Die Einwohner von Sonnendorf wurden aufgefordert, ihre Auffassung zu der Kaufabsicht der Interessenten der Stadtverwaltung mitzuteilen.
Hierbei handelt es sich sowohl um eine Übermittlung als auch um eine Erhebung von personenbezogenen Daten. Beides ist nach § 4 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.
Da sowohl die oben genannte Übermittlung als auch die Datenerhebung mittels einer Befragung ohne Rechtsgrundlage und Einwilligung der Betroffenen erfolgte, lag ein Verstoß gegen datenschutzrechtliche Bestimmungen vor. Daher hat der TLfDI eine Beanstandung gemäß § 39 ThürDSG ausgesprochen.

Die Erhebung und Übermittlung personenbezogener Daten durch Kommunen ist, auch in Form von Umfragen, nur dann zulässig, wenn das ThürDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat und die Voraussetzungen des § 4 Abs. 1 Satz 2 ThürDSG vorliegen.

5.26 Bleibt der Informant anonym?

Immer wieder fragen öffentliche Stellen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), ob der Betroffene im Verfahren wissen darf, wer ihn angezeigt hat. Nach § 4 Thüringer Datenschutzgesetz (ThürDSG) ist eine Verarbeitung und damit auch eine Übermittlung (§ 3 Abs. 3 ThürDSG) personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Wenn, wie im Regelfall, eine Einwilligung nicht vorliegt, muss eine

Rechtsvorschrift die Information des Betroffenen über den Anzeigenden zulassen.
Hier ist nach der Art des Verfahrens zu unterscheiden. Im normalen Verwaltungsverfahren besteht das Recht auf Akteneinsicht, § 29 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG). Nach § 29 Abs. 1 ThürVwVfG hat die Behörde dem Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gewähren, soweit deren Kenntnis zur Geltendmachung oder Verteidigung seiner rechtlichen Interessen erforderlich ist. Dieses Recht steht nur am Verfahren Beteiligten zu. Sie müssen ein rechtliches Interesse nachweisen, das immer dann gegeben ist, wenn die Einsichtnahme bezweckt, eine tatsächliche Unsicherheit über ein Rechtsverhältnis zu klären, ein rechtlich relevantes Verhalten nach dem Ergebnis der Einsichtnahme zu regeln oder eine gesicherte Grundlage für die Verfolgung eines Anspruchs zu erhalten. Die Einsichtnahme ist aber nur soweit zu gewähren, wie sie für die Geltendmachung der rechtlichen Interessen erforderlich ist. Dies ist im Einzelfall zu prüfen. Für die Gewährung der Akteneinsicht reicht es aus, dass das geltend gemachte rechtliche Interesse bei überschlägiger Prüfung nicht offensichtlich rechtsmissbräuchlich wahrgenommen wird und ohne die Kenntnis der Identität des Anzeigeerstatters eine Beeinträchtigung rechtlicher Interessen möglich erscheint. Der Betroffene muss beispielsweise wissen, wer ihn angezeigt hat, um gegebenenfalls gegen den Anzeigenden rechtliche Ansprüche geltend zu machen, beispielsweise, um sich gegen eine mögliche Verleumdung zu wenden.
Keine Verpflichtung zur Gewährung der Akteneinsicht besteht nach § 29 Abs. 2 ThürVwVfG insbesondere dann, soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der am Verfahren Beteiligten oder dritter Personen, geheim gehalten werden müssen.
Im Ordnungswidrigkeitenverfahren ist das Recht auf Akteneinsicht des Betroffenen in § 49 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) speziell geregelt. Danach kann die Verwaltungsbehörde dem Betroffenen Einsicht in die Akten unter Aufsicht gewähren, soweit nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Dies ist von Amts wegen zu prüfen. Die Verfolgungsbehörde hat einen Ermessensspielraum, ob sie den Namen und die Anschrift des Zeugen bzw. Anzeigenden in Ordnungswidrigkeitenverfahren angibt oder dies unterlässt. Hierbei hat sie das Datenschutzinteresse des Zeugen gegen das Informationsinteresse des Betroffenen abzu-

wägen. Hier gelten die gleichen Grundsätze wie zu § 29 ThürVwVfG. Ein zu erwartendes Bußgeld setzt in aller Regel die Kenntnis der Zeugen voraus. Im Bußgeldverfahren ist es deshalb erforderlich, dass im Anhörungsschreiben der Name und der Wohnort des Zeugen benannt werden. Auf die Angabe der vollständigen Anschrift des Zeugen kann allerdings verzichtet werden. Auf Anfrage oder durch Akteneinsichtnahme steht sie jedoch dem Betroffenen zur Verfügung. Die Abwägung zwischen den datenschutzrechtlichen Interessen der Zeugen und dem Informationsinteresse der Betroffenen führt in diesem Fall zur Zurückstellung der Zeugenbelange. Zeugen müssen hinnehmen, dass der angezeigten Person ihre Identifikationsdaten (Name und Wohnort) sowie der Gegenstand der Zeugenaussage bekannt werden. Ausnahmen hiervon sind hier nur bei besonderer Schutzbedürftigkeit der Zeugen zu machen. Wenn Anhaltspunkte dafür vorliegen, dass der Beschuldigte gewaltsam reagieren könnte oder bei besonderer Schutzbedürftigkeit des Zeugen, ist das Recht auf Akteneinsicht zu verwehren und von der damit verbundenen Offenbarung personenbezogener Daten des Anzeigeerstalters bzw. Zeugen abzusehen.

Außerhalb des Verwaltungs- bzw. Ordnungswidrigkeitenverfahrens gibt § 13 ThürDSG den Betroffenen ein Auskunfts- und Akteneinsichtsrecht. Danach hat die datenverarbeitende Stelle dem Betroffenen auf Antrag Auskunft über die zu seiner Person verarbeiteten Daten und auf deren Herkunft zu erteilen. Nach § 13 Abs. 5 ThürDSG unterbleibt die Auskunftserteilung und Akteneinsicht, soweit die personenbezogenen Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Auch hier gelten die oben bereits dargelegten Grundsätze.

Bei Vorliegen eines Ersuchens nach dem Thüringer Informationsfreiheitsgesetz (ThürIFG) ist zu beachten, dass der Anzeigeerstatter immer Drittbetroffener ist, der nach den Verfahrensvorschriften des ThürIFG in das Verfahren einzubeziehen ist. Die Behörde hat dann nach § 6 Abs. 4 Satz 3 ThürIFG zu prüfen, ob dem Auskunftsersuchen schutzwürdige Belange des Anzeigeerstatters entgegenstehen und ob das Interesse des Antragstellers an der Kenntnis der Identität des Anzeigeerstatters dessen Geheimhaltungsinteresse übersteigt.

Der Name des Anzeigeerstatters darf an den Betroffenen nicht ohne rechtliche Prüfung herausgegeben werden. Im Verwaltungsverfahren

muss die Kenntnis der Identität des Anzeigeerstatters für die Wahrnehmung eigener Rechte erforderlich sein; im Ordnungswidrigkeitenverfahren und beim Verfahren nach dem ThürIFG dürfen keine überwiegenden schutzwürdigen Interessen Dritter entgegenstehen.

5.27 Liveübertragung von Sitzungen des Stadtrates im Internet: Video 5

Nach derzeitiger Rechtslage ist eine Videoübertragung von Stadtratssitzungen im Internet sowohl durch die Kommune selbst als auch in ihrem Auftrag – hierbei bleibt die Kommune die verantwortliche Stelle gemäß § 8 Thüringer Datenschutzgesetz (ThürDSG) – mangels einer geeigneten spezialgesetzlichen Rechtsgrundlage als unzulässig anzusehen. Sie würde mithin einen Verstoß gegen datenschutzrechtliche Vorschriften darstellen. Die hierfür maßgeblichen Gründe legte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits im 8. (Punkt 5.3) und 9. Tätigkeitsbericht (Punkt 5.2) ausführlich dar. Bei der Veröffentlichung von Livemitschnitten der Ratssitzungen im Internet handelt es sich aufgrund der Möglichkeit, weltweit Einsicht nehmen zu können, um eine Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes, deren Zulässigkeit nach § 23 ThürDSG zu beurteilen ist. Eine solche Übermittlung ist gemäß § 23 Abs. 1 Satz 3 ThürDSG jedoch nur zulässig, wenn ein angemessenes Datenschutzniveau gewährleistet ist. Daran fehlt es jedoch regelmäßig, da die Veröffentlichung immer auch in Staaten erfolgt, die kein angemessenes Datenschutzniveau besitzen. Im Ergebnis ist nach der augenblicklichen Rechtslage die datenschutzrechtliche Zulässigkeit für die Veröffentlichung von Filmaufnahmen im Internet nicht gegeben.
Dieser Rechtsauffassung widersprach die Thüringer Landesregierung in ihrer Stellungnahme zum 9. Tätigkeitsbericht des TLfDI unter anderem wie folgt:
Der Europäische Gerichtshof (EuGH) habe in der sog. Lindqvist-Entscheidung (Urteil vom 6. November 2003, Az.: C – 101/01) angenommen, dass keine Übermittlung von Daten in ein Drittland im Sinne von Art. 25 der EG-Datenschutzrichtlinie vorliegt, wenn eine sich in einem Mitgliedsstaat aufhaltende Person in eine Internetseite, die bei ihrem in demselben oder einem anderen Mitgliedsstaat ansässigen Provider gespeichert ist, personenbezogene Daten aufnimmt

und diese damit jeder Person, auch in Drittländern, zugänglich macht. Diese Argumentation ist jedoch für öffentliche Stellen in Thüringen nicht anwendbar, da das ThürDSG im Unterschied zur EG-Datenschutzrichtlinie eine ausdrückliche Definition des Begriffs „übermitteln“ enthält. Nach § 3 Abs. 3 Nr. 4 ThürDSG handelt es sich dabei um die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an Dritte in der Weise, dass die Daten durch die Daten verarbeitende Stelle an den Dritten weitergegeben werden oder der Dritte von der Daten verarbeitenden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder dort abruft. Da eine Übermittlung von Daten gegeben ist, wenn der Dritte die Daten einsieht oder abruft, ist festzustellen, dass die Definition des ThürDSG ausdrücklich auch das Einstellen in das Internet umfasst. Somit ist davon auszugehen, dass der Bewertungsmaßstab des § 23 ThürDSG, aus dem die Unzulässigkeit der Internetveröffentlichung von Stadtratssitzungen letztlich abgeleitet wird, anzuwenden ist.

Weiterhin vertrat die Landesregierung die Auffassung, dass der Gemeinderat auch eine weitergehende Öffentlichkeit mittels Übertragung öffentlicher Gemeinderatssitzungen im Internet herstellen kann. Dem ist jedoch aus folgenden Gründen nicht zuzustimmen:

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 kleine-

ren 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 BVerwG 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 des Thüringer Kommunalrechts, 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 im Jahre 2013 einen Gesetzentwurf zur Änderung der Thüringer Kommunalordnung zwecks Verbesserung der Transparenz von Gemeinderatssitzungen ausgearbeitet. Diesen Gesetzentwurf hat er an die Fraktionen des Thüringer Landtags zur Prüfung weitergegeben. Derzeit ist jedoch nicht absehbar, ob und wann die parlamentarische Befassung mit dieser Angelegenheit abgeschlossen sein wird.

Der Gesetzentwurf orientiert 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 Livemitschnitt 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 Stadtratsmitglieder, 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“.

Nach gegenwärtiger Rechtslage ist die Veröffentlichung von Livemitschnitten von Ratssitzungen sowohl durch die Kommune selbst als auch im Auftrag der Kommune datenschutzrechtlich unzulässig. Jedoch sind in eigener Verantwortung handelnde Medienunternehmen unter der Voraussetzung, dass das Persönlichkeitsrecht der bei der Sitzung anwesenden Personen nicht durch die Berichterstattung beeinträchtigt wird, berechtigt, von öffentlichen Stadtratssitzungen in Bild und Ton zu berichten. Unter diesen Voraussetzungen ist auch ein Livemitschnitt einer öffentlichen Stadtratssitzung im Internet als zulässig anzusehen. Die Stadt Erfurt hat diese Voraussetzungen in der Geschäftsordnung des Stadtrates datenschutzrechtskonform konkretisiert.

5.28 Zuviel Information für Fraktionsvorsitzende in Suhl

Nach einem Passus der Geschäftsordnung des Stadtrats Suhl sollten die Sitzungsniederschriften sowohl vom öffentlichen als auch vom nicht-öffentlichen Teil der Sitzung den Fraktionsvorsitzenden zugeleitet werden. Nach § 42 Thüringer Kommunalordnung (ThürKO) ist eine Weitergabe der Abschriften von Beschlüssen und Niederschriften aus nicht-öffentlichen Sitzungen unzulässig. Die Niederschriften öffentlicher und nicht-öffentlicher Sitzungen können jedoch gemäß § 42 Abs. 2 Satz 1 ThürKO durch die Mitglieder des Gemeinderats jederzeit eingesehen werden. Abschriften können aber nach der eindeutigen Gesetzeslage nur über die Niederschriften öffentlicher Sitzungen erteilt werden. Von dieser gesetzlichen Vorgabe darf eine rechtlich niederrangigere Geschäftsordnung auch nicht zugunsten der Fraktionsvorsitzenden etwa wegen eines effizienteren Arbeitens abweichen. Daher verstieß die Weitergabe von Kopien der vollstän-

digen Niederschriften einschließlich des nicht-öffentlichen Teils gegen das Gesetz (Uckel/Hauth/Hoffmann § 42, Anm. 3, S. 118) und der betreffende Passus der Geschäftsordnung des Stadtrats Suhl war missverständlich bzw. rechtswidrig. Da die Niederschriften über nicht-öffentliche Sitzungen im Zweifel immer auch personenbezogene Daten enthalten, hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gefordert, die Geschäftsordnung des Stadtrats Suhl zu überarbeiten. Dies hat der Stadtrat abgelehnt. Daher hat der TLfDI die rechtswidrige Regelung der Geschäftsordnung des Stadtrates Suhl bzw. die rechtswidrige Umsetzung dieser Regelung durch die Stadtverwaltung gem. § 39 Thüringer Datenschutzgesetz beanstandet und eine rechtskonforme Änderung der Geschäftsordnung gefordert. Dem Stadtrat wurde eine entsprechend den gesetzlichen Vorgaben geänderte Geschäftsordnung zur Beschlussfassung vorgelegt, die aber durch den Stadtrat abgelehnt wurde. Der Oberbürgermeister der Stadt Suhl hat den ablehnenden Beschluss des Stadtrats beanstandet und außer Vollzug gesetzt. Der Oberbürgermeister hat sich daraufhin an die Rechtsaufsichtsbehörde gewandt. Das dortige Verfahren ist noch nicht abgeschlossen.

Von einer gesetzlichen Vorschrift darf eine Geschäftsordnung keine abweichende Regelung treffen. Eine Weitergabe von Kopien der Niederschriften des nicht-öffentlichen Teils einer Stadtratssitzung stellt einen Gesetzesverstoß dar.

5.29 Vorsicht beim Versand von Unterlagen für Stadtratssitzungen

Ein Stadtratsmitglied bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Mitteilung, welche rechtlichen Bestimmungen der Übersendung aller Sitzungsunterlagen für öffentliche sowie nicht-öffentliche Stadtratssitzungen per E-Mail entgegenstehen. Dem Stadtratsmitglied wurde zunächst mitgeteilt, dass eine Weitergabe von Abschriften von Beschlüssen und Niederschriften aus nicht-öffentlichen Sitzungen nach § 42 der Thüringer Kommunalordnung (ThürKO) unzulässig ist. Die Niederschriften öffentlicher und nicht-öffentlicher Sitzungen können nach § 42 Abs. 2 Satz 1 ThürKO durch die Mitglieder des Stadtrates jederzeit eingesehen werden. *Abschriften* können nach dem Gesetz aber nur über die Niederschriften *öffentlicher* Sitzungen erteilt wer-

den. Somit verstößt eine Weitergabe von Kopien der vollständigen Niederschriften einschließlich des nicht-öffentlichen Teils gegen das Gesetz (Uckel/Hauth/Hoffmann/Noll, Kommunalrecht in Thüringen, Anm. 3 zu § 42 ThürKO).
Gemäß § 9 Thüringer Datenschutzgesetz (ThürDSG) muss bei der Übermittlung insbesondere die Vertraulichkeit und Integrität der personenbezogenen Daten gewährleistet sein. Daher sollten Mitteilungen mit sensiblen personenbezogenen bzw. geheimhaltungsbedürftigen Daten nicht unverschlüsselt per E-Mail versandt werden, da es sich bei E-Mailversand nicht um ein sicheres Medium handelt. Eine datenschutzgerechte Kommunikation kann erreicht werden, indem der Text oder die Anlage in der E-Mail mittels eines sicheren Verschlüsselungsverfahrens verschlüsselt übertragen oder aber solche Dokumente auf dem Postverkehrsweg verschickt werden.

Eine Weitergabe der Abschriften von Beschlüssen und Niederschriften aus nicht-öffentlichen Stadtratssitzungen ist nach § 42 ThürKO unzulässig.
Mitteilungen mit personenbezogenen Daten sind nicht unverschlüsselt per E-Mail zu versenden, da der E-Mailversand kein sicheres Medium ist.

5.30 „Hunger“ auf Gewerbedaten – innerhalb der Behörde erlaubt?

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) hatte ein Landratsamt folgende Fragen zur Beurteilung vorgelegt:
1. Dürfen die Grunddaten gem. § 14 Abs. 5 Gewerbeordnung (GewO) Name/Firma, Tätigkeit und Anschrift innerhalb eines Landratsamtes vom Gewerbeamt an die Wirtschaftsförderung übermittelt werden?
Zunächst war festzustellen, dass die thematisierte Übermittlung von personenbezogenen Gewerbedaten mit einer Zweckänderung verbunden ist. Gemäß § 21 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist eine Übermittlung personenbezogener Daten an andere öffentliche Stellen 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 zulassen würden. Das Speichern, Verändern oder Nutzen von Daten für andere Zwecke ist zulässig, wenn eine

Rechtsvorschrift dies vorsieht oder zwingend voraussetzt (§ 20 Abs. 2 Nr. 1 ThürDSG) oder der Betroffene eingewilligt hat (§ 20 Abs. 2 Nr. 2 ThürDSG).
Spezialgesetzliche Rechtsvorschriften zu Gewerbedaten finden sich in der GewO. Nach § 14 Abs. 5 Satz 2 GewO dürfen der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden allgemein zugänglich gemacht werden. Die Daten können nach § 14 Abs. 6 Satz 2 GewO innerhalb der Verwaltungseinheiten, denen die für die Entgegennahme der Anzeige und die Überwachung der Gewerbeausübung zuständigen Behörden angehören, weitergegeben werden. Insofern ist eine Übermittlung der Grunddaten nach § 14 Abs. 5 Satz 2 GewO innerhalb eines Landratsamtes vom Gewerbeamt an die Wirtschaftsförderung als zulässig anzusehen.
Die weitere Frage des Landratsamtes an den TLfDI lautete wie folgt:
2. Dürfen darüber hinaus noch weitere Daten, wie Beginn und Ende der Gewerbetätigkeit, Privatanschrift, Geburtsdatum und E-Mail-Adresse der Gewerbetreibenden an die Wirtschaftsförderung übermittelt werden?
Eine Rechtgrundlage zur Übermittlung weiterer Gewerbedaten an die Wirtschaftsförderung ist nicht ersichtlich. Allenfalls unter den Voraussetzungen, dass die Betroffenen darin eingewilligt haben und die übermittelten Daten für die Aufgabenerfüllung der Wirtschaftsförderung erforderlich wären, wäre eine solche Datenübermittlung nach § 2 i. V. m. § 20 Abs. 2 Nr. 2 ThürDSG als zulässig anzusehen.
Schließlich wollte das Landratsamt vom TLfDI folgende Frage beantwortet wissen:
3. Dürfen personenbezogene Gewerbedaten im Internet veröffentlicht werden?
Bei einer Internetpublikation personenbezogener Daten handelt es sich um eine Datenübermittlung auch an Drittstaaten nach § 23 Abs. 2 ThürDSG, in denen kein angemessenes Datenschutzniveau gewährleistet ist. Eine solche Datenübermittlung wäre nur dann zulässig, wenn die Betroffenen darin gemäß § 23 Abs. 2 Satz 1 Nr. 1 ThürDSG zweifelsfrei eingewilligt haben und die Datenübermittlung zur Aufgabenwahrnehmung der übermittelnden Stelle erforderlich ist (siehe hierzu 9. Tätigkeitsbericht des TLfDI, Punkt 5.2).
Im Ergebnis ist eine Übermittlung der Grunddaten Name/Firma, Tätigkeit und Anschrift gemäß § 14 Abs. 5 Satz 2 GewO innerhalb einer Landratsamtes an die Wirtschaftsförderung zulässig, nicht

jedoch deren Veröffentlichung im Internet. Eine Übermittlung weiterer Gewerbedaten an die Wirtschaftsförderung ist unzulässig.

Eine Übermittlung der Grunddaten Name/Firma, Tätigkeit und Anschrift nach § 14 Abs. 5 Satz 2 GewO innerhalb eines Landratsamtes vom Gewerbeamt an die Wirtschaftsförderung ist zulässig, nicht jedoch deren Veröffentlichung im Internet. Eine Rechtgrundlage zur Übermittlung weiterer Gewerbedaten an die Wirtschaftsförderung besteht nicht.

5.31 Bürgerbefragung ist Datenerhebung

Die Beschwerde eines Bürgers hatte eine „Bürgerbefragung“ durch die Stadtverwaltung Buttelstedt zum Gegenstand. Wie der Bürgermeister von Buttelstedt mitteilte, sollte den Einwohnern damit die Möglichkeit gegeben werden, sich zur Änderung der Verwaltungsstruktur zu äußern. Hierzu konnten die Bürger, die sich mit dem Inhalt eines vorgefertigten Schreibens zur Thematik identifizieren wollten, dieses adressiert und unterschrieben an die Stadtverwaltung zurücksenden. Zunächst war in diesem Falle seitens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) der irrigen Auffassung der Verwaltung entgegenzutreten, dass in dieser Angelegenheit keine personenbezogenen Daten erhoben wurden. Zu den persönlichen und sachlichen Verhältnissen im Sinne von § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) gehören auch geistige Zustände (Einstellungen, Motive, Wünsche, politische, religiöse oder sexuelle Einstellungen und Präferenzen), ferner Handlungen und Äußerungen (Simitis, Kommentar zum Bundesdatenschutzgesetz, 7. Auflage, Anm. 10 zu § 3, S. 304). Daher stellen die Unterschrift und auch die persönliche Auffassung der Betroffenen zur Änderung der Verwaltungsstruktur personenbezogene Daten gemäß § 3 Abs. 1 ThürDSG dar, die von der Stadt erhoben wurden.
Gemäß § 4 Abs. 1 Satz 1 ThürDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.
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. Zudem ist eine Einwilligung im Sinne des § 4 Abs. 2 ThürDSG als eine auf

einer freiwilligen Entscheidung des Betroffenen beruhenden Willenserklärung anzusehen, und der Betroffene ist gemäß § 4 Abs. 3 ThürDSG auf den Zweck und den Umfang der Verarbeitung und Nutzung und die voraussichtliche Dauer der Speicherung seiner Daten, auf seine Rechte der Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung seiner Einwilligung hinzuweisen. Da die Betroffenen nicht auf den Zweck der Befragung, die voraussichtliche Dauer der Speicherung ihrer Daten und auf ihre Rechte auf Auskunft, Berichtigung und Löschung hingewiesen wurden und auch keine Rechtsgrundlage für die Befragung vorlag, erfolgte diese Datenerhebung ohne Rechtsgrundlage. Das Erheben personenbezogener Daten ist nach § 19 Abs. 1 ThürDSG nur dann zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Hierfür gab es im vorliegenden Fall keine Anhaltspunkte. Auch hat die Stadtverwaltung nicht dargelegt, zur Erfüllung welcher Aufgabe Auffassungen der Bürger zur Änderung der Verwaltungsstruktur erforderlich waren.
Insofern handelte es sich bei der Erhebung der persönlichen Auffassungen der Bürger zur Änderung der Verwaltungsstruktur um einen Verstoß gegen datenschutzrechtliche Vorschriften.

Zu den persönlichen und sachlichen Verhältnissen im Sinne von § 3 Abs. 1 ThürDSG gehören auch geistige Zustände (Einstellungen, Motive, Wünsche, politische, religiöse oder sexuelle Einstellungen und Präferenzen), ferner Handlungen und Äußerungen.
Auch im Falle der Einwilligung ist die Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist, § 4 Abs. 1 ThürDSG.

5.32 Übermittlung gaststättenbezogener Außenbewirtschaftungszeiten von der Bauaufsichtsbehörde an die Gewerbebehörde

Die Anfrage eines Landratsamtes betraf die Zulässigkeit der Datenübermittlung von der Bauaufsichts- an die Gewerbebehörde. Für die Außenbewirtschaftung von Gaststätten auf Freiflächen werden durch die Bauaufsicht regelmäßig Nebenbestimmungen zum Schutz der Nachbarschaft festgelegt. Beispielsweise ist die Außenbewirtschaftungszeit auf spätestens 22.00 Uhr zu begrenzen. Da der Gewerbebehörde dieser Sachverhalt grundsätzlich nicht bekannt ist, soll sie

eine entsprechende Mitteilung erhalten, damit die Nebenbestimmung bei einem entsprechenden Antrag auf Sperrzeitenverlängerung Beachtung finden kann. Hierbei handelt es sich um die Übermittlung personenbezogener Daten seitens der Bauaufsichtsbehörde, die zur Aufgabenerfüllung der Gewerbebehörde erforderlich ist. Diese muss bei der Festlegung von Sperrzeiten auch dafür sorgen, dass Ruhestörungen von der Wohnbevölkerung abgewendet werden. Diesem Zweck dient die Übermittlung der zum Schutz der Nachbarn festgesetzten Nebenbestimmungen zu zulässigen Außenbewirtschaftungszeiten in der Baugenehmigung von Gaststätten. Die Übermittlung sollte jedoch nur auf die Angabe der jeweiligen Zeiten beschränkt werden und keine weiteren Angaben erhalten.

Eine Übermittlung von Nebenbestimmungen einer Baugenehmigung zu gaststättenbezogenen Außenbewirtschaftungszeiten an die Gewerbebehörde ist zur Erfüllung der Aufgaben der Gewerbebehörde erforderlich, § 21 ThürDSG.

5.33 Widerspruchsmöglichkeit des Bürgers gegen Weitergabe seiner Daten durch die Meldebehörde

Nach Einstellung eines Ermittlungsverfahrens gegen einen kommunalen Amtsträger nach § 170 Abs. 2 Strafprozessordnung (StPO) übermittelte die zuständige Staatsanwaltschaft dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Angelegenheit nach § 43 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) zur möglichen Verfolgung einer datenschutzrechtlichen Ordnungswidrigkeit.
Bei der datenschutzrechtlichen Prüfung stellte sich der Sachverhalt wie folgt dar: Ein Bürger hatte Strafanzeige erstattet, nachdem er von einem Kandidaten der Bürgermeisterwahl als Erstwähler angeschrieben worden war. Der Betroffene vermutete, dass sich der Kandidat seine Personalien und seine Anschrift widerrechtlich verschafft habe.
Nach § 32 Abs. 1 Thüringer Meldegesetz (ThürMeldeG) darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen sechs Monate vor der Wahl Auskunft aus den Melderegister über die in § 31 Abs. 1 Satz 1 ThürMeldeG bezeichneten Daten zu Gruppen von Wahlberechtigten erteilen, soweit für die

Zusammensetzung dieser Gruppen das Lebensalter der Betroffenen bestimmend ist. Dem kann der Betroffene nach § 32 Abs. 4 Satz 1 ThürMeldeG widersprechen. Hierzu steht auf der Homepage des TLfDI unter den Menü-Punkten „Wir über uns“ – „Informationsmaterial“ – „Mustervordrucke“ ein Muster eines Widerspruchsschreibens namens „Ärger mit den Meldedaten“ zum Herunterladen zur Verfügung.
Im konkreten Fall waren keine Anhaltspunkte für eine widerrechtliche Beschaffung der personenbezogenen Daten des Betroffenen ersichtlich. Auch hatte der Betroffene gegenüber dem zuständigen Meldeamt der Weitergabe seiner Daten nicht widersprochen. Daher war das Bußgeldverfahren des TLfDI wegen nicht zu führenden Tatnachweises aus tatsächlichen Gründen gem. § 170 Abs. 2 Satz1 StPO i. V. m. § 46 Abs. 1 OWiG einzustellen.

Bürger können der Weitergabe ihrer Daten nach § 32 Abs. 4 ThürMeldeG widersprechen. Von der Homepage des TLfDI kann zu diesem Zwecke ein Musterschreiben heruntergeladen werden.

6 Personaldaten

Akten ansehen
© fotomek – fotolia.com

6.1 Verwaltungsschule veröffentlicht Beschäftigtenfotos

Durch einen Hinweis wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass die Thüringer Verwaltungsschule Weimar in ihrem Internetauftritt auch Fotos ihrer Beschäftigten veröffentlicht. Nach einem Urteil des Bundesverwaltungsgerichts (BVerwG B 131/07) ist eine Veröffentlichung von Beschäftigtendaten im Internet dann zulässig, soweit der betreffende Beschäftigte dem außenstehenden Publikum zur Verfügung stehen soll. Diese Voraussetzung war nicht bei allen Beschäftigten, deren Fotos veröffentlicht worden sind, gegeben. Zudem bezieht sich die Entscheidung des Bundesverwaltungsgerichts nur auf die Nennung von Name, Dienstbezeichnung, dienstlicher Telefonnummer und E-Mail-Adresse, nicht aber auf Fotos. Die Veröffentlichung von Beschäftigtendaten im Internet ist eine Übermittlung personenbezogener Daten aufgrund der weltweiten Abrufbarkeit an Stellen auch außerhalb des Geltungsbereiches des Grundgesetzes. Eine derartige Übermittlung ist durch öffentliche Stellen nur unter denen in § 23 Thüringer Datenschutzgesetz (ThürDSG) genannten Voraussetzungen zulässig. Dabei ist davon auszugehen, dass in einigen der Drittstaaten kein angemessenes Datenschutzniveau gewährleistet ist. Daher ist die Übermittlung dieser Daten nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Es ist nicht ersichtlich, aus welchem Grund die weltweite Veröffentlichung von Fotos bestimmter Sachbearbeiter oder von Beschäftigten des technischen Hausdienstes im Internet für die Aufgabenerfüllung der Thüringer Verwaltungsschule erforderlich sein sollte. Diese Bewertung hat der TLfDI bereits in seinem 8. Tätigkeitsbericht unter Nummer 5.4 vor-

genommen. An dieser Bewertung ändert auch das Vorliegen einer Einwilligung der Betroffenen nichts. Zum einen ist nach § 4 Abs. 1 Satz 2 ThürDSG die Verarbeitung und Nutzung personenbezogener Daten auf Einwilligungsbasis nur zulässig, wenn dies zur Nutzung anerkannter Zwecke erforderlich ist. Als anerkannte Zwecke im Sinne der Vorschrift kommen neben der Aufgabenerfüllung öffentlicher Stellen unter anderem auch behördeninterne Zwecke in Betracht. Auch diese Voraussetzungen sind nicht gegeben. Zum anderen ist nach § 4 Abs. 2 ThürDSG die Einwilligung die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten seine personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen. Aufgrund des Beschäftigungsverhältnisses der Betroffenen mit der datenverarbeitenden Stelle besteht hier ein Abhängigkeitsverhältnis, das eine Freiwilligkeit der abgegebenen Einwilligung äußerst zweifelhaft macht.

Nachdem sich die Thüringer Verwaltungsschule trotz mehrfachen Hinweises des TLfDI weigerte, die Beschäftigtenfotos aus dem Netz zu nehmen, führte der TLfDI am 11. Februar 2013 eine Kontrolle vor Ort durch. Dabei wurde neben weiteren Mängeln, wie beispielsweise fehlende Löschfristen bei Verfahren, auch festgestellt, dass die Datenschutzbeauftragte gleichzeitig auch Aufgaben der IT-Administration wahrnimmt. Zum Datenschutzbeauftragten darf nur bestellt werden, wer durch seine Tätigkeit in keinen unüberwindbaren Interessenkonflikt mit seinen sonstigen dienstlichen Aufgaben kommt. Ein solcher Interessenkonflikt steht bei der Wahrnehmung der Aufgaben der IT-Administration zu befürchten, wenn sie in leitender Tätigkeit wahrgenommen wird. Dies wird derzeit geprüft. Nach wie vor veröffentlicht die Verwaltungsschule die Fotos ihrer Beschäftigten in ihrem Internetauftritt.

Der TLfDI beanstandete die festgestellten Mängel und forderte ihre Behebung. Gleichzeitig teilte er mit, dass er nach § 39 Abs. 2 ThürDSG das Thüringer Innenministerium als Aufsichtsbehörde einschalten wird, wenn die Mängel nicht behoben werden. Einigen datenschutzrechtlichen Forderungen kam die Thüringer Verwaltungsschule bereits nach. Das Verfahren läuft noch und das Ergebnis bleibt abzuwarten.

Die Veröffentlichung von Beschäftigtendaten im Internet ist nur dann datenschutzrechtlich zulässig, wenn die betreffenden Beschäftigten einem außenstehenden Publikum zur Verfügung stehen sollen.

Insbesondere die Veröffentlichung von Fotos ist für die Aufgabenwahrnehmung der öffentlichen Stelle in aller Regel nicht erforderlich.

6.2 Ist die moderne Verwaltung in allen obersten Landesbehörden angekommen?

Jeder von uns wünscht sich nichts sehnlicher, als die schnelle Bearbeitung seines Anliegens. Und nichts ist schlimmer als die Vorstellung von einem großen, der Bearbeitung harrenden Aktenberg. In dieser Hinsicht haben sich die Anforderungen an alle Einrichtungen der öffentlichen Verwaltung in den letzten Jahren tiefgehend verändert. Zunehmend werden nicht nur Papierakten bearbeitet, sondern Akten auch in elektronischer Form geführt. Die elektronische Aktenführung bietet viele Vorteile, aber sie enthält aus datenschutzrechtlicher Sicht auch einige Fallstricke. Oftmals sind alle Dokumente im Zugriff aller Beschäftigten und können mit ein paar Mouseclicks eingesehen werden. Auch von Personen, die eigentlich keinen Zugriff auf sie haben sollten. Durch Abbildung und Speicherung sämtlicher Bearbeitungsschritte mit Datum und Namen entstehen eine Vielzahl nachvollziehbarer Handlungen, die beschäftigtenbezogen ausgewertet und zu Verhaltens- und Leistungskontrollen herangezogen werden könnten. Dies gilt es zu verhindern.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beobachtete daher die Einführung eines einheitlichen Dokumentenmanagementsystems (DMS) in der Thüringer Landesverwaltung und berichtete darüber bereits im 9. Tätigkeitbericht (Punkt 15.1). Das zentral lizenzorientierte DMS "VISkompakt" kommt in der Thüringer Landesverwaltung seitdem in unterschiedlichen Versionen zum Einsatz. VISkompakt ist ein Dokumenten- und Vorgangsverwaltungssystem zur Erstellung und zum Verwalten von Dokumenten, Vorgängen, Akten und Geschäftsgängen. Die öffentliche Stelle legt in einem Feinkonzept die Zugriffsrechte für Nutzer, Nutzergruppen etc. fest. Weiterhin beschreibt das Feinkonzept alle Regelungen zu Akten, Vorgängen, Dokumententypen und Geschäftsvorgängen. Es unterliegt einer ständigen Aktualisierung. Alle zutreffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines Sicherheitskonzepts zu ermitteln, § 9 Abs. 2 Thüringer Datenschutzgesetz. Diese und weitere Anforderungen für datenschutzgerechte Lösungen müssen bereits

vor dem Einsatz von Dokumentenmanagementsystemen formuliert und umgesetzt werden.
Das DMS birgt neben der effizienten Arbeitsweise in den öffentlichen Stellen auch einige Risiken, denn mit einem solchen DMS können auch andere nutzerbezogene Informationen abgerufen werden.
In diesem Berichtszeitraum hat der TLfDI bei den vier Ministerien nachgehakt, die bei der ersten Befragung angegeben hatten, ein Dokumentenmanagementsystem im Einsatz zu haben. Bei einer weiteren obersten Landesbehörde wurde der Stand zum IT-Sicherheitskonzept unter Berücksichtigung der Einbindung unseres Fragenkataloges nachgefragt.
Im Ergebnis der Rückmeldungen ist bei einem der Ministerien weiterhin kein Dokumentenmanagementsystem zum Einsatz gekommen und auch nicht geplant. Drei weitere Ministerien nutzen das DMS derzeit noch zur reinen Schriftgutverwaltung. Zwei dieser Ressorts befinden sich aber in der Planungs- und Projektphase bzw. Testphase zur Einführung von VISkompakt. Im Rahmen dieser veränderten Sachlage besteht nunmehr Erörterungsbedarf bezüglich der Datenschutz- sowie Sicherheitskonzepte. Der TLfDI hat beide Ministerien um zeitnahe Unterrichtung zum Fortgang gebeten und signalisierte seine Gesprächsbereitschaft.

Vor dem Einsatz von Dokumentenmanagementsystemen (DMS) sind die Anforderungen für datenschutzgerechte Lösungen zu formulieren und umzusetzen (§ 9 Abs. 2 ThürDSG).

6.3 Kein Datenschutz am Sonntag

Aus der Presse erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass das Landesamt für Verbraucherschutz in einem Streitverfahren um die Sonntagsarbeit in einem Unternehmen den Namen eines Widerspruchsführers an das Unternehmen weitergegeben hatte. Das Landesamt für Verbraucherschutz teilte dem TLfDI auf Nachfrage mit, dass ein Unternehmen einen Antrag auf die Bewilligung von Sonntagsarbeit gestellt hatte. Dieser Antrag war vom Landesamt positiv beschieden worden. Hiergegen kann der einzelne von der Sonntagsarbeit betroffene Beschäftigte Widerspruch einlegen. Um festzustellen, ob der Antrag des Beschäftigten zulässig ist, muss das Landesamt prüfen,

ob der Beschäftigte zur Sonn- und Feiertagsarbeit überhaupt herangezogen werden soll. Dazu wurde der Bescheidadressat, also das Unternehmen, das die Sonntagsarbeit beantragt hat, befragt und es erfuhr so die Namen der Beschäftigten, die Widerspruch eingelegt hatten. Für die Notwendigkeit der Prüfung, ob der Beschäftigte, der Widerspruch eingelegt hat, überhaupt von der anstehenden Sonntags- bzw. Feiertagsarbeit betroffen ist zeigte der TLfDI in einem gemeinsamen Termin mit dem Thüringer Landesamt für Verbraucherschutz durchaus Verständnis. Er wies jedoch einen anderen Verfahrensweg auf, der die Rechte der betroffenen Beschäftigten besser schützt: Im Falle eines Widerspruchs wird das Thüringer Landesamt für Verbraucherschutz künftig an den antragstellenden Arbeitgeber herantreten und diesen bitten, möglichst zeitnah eine Liste der Beschäftigten zu übermitteln, die von der Sonntagsarbeit potenziell betroffen sind. Das Landesamt kann diese Liste dann selbst mit den Namen der jeweiligen Widerspruchsführer abgleichen, um die Zulässigkeit der Widersprüche prüfen zu können, ohne dass das Unternehmen den Namen des Widerspruchsführers erfährt. Bereits bei der Bescheiderteilung kann ein Hinweis an das Unternehmen ergehen, dass im Fall der Einlegung des Widerspruchs eines Beschäftigten eine derartige Liste benötigt wird. Diese kann dann von dem Unternehmen schon vorgehalten werden, damit im Zweifelsfall schnell eine Entscheidung des Landesamtes für Verbraucherschutz möglich ist. Das Thüringer Landesamt für Verbraucherschutz sicherte zu, künftig diese Verfahrensweise anzuwenden.

Bei der Übermittlung von Beschäftigtendaten an den Arbeitgeber ist besondere Vorsicht geboten, da immer auch der Bestand des Arbeitsverhältnisses betroffen sein kann. Im Zweifel ist nach Alternativen zu suchen, die weniger in die Rechte der betroffenen Beschäftigten eingreifen.

6.4 Alkoholabhängigkeit eines Bediensteten

Ein Landratsamt wandte sich mit einer heiklen Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Bei einem der im Landratsamt Beschäftigen wurde eine Alkoholabhängigkeit festgestellt. Da er immer wieder durch Rückfälle auffällig geworden war, stellte der Facharzt für Psychiatrie/Neurologie fest, dass der Beamte für eine gewisse Zeit für dienst-

liche Zwecke nicht fahrtauglich ist. Das Landratsamt wollte wissen, ob es datenschutzrechtlich zulässig ist, die betroffenen Organisationseinheiten des Landratsamtes auf dem Dienstweg über die Fahruntauglichkeit der betroffenen Person zu informieren. Außerdem sollte geprüft werden, ob aufgrund des Fürsorgeprinzips seitens des Dienstherrn die Zulassungsstelle informiert werden durfte, da anzunehmen sei, dass der Beamte weiterhin sein privates Fahrzeug nutzt.
Nach § 20 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) ist die innerbehördliche Nutzung personenbezogener Daten nur zulässig, wenn es zur Erfüllung der und der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben erforderlich ist. Grundsätzlich sollte innerhalb der Behörde ein Informationsaustausch über Gesundheitsdaten nur im Einzelfall erfolgen, um die für die Gesundheit des Bediensteten erforderlichen Maßnahmen ergreifen zu können. Keinesfalls sollten die betroffenen Organisationseinheiten über die Tatsache der Alkoholabhängigkeit bzw. des Rückfalls informiert werden. Mitgeteilt werden sollte lediglich, dass der Beamte derzeit fahruntauglich ist und ihm kein Fahrzeug auszuhändigen ist.
Im Hinblick auf die Beantwortung der zweiten Frage ist zu differenzieren. Keinesfalls ist es datenschutzrechtlich zulässig, aufgrund des Führsorgeprinzips generell in einem derartigen Fall den Fachdienst Zulassung zu informieren. Es ist im Einzelfall jeweils eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung der Betroffenen und den betroffenen Grundrechten Dritter zu differenzieren. Nach § 20 Abs. 2 Nr. 6 ThürDSG ist die Datennutzung zulässig, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist. Hiervon kann ausgegangen werden, wenn konkrete Anhaltspunkte dafür bestehen, dass der jeweilige Bedienstete in alkoholisiertem Zustand ein Fahrzeug führt. Andernfalls erscheint die Information der Zulassungsstelle unverhältnismäßig. Sollte der Dienststelle jedoch positiv bekannt sein, dass der Bedienstete sein privates Kraftfahrzeug führt, obwohl er nicht fahrtüchtig ist und sollte es hierzu bereits zu einer abstrakten Gefährdung Dritter gekommen sein, kann im Einzelfall eine Information des Fachdienstes Zulassung über die mögliche Fahruntauglichkeit des Bediensteten zulässig sein. Hierbei ist jedoch nur über die mögliche Fahruntüchtigkeit zu informieren und keinesfalls über die Ursache der Fahruntüchtigkeit.

Gesundheitsdaten von Beschäftigten dürfen nur unter äußerst engen Voraussetzungen bekannt gegeben werden. Die Information über die Alkoholabhängigkeit eines Beamten an die Zulassungsstelle ist nur bei einer konkreten Gefahr für die öffentliche Sicherheit und Ordnung zulässig. In diesem Fall hat eine Benachrichtigung nach § 21 Abs. 6 ThürDSG zu erfolgen.

6.5 Datenschutz-(Bei-)Hilfe

Das Thüringer Finanzministerium (TFM) informierte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass ein automatisiertes Verfahren zur Berechnung der Beihilfe und der Erstellung der Bescheide eingerichtet worden sei. Für das automatisierte Verfahren wird eine dritte Stelle Fernwartungs- und Teleserviceleistungen erbringen. Da es sich bei Beihilfedaten um besonders sensible personenbezogene Daten handelt, kommt dem Schutz vor unbefugtem Zugriff auf diese Daten besondere Bedeutung zu. Der TLfDI bat daher das TFM um Mitteilung, wie sichergestellt ist, dass ein Zugriff auf die personenbezogenen Daten im Rahmen der Fernwartung ausgeschlossen ist. Das TFM übersandte daraufhin einen Auszug aus der Fernwartungs- und Teleservicevereinbarung mit dem Dienstleister und das entsprechende Formblatt zum Verfahrensverzeichnis. Anhand der eingereichten Unterlagen war erkennbar, dass die Verarbeitung personenbezogener Daten im Auftrag auch Gegenstand der Vereinbarung war, sodass § 8 Abs. 7 Thüringer Datenschutzgesetz, der auch einen Vertrag bei Wartung und Fernwartung vorschreibt, wenn ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, nach Prüfung der vorgelegten Fernwartungs- und Teleservicevereinbarung als umgesetzt angesehen werden konnte. Da allerdings für das automatisierte Beihilfeverfahren selbst ein Konzept für die Löschung der Daten fehlte, forderte der TLfDI hierzu weitere Informationen. Das TFM teilte mit, dass die Beihilfestelle erstmals Anfang 2018 eine regelmäßige Datenlöschung vornehmen wird. Der TLfDI wird dies zu gegebener Zeit prüfen.

Der Zugriff auf personenbezogene Daten ist bei der Fernwartung nicht die Regel, er kann aber durch die verantwortliche Stelle nicht immer ausgeschlossen werden. Den technischen und organisatorischen Maßnahmen zur Verhinderung von unbefugten Zugriffen

kommt daher gerade bei Gesundheitsdaten eine hohe Bedeutung zu; sie müssen im Auftragsdatenverarbeitungsvertrag ihren Niederschlag finden.

6.6 Erkennungsdienstliche Maßnahmen des Arbeitgebers?

An den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde ein Fall der biometrischen Zeiterfassung seitens des Arbeitgebers mittels eines Fingerabdrucks herangetragen.
Die datenschutzrechtliche Beurteilung dieser Causa muss nach wie vor an § 32 Bundesdatenschutzgesetz (BDSG) gemessen werden, da es dem bisherigen Bundesgesetzgeber nicht (mehr) gelungen ist, das Arbeitnehmerdatenschutzrecht auf rechtlich ausbalancierte Füße zu stellen, sodass auch diese Frage bisher keiner spezielleren Regelung zugeführt werden konnte.
Zwar mag beispielsweise die Erfassung des Irismusters im Vergleich zum Fingerabdruck einen noch erheblicheren Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Beschäftigten darstellen, da hierdurch Rückschlüsse auf persönliche Merkmale und Eigenschaften möglich sind. Gleichwohl ist mit der herrschenden datenschutzrechtlichen Literaturmeinung eine Zeiterfassung mittels Fingerabdrucks grundsätzlich abzulehnen. Denn zum einen kann sich eine solche Maßnahme des Arbeitgebers nicht auf § 32 Abs. 1 BDSG stützen, da sie nicht erforderlich ist. Denn für den Beschäftigten weniger einschneidende Mittel der Zeiterfassung, die ebenso gut geeignet sind, wären die Zeiterfassung per Chipkarte oder Ausweis. Zum anderen wäre § 32 BDSG als nur allgemeine datenschutzrechtliche Erlaubnisregel zu unbestimmt, um einen derart intensiven Grundrechtseingriff rechtfertigen zu können; hierfür bedarf es einer präzisen bereichsspezifischen Regelung. Hinzu kommt, dass derart höchstpersönliche Daten – bei wem auch immer – Begehrlichkeiten wecken werden, denen von Beginn an gewehrt werden muss. Schließlich erscheint auch eine etwaige Einwilligung des Beschäftigten in derartige Praktiken als nicht freiwillig – wie jedoch von § 4 a BDSG gefordert –, denn sie erfolgt in einem Über-Unterordnungsverhältnis zwischen Arbeitgeber und Beschäftigten.
Im seltenen Ausnahmefall – etwa zur Zugangskontrolle in Hochsicherheitsbereichen – mag sich eine andere datenschutzrechtliche Beurteilung ergeben. Der TLfDI hat zur Zulässigkeit der biometri-

schen Zeiterfassung eine Pressemitteilung herausgegeben, in der er den Arbeitgebern und Arbeitgeberinnen vor dem Einsatz von derartigen Systemen die Lektüre der „Hinweise zur biometrischen Datenerfassung am Arbeitsplatz“ empfiehlt, die unter folgendem Link veröffentlicht sind:
http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/hinweis_biometrischen_datenerfassung_am_arbeitsplatz.pdf

Die Erhebung der Fingerabdruckdaten von Beschäftigten zwecks Zeiterfassung stellt einen grundsätzlichen Verstoß gegen die in § 32 Abs. 1 BDSG verankerten Erforderlichkeitsgrundsatz dar. Eine Zeiterfassung per Chipkarte oder Ausweis erfüllt denselben Zweck, stellt für den Beschäftigten indes den weniger einschneidenden Grundrechtseingriff dar. Zudem stellt § 32 Abs. 1 BDSG keine bereichsspezifische Regelung dar, die bestimmt genug wäre, einen derart intensiven Grundrechtseingriff zu rechtfertigen. Eine etwaige Einwilligung des Beschäftigten in solche Praktiken scheitert in aller Regel an der mangelnden Freiwilligkeit (§ 4 a BDSG) im Über-Unterordnungsverhältnis zwischen Arbeitgeber und Beschäftigten.

6.7 Manchmal müssen Zeiterfassungsdaten auch länger aufbewahrt werden

Eine öffentliche Stelle bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um Beratung im Hinblick auf Löschung von Arbeitszeiterfassungsdaten. In dem betreffenden Fall gab es eine Gleitzeitvereinbarung, die die Löschung der Daten nach drei Monaten vorsah. Es gab aber den Verdacht von Unregelmäßigkeiten bei der Zeiterfassung eines Beschäftigten; deswegen sollten die Daten länger aufbewahrt werden. Die Löschung personenbezogener Daten unterfällt nach § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) dem Begriff des Verarbeitens von Daten. Eine Datenverarbeitung ist nach § 4 Abs. 1 Satz 1 ThürDSG nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene einwilligt. Nach § 33 Abs. 1 ThürDSG finden die §§ 89 bis 96 des Thüringer Beamtengesetzes (ThürBG) bei Beschäftigten entsprechende Anwendung. Da diese Bestimmungen keine Regelung zur Löschung von Daten enthalten, gelten die allgemeinen Regelungen des ThürDSG. Personenbezogene Daten sind nach § 16 Abs. 1 Nr. 1 und 2 ThürDSG zu löschen, wenn ihre Speiche-

rung unzulässig ist oder wenn ihre Kenntnis für die Daten verarbeitende Stelle nicht mehr erforderlich ist.
Wenn Anhaltspunkte vorliegen, die auf die Unrichtigkeit der gespeicherten Daten hinweisen, ist eine weitere Speicherung zum Zweck des Nachweises des Verstoßes zulässig und geboten, § 20 Abs. 2 Nr. 4 ThürDSG. Dem stand auch die Regelung der Gleitzeitvereinbarung nicht entgegen. Zwar schreibt diese vor, dass die erfassten Daten nach einem Zeitraum von drei Monaten zu löschen sind. Sie traf für den Fall einer Unstimmigkeit über die Arbeitszeit keine konkrete Regelung und war daher für diese Fälle gesetzeskonform auszulegen. Die Aufklärung eines möglichen Verstoßes gegen die Arbeitszeitregelung muss bei konkreten Anhaltspunkten möglich sein. Die Speicherung der Daten ist in diesen Fällen über die in der Gleitzeitvereinbarung festgehaltene Frist hinaus zulässig.

Wenn Arbeitszeiterfassungsdaten benötigt werden, um bei konkreten Anhaltspunkten einen Verstoß nachzuweisen, dürfen Sie so lange gespeichert werden, wie dies für den Nachweis erforderlich ist.

6.8 Darf der Dienstherr den behandelnden Arzt kennen?

Ein Beschwerdeführer wandte sich mit der Frage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ob es sich verhindern lässt, dass der Dienstherr erfährt, welcher Arzt eine Krankschreibung ausgestellt hat. Grundsätzlich ist hierzu festzustellen, dass der Dienststelle die Kenntnisnahme einer Krankschreibung, auf der auch der Name des ausstellenden Arztes angegeben ist, in der Regel nicht verwehrt werden kann. Der Dienstherr muss aufgrund der Krankschreibung weitere Maßnahmen in der Dienststelle treffen können, insbesondere die Regelung der Vertretung. Die Dienststelle muss allerdings die organisatorischen Maßnahmen treffen, die erforderlich sind, damit die datenschutzrechtlichen Anforderungen gewahrt werden. So muss geregelt sein, wer die Krankschreibungen in der Dienststelle zur Kenntnis nimmt. Diese Person unterliegt selbstverständlich der Verschwiegenheit, zumal es sich bei den Arbeitsunfähigkeitsdaten um Gesundheitsdaten und damit um besonders geschützte Daten handelt, § 4 Abs. 5 Thüringer Datenschutzgesetz. Es muss festgelegt werden, wie mit den Krankschreibungen im Einzelfall zu verfahren ist. Keinesfalls dürfen die

Krankschreibungen Unbefugten zugänglich sein. Es darf für die genannten Zwecke notiert werden, für welchen Zeitraum die Krankschreibung besteht, dann ist die Krankschreibung für Tarifbedienstete zuständigkeitshalber an die Zentrale Gehaltsstelle weiterzuleiten.
Daneben besteht die Problematik, dass mit der Angabe eines Facharztes auf der Arbeitsunfähigkeitsbescheinigung unter Umständen auf die Art der Erkrankung rückgeschlossen werden kann, auch wenn eine konkrete Diagnose selbstverständlich nicht enthalten sein darf. Dies ist aber nicht zu vermeiden, weil die Ausstellerin/der Aussteller zweifelsfrei erkennbar sein muss, damit das Dokument als gültig anerkannt werden kann. Die telefonische Meldung durch den Erkrankten reicht daher bei einer längeren Arbeitsunfähigkeit nicht aus, zumal die Vorlage eines ärztlichen Attests in der Regel ab dem 3. Tag vorgeschrieben ist. Die Kenntnisnahme der Krankschreibung ist aber nur für die personalverwaltende Dienststelle erforderlich. Personalaktendatenschutzrechtliche Vorschriften sind zu beachten.

Eine ärztliche Krankschreibung enthält besonders geschützte Daten; daher hat der Dienstherr alle organisatorischen Maßnahmen zu treffen, die erforderlich sind, damit die datenschutzrechtlichen Anforderungen gewahrt werden.

7 Polizei

Rücken eines Polizisten
© Picture-Factory – fotolia.com

7.1 „Datenleck" und andere Datenschutzpannen im Bildungszentrum der Thüringer Polizei in Meiningen

Zu den Aufgaben des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gehört es gemäß § 37 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG), die Einhaltung der Vorschriften des Landesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz bei allen öffentlichen Stellen zu kontrollieren. Dabei sind der TLfDI und seine Beauftragten gemäß § 38 Abs. 1 Satz 1 ThürDSG von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist gemäß § 38 Abs. 1 Satz 2 Nr. 1 ThürDSG im Rahmen der Kontrollbefugnis insbesondere Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, die im Zusammenhang mit der Kontrolle stehen, zu gewähren. Darüber hinaus ist dem TLfDI und seinen Beauftragten gem. § 38 Abs. 1 Satz 2 Nr. 2 ThürDSG jederzeit Zutritt in alle Diensträume zu gestatten.
Eine solche Kontrolle fand im Berichtszeitraum auch beim Bildungszentrum der Thüringer Polizei in Meiningen statt. Im Zuge dieser Kontrolle zeigten sich erhebliche datenschutzrechtliche Mängel, die der TLfDI förmlich nach § 39 Abs. 1 Satz 1 ThürDSG beanstandete.
So wurde bei der stichprobenartigen Überprüfung von Zugriffsrechten auf Dateien und Verzeichnisse des Bildungszentrums der Thüringer Polizei vom TLfDI festgestellt, dass eine Vielzahl der Beschäftigten fachbereichs- und abteilungsübergreifend Zugriffsrechte auf mehrere Dateien und Ordner mit personenbezogenen Daten hatte, die außerhalb ihrer Kompetenzbereiche lagen. Als sofortige Notfallmaßnahme wurde die Abschaltung des Servers des Bildungszent-

rums der Thüringer Polizei durch den Behördenleiter veranlasst, wohl auch, um unberechtigten Dritten keine weiteren unerlaubten Zugriffe auf die Dateien zu gestatten und Maßnahmen für eine rechtskonforme Datenverarbeitung einzuleiten.
Weiterhin befanden sich im Dienstzimmer eines Mitarbeiters „mobile“ Postfächer mit Unterlagen – darunter unverschlossene Klausurergebnisse mehrerer Kurse mit Klarnamen sowie Anträge zur Klausureinsicht –, obwohl der Mitarbeiter nicht für die Poststelle zuständig bzw. kein Vertreter war. Zudem bestand die Möglichkeit, dass dort weitere Personen unberechtigt Einsicht in die genannten Unterlagen mit den personenbezogenen Daten nehmen konnten. Warum diese Unterlagen nicht sofort ordnungsgemäß weggeschlossen wurden, blieb trotz Nachfrage des TLfDI unklar. Auch bei der Nachkontrolle stellte der TLfDI fest, dass sich die „mobilen“ Postfächer noch in besagtem Dienstzimmer befanden. Zudem stieß der TLfDI auf einen dienstlichen USB-Stick dieses Mitarbeiters, auf dem unter anderem ein Vermerk existierte, der Kommentare von mehreren Auszubildenden enthielt, die diese privat im sozialen Netzwerk Facebook veröffentlicht hatten. Auf Nachfrage wurde dazu erklärt, dass die Datei für ein Ermittlungsverfahren benötigt worden sei, sodass eine Löschung der Datei deswegen auch unterblieben sei. Ebenso verhielt es sich mit weiteren Dateien. Dies stellte im Ergebnis einen Verstoß gegen § 6 ThürDSG (i. V. m. § 19 ThürDSG) dar. Aufgrund der datenschutzrechtlichen Mängel wurde die Bestellung des bDSB im Nachgang der Kontrolle durch die Leitung des Bildungszentrums der Polizei widerrufen, ohne zugleich einen neuen bDSB zu bestellen. Erst einige Zeit später nahm eine andere Person das Amt des bDSB am Bildungszentrum der Thüringer Polizei wahr. Bis zu diesem Zeitpunkt blieb das Amt des bDSB unbesetzt, was der TLfDI gemäß § 39 ThürDSG beanstandete.
Im Rahmen der Kontrolle des TLfDI wurde im weiteren Verlauf auch ein von einer Fremdfirma bereitgestellter Aktensammelcontainer in den Räumen des Bildungszentrums der Thüringer Polizei festgestellt, der von den Bediensteten für ihren anfallenden Papierabfall genutzt wurde. Der Inhalt der darin eingeworfenen Unterlagen konnte teilweise von außen sichtbar zur Kenntnis genommen werden. Auch eine Entnahme der Unterlagen wäre durch den Einwurfschlitz möglich gewesen. Die Nachfrage, ob den Bediensteten zusätzlich zu dem Sammel-Container Aktenvernichter in ihren Diensträumen bereitgestellt werden, wurde verneint. Dem TLfDI wurde

jedoch unmittelbar nach Abschluss der Kontrolle dazu mitgeteilt, dass der betreffende Container durch einen anderen ersetzt werden solle, der höheren Sicherheitsstandards entsprechen würde.
Darüber hinaus wurde die Personalabteilung des Bildungszentrums der Thüringer Polizei mit verschließbaren Schränken ausgestattet, nachdem der TLfDI bei seiner Kontrolle die offene Lagerung von Personalunterlagen bemängelt hatte. Zudem werden personenbezogene Daten der Ausbildungs- und Studienleitung nunmehr in verschließbaren Umschlägen an die zuständigen Organisationseinheiten versandt.
Auch die Tatsache, dass als langfristige Maßnahmen umfassende datenschutzrechtliche Schulungen des Stammpersonals des Bildungszentrums der Thüringer Polizei und der Fachhochschule für öffentliche Verwaltung, Fachbereich Polizei Thüringen, die dauerhafte Sensibilisierung für den Datenschutz und die anlassbezogenen und stichprobenartige Kontrollen durch den neu ernannten bDSB vorgesehen sind, wird vom TLfDI ausdrücklich begrüßt und als positiv gewertet.

Als „schärfstes Schwert“ im öffentlichen Bereich sieht das Thüringer Datenschutzgesetz gemäß § 39 ThürDSG die Beanstandung vor. Der TLfDI beanstandet festgestellte Verletzungen von Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten und fordert ihre Behebung in angemessener Frist. Die für die Sicherstellung des Datenschutzes nach § 34 Abs. 1 ThürDSG verantwortliche Stelle und die Aufsichtsbehörde sind davon zu verständigen.
Wird die Beanstandung nicht behoben, so fordert der Landesbeauftragte nach § 39 Abs. 2 ThürDSG von der für die Sicherstellung des Datenschutzes nach § 34 ThürDSG verantwortlichen Stelle und der Aufsichtsbehörde binnen angemessener Frist geeignete Maßnahmen. Haben diese nach Ablauf dieser Frist keinen Erfolg, verständigt der Landesbeauftragte den Landtag und die Landesregierung.

7.2 Wem gehören die Dateien auf dem Dienst-Computer?

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bekannt, dass die Vorsitzenden der Thüringer Polizeigewerkschaften GdP und DPolG Anzeige gegen Unbekannt wegen illegaler Datenausspähung erstattet hatten, da

das E-Mail Postfach eines Beamten am Bildungszentrum der Thüringer Polizei auf Anweisung von Vorgesetzten illegal durchsucht worden sei.
Wie sich herausstellte, lief gegen die betroffene Person tatsächlich ein Disziplinarverfahren wegen des Verdachts des Geheimnisverrates. Ihm wurde vorgeworfen, Polizeischüler über den Inhalt einer Klausur vorab informiert zu haben.
Nach der vom TLfDI geforderten Stellungnahme des Thüringer Innenministeriums gab es in der Tat eine geschriebene Klausur, die teilweise identisch mit der Lösungsskizze war und mit Abstand das beste Ergebnis aufwies. Dies begründete beim Vorgesetzten den Verdacht, dass die Lösungsskizze der Klausur an diese dritte Person weitergegeben worden sei. Im Zuge der weiteren Ermittlungen wurde der dienstliche E-Mail-Account des verdächtigen Beamten geprüft. Daran seien laut Aussage des Thüringer Innenministeriums die Personalvertretung und der Datenschutzbeauftragte des Bildungszentrums der Thüringer Polizei beteiligt worden und hätten der Maßnahme zugestimmt. Überprüft worden sei ferner die Protokolldatei mit den Protokolleinträgen der gesendeten Nachrichten auf dem E-Mail-Server des dienstlichen Postfaches. Jedoch habe sich die Weitergabe der Klausur durch den betreffenden Beamten an Polizeischüler nicht bestätigt.
Bei einem Vor-Ort Termin des TLfDI am Bildungszentrum der Thüringer Polizei stellte sich allerdings heraus, dass der Personalrat – entgegen der Vorschriften der Dienstvereinbarung und der Aussage des Thüringer Innenministeriums – bei der Auswertung der Protokoll- und Sicherungsdateien nicht beteiligt wurde.
Die Überprüfung der Protokolldatei war aufgrund der fehlenden Personalratsbeteiligung somit unzulässig und wurde förmlich nach Ablauf des Berichtszeitraums nach § 39 ThürDSG vom TLfDI beanstandet.
In Zusammenhang mit diesem Fall stellt sich die grundsätzliche Frage über die Erhebung der Daten aus dienstlichen Rechnern und den persönlichen E-Mail Postfächern bei Beamten.
Die generelle Verfügungsbefugnis und damit auch den Gewahrsam über die Dienst-PC, die Laufwerke und alle weiteren Komponenten elektronischer Datenverarbeitung besitzt der Dienstherr bzw. -vorgesetzte nur in der Regel. Dieser darf daher nur dann auf die Dateien zugreifen und sie zum Gegenstand einer Beweiserhebung im Disziplinarverfahren machen und entsprechend auswerten, wenn sie

als dienstliche Dateien zu qualifizieren sind. Eines richterlichen Durchsuchungsbeschlusses bedarf es in diesem Falle nicht.
Anders ist die Rechtslage allerdings dann zu bewerten, wenn der Beamte auf seinem Dienst-PC *private* Dateien angelegt hat. Eine solche Fallkonstellation liegt vor, wenn der Beamte die Dateien deutlich als private Dateien gekennzeichnet hat und wenn er durch ein Passwort andere Personen (außer den Systemadministrator) vom Zugriff auf die ihm dienstlich zur Verfügung gestellten Datenspeicher ausgeschlossen hat. In diesen Fällen hat der Beamte (Mit-)Gewahrsam an den „ihm gehörenden“ Dateien, die dann auch dem Schutzbereich seines Rechtes auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz (GG) und Artikel 6 Abs. 2 der Verfassung des Freistaats Thüringen (ThürVerf) unterfallen. Die Öffnung dieser privaten Dateien ist nur mittels eines richterlichen Beschlusses gemäß § 32 Thüringer Disziplinargesetz (ThürDG) zulässig. Nach der Entscheidung des Oberverwaltungsgerichts Bremen (Beschluss vom 21. Juli 2006 – DL A 420/05 –, nachzulesen bei juris) gilt dies auch für private Dateien, die in einem Unterverzeichnis gespeichert sind, das aufgrund seiner dienstlichen Bezeichnung vor seiner Öffnung nicht als privates Unterverzeichnis identifiziert werden konnte, gerade weil es an der privaten Bezeichnung mangelte. Nichts anderes gilt selbst für den Fall, dass die Speicherung privater Dateien auf einem dienstlichen Datenträger nach einer dienstinternen Anordnung oder Regelung nicht zulässig ist. Das Bundesverwaltungsgericht hat in seiner Entscheidung aus dem Jahr 2011 (Az.: 2 A 11/08, nachzulesen bei juris) klargestellt, dass selbst die von einem Beamten unter Verletzung dienstlicher Pflichten – etwa wegen des Verstoßes gegen eine die Speicherung privater Daten verbietenden Richtlinie – angelegten privaten Dateien gleichwohl *keine* dienstlichen Dateien sind.
Zu der geschilderten Problematik hat der TLfDI in Zusammenarbeit mit seinem Mitarbeiter Tim Fellmann einen zweiteiligen Aufsatz verfasst (Dr. Hasse/Fellmann, Mein ist der PC und also auch die Daten – vom Irrtum des Dienstherrn bzw. Vorgesetzen, ThürVBl. 2014, S. 1 ff. (Teil 1), S. 36 ff. (Teil 2)), der die Rechtslage nicht nur aus dem *disziplinarrechtlichen*, sondern auch aus dem *strafprozessrechtlichem* Blickwinkel nach den § 102 ff. Strafprozessordnung ausleuchtet.

Das Disziplinarverfahren gegen den betroffenen Beamten soll inzwischen mangels hinreichender Anhaltspunkte für das Vorliegen eines Dienstvergehens bzw. einer Straftat eingestellt worden sein.

Der Dienstherr bzw. -vorgesetzte besitzt nur die grundsätzliche Verfügungsbefugnis und damit auch den Gewahrsam über die dienstlichen Computer. Anders ist die Rechtslage allerdings dann, wenn der Beamte auf seinem Dienst-PC private Dateien angelegt hat, an denen er (Mit-)Gewahrsam hat. Diese Dateien unterfallen dann auch dem Schutzbereich seines Rechtes auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG und Artikel 6 Abs. 2 ThürVerf. Die Öffnung dieser privaten Dateien ist sowohl im Straf- als auch im Disziplinarverfahren nur mittels eines richterlichen Beschlusses zulässig. Das gilt selbst dann, wenn die Speicherung privater Dateien durch Richtlinien oder Erlasse untersagt ist.
Um Missverständnisse und Unklarheiten zu vermeiden, sollte in einer Dienstvereinbarung der Zugriff des Dienstherrn bzw. -vorgesetzten auf den Dienst-PC sowie die private Nutzung des Dienst-PC seitens des Beschäftigten geregelt werden. Der private Charakter einer gleichwohl gespeicherten Datei geht dadurch jedoch nicht verloren.
Hiervon unberührt bleibt die dienstrechtliche Beurteilung, wenn entgegen bestehender Dienstanweisungen private Dateien auf dienstlichen Rechnern gespeichert werden. Auch archivrechtliche Vorschriften müssen Beachtung finden.

7.3 Polizei auf Abwegen

Einer Presseinformation zufolge ermittelte die Staatsanwaltschaft Mühlhausen gegen Polizeibeamte der Polizeiinspektion (PI) Mühlhausen wegen des Verdachts des Betrugs und der Untreue. Auslöser der Ermittlungen war eine anonyme Anzeige gegen vier namentlich benannte Tatverdächtige. Dabei wurde zwei Beamten zur Last gelegt, während der Dienstzeit für private Zwecke dienstliche Kraftfahrzeuge und Telekommunikationsmittel genutzt zu haben. Zwei weiteren Beamten wurde vorgeworfen, dies geduldet bzw. unterstützt zu haben. Daraufhin wurde gegen diese Beamten von Amts wegen ein Ermittlungsverfahren zum Verdacht der Untreue und des Betrugs eingeleitet. Das zuständige Amtsgericht erließ auf Antrag

der Staatsanwaltschaft einen Beschluss für eine längerfristige Observation gemäß § 163 f Strafprozessordnung (StPO) gegen die Beschuldigten, welcher im weiteren Ermittlungsverlauf um drei Monate verlängert wurde. Die Umsetzung der gerichtlich angeordneten Maßnahmen erfolgte durch Spezialeinheiten des Thüringer Landeskriminalamtes (TLKA) an zehn Arbeitstagen in einem Zeitraum von sechs Monaten.

Da für die längerfristige Observation der vier Beschuldigten nach § 163 f StPO eine richterliche Anordnung vorlag, diese auch befolgt wurde und damit eine rechtliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung gegeben war, war diese datenschutzrechtlich nicht zu beanstanden.

Darüber hinaus wurden im Zuge der Observationsmaßnahmen zwei weitere Verfahren gegen Beamte der PI Mühlhausen eingeleitet. Zudem wurde eine dritte Person der PI Mühlhausen observiert, welche ebenfalls verdächtigt wurde, ein Dienstfahrzeug für private Zwecke genutzt zu haben; in diesem Fall wurde kein Verfahren eingeleitet.

Aus datenschutzrechtlicher Sicht war insoweit entscheidend, ob auch die weiteren drei Observationen auf einer rechtlichen Grundlage beruhten. Aus den vorgelegten Akteninhalten der Staatsanwaltschaft Mühlhausen war eine solche nicht zu erkennen. Vielmehr konnte den Akten lediglich eine „geschwärzte“ richterliche Anordnung entnommen werden. Das bedeutet, eine richterlicher Anordnung gegen eine Person wurde als Vorlage für weitere Anordnungen gegenüber anderen Personen verwendet. Lediglich der ursprüngliche Name in der Anordnung wurde ausgetauscht. Die Aktenzeichen waren identisch mit dem Verfahren, das gegen die vier beschuldigten Personen lief. Eine solche „geschwärzte“ Anordnung, die quasi als richterliche Blankoanordnung für sämtliche Observationsmaßnahmen verwendet wurde, stellt jedoch keine rechtliche Grundlage dar, auf die eine längerfristige Observation gestützt werden kann. Durch den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) konnten im Rahmen der Akteneinsicht diesbezüglich weder Einlassungen seitens des Gerichts noch seitens der Staatsanwaltschaft festgestellt werden.

Im Übrigen waren in den vorliegenden Fällen auch die Voraussetzungen für eine kurzfristige Observation einschließlich Fotodokumentationen gemäß §§ 161 Abs. 1, 163 Abs. 1 i. V. m. § 100 h StPO nicht erfüllt. Zwar ist für kurzfristige Observationsmaßnahmen und

in diesem Zusammenhang auch für die Herstellung von Lichtbildern keine richterliche Anordnung vorgesehen, dennoch muss auch hier der Anfangsverdacht begründet sein. Dieser muss sich auf zureichende tatsächliche Anhaltspunkte, das heißt auf konkrete Tatsachen stützen, die dafür sprechen, dass gerade der zu untersuchende Lebenssachverhalt eine Straftat enthält (vgl. Graf, StPO Kommentar, § 152 Rn. 4). Die bloße Vermutung rechtfertigt es nicht, einer Person eine Tat zur Last zu legen. Demnach reichte es hier für einen (Anfangs-)Verdacht auch nicht aus, dass unbekannte und daher unverdächtige Personen in ein Dienstfahrzeug der PI Mühlhausen einstiegen.
Der TLfDI musste im Ergebnis davon ausgehen, dass – im Rahmen der zulässigen durchgeführten längerfristigen Observation – grundsätzlich alle Personen, die die Dienstfahrzeuge der PI Mühlhausen nutzten, observiert wurden. Die konkreten Verdachtsmomente beschränkten sich indes nur auf die in den richterlichen Anordnungen erwähnten vier Zielpersonen.
Durch den Einsatz heimlicher Observationsmaßnahmen ohne rechtliche Grundlage wurde intensiv in das Recht auf informationelle Selbstbestimmung der drei betroffenen Personen eingegriffen. Diese erhebliche datenschutzrechtliche Verletzung hat der TLfDI förmlich nach § 39 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet.

Da die heimlichen Observationsmaßnahmen durchgeführt und bereits abgeschlossen waren, konnte die datenschutzrechtliche Verletzung im Sinne des § 39 Abs. 1 Satz 1 ThürDSG nicht mehr behoben werden. Der TLfDI fordert jedoch in einem solchen Fall die zuständigen Stellen dazu auf, für die Zukunft darauf hinzuwirken, dass solche datenschutzrechtlichen Verstöße im Rahmen der Verarbeitung und Nutzung personenbezogener Daten unterbleiben. Die Umsetzung solcher Maßnahmen prüft der TLfDI im Rahmen einer Nachkontrolle.

7.4 Die Polizei auf Abwegen – Teil 2

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bekannt, dass auch gegen Polizeibeamte der Landespolizeiinspektion (LPI) Jena ermittelt wurde. Auslöser der Ermittlungen war auch hier eine anonyme Anzeige

gegen zwei namentlich benannte Tatverdächtige. In dieser wurde den zwei Beamten zur Last gelegt, dass sie während der Dienstzeit für private Zwecke (Einkäufe und Wohnungskontrollen) dienstliche Kraftfahrzeuge nutzen würden.
Daraufhin wurde gegen die zwei Beamten von Amts wegen ein Ermittlungsverfahren wegen des Verdachts der Untreue und des Betruges eingeleitet. Das zuständige Amtsgericht erließ Beschlüsse für eine längerfristige Observation der zwei Beschuldigten. Da für die längerfristige Observation der zwei beschuldigten Personen nach § 163 f Strafprozessordnung (StPO) zu Beginn der Ermittlungen richterliche Beschlüsse vorlagen und damit eine gesetzliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung gegeben war, war die längerfristige Observation der zwei Beamten datenschutzrechtlich nicht zu beanstanden.
Darüber hinaus war den Akten zu entnehmen, dass im Zuge der oben genannten zulässigen Observationsmaßnahmen auch weitere Beamte von der Maßnahme betroffenen waren. Aus datenschutzrechtlicher Sicht ist insoweit entscheidend, ob die weiteren Observationen ebenfalls auf einer rechtlichen Grundlage beruhten. Anhand der vorgelegten Akten konnte jedoch ein Anfangsverdacht gegen zwei weitere Personen auch bei Beginn einer nur kurzfristigen Observationen nach §§ 161 Abs. 1, 163 Abs. 1 i. V. m. § 100 h StPO nicht begründet werden. Vielmehr ergab sich aus den Unterlagen, dass zunächst unbekannte und daher unverdächtige Polizeibeamte, die die Dienstfahrzeuge nutzten, observiert wurden. Der TLfDI musste deshalb davon ausgehen, dass – im Rahmen der durchgeführten längerfristigen Observation – grundsätzlich alle Personen, die die Dienstfahrzeuge der LPI Jena nutzten, observiert wurden. Die Verdachtsmomente beschränkten sich aber zu Beginn der Ermittlungen indes nur auf die in den richterlichen Anordnungen erwähnten zwei Zielpersonen. Da durch die Ermittlungsbeamten nicht festgestellt werden konnte, welche Person sich jeweils im Fahrzeug befand, hätte auch aus Verhältnismäßigkeitsgesichtspunkten die Observation unterlassen oder die zuständige Behördenleitung um Auskunft über die Identität der jeweiligen Person ersucht werden müssen. Dies ist aber nicht geschehen. Das Verhalten der Observationskräfte erscheint daher vielmehr so, als wäre eine Vielzahl der Polizeibeamten so lange beobachtet worden, bis sie „negativ“ aufgefallen sind. Die datenschutzrechtliche Würdigung war zum Zeitpunkt des Tätigkeits-

berichts noch nicht abgeschlossen. Über dessen Ausgang wird im kommenden Tätigkeitsbericht berichtet werden.

Die Strafprozessordnung unterscheidet bei Observationen zwischen einer längerfristigen Observation und einer kurzfristigen Observation. Die längerfristige Observation ist in § 163 f StPO geregelt und muss grundsätzlich durch ein Gericht angeordnet werden. Die kurzfristige Observation, sofern sie unter Einsatz technischer Mittel vorgenommen wird, richtet sich hingegen nach §§ 161 Abs. 1, 163 Abs. 1 i. V. m. § 100 h StPO und ist beim Anfangsverdacht einer Straftat zulässig. Einschränkungen können sich aber aus dem Grundsatz der Verhältnismäßigkeit ergeben, den die Ermittlungsbeamten stets zu beachten haben.

7.5 Auch Bilder und Videos können Träger personenbezogener Daten sein

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Eingabe eines besorgten Bürgers. Dieser trug vor, dass er sich an das Thüringer Landeskriminalamt (TLKA) mit der Bitte gewandt habe, ihm auf Rechtsgrundlage des § 47 Thüringer Gesetzes über die Aufgaben und Befugnisse der Polizei (ThürPAG) seine dort gespeicherten personenbezogenen Daten mitzuteilen. Gemäß § 47 Abs. 1 Satz 1 ThürPAG erteilt die Polizei dem Betroffenen auf Antrag über die zu seiner Person gespeicherten Daten (hierzu zählt auch etwaiges Bild- oder Videomaterial) Auskunft. Der Betroffene hegte insbesondere im Hinblick auf eventuell vom TLKA gespeichertes Bild- oder Videomaterial Zweifel an der Vollständigkeit der Auskunft und beschwerte sich über die Vorenthaltung seiner personenbezogenen Daten.
Der TLfDI forderte das TLKA zunächst schriftlich auf, zum Vorwurf Stellung zu nehmen. Das TLKA wies den Vorwurf zurück und bekräftigte, weder Bild- noch Videomaterial dem Bürger vorzuenthalten.
Der TLfDI sah es sodann als sinnvoll an, sich in einem Ortstermin beim TLKA von der Richtigkeit dieser Aussage zu überzeugen. Im Rahmen dieses Termins wurde auch die betreffende Kriminalakte des Bürgers gesichtet. Dabei konnte festgestellt werden, dass kein Bild- oder Videomaterial zum Betroffenen beim TLKA existiert.

Daneben überprüfte der TLfDI auch die einzelnen Datenspeicherungen zum Bürger sowie die Einhaltung der dazu festgelegten Prüffristen. Auch diese entsprachen den bestehenden Regelungen, sodass der TLfDI nach einer entsprechenden Auskunft an den Bürger den Vorgang abschließen konnte.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 ThürDSG). Beispiele hierfür sind: Name, Alter, Geburtsdatum, Anschrift, Kfz-Kennzeichen, Personalausweisnummer, Vorstrafen, genetische Daten usw.
Die technische Form personenbezogener Daten ist dabei nicht von Bedeutung. Auch Fotos, Videoaufnahmen, Röntgenbilder oder Tonbandaufnahmen (Aufzählung ist nicht abschließend) können demnach personenbezogene Daten enthalten.

7.6 Videoüberwachung von Gewahrsamsräumen – in Thüringen ohne gesetzliche Grundlage unzulässig: Videogaga 6

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) haben in der jüngeren Vergangenheit mehrfach Anfragen von Thüringer Polizeibeamten erreicht, ob und unter welchen gesetzlichen Voraussetzungen die Überwachung von Gewahrsamsräumen der Thüringer Polizei mittels Bildübertragung zulässig ist. Hintergrund dieser Anfrage waren unter anderem durch Insassen verursachte (Sach-)Beschädigungen in den Gewahrsamsräumen der Polizei.
Eine Regelung, durch die die Polizei befugt ist, eine Überwachung mittels Bildübertragung in Gewahrsamsräumen durchzuführen, gibt es bis dato in Thüringen nicht. Weder das Thüringer Datenschutzgesetz (ThürDSG) noch das Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (ThürPAG) bieten dazu eine ausreichende Rechtsgrundlage. Auch § 19 Abs. 1 ThürDSG ist als Ermächtigungsgrundlage für eine Videoüberwachung mit Aufzeichnung des gewonnenen Bildmaterials nicht hinreichend bestimmt. Hierzu kann vergleichsweise die Entscheidung des Bundesverfassungsgerichts vom 23. Februar 2007 (Az. 1 BvR 2368/06) herangezogen werden. Das Bundesverfassungsgericht hatte in dieser Entscheidung die Anwendung von § 16 Abs. 1 Bayerisches Datenschutzgesetz, der vom

Wortlaut mit § 19 Abs. 1 ThürDSG identisch ist, für unzulässig erklärt.
Aus datenschutzrechtlicher Sicht ist daher die Videoüberwachung bzw. die akustische Überwachung von Gewahrsamsräumen bei der Polizei in Thüringen zum jetzigen Zeitpunkt nicht zulässig.
Der TLfDI hat die Problematik im Kreise der Datenschutzbeauftragten des Bundes und der Länder aufgegriffen und diese um Rückmeldung hinsichtlich der Praxis in den übrigen Bundesländern gebeten.
Die Rückmeldungen aus den anderen Bundesländern haben ergeben, dass in den meisten Polizei-/Ordnungsbehördengesetzen eindeutige Rechtsgrundlagen für eine Videoüberwachung (und teilweise auch für Tonaufzeichnungen) in Gewahrsamsräumen vorhanden sind, so z. B. in Baden-Württemberg, Hamburg, Hessen, Rheinland-Pfalz und Sachsen-Anhalt.
Da eine Bild-/ Tonaufzeichnung in Gewahrsamsräumen durchaus erforderlich scheint, jedoch weder im ThürPAG noch im ThürDSG ausreichende Rechtsgrundlagen für eine solche Überwachung enthalten sind, hat es sich der TLfDI zur Aufgabe gemacht, weiterhin auf eine entsprechende normative Klärung im Rahmen einer künftigen Novellierung des ThürPAG hinzuwirken.

Eine entsprechende Stellungnahme inklusive Formulierungs- und Ergänzungsvorschlag zu § 21 ThürPAG („Behandlung festgehaltener Personen“) hat der TLfDI dem Thüringer Landtag im Rahmen des Anhörungsverfahrens zur Novellierung des Thüringer Polizeiaufgabengesetzes vorgelegt. Dieser Vorschlag wurde vom Thüringer Landtag aber leider nicht aufgegriffen. Es fehlt daher in Thüringen weiterhin eine eindeutige Rechtsgrundlage zur Videoüberwachung von Gewahrsamsräumen.
Weitere Ausführungen zur Novellierung des Thüringer Polizeiaufgabengesetzes finden Sie in dem Beitrag unter der Überschrift: „Novellierung des Thüringer Polizeiaufgabengesetzes – auf die lange Bank geschoben und am Ende wenig erreicht.“

7.7 "Betäubungsmittel-Konsument" – eine Jugendsünde fürs Leben?

Im Berichtszeitraum wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde eines Bürgers zugeleitet, der zu entnehmen war, dass im

bundesweiten Informationssystem der Polizei (INPOL BUND) Eintragungen über ihn enthalten seien – eingestellt vom Bundeskriminalamt (BKA) und vom Thüringer Landeskriminalamt (TLKA). Dabei handele es sich unter anderem um eine Eintragung zu einem Verstoß gegen das Betäubungsmittelgesetz (BtmG). Die Aussonderungsprüffrist war für Mitte 2015 festgelegt. Die Aussonderungsprüffrist ist die Frist, nach der regelmäßig zu prüfen ist, ob eine weitere Speicherung erforderlich ist. Nach Aussage des Beschwerdeführers war der Grund für die Eintragung ein Ermittlungsverfahren einer thüringischen Polizeiinspektion, das bereits 17 Jahre zurückliege. Der Betroffene gab an, in der Vergangenheit regelmäßig Opfer von polizeilichen Maßnahmen (z. B. Drogentests, Fahrzeug- oder Gepäckdurchsuchungen, Verkehrs- und Personenkontrollen, Befragungen) gewesen zu sein. Der Beschwerdeführer war der Auffassung, dass der Eintrag „Betäubungsmittel (BtM)-Konsument“ längst hätte gelöscht sein müssen.

Der TLfDI ist gemäß § 2 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) für die datenschutzrechtliche Prüfung des Vorganges beim TLKA zuständig. Dabei stellte sich heraus, dass das Delikt im Bereich des BtmG bereits im Jahr 1994 begangen wurde. Die zuständige Polizeidienstelle konnte gegenüber dem TLfDI nicht mehr plausibel darlegen, warum der Datensatz aus dem Jahr 1994 mit dem personengebundenen Hinweis „BtM-Konsument“ bis ins Jahr 2015 vorgehalten werden sollte. Ferner war auch die Beendigung des Ermittlungsverfahrens durch die Polizei nicht mehr nachvollziehbar. Es ist zwar richtig, dass bei neuen Ereignissen nach der Thüringer Verordnung über die Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) die Prüffrist/Aussonderungsfrist durch die Polizei verlängert werden kann. Jedoch hat dies der TLfDI im vorliegenden Falle weder für zwingend noch für sachlich begründbar gehalten.

Das TLKA hat sodann eine neuerliche Löschüberprüfung des Datensatzes vorgenommen. Da inzwischen keine neuen Erkenntnisse aus dem Deliktsbereich des BtMG gewonnen werden konnten, erfolgte die Löschung des personengebundenen Hinweises „BtM-Konsument.“

Der Vorgang konnte sodann vom TLfDI mit einem abschließenden Prüfbericht an den Betroffenen abgeschlossen werden.

Die ThürPolPrüffristVO schreibt keine absoluten Speicher- und Aufbewahrungsfristen vor, nach denen die Polizei zu einem bestimmten Zeitpunkt zur Löschung oder Aktenvernichtung verpflichtet ist. Die Datenspeicherung richtet sich vielmehr nach dem Grundsatz der Erforderlichkeit für die polizeiliche Aufgabe. Somit ist die Polizei auch nach Ablauf der Prüffrist nicht zur Löschung verpflichtet, wenn fachliche Gesichtspunkte (z. B. Art und Weise der Tat, Persönlichkeit des Täters oder sonstige kriminalistische Erfahrungen) eine weitere Speicherung erfordern.

7.8 „Jungbrunnen" für Prüf- und Löschfristen

Im Berichtszeitraum hatte sich ein Rechtsanwalt an den Thüringer Landesbeauftragten für den Datenschutz und Informationsfreiheit (TLfDI) gewandt, um für seinen Mandanten die polizeiliche Datenspeicherung innerhalb der Thüringer Polizei zu überprüfen. Der Rechtsanwalt trug vor, dass eine Polizeidienstelle in einem Abschlussbericht die Formulierung „mehrfach polizeilich in Erscheinung getreten“, bezogen auf seinen Mandanten verwendet habe. Diese sei nach Auffassung des Rechtsanwaltes eine fehlerhafte Bezeichnung, da im Bundeszentralregister nur ein einziger Eintrag seines Mandanten enthalten und gegen ihn nur einmalig wegen Körperverletzung ermittelt worden sei.
In dem vom Rechtsanwalt erwähnten Abschlussbericht waren die Delikte aufgeführt, bei denen sein Mandant im polizeilichen Datenbestand als Beschuldigter geführt wurde. Gemäß Mitteilung der Landespolizeidirektion orientierte sich der Abschlussbericht (der unter anderem die Angabe der Delikte „Warenbetrug, Körperverletzung, Diebstahl“ enthielt) am polizeilichen Datenbestand und nicht an den Eintragungen des Bundeszentralregisters, auf das die Polizei in der Regel keinen Zugriff hat. Der Begriff „polizeilich in Erscheinung getreten“ umfasst Fälle, in denen zurückliegend gegen den Beschuldigten aufgrund eines Tatverdachts ermittelt wurde – unabhängig vom Ausgang des Verfahrens.
Der TLfDI konnte im Rahmen seiner datenschutzrechtlichen Prüfung feststellen, dass entgegen der Aussage des Rechtsanwaltes, es seien keine weiteren Verfahren gegen seinen Mandanten bekannt, derzeit sehr wohl noch weitere Verfahren gegen diesen anhängig sind.
Gemäß Aufforderung des TLfDI überprüfte die zuständige Landespolizeiinspektion die jeweiligen Speicherungen auf einzuhaltende

Aussonderungsprüffristen und kam zu dem Ergebnis, dass die vorgenommenen und noch existenten Speicherungen den Vorgaben der §§ 38, 40 Abs. 2 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (ThürPAG) in Verbindung mit der Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) bis auf einen Fall entsprach. Aus diesem Grunde wurde lediglich die Löschung eines Datensatzes wegen einer Verkehrsordnungswidrigkeit aus dem Jahr 2004 veranlasst, da der Betroffene hier seitdem nicht mehr auffällig wurde.
Das Vorgehen der Landespolizeiinspektion erfüllte die geltenden Regelungen. Gemäß § 5 Abs. 1 ThürPolPrüffristVO beginnt die Prüffrist an dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung geführt hat. Dies bedeutet konkret, dass, falls vor Ablauf der Prüffrist eines Ermittlungsverfahrens ein weiteres Ereignis (in dem sich der Verdacht gegen dieselbe Person richtet) hinzugetreten ist, sich die Prüffrist des ersten Verfahrens nach der des neu hinzugekommenen bestimmt. Hierbei handelt es sich nicht um eine Verlängerung nach § 2 Abs. 4 ThürPolPrüffristVO, sondern um einen neuen Beginn der Prüffrist, dessen Ende sich am letzten eingetretenen Ereignis, das Anlass für eine Speicherung der Daten bot, ausrichtet. Bezogen auf den Mandanten ließ sich generell feststellen, dass vor dem jeweiligen Ablauf der Prüffrist eines Delikts, das dem Tatverdacht zu Grunde lag, ein neues Ermittlungsverfahren eingeleitet wurde und sich daher die Prüffristen für alle in der Vergangenheit liegenden Ereignisse nach der Prüffrist des letzten neuen Ereignisses (Verdachts der Bedrohung und gefährlichen Körperverletzung vom Frühjahr 2012) richtete. Die Prüffrist betrug in diesem Fall gemäß § 2 Abs. 1 ThürPolPrüffristVO fünf Jahre. Demnach sind die personenbezogenen Daten zum Betroffenen im Frühjahr 2017 – soweit kein weiteres Ermittlungsverfahren gegen ihn eingeleitet werden wird – zu löschen.
Auch wenn die Speicherungen der personenbezogenen Daten des Mandanten teils mehrere Jahre zurück lagen, entspricht dies den geltenden gesetzlichen Regelungen und konnte damit seitens des TLfDI nicht beanstandet werden. Dieser „Jungbrunnen“ für Prüf-/Löschfristen ist aus datenschutzrechtlicher Sicht nicht akzeptabel.

In der Praxis ist regelmäßig festzustellen, dass § 5 Abs. 1 Satz 1 ThürPolPrüffristVO erhebliche Bedeutung zukommt. Soweit innerhalb der Speicherfrist für ein Ereignis – auf-

grund eines neuen Ereignisses (Straftat) – eine weitere Speicherung hinzukommt, wird das für den neuen Fall berechnete Prüfdatum bzw. die Prüffrist (aus §§ 38, 40 Abs. 2 ThürPAG in Verbindung mit ThürPolPrüffristVO) für die gesamte Speicherung maßgeblich; es kommt damit zum einem „Neustart“ der jeweiligen Prüffrist. Aufgrund der neuen Speicherung unterfallen weiter zurückliegende Ereignisse letztendlich der festgesetzten neuen Prüffrist.
Dieser „Jungbrunnen“ für Prüf-/ Löschfristen ist aus datenschutzrechtlicher Sicht nicht akzeptabel. Vielmehr muss für jedes einzelne Ereignis auch eine separate Prüffrist gelten. Dabei ist entscheidend, dass die Akten anlässlich der Einzelfallbearbeitung oder nach Ablauf der jeweiligen Prüffrist „in die Hand genommen werden“, eine Erforderlichkeitsprüfung durchgeführt wird und in diesem Zusammenhang entweder eine weitere Prüffrist (für das jeweilige Ereignis) festgelegt wird oder die Daten gelöscht bzw. vor Aktenvernichtung dem Archiv angeboten werden.
Weitere Ausführungen hierzu finden sie im Leitfaden des TLfDI zu den Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut; zu finden auf der Internetseite des TLfDI (http://www.tlfdi.de/tlfdi/, dort unter Themen / Orientierungshilfen).

7.9 Moratorium gegen die Vernichtung von Akten mit Bezügen zum Nationalsozialistischen Untergrund (NSU)

Nach der Aufdeckung der rechtsextremen Zelle des „Nationalsozialistischen Untergrunds“ und des „Schredderns“ von Akten hatte der zuständige Untersuchungsausschuss im Deutschen Bundestag ein Moratorium gegen die Vernichtung von Unterlagen, die im Zusammenhang mit den Untersuchungsgegenstand stehen könnten, gefordert. In der Sache ging es dem Untersuchungsausschuss primär um die Sicherstellung seines verfassungsrechtlich verankerten Auskunfts- und Aufklärungsanspruchs bzw. Amtshilfeanspruchs gegenüber der exekutiven Gewalt. Dieser sollte nicht dadurch vereitelt werden, dass im Bereich der Exekutiven durch die Berufung auf datenschutzrechtliche Löschungs- und Sperrungsvorschriften entsprechende Unterlagen und Dateien vernichtet werden können.
Das Thüringer Innenministerium bat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine datenschutzrechtliche Einschätzung zu einem möglichen Erlass

auf Landesebene im Sinne des Petitums des Untersuchungsausschusses des Deutschen Bundestages.
Dem standen aus datenschutzrechtlicher Sicht keine Bedenken entgegen.
Das Thüringer Polizeiaufgabengesetz (ThürPAG) sieht in § 45 Abs. 4 Nr. 2 ThürPAG unter anderem vor, dass eine Löschung und Vernichtung von Unterlagen unterbleibt, wenn die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind. Soweit die allgemeinen Aufbewahrungsfristen zu den gespeicherten personenbezogenen Daten verstrichen sind, kommt eine Aufbewahrung nach dieser Norm in Betracht, worunter aus Sicht des TLfDI auch das Verfahren des Untersuchungsausschusses zu zählen ist. Soweit es für die Behebung einer Beweisnot unerlässlich ist, weil entscheidungserhebliche Tatsachen nicht anders als durch die Vorlagen der zur Löschung oder Vernichtung heranstehenden Daten bzw. Unterlagen bewiesen werden könnten, muss eine Löschung unterbleiben. Aus Sicht des TLfDI sind somit grundsätzlich alle Unterlagen und Dateien von dem Moratorium erfasst, die nicht nur bis zum Beginn des Moratoriums bzw. der Einsetzung der Untersuchungsausschüsse vorgelegen haben, sondern auch künftige Unterlagen und Dateien, die während der Untersuchungsausschüsse bis zu deren Abschluss hinzukommen und hinsichtlich des Untersuchungszweckes relevant sind. In dieser Hinsicht ist der § 45 Abs. 4 Nr. 2 ThürPAG verfassungskonform auszulegen.
Das Thüringer Verfassungsschutzgesetz (ThürVSG) sieht in § 9 Abs. 2 ThürVSG hingegen vor, dass Daten zu löschen sind, wenn ihre Speicherung unzulässig war oder ist oder ihre Kenntnis für die Erfüllung der gesetzlichen Aufgaben nicht mehr erforderlich ist. Nur wenn Grund zu der Annahme besteht, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt würden, unterbleibt gemäß § 9 Abs. 2 Satz 3 ThürVSG die Löschung oder Vernichtung. Die schutzwürdigen Belange der jeweils Betroffenen würden jedoch im Zusammenhang mit der Aufbewahrung für Zwecke des Untersuchungsausschusses nicht zum Tragen kommen. Auch eine ergänzende Anwendung des § 16 Thüringer Datenschutzgesetz (ThürDSG), der den Anspruch auf Löschung personenbezogener Daten normiert, scheidet aus, weil dies § 30 ThürVSG ausdrücklich ausschließt.
Dies bedeutet aus der Sicht des TLfDI jedoch nicht, dass nicht weitere Gründe eine endgültige Löschung oder Vernichtung insbesondere von Unterlagen, die für die Untersuchung in einen parlamentarischen

Untersuchungsausschuss benötigt werden könnten, verbieten können.
In Anbetracht des verfassungsrechtlichen Rangs eines eingesetzten Untersuchungsausschusses ist jeweils im Hinblick auf den Untersuchungsgegenstand und den Kompetenzbereich Art. 44 Abs. 3 Grundgesetz (GG) auf Bundesebene und Art. 64 Abs. 4 der Verfassung des Freistaats Thüringen (VerfThür) auf Landesebene zu beachten. Nach der bundesrechtlichen Vorschrift sind die Gerichte und Verwaltungsbehörden einem Untersuchungsausschuss zur Amtshilfe verpflichtet. Näheres ist in § 18 Gesetz zur Regelung des Rechts der Untersuchungsausschüsse des Deutschen Bundestages (PUAG) geregelt. Im Rahmen der Beweiserhebung können unter anderem auch Akten beigezogen werden. Dasselbe gilt auf Landesebene. Die Landesregierung und die öffentlichen Stellen sind nach Art. 64 Abs. 4 Satz 2 VerfThür verpflichtet, die von den Untersuchungsausschüssen angeforderten Akten vorzulegen und Auskünfte zu erteilen. Näheres hierzu ist in §§ 13, 14 Thüringer Untersuchungsausschussgesetz (ThürUAG) ausgestaltet. Würde das Landesamt für Verfassungsschutz nach Anforderung von Akten und Auskünften diese personenbezogenen Daten mangels weiterer Erforderlichkeit zur eigenen Aufgabenerfüllung oder wegen Ablaufs von Aufbewahrungsfristen löschen oder vernichten, wäre damit die parlamentarische Untersuchung vereitelt. Aufgrund des Rangs und der Bedeutung der parlamentarischen Untersuchung ist aus der Sicht des TLfDI nach Bekanntwerden der Einsetzung eines Untersuchungsausschusses mit einem konkreten Auftrag, der sich auch auf beim Verfassungsschutz vorhandene Unterlagen bezieht, eine Löschung wegen Wegfalls der Erforderlichkeit zur eigenen Aufgabenerfüllung oder dem Ablauf etwaiger Aufbewahrungsfristen nicht mehr zulässig.
Daher ist hinsichtlich § 9 Abs. 2 ThürVSG im Lichte des Art. 64 Abs. 4 VerfThür eine verfassungskonforme Auslegung angezeigt.

Im Ergebnis der Stellungnahme des TLfDI wurde der gesamte Geschäftsbereich des Thüringer Innenministeriums angewiesen bis auf weiteres die Aktenvernichtung und -löschung auszusetzen, die den Untersuchungsgegenstand der gegenständlichen Untersuchungsausschüsse betreffen.

Der rechtsextremen Zelle Nationalsozialistischer Untergrund (NSU) werden bundesweit zehn Morde zur Last gelegt. Aufgrund einer Reihe von „Ermittlungspannen“ sind bundesweit die Verfassungsschutzämter stark in die Kritik geraten. So sind wichtige Unterlagen von den Verfassungsschützern vernichtet worden. Erst aufgrund eines Moratoriums konnte das „vorläufige Einfrieren“ der Unterlagen, die im Zusammenhang mit der Aufklärungsarbeit der Untersuchungsausschüsse des Bundestages und des Thüringer Landtages erforderlich sind, bewirkt werden.

7.10 Videoüberwachung aus dem Blumentopf – zur Aufklärung von Einbrüchen erlaubt!: Videogaga 7

Im Herbst 2012 erhielt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) Kenntnis über eine ungewöhnliche Videoüberwachung: Einem Bürger aus Weimar war auf dem Grundstück seines Nachbarn eine als Blumentopf getarnte Videokamera aufgefallen. Die Videokamera erfasste nach Aussage des Bürgers den gesamten Straßenbereich und damit auch seinen Einfahrtbereich. Nach Aussage der anderen Nachbarn sei die Kamera bereits länger zur Aufklärung von Einbrüchen installiert gewesen. Ein Anruf bei der Polizei bestätigte diesen Zweck der Videoüberwachung. Der Bürger fragte den TLfDI unter anderem, ob er sich mit dieser Art der Videoüberwachung abfinden müsse.

Der TLfDI wandte sich zwecks Sachaufklärung zunächst an die Landespolizeiinspektion (LPI) Jena und bat um Auskünfte zum geschilderten Sachverhalt. Als diese Auskunft dem TLfDI vorlag, stellte sich der Fall folgendermaßen dar:

In der Tat hatte die Polizei die besagte Videokamera installiert, nachdem es im Jahr 2011 zu insgesamt 20 Einbrüchen im Wohnumfeld des Bürgers aus Weimar gekommen war. Die Einrichtung einer solchen Videoüberwachungsanlage ist nach § 100 h Abs. 1 Satz 1 Strafprozessordnung (StPO) zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes auf andere Weise weniger erfolgversprechend oder erschwert wäre.

Der Schwerpunkt der Videoüberwachung bestand nach Auskunft der LPI Jena in der Erkennbarkeit von Fahrzeugkennzeichen sowie von Personen im Bereich der Straßenzufahrten des Wohngebietes. Weiterhin versicherte die LPI Jena, dass das Einverständnis der Hausbe-

wohner, bei denen die Videoüberwachung erfolgte, vorher schriftlich eingeholt wurde. Zudem informierte die Polizei vor dem Zeitpunkt der Installation der Kameras im Rahmen einer Einwohnerversammlung für den betroffenen Bereich. Wie die Einladungen zu dieser Veranstaltung erfolgten und warum gerade der betroffene Bürger eine solche Einladung nicht erhalten hatte, ließ sich dabei durch den TLfDI nicht mehr aufklären.

Die im Rahmen der Videoüberwachung entstandenen Aufzeichnungen wurden maximal nach drei Tagen durch aktuelle Aufnahmen überschrieben und nach Abbruch der Videoüberwachung im August 2012 insgesamt gelöscht.

Der TLfDI kam nach datenschutzrechtlicher Prüfung zu dem Ergebnis, dass die von der Polizei dargelegte Vorgehensweise datenschutzrechtlich unbedenklich war. Ausschlaggebend dafür war zunächst, dass die von der Videoüberwachung betroffenen Anwohner vorab auf geeignete Weise darüber informiert wurden und die angefertigten Videoaufnahmen kurzzeitig wieder gelöscht wurden. Ferner lässt sich im Rahmen einer Herstellung von Bildaufnahmen nach § 100 h StPO niemals ausschließen, dass Dritte von dieser Maßnahme betroffen sein werden, denn ansonsten wäre diese Vorschrift sinnentleert (Meyer-Großner, StPO, § 100 h, Rz. 9). Dies berücksichtigte der TLfDI ebenfalls im Rahmen seiner datenschutzrechtlichen Prüfung.

Im Ergebnis teilte daher der TLfDI dem Bürger aus Weimar auf seine Frage mit, dass er die konkrete Videoüberwachung vom Grundstück seines Nachbarn zu dulden hatte.

Sofern Anwohner den Verdacht schöpfen, dass ihr Grundstück möglicherweise videoüberwacht wird, um damit die Aufklärung von Wohnungseinbrüchen zu erreichen, empfiehlt sich zunächst immer ein Gespräch mit der Polizei. Erst wenn hier Fragen des Bürgers offen bleiben, kann der TLfDI im Rahmen seiner Befugnisse nach § 38 Thüringer Datenschutzgesetz konkrete datenschutzrechtliche Prüfungen vornehmen, z. B. ob die Voraussetzungen einer Herstellung von Bildaufnahmen nach § 100 h StPO im konkreten Fall gegeben sind.

7.11 Mitteilung der Staatsanwaltschaften an Ausländerbehörden: Unterrichtung, statt Aktenübersendung

Bislang übermittelten die Thüringer Staatsanwaltschaften Abschriften der Strafbefehlsanträge und Anklageschriften auf Grundlage der Nr. 42 der Anordnung über Mitteilung in Strafsachen (MiStra) in Verbindung mit § 87 Abs. 4 Satz 1 Aufenthaltsgesetz (AufenthG) an die Ausländerbehörden.
§ 87 Abs. 4 Satz 1 AufenthG sieht jedoch lediglich vor, dass die für die Einleitung und Durchführung eines Strafverfahrens zuständigen Stellen die zuständige Ausländerbehörde unverzüglich über die Einleitung des Strafverfahrens sowie dessen Erledigung bei der Staatsanwaltschaft oder bei Gericht unter Angabe der gesetzlichen Vorschriften zu unterrichten haben.
Dies umfasst aus datenschutzrechtlicher Sicht nicht die Erlaubnis, alle oben genannten Abschriften an die Ausländerbehörden zu übersenden. Mit den Kopien werden in der Regel mehr Angaben zu den Betroffenen und gegebenenfalls auch Daten Dritter übermittelt, als für die Aufgabenerfüllung der empfangenden Ausländerbehörden erforderlich sind. Nach einhelliger Auffassung im Kreise der Datenschutzbeauftragten des Bundes und der Länder ist die Übermittlung der Anklageschrift oder entsprechender Strafbefehlsanträge an die örtliche Ausländerbehörde daher nicht zulässig.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hat dem Thüringer Justizministerium (TJM) mitgeteilt, dass er die Übermittlung der Anklageschrift bzw. des Strafbefehlsantrages an die örtliche Ausländerbehörde für unzulässig erachtet, da die gesetzliche Erlaubnis nach § 87 Abs. 4 AufenthG eine Übersendung entsprechender Abschriften nicht umfasst.

Das Thüringer Justizministerium hat sich entgegen früherer Äußerungen nunmehr der Auffassung des TLfDI angeschlossen und den Generalstaatsanwalt per Erlass aufgefordert, im Falle der Anklageerhebung nicht mehr von Amts wegen eine Abschrift der Anklageschrift an die Ausländerbehörden zu übersenden.

7.12 Erkennungsdienstliche Erfassung in den Polizeidienststellen

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten in der Vergangenheit vermehrt Beschwerden hinsichtlich erkennungsdienstlicher Erfassungen durch Beamte der Polizeidienststellen. Zumeist handelte es sich dabei um Beschwerden gegen die erkennungsdienstliche Behandlung an sich sowie die Ablehnung der Löschung erkennungsdienstlicher Daten durch die Polizei.

Die Polizei darf gemäß § 40 Abs. 1 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei rechtmäßig erlangte Daten in Akten und Dateien speichern, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Dies gilt auch für personenbezogene Daten, die im Rahmen der Verfolgung von Straftaten gewonnen worden sind.

So wurde in einem Fall die durchgeführte Erkennungsdienstliche (ED) - Behandlung im Rahmen eines Verfahrens wegen versuchten räuberischen Diebstahls angeordnet und durch die Landespolizeiinspektion Nordhausen durchgeführt. Zwar wurde das Ermittlungsverfahren gegen den Beschuldigten gemäß § 153 a Strafprozessordnung (StPO) eingestellt. Der Tatvorwurf wurde durch die geführten Ermittlungen und die Einstellung des Verfahrens jedoch nicht ausgeräumt. Vielmehr war die Einstellung mit einer Auflage verbunden. Somit bestand gegen den Beschuldigten weiterhin ein Restverdacht, welcher nicht zuletzt durch weitere Ermittlungsverfahren gegen ihn begründet wurde.

Aus diesem Grund liegen die Voraussetzungen einer weiteren Aufbewahrung der erkennungsdienstlichen Unterlagen bis zum Ende der durch Verordnung festgelegten Prüffrist (Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung) vor, sodass aus datenschutzrechtlicher Sicht der TLfDI keine Löschung der Daten verlangen konnte.

In einem anderen Fall wurde ein Jugendlicher durch die Polizeiinspektion (PI) Kyffhäuser auf Grundlage des § 81 b StPO erkennungsdienstlich erfasst. Danach dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden, soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist.

Dabei gibt es keine Sonderregelungen für die Behandlung von beschuldigten Jugendlichen. Lediglich die ED-Behandlung von Kin-

dern ist unzulässig. Jugendlicher ist gemäß § 2 Jugendgerichtsgesetz, wer zurzeit der (vorgeworfenen) Tat vierzehn, aber noch nicht achtzehn Jahre alt ist. Zum Zeitpunkt der ED-Behandlung war der Betroffene siebzehn Jahre jung und damit Jugendlicher im Sinne des Gesetzes. Grundsätzlich sind Jugendliche vor der ersten Vernehmung in angemessener Weise über ihre Rechte zu belehren. Dabei ist ihnen vor ihrer Entscheidung, in die Beschuldigtenvernehmung einzuwilligen, die Möglichkeit zu geben, mit einem Personensorgeberechtigten bzw. gesetzlichen Vertreter zu sprechen. Soweit der Jugendliche in die Beschuldigtenvernehmung einwilligt, ist eine Einwilligung des gesetzlichen Vertreters zur Entscheidung des Jugendlichen nicht mehr erforderlich.
Da der Jugendliche im vorliegenden Fall die Möglichkeit zur Rücksprache mit seinen Eltern hatte und freiwillig sein Einverständnis für die ED-Behandlung per Unterschrift erteilt hat, bedurfte es auch keiner nachträglichen Entscheidung des Erziehungsberechtigten.
Die PI Kyffhäuser hat den Jugendlichen vor der ED-Maßnahme belehrt sowie über die Aussonderungsprüffrist informiert. Ein Verstoß gegen datenschutzrechtliche Vorschriften war durch den TLfDI nicht feststellbar.

Unter den Begriff der Erkennungsdienstlichen Behandlung fasst die Strafprozessordnung alle Maßnahmen zusammen, die der Identifizierung eines Beschuldigten dienen. Sie kann sowohl der Aufklärung einer konkreten Straftat als auch der „Vorsorge für die künftige Strafverfolgung“ dienen. Im Zusammenhang mit einer ED-Behandlung können unter anderem Personalien, 10-Finger-Abdrücke, Handabdrücke, Lichtbilder sowie Personenbeschreibungen des Betroffenen erfasst werden.

7.13 Die Novellierung des Thüringer Polizeiaufgabengesetzes – auf die „lange Bank“ geschoben und am Ende wenig erreicht

Im März 2013 legte das Thüringer Innenministerium dem Kabinett den Gesetzentwurf „Thüringer Gesetz zur Änderung des Polizeiaufgabengesetzes und des Ordnungsbehördengesetzes“ zur ersten Beratung vor. Grund für den dringenden Novellierungsbedarf des Thüringer Polizeiaufgabengesetzes (ThürPAG) waren vor allem zwei verfassungsgerichtliche Entscheidungen: Zum einen der Beschluss des Bundesverfassungsgerichts (BVerfG) vom 24. Januar 2012 zur

Bestandsdatenspeicherung (Aktenzeichen 1 BvR 1299/05). In seinem Beschluss forderte das BVerfG unter anderem, dass eine Norm des Fach- bzw. Landesrechts die Rechtsgrundlage für die Auskunftsplicht eines Telekommunikationsunternehmens (Datenabruf) bilden muss, da § 113 Abs. 1 Satz 1 Telekommunikationsgesetz (TKG) eine solche Rechtsgrundlage nicht normenklar begründe (siehe dazu den Punkt 7.19 „Bestandsdatenabfrage nach § 113 Abs. 1 TKG – auch in Übergangszeiten kein rechtsfreier Raum“ in diesem Tätigkeitsbericht).

Zum anderen „fegte“ der Thüringer Verfassungsgerichtshof (ThürVerfGH) mit Urteil vom 21. November 2012 (VerfGH 19/09) das damals geltende ThürPAG in die „Gesetzesmülltonne“, weil viele der darin enthaltenen Regelungen „eine rechtssichere Gesetzesanwendung“ nicht zuließen, eine „schwer lesbare Formulierung“ enthielten, die „zu Missdeutungen Anlass“ gäben, oder aber „Voraussetzungen der polizeilichen Befugnisse nicht hinreichend bestimmt“ festlegten. Demzufolge erklärte der ThürVerfGH unter anderem die Regelungen zum Schutz von Berufsgeheimnisträgern (Geistliche, Verteidiger und Rechtsanwälte) in § 5 Abs. 4 ThürPAG alte Fassung (a. F.), Teile der Regelung zum Schutz des Kernbereichs privater Lebensgestaltung in § 35 Abs. 7 ThürPAG a. F. sowie wesentliche Passagen von § 34 a Abs. 3 ThürPAG a. F. zur Überwachung der Telekommunikation als mit der Verfassung des Freistaats Thüringen unvereinbar. Schließlich forderte der ThürVerfGH den Gesetzgeber auf, bis zum 30. September 2013 eine Neuregelung der gerügten Regelungen des ThürPAG zu treffen. Dieses „sportlich“ gesetzte Datum für die Gesetzgebung des Thüringer Landtages wird später noch interessant werden.

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) gab im Rahmen der so genannten Kabinettanhörung nach § 21 der gemeinsamen Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen (ThürGGO) im April 2013 eine erste Stellungnahme zum oben genannten Gesetzentwurf ab. Darin wies er insbesondere auf Folgendes hin:

- Der TLfDI empfahl, im Hinblick auf die deutliche Kritik des ThürVerfGHs, keinen konkreten Gefahrenbegriff im ThürPAG als Eingriffsvoraussetzung verwendet zu haben, diesen konkreten Gefahrenbegriff in § 34 Abs. 1, § 34 Abs. 2 Nr. 6, § 34 a Abs. 1 Satz 1,

§ 34 b Abs. 1 Satz 1, § 34 c Abs. 1, § 34 d Abs. 1 Satz 1 und § 34 e Abs. 1 Satz 1 ThürPAG aufzunehmen.

– Ebenfalls unter Hinweis auf das Urteil des ThürVerfGHs vom 21. November 2012 sah es der TLfDI als erforderlich an, auch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen nach § 34 Abs. 2 Nr. 2 b) ThürPAG unter den Vorbehalt einer richterlichen Anordnung zu stellen, soweit dieser Einsatz längerfristig erfolgt.
– Unter Hinweis auf die datenschutzrechtlich gelungene Regelung zur Bestandsdatenauskunft und zur Auskunft über so genannte dynamische Internetprotokoll (IP)-Adressen in Schleswig-Holstein hat der TLfDI sowohl die Einfügung eines Richtervorbehalts als auch die Aufnahme von konkreten Tatbestandsvoraussetzungen für die Auskunft zur Identifizierung von dynamischen IP-Adressen in das ThürPAG gefordert. In § 180 a Abs. 2 Satz 2 des Landesverwaltungsgesetzes Schleswig-Holstein ist dieses Instrument der Datenerhebung nur zulässig, wenn es im Einzelfall zur Abwehr einer bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Abwehr einer gegenwärtigen Gefahr eines gleichwertigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt erforderlich ist.

Nachdem im Mai 2013 der oben genannte Gesetzentwurf der Landesregierung in der Drucksache 5/6118 – ohne die genannten angeregten Änderungen des TLfDI – zur ersten Beratung in den Landtag eingereicht worden war, lag die weitere Gestaltungstätigkeit am Gesetzentwurf in den Händen des Innenausschusses. Dieser Ausschuss bat den TLfDI dann im Rahmen der parlamentarischen Anhörung um eine weitere Stellungnahme. Der TLfDI empfahl in seinem Schreiben an den Innenausschuss des Thüringer Landtags zusätzlich folgende Änderungen und Ergänzungen:

– Neben der Regelung über die Auskunftserteilung über dynamische IP-Adressen mahnte der TLfDI auch eine entsprechende Regelung zur Auskunftserteilung bei fest zugewiesenen IP-Adressen an.
– Ferner griff der TLfDI die massive Kritik auf, die nach Verabschiedung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsda-

tenauskunft durch Bundestag und Bundesrat laut geworden war, und legte seine Rechtsausfassung dar, dass eine Auskunftserteilung über dynamische IP-Adressen nicht zur Verfolgung von Ordnungswidrigkeiten eingesetzt werden könne. Dies ergibt sich nach Auffassung des TLfDI, die von anderen Landesdatenschutzbeauftragten geteilt wird, einerseits aus dem präzise gefassten Inhalt des genannten BVerfG-Beschlusses zur Bestandsdatenauskunft und andererseits aus dem Wortlaut des § 46 Abs. 3 Satz 1 des Gesetzes über Ordnungswidrigkeiten (OWiG), der Auskunftsersuchen über Umstände, die dem Post- und Fernmeldegeheimnis unterliegen, für unzulässig erklärt.

– Schließlich rügte der TLfDI auch die Regelung des § 34 e Abs. 3 Satz 4 ThürPAG, wonach eine richterliche Anordnung über eine Bestandsdatenauskunft dann nicht erforderlich ist, wenn der Betroffene über die Auskunft bereits Kenntnis erlangt hat. Der Eingriff in das Grundrecht des Betroffenen auf die informationelle Selbstbestimmung ist im Fall seiner Kenntnis nicht weniger schwerwiegend als in dem Fall, in dem der Betroffene nichts von der Auskunft über seine Bestandsdaten weiß.

Nun war es Aufgabe des Innenausschusses, die zahlreichen und wirklich konstruktiven Verbesserungsvorschläge der angehörten Experten zum suboptimal ausgearbeiteten Gesetzentwurf zu sichten und diesen dann mittels Beschlussempfehlung deutlich inhaltlich zu verbessern. Doch es geschah fast nichts. Denn zwischen der letzten Sitzung des Innenausschusses, in der das ThürPAG beraten wurde, und der abschließenden Beratung im Landtag am 19. September 2013 blieben gerade einmal fünf Tage Zeit. Und der ThürVerfGH hatte den Landtagsabgeordneten ja aufgegeben, die gerichtlich vorgegebenen Änderungen bis zum 30. September 2013 vorzunehmen. Beschlossen wurde daher von der Mehrheit im Innenausschuss und im Landtag lediglich noch eine inhaltliche Änderung zu § 34 ThürPAG. Änderungsanträge der Oppositionsfraktionen des Thüringer Landtags fanden keine Mehrheit. Mehr oder weniger aus der zeitlichen Not geboren wurde ferner die Idee, das ThürPAG mit einer Evaluierungsklausel in § 78 zu bereichern, die der Landesregierung auferlegt, dem Landtag spätestens Ende September 2014 einen Bericht über den notwendigen Anpassungs- und Ergänzungsbedarf

im ThürPAG vorzulegen. Der TLfDI beobachtet, ob dieses Zeitschema angesichts der Landtagswahl am 14. September 2014 realistisch ist oder ob nicht bereits zuvor der ThürVerfGH erneut in Sachen ThürPAG angerufen werden wird, was wahrscheinlich sein dürfte. Es bleibt spannend …

Das ThürPAG entspricht auch nach seiner Novellierung durch den Thüringer Landtag nicht den Vorgaben des ThürVerfGHs aus seinem Urteil vom 21. November 2012. Auch den Beschluss des BVerfGs zur Bestandsdatenspeicherung berücksichtigt das „neue“ ThürPAG nicht in dem erforderlichen Umfang. Unzureichend sind dabei insbesondere die Regelungen zur Auskunftserteilung über dynamische IP-Adressen und die Verwendung dieser Daten zur Verfolgung von Ordnungswidrigkeiten. Es ist daher sehr wahrscheinlich, dass auch das geltende ThürPAG erneut vom ThürVerfGH auf seine Verfassungswidrigkeit überprüft und verfassungskonform ausgerichtet werden wird.

7.14 IGVP und Findus

Im Spätherbst 2011 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Anfrage eines Berliner Rechtsanwalts. Namens seines Mandanten bat der Rechtsanwalt den TLfDI um Klärung der Rechtsfragen, auf welcher Rechtsgrundlage, aus welchem Anlass und mit welchem Inhalt personenbezogene Daten des Mandanten in den landesweiten polizeilichen Informationssystemen „IGVP“ (= Integrationsverfahren Polizei) und „Findus“ (= Fallinformation durchsuchen mit System) gesammelt worden waren. Obwohl sein Mandant nicht vorbestraft sei, hätten sich im „IGVP“ 19 Treffer als Beschuldigter und im „Findus“ 21 Treffer als Beschuldigter in den Jahren von 2003 bis 2010 gefunden. Ferner bat der Rechtsanwalt darum, dass bis zur Klärung der Rechtmäßigkeit der Datensammlung und ihres Inhalts keine Veränderungen oder Löschungen daran stattfinden.
Der TLfDI bat darauf die Polizeidirektion (PD) Erfurt um schriftliche Stellungnahme zu den aufgeworfenen Fragen und leitete zunächst die Bitte, keine Veränderungen oder Löschungen an der Datensammlung vorzunehmen, weiter. Die Polizeidirektion (PD) Erfurt antwortete darauf mit Schreiben vom Juni 2012 und teilte Folgendes mit:

Die Grundlagen für die Datenspeicherung, Zweckbindung und Datenübermittlung bildeten die §§ 39, 40 und 41 des Thüringer Polizeiaufgabengesetzes (ThürPAG), die darauf basierende Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) sowie die Dienstanweisung Kriminalaktennachweis (DA KAN) des Thüringer Innenministeriums im System ISTPOL und die Richtlinie zum Umgang mit dienstlichem Schriftgut sowie zur Akten- und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei (RLAktenThürPol).

Im System IGVP fanden sich zum Stichtag Mitte November 2011 über den betreffenden Mandanten insgesamt 42 Datensätze. 18 Einträge betrafen den Mandanten dabei als Beschuldigten. Dabei sei die letzte Tat (Verwenden von Kennzeichen verfassungswidriger Organisationen) mit dem Datum Ende August 2011 vermerkt worden. Die Prüffrist für alle diese Vorgänge resultiere – was zutreffend ist – aus der zeitlich längsten, rechtlich zulässigen Frist. Dabei entschieden entweder der jüngste aufgenommene Sachverhalt oder aber zurückliegende aufgenommene Sachverhalte auf Grund der Deliktschwere über die Dauer der weiteren Speicherung. Als spätester Prüfungstermin für die Löschung der personenbezogenen Daten wurde von der Polizeidirektion Erfurt dabei Ende August 2021 vermerkt. Dieser Termin ergäbe sich zu der aus zu diesem Zeitpunkt aktuellen Bewertung des letzten strafrechtlichen Sachverhalts (Tatzeit: Ende August 2011) und könne sich – was ebenfalls zutreffend ist – entweder durch Hinzukommen weiterer Ereignisse oder durch Wegfall eines Tatverdachts verändern.

Das heißt, dass, soweit innerhalb der Speicherfrist ein neues Vergehen hinzukommt, die neu für den aktuellen Fall berechnete Prüffrist für die gesamte Speicherung maßgeblich wird. Es kommt damit zu einem Neustart der jeweiligen Prüffrist. Aufgrund der neuen Speicherung unterfallen weiter zurückliegende Delikte letztendlich der festgesetzten neuen Prüffrist; ein „Jungbrunnen“ für Prüf-/Löschfristen. An dieser Stelle ist bereits darauf hinzuweisen, dass der beschriebene „Jungbrunnen für Prüf-/Löschfristen“ aus datenschutzrechtlicher Sicht nicht akzeptabel ist. Der TLfDI hat diese Verfahrensweise unter anderem in seinem Leitfaden „Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut beim Thüringer Landesamt für Verfassungsschutz, in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei sowie in den

Thüringer Staatsanwaltschaften“ kritisiert und eine händische Erforderlichkeitsprüfung jeder einzelnen Prüffrist angemahnt. Auf eine entsprechende normative Klärung dieser wesentlichen datenschutzrechtlichen Frage will der TLfDI hinwirken (siehe dazu Seite 23 des genannten Leitfadens).
Aber zurück zum Fall: Über den Mandanten seien nach Auskunft der PD Erfurt ferner im System IGVP sieben Einträge als Betroffener bzw. Beteiligter gespeichert und ferner 17 Datensätze abgelegt, in denen der Mandant als Zeuge, Geschädigter, Mitteiler oder Auskunftsperson geführt worden sei. All diese Datensätze unterlägen wiederum dem bereits dargestellten Aussonderungsverfahren.
Im System FINDUS fanden sich nach Auskunft der PD Erfurt über den Mandanten des Rechtsanwalts insgesamt 17 Einträge (ebenfalls zum Stichtag Mitte November 2011), wobei die längste Prüffrist hier bis zum 28. Mai 2019 für ein Verfahren wegen Beleidigung zur Tatzeit 28. Mai 2009 festgesetzt worden sei. Die Speicherfristen für die Daten im System FINDUS richten sich dabei gemäß der Errichtungsanordnung nach den Bestimmungen der §§ 38, 40 Abs. 2 und 45 PAG in Verbindung mit den §§ 2, 4, und 5 ThürPolPrüffristVO.
Schließlich fanden sich nach Auskunft der PD Erfurt auch Einträge in dem Kriminalaktennachweis (KAN), bei dem es sich um ein auf EDV-Basis geführtes Verzeichnis über alle Kriminalakten handelt, die nach den Richtlinien für die Führung polizeilicher personenbezogener Sammlungen (PPS-Richtlinien) zu Beschuldigten, Tatverdächtigen oder Personen, bei denen zur polizeilichen Gefahrenabwehr die Führung von Unterlagen erforderlich ist, geführt werden.

Abschließend teilte die PD Erfurt dem TLfDI mit, dass der Bitte des Rechtsanwalts des Mandanten, die Löschung von dessen Daten zu stoppen, im Rahmen der zur Verfügung stehenden Möglichkeiten Rechnung getragen worden sei.

Der TLfDI hat dann im Anschluss alle von der PD Erfurt zur Verfügung gestellten Angaben überprüft und im Ergebnis bei den Datenspeicherungen keine Verstöße gegen die genannten Rechtsgrundlagen festgestellt. Allerdings ist nicht zu verkennen, dass der Mandant aufgrund seines Engagements im zivilgesellschaftlichen Bereich immer wieder mit Straftaten oder Ordnungswidrigkeiten in Zusammenhang gebracht worden ist. Ob dies – insbesondere, weil es sich

teilweise gerade nicht um Straftaten mit erheblicher Bedeutung handelte- trotzdem eine Speicherung aller Datenbestände rechtfertigt und erforderlich macht, wird der TLfDI auch in seiner weiteren Arbeit und in Gesprächen mit der Polizei kritisch hinterfragen; auf eine Änderung der Vorschriften wirkt er hin.

§ 5 Abs. 1 Satz ThürPolPrüffristVO ist in seiner Wirkung nicht zu unterschätzen: Soweit innerhalb der Speicherfrist für ein Ereignis – aufgrund eines weiteren Vorfalls (Straftat) – eine weitere Speicherfrist hinzukommt, ist insoweit das für den neuen Vorfall berechnete Prüfdatum bzw. die Prüffrist (aus §§ 38, 40 Abs. 2 ThürPAG in Verbindung mit der ThürPolPrüffristVO für die Speicherung aller Vorfälle relevant. Der TLfDI hält diese Verfahrensweise für kritikwürdig und änderungsbedürftig. Daher empfiehlt es sich, bei gegebenen Anlässen, den Auskunftsanspruch nach § 47 Abs. 1 PAG gegenüber der Polizei – und bei Bedarf mit Unterstützung des TLfDI – geltend zu machen.

7.15 Vernichtung von Ermittlungsakten des TLKA nach der Ablauf der Aufbewahrungsbestimmungen – Leitfaden

Im Rahmen seines gesetzlichen Auftrages kontrolliert der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bei allen öffentlichen Stellen die Einhaltung der Bestimmungen des Thüringer Datenschutzgesetzes (ThürDSG) und anderer Rechtsvorschriften über den Datenschutz. Diese Regelung schließt nicht aus, auch bestehende datenschutzrechtliche Regelungen zu hinterfragen. Darüber hinaus berät der TLfDI die öffentlichen Stellen und gibt Empfehlungen zur Verbesserung des Datenschutzes.
In der Vergangenheit haben den TLfDI vielfach die komplexen und mitunter recht undurchsichtigen „Regelungslandschaften“ der Aufbewahrungs- und Prüffristen beim Thüringer Landesamt für Verfassungsschutz (TLfV), der Thüringer Polizei sowie in den Thüringer Staatsanwaltschaften beschäftigt. Diverse Fragestellungen sowohl seitens dieser öffentlichen Stellen als auch von Thüringer Bürgerinnen und Bürgern werden an den TLfDI herangetragen, mit denen die unterschiedlichen Aufbewahrungsfristen von personenbezogenen Daten und dienstlichem Schriftgut, insbesondere bei den erwähnten öffentlichen Stellen thematisiert werden. Deshalb ist vom TLfDI nun ein Leitfaden über die entsprechenden Aufbewahrungsfristen für

personenbezogene Daten und dienstliches Schriftgut unter Beachtung der archivrechtlichen Bestimmungen erarbeitet worden. Der TLfDI möchte damit den Praktikern einen ‚roten Faden' an die Hand geben, damit Probleme erst gar nicht entstehen oder aber bürgerfreundlich schnell gelöst werden können.

Schwerpunktmäßig thematisiert die Broschüre die Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut und weist dabei insbesondere im komplexen Regelungssystem der Thüringer Polizei auch auf Novellierungsbedarf hin.

So bilden beispielsweise die §§ 38 bis 45 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (ThürPAG) die gesetzlichen Rechtsgrundlagen für die Dauer der polizeilichen Datenspeicherung. Während § 38 ThürPAG allgemeine Regeln über die Dauer der Datenspeicherung aufstellt, hält § 45 Abs. 2 ThürPAG die zentrale Löschungsbestimmung bereit. Danach sind personenbezogene Daten zu löschen und die zugehörigen Unterlagen zu vernichten, wenn

1. ihre Speicherung unzulässig ist oder
2. bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Insbesondere Nr. 2 dieser Vorschrift sowie die damit verbundenen komplizierten Verweisungen auf weitere nachrangige Vorschriften bereiten in der polizeilichen Praxis oft Schwierigkeiten.

Dabei trifft § 40 Abs. 2 ThürPAG explizite Regelungen zu Prüffristen, jedoch nur für personenbezogene Daten aus strafrechtlichen Ermittlungsverfahren. Demgegenüber enthält die Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung Regelungen – wie es der Wortlaut schon sagt – für vollzugspolizeiliche Datenspeicherung bereit. Daneben sind jedoch auch unter anderem die Richtlinie für die Führung polizeilicher personenbezogener Sammlungen des Landes Thüringen sowie die Dienstanweisung Kriminalaktennachweis als auch die Richtlinie zum Umgang mit dienstlichem Schriftgut sowie Akten und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei zu beachten.

Der Leitfaden des TLfDI geht auf die einzelnen Regelungen ein und stellt auch das Verhältnis der einzelnen Vorschriften zueinander dar.

Generell macht der Leitfaden deutlich, dass es sich bei den genannten Fristen um Prüffristen handelt, nach deren Ablauf das Gesetz

eine Überprüfung der weiteren Aufbewahrung vorschreibt (sozusagen ein „Lösch-Überprüfungs-Datum“), nicht aber zwingend deren Löschung gebietet. Somit handelt es sich um Höchstfristen, die festlegen, zu welchem Termin die Erforderlichkeitsprüfung spätestens zu erfolgen hat. Das heißt auch, dass die maximale Speicherdauer nicht vollumfänglich ausgenutzt werden muss, sondern der jeweilige polizeiliche Sachbearbeiter vielmehr bei jeder Einzelfallbearbeitung zu hinterfragen hat, ob die Voraussetzungen für eine Löschung oder Vernichtung vorliegen oder aber eine Verkürzung der Speicherdauer von Anfang an in Frage kommt. Dabei kann in der Einzelfallbearbeitung insbesondere über die weitere Speicherung von Daten oder Aufbewahrung von Unterlagen zu entscheiden sein, wenn beispielsweise vom Betroffenen ein Antrag auf Löschung bzw. Vernichtung gestellt wird.
Abschließend wird daher im Leitfaden festgehalten, dass sowohl mit Ablauf einer gesetzlichen Prüf-/ Aufbewahrungsfrist als auch bei der Einzelfallbearbeitung, das heißt vor Ablauf einer etwaigen Prüffrist, sämtliche Personendatensätze oder Unterlagen auf die Erforderlichkeit einer weiteren Speicherung zu überprüfen sind (Erforderlichkeitsprüfung). Dabei sind die Voraussetzungen für eine Löschung oder Vernichtung regelmäßig dann erfüllt, wenn die personenbezogenen Daten für die konkrete Aufgabenerfüllung der Polizei nicht mehr erforderlich sind.
Diese und viele weitere aus datenschutzrechtlicher Sicht interessante Hinweise sowie eine Synopse und eine Normenübersicht sind im Leitfaden über die Aufbewahrungsfristen für personenbezogene Daten und dienstlichem Schriftgut beim Thüringer Landesamt für Verfassungsschutz, in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei sowie in den Thüringer Staatsanwaltschaften zu finden.
Der Leitfaden ist auf der Internetseite des TLfDI abrufbar.

Der TLfDI stellt in seinem Leitfaden fest, dass sowohl das Thüringer Landesamt für Verfassungsschutz, die Thüringer Polizei, als auch die Thüringer Staatsanwaltschaften dazu verpflichtet sind, nicht mehr erforderliche Daten/ Unterlagen dem Archiv zur Übernahme anzubieten. Dies ergibt sich aus § 11 Abs. 1 S. 1 Thüringer Archivgesetz (ThürArchivG). Danach sind die öffentlichen Stellen verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erfor-

derlich und deren Aufbewahrungsfristen abgelaufen sind, auszusondern und dem zuständigen Archiv zur Übernahme anzubieten.

7.16 Löschung personenbezogener Daten in INPOL sowie bei der zuständigen Landespolizeidirektion

Ein Bürger hat sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt und um Überprüfung des Löschungsvollzuges seiner personenbezogenen Daten sowohl im Informationssystem der Polizei (INPOL) als auch bei der zuständigen Landespolizeiinspektion (LPI) gebeten.
Der TLfDI hatte sich bereits in den Jahren 2002 und 2004 mit der Eingabe des Petenten beschäftigt. Zum damaligen Zeitpunkt war die Speicherung der personenbezogenen Daten in den polizeilichen Systemen bis zum Ablauf der polizeilichen Prüffrist gemäß § 2 Abs. 1 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) unter datenschutzrechtlichen Gesichtspunkten nicht zu beanstanden.
Zwischenzeitlich sind die jeweiligen Prüffristen abgelaufen gewesen. Der Vollzug der Datenlöschung wurde daher durch den TLfDI kontrolliert. Nach Eingang der Stellungnahmen des Thüringer Landeskriminalamtes (TLKA) sowie der zuständigen LPI konnte dem Petenten mitgeteilt werden, dass die Löschung seiner personenbezogenen Daten nunmehr vorschriftsmäßig erfolgt ist. Auch im INPOL waren keine Daten zu seiner Person gespeichert.

Nach Ablauf der Prüffrist sind personenbezogene Daten zu löschen, soweit nicht vor Ablauf der Prüffrist eines Ermittlungsverfahrens ein weiteres Ereignis (in dem sich der Verdacht gegen dieselbe Person richtet) hinzugetreten ist. Insoweit richtet sich die Prüffrist des ersten Verfahrens nach der des neu hinzugekommenen. Hierbei handelt es sich nicht um eine Verlängerung nach § 2 Abs. 4 ThürPolPrüffristVO, sondern um einen neuen Beginn der Prüffrist, dessen Ende sich am letzten eingetretenen Ereignis, das Anlass für eine Speicherung der Daten bot, ausrichtet.

7.17 Anmeldeverfahren zum Tag der Deutschen Einheit 2012

Ob der Mord an Präsident Kennedy 1963, die Geiselnahme bei den Olympischen Spielen in München 1972 oder das Attentat auf Wolf-

gang Schäuble 1990 – Politiker und Gäste von Großveranstaltungen geraten immer wieder in das Visier von Attentätern. Umso wichtiger ist es, dass an einem der bedeutendsten Tage in der deutschen Geschichte, dem Tag der deutschen Einheit am 3. Oktober, auch sicherheitsrelevante Belange ausreichend geplant werden.
Bedeutende Persönlichkeiten aus dem Freistaat Thüringen sowie aus der gesamten Bundesrepublik nahmen auch am Festakt der Thüringer Staatskanzlei zum 3. Oktober 2012 teil.
Natürlich mussten auch für diese Veranstaltung präventive Maßnahmen getroffen werden. Die Bürgerinnen und Bürger sollten bei der Voranmeldung zur Teilnahme an dem Festakt ihre personenbezogenen Daten angeben und eine Einwilligung mit beigefügter Datenschutzerklärung unterschreiben. Im Einzelnen handelte es sich dabei um Name, Adresse, Geburtstag und Geburtsort. Die Erklärung informierte den Bürger über den Zweck der Datenverarbeitung, die Sicherheit aller Beteiligten zu gewährleisten und lediglich denjenigen Personen den Aufenthalt in definierten sicherheitsrelevanten Bereichen zu gestatten, die zuvor einer Sicherheitsprüfung unterzogen wurden. Mit der abgesendeten Anmeldung stimmten die Teilnehmer der Datenverarbeitung, insbesondere der Sicherheitsüberprüfung durch die Thüringer Polizeibehörden zu. Nach der Veranstaltung sollten die Daten wieder gelöscht werden.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erfuhr durch die Medien über das Verfahren, woraufhin er die Datenschutzerklärung einer eingehenden Prüfung unterzog. Neben der Sicherheit der Menschen sollte auch der Datenschutz der Veranstaltungsteilnehmer nicht in Vergessenheit geraten, da die Datenerhebung und Datenverarbeitung nur unter besonderen Voraussetzungen rechtlich zulässig sind.
Bei der Überprüfung wurde festgestellt, dass die verwendete Datenschutzerklärung die geltende Rechtslage nur unzureichend umsetzt. Im Ergebnis rügte der TLfDI die Nichteinhaltung der Anforderungen an eine wirksame Einwilligung nach § 4 Abs. 3 Thüringer Datenschutzgesetz (ThürDSG). Danach ist der Betroffene auf den Zweck und den Umfang der Verarbeitung, auf seine Rechte auf Auskunftserteilung, Berichtigung und Löschung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Vorliegend konnten die Betroffenen nicht erkennen, welche konkreten Maßnahmen bei der Sicherheitsüberprüfung durch die Polizeibehörden getroffen werden. Um auch in den folgenden Jahren die Einhal-

tung datenschutzrechtlicher Belange zu gewährleisten, wurden Gespräche mit der Thüringer Staatskanzlei (TSK), der Landespolizeidirektion (LPD) und dem Landeskriminalamt (LKA) geführt. Nach einem Gespräch zwischen TSK und dem TLfDI wurde festgelegt, dass Einwilligungserklärungen künftig die folgenden Punkte gem. § 19 ThürDSG enthalten sollen: 1. Zweck der Datenerhebung, 2. Identität der datenerfassenden und datenprüfenden Behörde, 3. Liste, welche Dateien oder Register die Daten durchlaufen, 4. Dauer der Speicherung, 5. Freiwilligkeit der Angaben.

Zudem ist es aus Sicht des LKA notwendig, dass der Veranstalter zunächst einen Antrag auf Überprüfung von Personendaten stellt und die Einwilligungserklärungen bei der Einreichung der Personendatenlisten diesem gegenüber schriftlich nachweist. Die LPD bot als mögliches Muster die Datenschutzerklärung vom Papstbesuch im Jahr 2011 an. Darin fand sich eine präzise Beschreibung zur Vorgehensweise bei der Kontrolle der Daten. Dieser Erklärung zufolge prüfen die Polizeibehörden, ob gespeicherte Informationen bestehen, die dem Einsatz der Personen im Sicherheitsbereich entgegenstehen. Die Daten werden mit polizeilichen Dateien abgeglichen, die zum Zwecke der Gefahrenabwehr und Strafverfolgung geführt werden. Diese können ausführlicher sein, als die des Bundeszentralregistergesetzes, da auch durch Gerichte eingestellte Verfahren gespeichert werden dürfen. Darin sah der TLfDI eine lediglich bedingt geeignete Vorlage, da sie an den Anforderungen des erheblichen Schutzbedarfs beim Papstbesuch ausgerichtet war. Zumindest in einem geringeren Umfang, angepasst an die jeweilige Veranstaltung, kann sie aber zur Orientierung herangezogen werden.

Abschließend verwies der TLfDI auf § 4 Abs. 1 Satz 2 ThürDSG, wonach im Falle der Einwilligung die Verarbeitung oder Nutzung personenbezogener Daten nur zulässig ist, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist. Hier sind gesteigerte Anforderungen zu stellen, da der Abgleich mit polizeilichen Dateien einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Daher muss festgelegt werden, in welchen Fällen der Schutzbedarf so hoch ist, dass ein Datenabgleich notwendig wird.

Eine Einwilligung in eine Datenverarbeitung ist nur dann wirksam, wenn die Datenschutzerklärung auch erkennen lässt, welchem Umfang die Verarbeitung entspricht, insbesondere welche konkreten Maßnahmen durchgeführt werden.

Sicherheit und Datenschutz sind keine Aufgaben, die sich ausschließen. Es ist die Aufgabe der Organisatoren von Großveranstaltungen, Sicherheit und Datenschutz in Einklang zu bringen, was stets möglich ist.

7.18 Klopapier: Thüringer Landeskriminalamt von der Datenschutz-Rolle – Videogaga 8

Aufgrund von Medienberichten wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt, dass das Thüringer Landeskriminalamt (TLKA) in seiner Außenstelle im ersten Quartal des Jahres 2011 verdeckte Videoaufnahmen angefertigt hatte. Auslöser für die Ermittlungen waren Beschwerden des Reinigungspersonals, das behauptete, dass dort immer wieder Toilettenpapierrollen gestohlen worden seien, was den Verdacht des Diebstahls begründete. Um diesen Verdacht aufzuklären, installierten Überwachungsspezialisten des TLKA eine Videokamera in einem Flur, unweit der Toiletten, wo die Toilettenpapierrollen in Liefersäcken gelagert wurden. Ziel war es, einen möglichen Täter / eine mögliche Täterin bei der Entwendung des angeblich so begehrten Toilettenpapiers zu überführen. Selbst nach wochenlanger Überwachung konnte mittels des Videomaterials kein Täter ermittelt werden. Auch die inzwischen eingeschaltete Staatsanwaltschaft stellte das Verfahren ergebnislos wieder ein.
Die datenschutzrechtliche Prüfung dieses Falles durch den TLfDI erwies sich zeitweise schwierig, da die angeforderten Unterlagen vom TLKA nicht an den TLfDI übermittelt wurden. Nach § 38 Abs. 1 Satz 1 Thüringer Datenschutzgesetz (ThürDSG) sind der TLfDI und seine Beauftragten aber von allen öffentlichen Stellen in der Erfüllung ihrer Aufgabe zu unterstützen. Ihnen ist dabei nach § 38 Abs. 1 Satz 2 Nr. 1 ThürDSG Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren. Die mangelnde Unterstützung seitens des TLKA wurde vom TLfDI gemäß § 39 ThürDSG beanstandet.
Die heimlichen längerfristigen Videoaufzeichnungen stellten indes eine Gefährdung des informationellen Selbstbestimmungsrechts der TLKA-Beschäftigten dar, soweit sich Personen tatsächlich durch den Aufnahmebereich der Videokamera bewegt hatten. Das Grundrecht auf informationelle Selbstbestimmung umfasst die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grund-

sätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (Bundesverfassungsgericht (BVerfG), Urteil vom 15. Dezember 1983 – 1 BvR 209/83 -). Eine Rechtsgrundlage hinsichtlich der heimlichen Videoaufzeichnungen konnte vom TLfDI nicht festgestellt werden. Die Fertigung verdeckter Bildaufnahmen mittels Videokamera stellte aus Sicht des TLfDI eine Observation dar, die der grundsätzlichen Anordnungskompetenz des Gerichts gemäß § 163 f Abs. 3 Strafprozessordnung unterlag. Eine entsprechende Anordnung lag hier jedoch nicht vor. Darüber hinaus entsprachen die Videoaufzeichnungen auch nicht dem Verhältnismäßigkeitsgrundsatz. Die konkrete Videoüberwachung konnte an sich schon nicht zur eindeutigen Überführung des Täters beitragen und war daher ungeeignet. Denn eine Entnahme der Toilettenpapierrollen aus dem Plastiksack hätte zunächst nicht geheißen, dass dieses auch gestohlen werden sollte. Selbst wenn eine Toilettenpapierrolle in Zueignungsabsicht entwendet worden wäre, hätte das keine Rückschlüsse auf den Dieb hinsichtlich der in den Toilettenräumen befindlichen Papierrollen zugelassen. Weiterhin hat man offenbar ohne Prüfung milderer Mittel strafverfolgende Schritte eingeleitet, die letztendlich erfolglos blieben und von einer hohen Gefährdung des Grundrechts auf informationelle Selbstbestimmung aller davon Betroffenen geprägt waren. So hätte man z. B. weniger Toilettenpapierrollen in die Toilettenräume legen bzw. zeitweise kontingentieren oder abschließbare Toilettenpapierrollenhalter anschaffen können. Zudem stand die Maßnahme außer Verhältnis zur Bedeutung der Sache und zur Stärke des bestehenden Tatverdachts. Festgestellt wurde hier lediglich ein hoher Verbrauch von Toilettenpapier im TLKA. Dass dieses entwendet wurde, versuchte man mit dem Indiz zu belegen, dass die inneren Papprollen nicht in den Papierkörben gefunden wurden. Ob dies der Maßstab sein kann, ist äußerst fraglich, denn was letztlich den hohen Verbrauch verursachte, konnte nicht belegt werden. Auch eine Mitbestimmung des Personalrates gem. § 74 Abs. 2 Nr. 11 Thüringer Personalvertretungsgesetz für eine Videomaßnahme hätte grundsätzlich in Betracht gezogen werden müssen.

Die datenschutzrechtlichen Verletzungen hat der TLfDI förmlich nach § 39 Abs. 1 ThürDSG beanstandet. Da die heimliche Videoüberwachung durchgeführt und bereits abgeschlossen war, konnte die Behebung der datenschutzrechtlichen Verletzungen im Sinne des

§ 39 Abs. 1 Satz 1 ThürDSG nicht mehr erfolgen. Der TLfDI wies jedoch das TLKA für die Zukunft darauf hin, darauf zu achten, dass solche datenschutzrechtlichen Verstöße im Rahmen der Verarbeitung und Nutzung personenbezogener Daten unterbleiben.

Die sich bietende Möglichkeit der Identifizierung einzelner Personen sowie die Erfassung ihrer Verhaltensweisen zu einer bestimmten Zeit durch die Erhebung personenbezogener Daten stellen eine faktisch drohende Beeinträchtigung des Schutzbereichs des Grundrechts auf informationelle Selbstbestimmung dar. Diese kommt als Grundrechtsgefährdung einem Eingriff gleich. Dazu hat bereits das Bundesverfassungsgericht Folgendes festgestellt: „Das Recht auf informationelle Selbstbestimmung flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt“ (BVerfG, 13. Juni 2007, 1 BVR 1550/03, Rn. 86 f. der JURIS-Fundstelle).

7.19 Bestandsdatenabfrage nach § 113 Abs. 1 Telekommunikationsgesetz (TKG) – auch in Übergangszeiten kein rechtsfreier Raum

Ein Beschluss des Bundesverfassungsgerichts (BVerfG) vom 24. Januar 2012 – 1 BVR 1299/05 – wirbelte die Datenschutzwelt in Bund und Ländern auf. Die Richter erklärten § 113 Abs. 1 Satz 2 Telekommunikationsgesetz (TKG) (Fassung 2004) als nicht mit dem Grundgesetz vereinbar und § 113 Abs. 1 Satz 1 TKG sollte nur noch mittels verfassungskonformer Auslegung anwendbar bleiben.
§ 113 Abs. 1 Satz 1 TKG regelt den Ablauf des manuellen Auskunftsverfahrens über Bestandsdaten der Kunden von Telekommunikationsdienstleistern gegenüber den Sicherheitsbehörden. Es handelt sich dabei um Kundendaten, die beim Vertragsschluss, bei dessen inhaltlicher Ausgestaltung, Vertragsänderungen oder der Beendigung des Vertrages erhoben werden, beispielweise Name, Anschrift, Bankverbindung oder Studentenstatus. Ergänzend hierzu regelt § 113 Abs. 1 Satz 2 TKG die Auskunftserteilung über Daten wie PIN und PUK, die den Zugriff auf Endgeräte oder Speichereinrichtungen ermöglichen.

Um der Praxis und der Gesetzgebung eine realistische Zeitvorgabe zur Umsetzung des Beschlusses zu geben, räumte das Bundesverfassungsgericht eine Übergangszeit bis zum 30. Juni 2013 ein, in der § 113 Abs. 1 Satz 1 TKG ohne Einschränkung weiter galt. Das Bundesverfassungsgericht forderte jedoch zugleich, § 113 Abs. 1 Satz 2 TKG entsprechend der Vorgaben des Beschlusses anzuwenden.

§ 113 Abs. 1 Satz 1 TKG sollte der Entscheidung zufolge lediglich unter zwei Voraussetzungen grundrechtskonform sein: Zum einen muss eine Norm des Fach- bzw. Landesrechts die Rechtsgrundlage für die Auskunftspflicht des Telekommunikationsunternehmens bilden, da § 113 Abs. 1 Satz 1 TKG selbst keine solche Rechtsgrundlage normenklar begründet. Zum anderen ist § 113 Abs. 1 Satz 1 TKG so auszulegen, dass er keine Zuordnung dynamischer Internetprotokoll-Adressen (IP-Adressen) zu ihren Nutzern erlaubt.

Die erste Voraussetzung begründet das BVerfG bildhaft mit dem „Doppeltüren-Modell“. Es bedarf sowohl für die Übermittlung, als auch für den Abruf von Daten spezieller Rechtsgrundlagen. Lediglich dann, wenn „beide Türen“, das heißt die „Tür“ der Übermittlung und die „Tür“ des Abrufs legitim geöffnet worden sind, besteht nach dem Durchschreiten dieser „Doppeltür“ eine Berechtigung zum Austausch personenbezogener Daten. Für die Berechtigung zum Abruf der Daten fehlt dem Bund jedoch die Gesetzgebungskompetenz, sodass § 113 Abs. 1 Satz 1 TKG lediglich die Berechtigung zur Übermittlung der Bestandsdaten regeln kann. Erst in Verbindung mit der landesrechtlichen Abrufnorm entsteht eine Auskunftsverpflichtung des Telekommunikationsunternehmens.

Die zweite Voraussetzung begründet sich durch den bei der Zuordnung erforderlichen Zwischenschritt, dass auf einzelne Verbindungsdaten, das heißt auf konkrete Telekommunikationsvorgänge, zugegriffen werden muss und dem damit verbundenen Eingriff in das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 Grundgesetz (GG).

§ 113 Abs. 1 Satz 2 TKG war deshalb mit der Maßgabe anzuwenden, dass der Zugriff auf Daten der Zugangssicherung **ausschließlich** in den Fällen gewährt werden darf, in denen auch die Voraussetzungen der Nutzung der Zugangsdaten erfüllt sind. Diese Voraussetzungen ergeben sich – gemäß dem oben genannten „Doppeltür“-Modell – aus dem Fach- bzw. Landesrecht. Denn ansonsten könnte der Vorbe-

halt der richterlichen Anordnung bei der Nutzung der Abrufdaten für eine Onlinedurchsuchung oder die Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorganges umgangen werden. Es ist nach Auffassung des Bundesverfassungsgerichts aber gerade kein Grund ersichtlich, warum die Behörden die in § 113 Abs. 1 Satz 2 TKG geregelten Zugangscodes **unabhängig** von den Anforderungen an deren Nutzung und damit unter Umständen unter erleichterten Umständen abfragen können sollen.

Die Konsequenzen dieses Beschlusses des Bundesverfassungsgerichts waren für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) klar: Die personenbezogenen Daten der Bürger in der vom Gericht genannten Übergangszeit, trotz der verfassungswidrigen Regelung, zu schützen, das Urteil auch effektiv mit den Rechtsanwendern umzusetzen und neue Normen auf landesrechtlicher Ebene zu schaffen.

Das Thüringer Innenministerium und das Thüringer Justizministerium wurden über das Urteil unterrichtet. Es erfolgten Hinweise, dass die Thüringer Polizei, das Thüringer Landesamt für Verfassungsschutz und die Strafverfolgungsbehörden, das auf Grundlage von Generalklauseln in Anspruch genommene manuelle Abrufverfahren nach der Übergangszeit nicht mehr nutzen dürfen. Zudem erkundigte sich der TLfDI, wie das manuelle Abrufverfahren seit der Entscheidung des BVerfG praktiziert wurde und ob eine Anpassung der landesspezifischen Rechtsgrundlagen geplant sei.

Der Auskunft des Thüringer Justizministeriums vom Oktober 2012 zufolge wurden jedoch keine gesonderten Handlungsanweisungen für die polizeiliche oder staatsanwaltliche Praxis zur Durchführung der Bestandsdatenabfrage getroffen. Das Erfordernis bestünde nicht, da Ersuchen zur Auskunft über Daten der Zugangssicherung den Ausnahmefall darstellen würden und der in der Praxis relevante Fall des Auslesens sichergestellter Mobiltelefone meist durch die Bereitschaft der Betroffenen, die PIN und PUK freiwillig herauszugeben, gelöst werden könne.

Zudem wurde mitgeteilt, dass das Bundesinnenministerium bereits einen Entwurf für ein Änderungsgesetz zum TKG vorgelegt habe, in welchem die Vorgaben des BVerfG umgesetzt und spezifische Erhebungsnormen geschaffen werden sollten. Darüber hinaus waren Anpassungen im Thüringer Polizeiaufgabengesetz und im Thüringer Verfassungsschutzgesetz geplant.

Nach einer Anfrage eines Landtagsabgeordneten über die Folgen des oben genannten Beschlusses sicherte der TLfDI die Unterstützung bei bevorstehenden Gesetzesänderungen zu.
In der Folgezeit wirkte der TLfDI in Form von Stellungnahmen bei der Änderung des Thüringer Polizeiaufgabengesetzes und Ordnungsbehördengesetzes und somit bei der Schaffung landesspezifischer Ermächtigungsgrundlagen zum Abruf von Daten mit (siehe dazu den Beitrag „Novellierung des Polizeiaufgabengesetzes (ThürPAG)) – auf die lange Bank geschoben und am Ende wenig erreicht“. Insbesondere machte der TLfDI Verbesserungsvorschläge für die möglichst präzise Ausgestaltung des § 34 e ThürPAG, der die aktuelle Befugnisnorm zur Erhebung von Bestandsdaten durch die Polizei in Thüringen bildet. So wurde angeregt, die Norm dem präziser formulierten § 180 a Landesverwaltungsgesetz (LVwG) Schleswig-Holstein anzupassen, dynamische Internetprotokoll-Adressen IP-Adressen nicht für die Verfolgung von Ordnungswidrigkeiten zu nutzen und die Ausnahme vom Richtervorbehalt bei Kenntnis des Betroffenen vom Auskunftsverlangen zu streichen.
Auch diesen wichtigen Änderungsvorschlägen des TLfDI ist die Mehrheit im Thüringer Landtag leider nicht nachgekommen.

§ 113 Abs. 1 TKG begründet allein noch keine Auskunftspflicht der Telekommunikationsunternehmen. Abschließend kann eine solche Verpflichtung gegenüber der jeweils abrufberechtigten Behörde nur durch eine Ermächtigungsgrundlage des Fach- bzw. Landesrechts geschaffen werden. Der TLfDI wird auch in Zukunft bei der Entwicklung fachgesetzlicher Rechtsgrundlagen die Einhaltung des Datenschutzes überwachen.

7.20 Abgeordnete des Thüringer Landtags zu Unrecht im Fokus der Polizei

Im Berichtszeitraum war dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt geworden, dass an Thüringer Medienvertreter anonym geheimhaltungsbedürftige polizeiliche Unterlagen zum Papstbesuch weitergeleitet wurden. Da man den Täter in den eigenen Reihen vermutete, startete die Thüringer Polizei ein groß angelegtes Ermittlungsverfahren gegen einen Polizeibeamten wegen des Verdachts der Verletzung des Dienstgeheimnisses.

Im Rahmen der Ermittlungen verarbeiteten die zuständigen Polizeibeamten unter anderem auch personenbezogene Daten von Abgeordneten des Thüringer Landtages. Die betroffenen Abgeordneten wandten sich nach § 11 Thüringer Datenschutzgesetz (ThürDSG) an den TLfDI mit der Bitte um Überprüfung des Sachverhalts, weil sie befürchteten, dass bei der Verarbeitung und Nutzung ihrer personenbezogenen Daten durch die Thüringer Polizei ihre schutzwürdigen Belange beeinträchtigt wurden.
Die Einsicht des TLfDI in die Ermittlungsakten ergab, dass bei dem beschuldigten Polizeibeamten eine Durchsuchung vorgenommen wurde, die laut dem hinreichend bestimmten Durchsuchungsbeschluss zur Auffindung von Beweismitteln, nämlich Abschriften oder Spuren des Einsatzbefehls zum Papstbesuch, führen sollte. Im Zuge der Durchsuchung wurden unter anderem auch das private Smartphone des Beschuldigten beschlagnahmt sowie Datenträger sichergestellt und ausgewertet. Auf dem Smartphone befand sich dabei unter anderem eine private Nachricht von einer der betroffenen Abgeordneten, die diese dem Beschuldigten gesandt hatte. Die Nachricht wurde als entsprechende Abbildung der Ermittlungsakte beigefügt. Im Schlussbericht der Ermittlungsbeamten erfolgte insbesondere auf Grundlage der Nachricht die Bewertung des sozialen Verhältnisses des Beschuldigten zu der Thüringer Landtagsabgeordneten. Damit war eindeutig, dass sie als Abgeordnete von den Ermittlungsbeamten erkannt worden war. Auf dem Datenträger wurde zudem die E-Mail einer weiteren Landtagsabgeordneten festgestellt, die diese dem Beschuldigten gesandt hatte. Auch eine Facebook Statuskommentierung von der Abgeordneten an den Beschuldigten war in den Ermittlungsunterlagen enthalten. Im Schlussbericht wurde das Verhältnis des Beschuldigten zu der Landtagsabgeordneten eingehend beurteilt.
Da die Nachrichten der beiden Abgeordneten des Thüringer Landtags an den Beschuldigten erkennbar nicht im Zusammenhang mit dem durch den Gerichtsbeschluss konkretisierten Durchsuchungszweck – dem Auffinden von Abschriften oder Spuren des Einsatzbefehls zum Papstbesuch – standen, hätten sie – weil irrelevant – nicht zu den Ermittlungsunterlagen genommen werden dürfen. Ein richterlicher Durchsuchungs- und Beschlagnahmebeschluss ist insofern für die Strafverfolgungsbehörden in seiner Konkretisierungs- und Umgrenzungsfunktion maßgeblich. Die Aufnahme beider Nachrichten in

die Ermittlungsunterlagen war somit vom richterlichen Beschluss nicht gedeckt und daher unzulässig.
Im Hinblick darauf, dass die Landtagsabgeordneten ausweislich der Ermittlungsakten als Abgeordnete des Thüringer Landtags und damit als Zeugnisverweigerungsberechtigte nach § 53 Abs. 1 Satz 1 Nr. 4 Strafprozessordnung (StPO) erkannt wurden, war auch der § 160 a StPO zu beachten. § 160 a Abs. 1 Satz 1 StPO bestimmt, dass eine Ermittlungsmaßnahme, die sich gegen eine zeugnisverweigerungsberechtigte Person richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig ist. Das Zeugnisverweigerungsrecht der Abgeordneten bezieht sich auch auf Privatpersonen, denen sie in ihrer Eigenschaft als Abgeordnete Tatsachen anvertraut haben, sowie über die Tatsachen selbst (Meyer-Goßner, StPO Kommentar, 55. Auflage, § 53, Rn. 24; Graf, StPO Kommentar, § 53, Rn. 21). Dennoch erlangte Erkenntnisse dürfen nach § 160 a Abs. 1 Satz 2 StPO nicht verwendet werden. Das Verwertungsverbot ist absolut ausgestaltet und keiner Abwägung zugänglich. Nach § 160 a Abs. 1 Satz 3 StPO sind gefertigte Aufzeichnungen unverzüglich zu löschen. Nach § 160 a Abs. 1 Satz 5 StPO gilt dies entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine zeugnisverweigerungsberechtigte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. Im vorliegenden Sachverhalt gelangten die Nachrichten der Abgeordneten an den Beschuldigten durch die Einsicht und Auswertung des sichergestellten Smartphones und des Datenträgers zur Kenntnis. Damit wurden – auch angesichts der intensiven Auswertung dieser Nachrichten – zweifellos Erkenntnisse zu den zwei Abgeordneten erlangt.
Dem § 160 a StPO geht nach dessen Abs. 5 zwar die Norm des § 97 StPO als Spezialvorschrift vor. Da § 97 StPO keine Regelungen zur Verwertung von beschlagnahmefreien Gegenständen trifft, bleibt § 160 a StPO jedoch neben § 97 StPO anwendbar (Meyer-Goßner, StPO-Kommentar, § 97 Rn. 50). Wird demnach gegen das Beschlagnahmeverbot in Hinblick auf die zeugnisverweigerungsberechtigten Abgeordneten verstoßen, richtet sich die Verwertung der so erlangen Beweismittel nach § 160 a Abs. 1 StPO (Radtke/Hohmann StPO-Kommentar, § 97, Rn. 43).
Der TLfDI hat die fehlende unverzügliche Löschung der Nachrichten der Abgeordneten an den Beschuldigten aus den Ermittlungsunterla-

gen gemäß § 39 ThürDSG beanstandet, da hierin ein ungerechtfertigter Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Abgeordneten zu sehen war.
Derzeit befinden sich beide Sachverhalte im gerichtlichen Verfahren, über dessen Ausgang im kommenden Tätigkeitsbericht berichtet werden wird.
Die Ermittlungsunterlagen enthielten darüber hinaus in einer Kontaktliste Einträge, die eindeutig Thüringer Landtagsabgeordneten zuzuordnen waren. Da auch diese in Rede stehenden Abgeordnetenkontaktdaten für die Ermittlungen keine weiterführenden Ansätze in sich trugen, war deren Aufnahme und Speicherung in der Ermittlungsakte nicht erforderlich und damit unzulässig. Nach einem entsprechenden Schreiben des TLfDI wurde die Kontaktliste mit den Abgeordnetendaten aus den Ermittlungsunterlagen gelöscht.

Die Strafprozessordnung (StPO) gibt den Abgeordneten im Rahmen ihrer Stellung ein Zeugnisverweigerungsrecht nach § 53 Abs. 1 Nr. 4 StPO, wonach sie als Zeugen vor Gericht oder anderen staatlichen Stellen berechtigt sind, Auskünfte zu verweigern. Dies entspricht auch dem Wortlaut des Art. 56 Abs. 1 der Verfassung des Freistaats Thüringen (ThürVerf).
§ 160 a StPO normiert als Schutznorm ein absolutes Verwertungsverbot hinsichtlich solcher Tatsachen, über die ein Abgeordneter das Zeugnis verweigern dürfte. Gefertigte Aufzeichnungen hierüber sind gemäß § 160 a Abs. 1 S. 3 StPO unverzüglich zu löschen.
Diese Normen sind Formen des verfassungsrechtlichen Status der Abgeordneten und dienen der Funktionsfähigkeit des Parlaments.

7.21 Polizei vs. Journalisten

Wegen des Verdachts der Verletzung des Dienstgeheimnisses durch Weiterleitung von geheimhaltungsbedürftigen polizeilichen Unterlagen zum Papstbesuch in Thüringen an Medienvertreter durch einen Polizeibeamten wurde bekannt, dass dabei auch personenbezogene Daten von Journalisten durch die Thüringer Polizei verarbeitet wurden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) überprüfte diesen Sachverhalt aus datenschutzrechtlicher Sicht und nahm dazu Einsicht in die Ermittlungsunterlagen. Dabei stellte sich zunächst heraus, dass ein Journalist dem Beschuldigten eine private Nachricht auf dessen Smartpho-

ne gesandt hatte. Zu diesem Zeitpunkt befand sich das Smartphone jedoch bereits in polizeilicher Verwahrung im Sinne des § 94 Abs. 1 Strafprozessordnung (StPO). Im polizeilichen Schlussbericht wurde die Nachricht des Journalisten als relevanter dokumentierter Inhalt aufgeführt und in Form einer Fotografie beigefügt. Einen Bezug zum Einsatzbefehl hinsichtlich des Papstbesuchs hatte die Nachricht jedoch nicht. Im weiteren Verlauf des Schlussberichts wurde das persönliche Verhältnis des Beschuldigten zum Journalisten auch auf Grundlage dieser Nachricht beurteilt. Damit wurden personenbezogene Daten des Journalisten in der Ermittlungsakte verarbeitet (gespeichert nach § 3 Abs. 3 Satz 2 Nr. 2 Thüringer Datenschutzgesetz (ThürDSG)). Die Aufnahme und Speicherung der Nachricht in die Ermittlungsunterlagen war jedoch aus mehreren Gründen unzulässig. Der richterliche Durchsuchungsbeschluss beschränkte sich in Bezug auf das Smartphone zum einen nur auf Nachrichten, die der Beschuldigte bis zum Zeitpunkt der Sicherstellung bereits „empfangen hat“. Da die Nachricht des Journalisten aber erst nach der Sicherstellung des Smartphones auf dieses gesandt wurde, hätte sie als irrelevant bewertet und nicht in die Ermittlungsakten aufgenommen werden dürfen. Zum anderen stand die Nachricht des Journalisten nicht im Zusammenhang mit dem konkret im Durchsuchungsbeschluss aufgeführten Zweck – dem Auffinden von Abschriften oder Spuren des Einsatzbefehls zum Papstbesuch. Demzufolge hätte die Nachricht auch aus diesem Grund als irrelevant bewertet werden müssen und nicht weitergehend in der Ermittlungsakte gespeichert werden dürfen. Auch die Tatsache, dass es sich bei der Nachricht um eine private Nachricht des Journalisten handelte, die in keinem dienstlichen Zusammenhang stand und darüber hinaus auf das private Smartphone des Beschuldigten gesandt wurde, machte die Speicherung unzulässig. Diese Konstellation war vom Durchsuchungsbeschluss nicht erfasst, da dieser lediglich private Nachrichten auf dienstliche Geräte und dienstliche Nachrichten auf private Geräte umfasste. Ein richterlicher Durchsuchungs- und Beschlagnahmebeschluss ist insofern für die Strafverfolgungsbehörden in seiner Umgrenzungsfunktion maßgeblich. Er konkretisiert die hier einschlägigen Durchsuchungs- und Beschlagnahmenormen der §§ 94, 98, 102, 105 StPO.

Der TLfDI hat die unzulässige Aufnahme und Speicherung der Nachricht des Journalisten in die Ermittlungsunterlagen gemäß § 39 ThürDSG beanstandet, da hierin ein ungerechtfertigter Eingriff

in das Grundrecht auf informationelle Selbstbestimmung zu erblicken war.
In den Ermittlungsunterlagen wurde außerdem die private Telefonnummer eines weiteren Journalisten gespeichert, welche die Polizei durch das polizeilichen Auskunftssystem SARS (Syborg Auskunft- und Recherche-System) ermitteln konnte. Durch die Eingabe des Namens und der Anschrift des Journalisten in das System wurden dem für die Ermittlung zuständigen Beamten alle angemeldeten Telefonnummern durch die Bundesnetzagentur zugänglich gemacht. Rechtsgrundlage für eine SARS-Abfrage sind §§ 161, 163 StPO i. V. m. § 112 Telekommunikationsgesetz (TKG). Nach § 112 Absatz 2 Nr. 1 TKG werden Auskünfte aus den Kundendateien den Gerichten und Strafverfolgungsbehörden nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden. Nach § 112 Abs. 4 TKG hat auf Ersuchen der in Absatz 2 genannten Stellen die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. Der Gesetzgeber hat die Verwendungszwecke der Daten sehr weit gefasst. Den in § 112 Abs. 2 TKG genannten Behörden dürfen die Daten allgemein zur Erfüllung ihrer gesetzlichen Aufgaben übermittelt werden. Im Rahmen der Erforschungspflicht stellen die §§ 163 Absatz 1, 161 Absatz 1 Satz 1 StPO grundsätzlich eine ausreichende Rechtsgrundlage für die Ermittlungsbehörde hinsichtlich einer SARS-Auskunft dar (Meyer-Goßner, StPO-Kommentar § 161, Rn. 3). Im vorliegenden Fall sollte unter anderem geklärt werden, ob der Tatverdächtige Telefongespräche aus der polizeiinternen Telefonnetzanlage geführt hatte. Laut Aussage der zuständigen Polizeiinspektion wurde davon ausgegangen, dass sich die Übermittlung des Dokumentes im Vorfeld über telefonische Kontakte oder andere Kommunikationsmedien zwischen dem Tatverdächtigen und dem Journalisten angebahnt und der Tatverdächtige dahingehend telefonischen Kontakt im Tatzeitraum unterhalten hatte. Die Überprüfung war aussagegemäß auch in entlastender Hinsicht für den damaligen Tatverdächtigen zu untersuchen gewesen.
Im Ergebnis stellten sich jedoch keine telefonischen Kontakte des damals Tatverdächtigen zu dem besagten Journalisten heraus. Mangels Vorhandensein weiterer schriftlicher Dokumentation des Abfragevorgangs musste der TLfDI hier jedoch davon ausgehen, dass die

Abfrage für die Aufgabenwahrnehmung der Polizei nicht auf andere Weise einfacher, aber ebenso effektiv beschafft werden konnte, sodass §§ 161, 163 StPO i. V. m. § 112 TKG genügt war.

Liegt ein richterlicher Durchsuchungs- und Beschlagnahmebeschluss vor, ist er für die Strafverfolgungsbehörden in seiner Umgrenzungsfunktion maßgeblich. Er konkretisiert die einschlägigen Durchsuchungs- und Beschlagnahmenormen der §§ 94, 98, 102, 105 StPO. Nach der Rechtsprechung des Bundesverfassungsgerichts ist deshalb im Durchsuchungsbeschluss der Gegenstand und der Zweck der Maßnahme hinreichend zu umschreiben (BVerfG, Beschluss v. 14. Juni 2006, 2 BvR 1117/06).

7.22 Papstbesuch in Thüringen – nicht nur der Himmel schaute zu: Video 9

Einer Presseinformation des Mitteldeutschen Rundfunks war Ende 2011 zu entnehmen, dass diensthabende Polizeibeamte beim Papstbesuch in Erfurt durch die Thüringer Polizei gefilmt wurden. Es stellte sich dabei die Frage, ob diese Videoaufzeichnungen auch dazu genutzt werden sollten, um mögliche dienstliche Verfehlungen der Beamten nachweisen zu können.
Auf Nachfrage des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bei dem für die Polizei zuständigen Thüringer Innenministerium und nach Einsichtnahme in die entsprechenden Unterlagen ergab sich, dass tatsächlich Videoaufzeichnungen gefertigt wurden, diese aber für eine Ahndung von Dienstvergehen nicht vorgesehen waren. Es war auch kein Zusammenhang dahingehend zu erkennen, dass ein einheitliches Erscheinungsbild der Polizeibeamten vor Ort kontrolliert werden sollte. Die Videodokumentation diente vielmehr der Sicherstellung der sofortigen Reaktionsmöglichkeit bei tätlichen Angriffen auf den Papst und auf mögliche Störungen der Kolonnenfahrt und konnte auf § 33 Thüringer Polizeiaufgabengesetz (ThürPAG) gestützt werden.
Die gefertigten Videoaufnahmen wurden gemäß § 33 Abs. 3 ThürPAG innerhalb eines Monats nach deren Aufzeichnung gelöscht, sodass keine Aufnahmen mehr vorhanden waren. Weitere Anhaltspunkte für einen Verstoß gegen datenschutzrechtliche Vorschriften lagen nicht vor.

Abschließend war vom TLfDI zu klären, ob – unabhängig von einem vorliegenden Einsatzbefehl – weitere Videoaufnahmen z. B. durch den Einsatz von mobilem Personal gefertigt wurden. Nachweisbare Anhaltspunkte hierfür liegen derzeit nicht vor.

§ 33 des Thüringer Polizeiaufgabengesetz (ThürPAG) gestattet der 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, zu erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen.
Diese Daten sind jedoch spätestens einen Monat nach ihrer Erhebung zu löschen oder zu vernichten, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten benötigt werden.

7.23 Unbemerktes Mithören und GPS-Daten-Übertragung beim digitalen Polizeifunk – Überwachung der Polizisten durch die Polizei?

Ein „heißes Eisen“ – nicht nur im Freistaat Thüringen – ist die Einführung des digitalen Polizeifunks. Nachdem es anfangs Differenzen über die Kostenteilung zwischen dem Bund und den Ländern gegeben hatte, kamen später technische Probleme bei der Einführung des digitalen Polizeifunks in Thüringen hinzu. Hauptziel der Einführung ist der Aufbau eines digitalen Netzes, mit dem die Arbeit der Thüringer Polizei vor allem abhörsicher ausgestaltet werden soll. Doch welche weiteren „Extrafunktionen“ enthält der BOS-Digitalfunk, so der Name des neuen digitalen Polizeifunks (wobei das Kürzel „BOS“ für „Behörden und Organisationen mit Sicherheitsaufgaben“ steht)?
Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten bereits im Frühjahr 2012 Hinweise darüber, dass die neuen Digitalfunkgeräte der Thüringer Polizei auch die Funktion des unbemerkten Mithörens (sogenanntes Ambience Listening) in ihrem Portfolio besäßen. Diese Funktion verfolgt den Zweck, dass durch das unbemerkte Mithören von Umgebungsgeräuschen eines Funkgerätes, zum Beispiel bei Entführun-

gen, Geiselnahmen oder schwer verletzten Einsatzbeamten, Informationen über die gegenwärtige Situation vor Ort erlangt werden können. Bei der Übertragung soll der Nutzer des Endgerätes von der Nutzung dieser Funktion allerdings nichts bemerken. Der TLfDI bat daher mit Schreiben vom Mai 2012 das Thüringer Innenministerium um Stellungnahme.

Das Thüringer Innenministerium teilte daraufhin Ende Mai 2012 mit, dass die Funktion des unbemerkten Mithörens (Ambience Listening) in den Funkgeräten des BOS-Digitalfunks zwar fest integriert, in der Thüringer Polizei aber nicht aktiviert sei. Ferner wies das Thüringer Innenministerium auf das von der Projektgruppe Digitalfunk BOS erstellte Rahmenkonzept hin. Dort heißt es: „Deshalb ist vor Einrichtung dieses Dienstes [gemeint ist die Funktion des unbemerkten Mithörens] durch die jeweilige BOS Vorsorge zu folgenden Aspekten zu treffen:

- Anordnungskompetenz,
- Datenschutz,
- IT-Sicherheit,
- Datenspeicherung und -löschung,
- Beteiligung Personalvertretung.“

Da sich die Einführung des digitalen Polizeifunks, wie bereits erwähnt, bis Mitte 2013 verzögerte, richtete der TLfDI im September 2013 ein erneutes Schreiben an das Thüringer Innenministerium und bat um aktuelle Mitteilung des Sachstands zur Funktion des unbemerkten Mithörens bei Digitalfunkgeräten der Thüringer Polizei. Das Thüringer Innenministerium antwortete in seinem Schreiben vom Oktober 2013 dahingehend, dass die Nutzung des Leistungsmerkmals *unbemerktes Mithören* (Ambience Listening) seitens der Thüringer Landespolizeidirektion (LPD) im dortigen Einsatzleitsystem (ELS) nicht beabsichtigt sei. Auch beim zuständigen Auftragnehmer, der Firma Siemens, seien die dafür notwendigen technischen Voraussetzungen (Komponenten) nicht beauftragt worden. Ferner beabsichtige auch das Thüringer Landeskriminalamt (TLKA) keine Nutzung der Funktion des unbemerkten Mithörens bei Digitalfunkgeräten. Das Recht zur Nutzung der Funktion des unbemerkten Mithörens sei administrativ für alle Leitstellenanwendungen bzw. Leitstellennutzer in Thüringen gesperrt worden. Abschließend wies das Thüringer Innenministerium darauf hin, dass beim Leistungsmerkmal „Notruf“ gerade kein *stilles*, sondern ein *willentliches* Mithören stattfinde. Der notrufende Beamte löse beim Betätigen der

Notruftaste einen Notruf aus. Dieser werde dann an das einprogrammierte Notrufziel gesendet. Damit verbunden sei dann die Freischaltung des Mikrofons des notrufauslösenden Gerätes.

Eine weitere Funktion, die der BOS-Digitalfunk bereithält, ist das Leistungsmerkmal GPS (Global Positioning System). Auch zur Nutzung dieser Funktion bat der TLfDI das Thüringer Innenministerium zuletzt im September 2013 um Stellungnahme und fragte dabei insbesondere nach, ob in Thüringen die technisch realisierbare Möglichkeit des Tracking-Verfahrens zur Anwendung kommt, bei dem die regelmäßige Speicherung und Verarbeitung von GPS-Standortkoordinaten zur automatisierten Herstellung eines Bewegungsbildes genutzt wird.
Das Thüringer Innenministerium erklärte mit Schreiben vom Oktober 2013, dass alle Funkgeräte der Thüringer Polizei das GPS-Leistungsmerkmal nutzten. Geregelt sei dies im „Rahmenkonzept für den BOS-Digitalfunk in Thüringen“, dem auch der Hauptpersonalrat des Thüringer Innenministeriums am 19. August 2009 und der Hauptpersonalrat der Thüringer Polizei am 17. September 2009 zugestimmt hätten.
Die erhobenen GPS-Daten würden derzeit (Stand: Oktober 2013) in der „Autorisierten Stelle“ (Technische Betriebsstelle des BOS-Digitalfund in Thüringen) des TLKA dargestellt. Damit verfüge die Autorisierte Stelle über die Möglichkeit, die zugehörige Dienststelle des Funkgerätes zu ermitteln, nicht aber den konkreten Nutzer.
Ferner teilte das Thüringer Innenministerium mit, dass im Rahmen der Einführung des ELS bei der Zentralen Leitstelle der Thüringer Polizei in der Andreasstraße in Erfurt die LPD plane, das Leistungsmerkmal GPS zu nutzen. In der dazugehörigen „Dienstvereinbarung zur Verarbeitung und Nutzung der Standortdaten im Einsatzleitsystem“ werde zwischen der Speicherung der GPS-Koordinaten im Digitalfunkgerät und der Speicherung der GPS-Koordinaten im Einsatzleitsystem (ELS) unterschieden: In den Digitalfunkgeräten erfolge die Speicherung der Standortkoordinaten in einem flüchtigen RAM-Speicher, der kontinuierlich von jeweils aktuelleren Koordinaten überschrieben werde. Beim Ausschalten des Digitalfunkgerätes werde der RAM-Speicher gelöscht. Im Speicher des ELS werde jede übermittelte Standortkoordinate gehalten, jedoch nur so lange, bis sie durch eine neu übermittelte Standortkoordinate des gleichen Absenders überschrieben werde. Mit Abschalten des Digitalfunkgerätes

werde auch die Standortkoordinate im ELS gelöscht. Ein Tracking, also die regelmäßige Speicherung und Verarbeitung von GPS-Daten zur automatisierten Herstellung eines Bewegungsbildes, sei mit den in Auftrag gegebenen Komponenten, so das Thüringer Innenministerium, nicht möglich. Dies sei auch perspektivisch nicht beabsichtigt.
Noch nicht abschließend konnte vom TLfDI geklärt werden, ob es neben dem ELS weitere „Parallelsysteme“ zum BOS-Digitalfunk gibt, mit denen eine Verarbeitung von sämtlichen GPS-Daten und damit letztlich doch ein Tracking ermöglicht wird. Der TLfDI wird dazu wieder im nächsten Tätigkeitsbericht informieren.

Die Einführung neuer, digitaler Kommunikationssystemen wie dem BOS-Digitalfunk besitzt immer die berühmten zwei Seiten einer Medaille: Einerseits soll die Technik sicherer und anwendungsfreundlicher sein, andererseits bietet sie aber auch mehr Möglichkeiten, Daten zu erheben und diese – im schlimmsten Falle – auch zur Anwendung von Bewegungsprofilen (Tracking) oder zur Überwachung von Polizisten (Ambience Listening) zu benutzen. Umso wichtiger sind daher klare Datenschutzregeln, unter welchen Voraussetzungen die Daten erhoben und gespeichert werden dürfen. Damit wird zugleich eine „Datenerhebung durch die Hintertür“ für unzulässig erklärt. Die Personalvertretungen sind bei Einführung solcher Systeme intensiv einzubinden.

8 Verfassungsschutz

Grunge Stempel rot VERTRAULICH
© Daniel Ernst – fotolia.com

8.1 Unkenntnis und Raummangel sind kein „Freibrief“ zur Aktenvernichtung – Nichtanbietung von Schriftgut des Thüringer Landesamtes für Verfassungsschutz an das Thüringer Staatsarchiv

In einer Pressemitteilung aus dem Oktober 2012 sah sich das Thüringer Landesamt für Verfassungsschutz (TLfV) dazu veranlasst, einen bislang selbst praktizierten Rechtsverstoß in den öffentlichen Fokus zu rücken. Demnach hatte das TLfV bislang Daten und Unterlagen – ohne vorherige Archivanbietung – gelöscht bzw. vernichtet. Ursache hierfür sei gewesen, dass das Staatsarchiv nicht über geeignete Räumlichkeiten verfügte.

Regelungen zur Archivierung finden sich im Thüringer Archivgesetz (ThürArchivG). Danach sind gemäß § 11 Abs. 1 ThürArchivG alle in § 3 Abs. 1 ThürArchivG genannten Behörden – also auch das TLfV – verpflichtet, sämtliche Unterlagen vor der Löschung dem Staatsarchiv zur Übernahme anzubieten. Allein das Staatsarchiv entscheidet im Nachgang darüber, welche dieser Unterlagen nicht archivwürdig sind und mithin gelöscht werden können. § 11 Abs. 3 ThürArchivG schreibt weiterhin fest, dass die in § 3 Abs. 1 ThürArchivG genannten öffentlichen Stellen – also auch das TLfV – Unterlagen nur vernichten oder Daten nur dann löschen dürfen, wenn das zuständige öffentliche Archiv die Übernahme abgelehnt oder nicht innerhalb eines Jahres über die Archivwürdigkeit angebotener Unterlagen entschieden hat.
Dass auch das Thüringer Verfassungsschutzgesetz (ThürVSG) Vorschriften zur Löschung enthält, ist unstreitig. Ebenso unstreitig ist allerdings der Umstand, dass – soweit das ThürVSG keine spezialgesetzlichen Regelungen hinsichtlich einer Archivierung von Daten /

Unterlagen enthält – die spezialgesetzlichen Regelungen des ThürArchivG Anwendung finden.
§ 11 Abs. 1 und 2 i. V. m. § 3 Abs. 1 ThürArchivG lassen keinen Zweifel daran, dass das TLfV auch der Geheimhaltung unterliegende Unterlagen dem Staatsarchiv vor deren Löschung anzubieten hat.

Nachdem der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) dieses Vorgehen kritisiert hatte, räumte das TLfV ein, sich nunmehr der allgemeinen Rechtsauffassung, dass das ThürArchivG auch für das TLfV gilt, anzuschließen. Diese Aussage machte allerdings deutlich, dass das TLfV bislang keine Unterlagen dem Thüringer Hauptstaatsarchiv angeboten hatte, bevor es diese vernichtete oder Daten löschte.
Die Nichtanbietung von Daten / Unterlagen stellte damit einen Verstoß gegen § 11 Abs. 1 i. V. m. § 3 Abs. 1 ThürArchivG dar, den der TLfDI nach § 39 Abs. 1 ThürDSG förmlich beanstandete.
Der Umstand, dass das Staatsarchiv nicht über geeignete Räumlichkeiten verfügte, stellte keine Ersatzbefugnis für das TLfV zur Aktenlöschung dar, da es dem TLfV jederzeit unbenommen war, die vom Staatsarchiv für archivwürdig gehalten Akten in eigenen Räumlichkeiten zu verwahren, bis das Staatsarchiv geeignete Archivierungsmöglichkeiten anbieten konnte.
Da die Löschung von Daten bzw. die Vernichtung von Unterlagen bereits abgeschlossen war, war die Behebung der datenschutzrechtlichen Verletzungen im Sinne des § 39 Abs. 1 Satz 1 ThürDSG nicht mehr möglich, sodass der Vorgang durch den TLfDI förmlich zu beanstanden war.
Der TLfDI hat das TLfV darauf hingewiesen, dem Thüringer Staatsarchiv Daten / Unterlagen vor der Löschung anzubieten, damit der vorgenannte datenschutzrechtliche Verstoß künftig unterbleibt.

Zwar hatte das TLfV dem TLfDI angekündigt, dass zwischenzeitlich eine Archivvereinbarung zwischen dem Weimarer Hauptstaatsarchiv und dem Landesamt für Verfassungsschutz (TLfV) erarbeitet würde. Eine Endfassung dieser Archivvereinbarung lag dem TLfDI allerdings bis zum Abschluss des Tätigkeitsberichtes nicht vor.
Der TLfDI wird in seinem nächsten Tätigkeitsbericht über den Fortgang der Zusammenarbeit zwischen dem Hauptstaatsarchiv und dem TLfV informieren.

8.2 Das Thüringer Landesamt für Verfassungsschutz schweigt – zu Recht?

Nach § 11 Abs. 1 Satz 1 Thüringer Verfassungsschutzgesetz (ThürVSG) ist das Landesamt für Verfassungsschutz (TLfV) verpflichtet, einem Betroffenen auf Antrag unentgeltlich Auskunft über die zu seiner Person beim TLfV gespeicherten Daten zu erteilen. Der Antragsteller muss insoweit ein besonderes Interesse an einer Auskunft darlegen.

In einem dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bekannt gewordenen Fall begründete der Antragsteller seine Auskunft mit dem Verdacht, Betroffener einer nachrichtendienstlichen Ermittlung gewesen zu sein.

Das TLfV erteilte dem Bürger – nur teilweise – Auskunft über seine beim TLfV gespeicherten personenbezogenen Daten. So wurde ihm einerseits ein Datensatz mitgeteilt, anderseits erhielt er die Information, weitere Daten über ihn seien zwar vorhanden, könnten ihm jedoch nicht mitgeteilt werden. Eine abschließende Auskunft über sämtliche zu seiner Person gespeicherten Daten unterblieb. Das TLfV hatte sich insoweit auf die Auskunftsverweigerungsgründe des § 11 Abs. 2 Satz 1 Nr. 1, 2 und 4 ThürVSG berufen. Der TLfDI sah sich daher veranlasst, die verweigerte Auskunft in einem Ortstermin beim TLfV zu hinterfragen.

Die datenschutzrechtliche Überprüfung seitens des TLfDI ergab, dass das TLfV sich zu Recht auf eine Verweigerung einer weitergehenden Auskunft an den Betroffenen berufen hat.

Demnach war lediglich ein Datensatz zur seiner Person gespeichert, bei dem rechtliche Gründe einer Auskunftserteilung nicht entgegenstanden und der dem Betroffenen im Rahmen der Auskunftserteilung durch das TLfV auch mitgeteilt wurde. Darüber hinaus musste eine Auskunft durch das TLfV unterbleiben, da Auskunftsverweigerungsgründe im Sinne des § 11 Abs. 2 Satz 1 ThürVSG vorlagen. Hiernach unterbleibt die Auskunftserteilung, soweit

1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist;
2. durch die Auskunftserteilung nachrichtendienstliche Zugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamtes für Verfassungsschutz zu befürchten ist;

3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Derartige Verweigerungsgründe waren hier gegeben, die gemäß § 11 Abs. 4 Satz 1 ThürVSG auch keiner näheren Begründung bedurften. Auch eine Auskunft über die Herkunft und mögliche Empfänger der Daten erfolgt durch das TLfV grundsätzlich nicht. Die Auskunftsverpflichtung erstreckt sich kraft ausdrücklicher gesetzlicher Regelung (§ 11 Abs. 3 ThürVSG) nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen. Die Regelung des § 13 Abs. 1 Satz 1 Nr. 3 ThürDSG, nach welcher sich die Auskunft auch auf die Herkunft der Daten erstreckt, findet auf Auskunftsersuchen gegenüber dem TLfV keine Anwendung (§ 30 ThürVSG). Woher also ein personenbezogenes Datum stammte oder an wen es übermittelt wurde, musste das TLfV nicht mitteilen.

Der TLfDI war aufgrund dessen dazu angehalten, dem Betroffenen keine weiteren Auskünfte zu erteilen. Dies ergibt sich aus § 11 Abs. 4 Satz 2 und Satz 4 ThürVSG. Es ist dem TLfDI daher nur möglich, die Rechtmäßigkeit der Datenspeicherung nachzuvollziehen.

Aus datenschutzrechtlicher Sicht war sowohl die Speicherung der personenbezogenen Daten des Betroffenen als auch die – nur teilweise – erteilte Auskunft durch das TLfV nicht zu beanstanden.

Wird die Auskunftserteilung abgelehnt, hat der Betroffene neben der Möglichkeit, Widerspruch beim TLfV einzulegen, auch die Möglichkeit, sich gemäß § 11 Abs. 4 Satz 2 ThürVSG an den TLfDI zu wenden. Dem TLfDI ist auf sein Verlangen grundsätzlich Auskunft zu erteilen.

Im Rahmen seiner Überprüfungs- und Kontrollbefugnisse prüft der TLfDI die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der Daten und erteilt dem Betroffenen hierüber Auskunft. Mitteilungen des Landesbeauftragten für den Datenschutz an den Betroffenen sind jedoch insoweit eingeschränkt, als sie keine Rückschlüsse auf den Erkenntnisstand des TLfV zulassen dürfen. Sie sind nur mög-

lich, wenn das TLfV einer weitergehenden Auskunft durch den TLfDI zugestimmt hat.

9 Finanzwesen

Euromünze Männchen
© fotomek – fotolia.com

9.1 Spezielle Probleme mit der Steuer-Identifikationsnummer

Der Bundesfinanzhof hat mit Urteil vom 18. Januar 2012 – II R 49/10 – (Bundessteuerblatt 2012 Teil II Seite 168) entschieden, dass die Zuteilung der Steuer-Identifikationsnummer (Steuer-ID) und die dazu erfolgte Datenspeicherung mit dem Recht auf informationelle Selbstbestimmung und sonstigem Verfassungsrecht vereinbar sind.
In jüngster Vergangenheit war zu beobachten, dass die lebenslang gültige Steuer-ID gem. § 139 a Abgabenordung (AO) auch außerhalb der Steuerverwaltung, z. B. bei der Eröffnung von Konten oder der Beantragung von Elterngeld, genutzt wird. Mit der Ausweitung ihrer Verwendung droht damit die Steuer-ID zu einem Personenkennzeichen zu werden, wodurch auch das Risiko der Erstellung von aussagekräftigen Persönlichkeitsprofilen wächst. Bereits in seinem grundlegenden Volkszählungsurteil vom 15. Dezember 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 hatte das Bundesverfassungsgericht die Verfassungswidrigkeit eines allgemeinen Personenkennzeichens festgestellt. Leider hat sich zu der nun drohenden Etablierung der Steuer-ID als faktisches Personenkennzeichen die neuere verfassungsgerichtliche Rechtsprechung bisher noch nicht geäußert.
Ein spezielles Problem stellt vor diesem Hintergrund der Grundsatz der Einmalvergabe einer Steuer-ID in Fällen eines hohen Schutzbedarfs dar. So sollte z. B. die ursprüngliche Identität des Betroffenen bei Zeugenschutzprogrammen, Inkognito-Adoptionen und Geschlechtsumwandlungen aus gerechtfertigten Gründen (vgl. die Regelungen zum besonderen Schutz sensibler Daten zum Adoptionsgeheimnis, im Zeugenschutz-Harmonisierungsgesetz und im Trans-

sexuellengesetz) verborgen bleiben. Jedoch könnte aufgrund der lebenslangen Beibehaltung der Steuer-ID angesichts ihrer weitreichenden Streuung auch in diesen Fällen die ursprüngliche Identität aufgedeckt werden. Dies wiederum könnte erhebliche Schutzeinbußen nach sich ziehen.
Daher sollte in diesen Fällen die Möglichkeit einer Neuvergabe der Steuer-ID gesetzlich verankert werden, da die steuerrechtlichen Schutzvorschriften von §§ 30 AO (Steuergeheimnis) und 139 b Abs. 5 AO (Zweckbindung der Steuer-ID) und die Übermittlungssperren des Melderechts in diesem Zusammenhang nicht ausreichen.

Beim Zeugenschutz, bei Inkognito-Adoptionen und in Fällen der Transsexualität sollten die Betroffenen die gesetzliche Möglichkeit erhalten, eine Neuvergabe ihre Steuer-ID zum Schutz ihrer ursprünglichen Identität zu bewirken.

9.2 Pflicht zur Online-Steuererklärung auch für Land- und Forstwirte, Gewerbetreibende und Selbstständige

Mussten bisher nur Unternehmer und Arbeitgeber ihre Steueranmeldung elektronisch übermitteln, sind ab dem 1. Januar 2012 auch alle Land- und Forstwirte, Gewerbetreibende und selbstständig Tätige, die Gewinneinkünfte erzielen, zur elektronischen Abgabe der Einkommensteuererklärung für Veranlagungszeiträume ab 2011 verpflichtet.
Es besteht jedoch die Möglichkeit, bei der Finanzbehörde den Antrag zu stellen, zwecks Vermeidung unbilliger Härten auf eine Übermittlung durch Datenfernübertragung zu verzichten, § 25 Abs. 4 Satz 2 Einkommensteuergesetz. Nach § 150 Abs. 8 Abgabenordnung ist einem solchen Antrag zu entsprechen, wenn eine elektronische Erklärungsabgabe nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung für den Steuerpflichtigen wirtschaftlich oder persönlich unzumutbar ist. Dies ist insbesondere der Fall, wenn die Schaffung der technischen Möglichkeiten für eine Datenfernübertragung des amtlich vorgeschriebenen Datensatzes nur mit einem nicht unerheblichen finanziellen Aufwand möglich wäre oder wenn der Steuerpflichtige nach seinen individuellen Kenntnissen und Fähigkeiten nicht oder nur eingeschränkt in der Lage ist, die Möglichkeiten der Datenfernübertragung zu nutzen.

Um die Einkommensteuererklärung via Internet an das Finanzamt übermitteln zu können, benötigt der Steuerpflichtige, wenn er keinen Steuerberater beauftragt, eine am Markt verfügbare Software, in die die Elster-Schnittstelle der Finanzverwaltung implementiert wurde. Eine Übermittlung ist aber auch über die kostenlose Software ElsterFormular möglich. Die neuen CD-ROMs von ElsterFormular wurden ab Anfang Februar 2013 gratis von vielen Finanzämtern bereitgestellt oder können unter http://www.elsterformular.de herunter geladen werden.
Um ElsterFormular dann nutzen zu können, bedarf es nach der Installation einer Registrierung (Anmeldung) in mehreren Schritten. Sofern der Steuerpflichtige bereits den neuen Personalausweis besitzt und darin die elektronische Identifikationsfunktion freigeschaltet ist, ist seit dem 17. April 2013 eine Registrierung auch hierüber möglich, allerdings werden diesbezüglich noch nicht alle Betriebssysteme unterstützt.
Nach Angaben der Finanzverwaltung erfolgt die gesamte Kommunikation zwischen dem Steuerpflichtigen und http://www.elsterformular.de in verschlüsselter Form. Die Vertraulichkeit der Daten ist gegeben.
Allerdings wird nach wie vor ein von der qualifizierten elektronischen Signatur abweichendes Authentifizierungsverfahren als Äquivalent zur eigenhändigen Unterschrift im manuellen Verfahren genutzt.
Für die Speicherung des dazu notwendigen Authentisierungszertifikates gibt es nach Angaben der Finanzverwaltung drei Möglichkeiten:

1. ELSTER-Basis: Software-Zertifikat

Das Software-Zertifikat des Steuerpflichtigen wird als Datei (VornameZuname_Kontokurzname_elster_2048.pfx) auf dem Computer des Steuerpflichtigen gespeichert, sollte aber nur verwendet werden, wenn er den Computer alleine nutzt und er auf dem aktuellsten Sicherheitsstand (Firewall, Virusscanner) ist.
Das Zertifikat als Datei auf einem Computer ist kostenfrei.

2. ELSTER-Spezial: Sicherheitsstick

Hierzu muss zuvor ein Sicherheitsstick gekauft werden. Nach Angaben des Herstellers, der Giesecke & Devrient GmbH, enthält er einen eigenen Kryptographieprozessor, der die Anmeldedaten verschlüsselt

abspeichert und zur Identifikation für den Datentransfer verwendet. Der Sicherheitsstick soll so zuverlässig Phishing-Attacken auf die digitale Identität, also den Identitätsdiebstahl verhindern. Für das Zertifikat auf einem Sicherheitsstick muss man derzeit 41 € als Anschaffungskosten einplanen.
Er ist im Online-Shop für Sicherheitssticks
(https://www.sicherheitsstick.de/) erhältlich.

3. ELSTER-Plus: Signaturkarte für die Authentifizierung

Um das Authentifizierungszertifikat mit einer Signaturkarte nutzen zu können, muss man in Besitz einer von ELSTER unterstützten Signaturkarte eines Kartenherausgebers bzw. Trustcenters sein. Derzeit werden bereits über 20 verschiedene Signaturkarten verschiedener Hersteller anerkannt, die den sicherheitstechnischen Mindeststandard und die technischen Anforderungen der Finanzverwaltung (ELSTER-Policy) erfüllen.
Für das persönliche Zertifikat auf der Signaturkarte müssen derzeit ca. 50 bis 150 € als Anschaffungskosten eingeplant werden. Die Kosten hängen insbesondere davon ab, ob man schon über eine Signaturkarte und ein entsprechendes Lesegerät verfügt.

Das Verfahren authentisiert nicht den Steuerpflichtigen, der die Steuerklärung oder Steuervoranmeldung abgeben muss, sondern lediglich die Person, die die Erklärung mit Elster tatsächlich abschickt. Das kann jedoch eine Person sein, die Zugang zum Authentifizierungszertifkat des Steuerpflichtigen erlangt hat. Um also die Möglichkeit des unberechtigten Zugriffs auf das Authentifizierungszertifkat einzuschränken, sollte aus datenschutzrechtlicher Sicht auf ELSTER-Basis verzichtet und ELSTER-Plus genutzt werden.

Sicherheitsinformationen für Anwender von Elster finden sich auf den Internetseiten von Elster unter https://www.elster.de/pro_sicher.php und Informationen zur „Authentifizierten Datenübermittlung durch Steuerberater“ unter https://www.elster.de/steuerb_info.php.

Ab 1. Januar 2012 sind alle Land- und Forstwirte, Gewerbetreibende und selbstständig Tätige, die Gewinneinkünfte erzielen, zur elektronischen Abgabe der Einkommensteuererklärung für Veranlagungszeiträume ab 2011 verpflichtet. Aus datenschutzrechtlicher Sicht

sollte auf ELSTER-Basis verzichtet und ELSTER-Plus genutzt werden.

9.3 Datensparsamkeit auch beim Glücksspiel

Die Länder haben aufgrund der Ergebnisse der Evaluierung, der Erkenntnisse aus der international vergleichenden Analyse des Glücksspielwesens sowie aus der Anhörung der Beteiligten und unter Beachtung der Stellungnahme der EU-Kommission die Regelungen des bestehenden Glücksspielvertrags fortentwickelt. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) nahm zu dem Gesetzentwurf der Landesregierung zum Thüringer Gesetz zur Anpassung an Neuregelungen im Bereich des Glückspielwesens aus datenschutzrechtlicher Sicht Stellung. Die Regelung zum System der Sperrdatei begegnete datenschutzrechtlichen Bedenken. Es soll ein übergreifendes Sperrsystem für Spielsuchtsperren als bundesweites Zentralregister zum Schutz von suchtgefährdeten Spielern errichtet werden. Das Gesetz ermöglicht den am übergreifenden Sperrsystem Mitwirkenden die gesonderte Speicherung von Dokumenten, die zur Sperrung eines Spielers geführt haben. Dies widerspricht dem Grundsatz der Sparsamkeit, nach dem Daten nur gespeichert werden sollen, soweit dies erforderlich ist. Von doppelter Datenvorhaltung sollte möglichst abgesehen werden. Vor diesem Hintergrund regte der TLfDI an zu prüfen, ob eine zusätzliche Speicherung der Dokumente bei dem am übergreifenden Sperrsystem Mitwirkenden tatsächlich erforderlich ist. Nach seiner Auffassung reicht es aus, dass die gespeicherten Dokumente im erforderlichen Umfang an die Stellen zu übermitteln sind, die Spielverbote überwachen.
Ebenso wurde angeregt eine Regelung aufzunehmen, nach der beim Erlass einer Verordnung, die beispielsweise die Mitwirkung am übergreifenden Sperrsystem oder Einzelheiten zur Erhebung, Verarbeitung und Nutzung der Daten der gesperrten Spieler sowie technische und organisatorische Maßnahmen zur Datensicherheit regelt, der TLfDI zu hören ist. So kann sichergestellt werden, dass beim Erlass der Verordnung datenschutzrechtlichen Anforderungen hinreichend Genüge getan wird. Die Vorschläge des TLfDI fanden in dem am 1. Juli 2012 in Kraft getretenen Änderungsgesetz leider keine Berücksichtigung.

Bei Verfahren zum Erlass von Verordnungen, die datenschutzrechtliche Fragestellungen betreffen, sollte der TLfDI zwingend in das Verfahren eingebunden werden, um sicherzustellen, dass datenschutzrechtliche Belange hinreichend Berücksichtigung finden. Der Gesetzgeber hat auch bei Gesetzesänderungen den Grundsatz der Datensparsamkeit zu beachten.

9.4 Großes Interesse an Steuerdaten

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde die Frage vorgelegt, ob eine Verwaltungsgemeinschaft (VG) einer Mitgliedsgemeinde die ungefähren jährlichen Gewerbesteuerzahlungen einzelner Unternehmen mitteilen muss. Nach Angaben des ehrenamtlichen Bürgermeisters würden diese Daten zur Planung des Haushalts der Gemeinde für das Folgejahr benötigt. Nur so könnten die wirtschaftliche Lage in groben Zügen eingeschätzt und daraus Folgerungen für die Gestaltung der Politik der Gemeinde abgeleitet werden. Außerdem könne beurteilt werden, wie viel Gewerbesteuer im nächsten Jahr zu erwarten sei und welche Unternehmen in wirtschaftlichen Schwierigkeiten steckten.
Der VG-Vorsitzende verweigerte die geforderten Angaben und teilte lediglich das Gewerbesteuer-Istaufkommen im Zeitraum 2007 bis 2011 und das Gewerbesteuer-Soll für 2011 sowie die Anzahl der Gewerbesteuerpflichtigen in der Gemeinde zur Festsetzung des Hebesatzes für die Grundsteuer mit.
Bei der Erhebung der Gewerbesteuer handelt es sich um eine Aufgabe des eigenen Wirkungskreises der Gemeinde, § 1 Gewerbesteuergesetz. Nach § 47 Abs.2 Satz 1 Thüringer Kommunalordnung (ThürKO) bleiben die Mitgliedsgemeinden einer VG für die Aufgaben des eigenen Wirkungskreises zuständig, es sei denn, sie haben diese Aufgabe nach § 47 Abs. 3 ThürKO durch Zweckvereinbarung auf die VG übertragen. Wenn eine solche Übertragung nicht stattgefunden hat, führt die VG die Aufgaben des eigenen Wirkungskreises nach § 47 Abs. 2 Satz 2 ThürKO als Behörde der jeweiligen Gemeinde „nach deren Weisung“ aus. Die VG hat in diesem Bereich keine eigenen Entscheidungen zu treffen, sondern nur die Entscheidungen der Mitgliedsgemeinde vorzubereiten und zu vollziehen. Die dafür notwendige Willensbildung ist bei der Mitgliedsgemeinde – ebenso wie die Ausübung des Weisungsrechts –

nur möglich, wenn sie über die erforderlichen Informationen verfügt. Grundsätzlich ist daher eine Datenübermittlung an die Mitgliedsgemeinde auf deren Verlangen dann geboten, wenn sie für die Erfüllung von Aufgaben des eigenen Wirkungskreises erforderlich ist.

Im konkreten Fall war aber von Bedeutung, dass es sich bei den verlangten Informationen um Steuerdaten handelt, die dem Steuergeheimnis nach § 30 der Abgabenordnung (AO) unterfallen, das eine umfassende Geheimhaltung aller personenbezogenen Dateien und darüber hinausgehend aller fremden Betriebs- und Geschäftsgeheimnisse verlangt. Nach § 30 Abs. 2 AO verletzt ein Amtsträger das Steuergeheimnis, wenn er Verhältnisse eines anderen, die ihm in einem Verwaltungsverfahren, bekannt geworden sind, unbefugt offenbart. Die Verletzung des Steuergeheimnisses ist eine Straftat, die nach § 355 Strafgesetzbuch mit Freiheitsstrafe bis zu zwei Jahren bestraft werden kann.

Unter welchen Voraussetzungen eine Offenbarung von Steuerdaten befugt erfolgen kann, ist in § 30 Abs. 4 AO geregelt. Sie ist zulässig, wenn sie der Durchführung des Steuerverfahrens dient, § 30 Abs. 4 Nr. 1 AO. Eine Bekanntgabe der Daten an den Bürgermeister dient hier nicht der Durchführung des Steuerverfahrens. Die Gewerbesteuererhebung wird durch die VG durchgeführt. Lediglich der Gewerbesteuerhebesatz wird durch die Gemeinde festgelegt. Für die Festsetzung des Hebesatzes benötigt der Bürgermeister nicht die Angabe, welche Steuern von den jeweiligen Gewerbetreibenden in vergangenen Jahren im Einzelnen gezahlt wurden.

Nach § 30 Abs. 4 Nr. 2 AO ist die Offenbarung auch zulässig, wenn sie durch Gesetz „ausdrücklich“ zugelassen ist. Eine derartige „ausdrückliche“ Zulassung der Offenbarung von Steuerdaten enthält § 47 ThürKO nicht.

Nach § 30 Abs. 4 Nr. 5 AO ist eine Offenlegung von Steuerdaten weiterhin zulässig, soweit für sie ein zwingendes öffentliches Interesse besteht. Der Begriff ist im Gesetz nicht definiert; die Vorschrift enthält lediglich eine nicht abschließende Aufzählung von Beispielsfällen. Keiner der dort genannten Fälle ist im vorliegenden Sachverhalt einschlägig.

Die Tatsache, dass eine Behörde eine Auskunft verlangt und sie sich nicht das Einverständnis des Steuerpflichtigen mit der Offenbarung oder Einsichtnahme in den Steuerbescheid zu verschaffen vermag, rechtfertigt auch im Vergleich mit den anderen gesetzlich aufgeführten Tatbeständen nicht die Annahme eines anderweitigen zwingen-

den öffentlichen Interesses. Weder im Gesetzestext, in der Rechtsprechung noch in der Kommentarliteratur zur AO (Franz Klein, 7. Auflage, § 30, Rn. 191 ff.; Koch/Scholz, 5. Auflage, § 30, Rn. 24) finden sich Ausführungen zur Einschränkung des Steuergeheimnisses gem. § 30 AO aus Zwecken der Planungssicherheit bzw. besseren Prognose des Steueraufkommens.
Im Ergebnis sah sich der TLfDI aus rechtlichen Gründen (§ 30 AO) gehindert, den ehrenamtlichen Bürgermeister in seinem verständlichen Planungsinteresse zu unterstützen.

Steuerdaten dürfen nur aus den im Gesetz genannten Gründen herausgegeben werden. Insofern darf eine VG Daten, die dem Steuergeheimnis unterliegen, nicht aus Zwecken der Planungssicherheit bzw. Prognose des Steueraufkommens an Mitgliedsgemeinden übermitteln.

9.5 Verarbeitung von Steuerdaten durch Privatfirmen?

Im Kreise der Datenschutzbeauftragten des Bundes und der Länder wurde die Frage aufgeworfen, inwieweit sich Kommunen für den Druck, die Aufbereitung zur Kuvertierung und den Versand von Bescheiden zu Steuern und Abgaben Dritter im Wege der Auftragsdatenverarbeitung bedienen dürfen. Hierzu vertritt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) folgende Auffassung: In Thüringen wird der Anwendungsbereich der Abgabenordnung (AO) nach § 15 Thüringer Kommunalabgabengesetz (ThürKAG) eröffnet. Hier wird 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 oben genannte Aufgaben privater Dritte als Verwaltungshelfer bedienen können, enthält das ThürKAG nicht. Daher ist im kommunalen Bereich davon abzusehen, privaten Dienstleistern den Zugang zu Steuerdaten zu ermöglichen.
Derzeit ist nur eine spezialgesetzliche Regelung im Kommunalabgabengesetz des Landes Brandenburg bekannt, die Gemeinden und Gemeindeverbänden ermöglicht, sich privater Dritter als Verwaltungshelfer zu bedienen und sie insbesondere damit beauftragen zu können, die Berechnungsgrundlagen zu ermitteln, die Abgaben zu

berechnen, Bescheide anzufertigen und zu versenden sowie die Abgaben entgegenzunehmen. Nach Auffassung des dortigen Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht ist es somit entsprechend der dortigen landesrechtlichen Regelungen datenschutzrechtlich unbedenklich, Abgabenbescheide durch Dritte drucken, zur Kuvertierung aufzubereiten und versenden zu lassen.

Thüringer Kommunen haben keine Möglichkeit, sich für den Druck, die Aufbereitung zur Kuvertierung und den Versand von Bescheiden zu Steuern und Abgaben privater Dritter zu bedienen.

9.6 Beschwerde über die Information der Finanzämter zum SEPA- Verfahren

Zu den ab dem 1. April 2014 geltenden Neuregelungen zum Lastschriftverfahren wurde der TLfDI um Prüfung der Zustellung von Briefen im Auftrag der Thüringer Finanzverwaltung gebeten. Die Beschwerde bezog sich darauf, dass Steuerpflichtige von Thüringer Finanzämtern unter vollständiger Nennung ihrer Single Euro Payments Area (SEPA) – Information zum Lastschrifteinzug der Kfz-Steuer benachrichtigt wurden. Problematisch sei insbesondere, dass die Zustellung in die allgemein zugänglichen Zeitungsröhren erfolge. In diesem Zusammenhang regte der Beschwerdeführer an, die SEPA-Information, ähnlich wie bei der Kontonummer in Kaufbelegen praktiziert, auf eine begrenzte Stellenzahl zu reduzieren.
Postdienstleistungsunternehmen sind nach § 39 Postgesetz (PostG) und § 206 Abs. 5 Satz 1 Strafgesetzbuch zur Einhaltung des Postgeheimnisses verpflichtet. Weitere datenschutzrechtliche Verpflichtungen der Postdienstleister ergeben sich aus § 41 PostG. Auch enthalten die bestehenden Verträge zwischen der Thüringer Finanzverwaltung und den beauftragten Postunternehmen die erforderlichen Regelungen zur Datenverarbeitung im Auftrag im Sinne des ThürDSG. Insofern ist eine Beauftragung von privaten Postdienstleistungsunternehmen in datenschutzrechtlicher Hinsicht nicht zu kritisieren. Eine Nachfrage bei Thüringer Landesfinanzdirektion ergab, dass die SEPA- Informationen mittels verschlossener Briefe versandt wurden, um den Steuerpflichtigen einen Abgleich ihrer Kontoinformationen zu ermöglichen. Da ein solcher Abgleich eine vollständige SEPA-Information voraussetzt, wäre eine Reduzierung der Stellenzahl der SEPA-Information in diesem Falle nicht sachdienlich.

Welche Einrichtungen (z. B. geschlossene Briefkästen oder offene Zeitungsröhren) die Kunden für den Empfang des Postguts vorgesehen haben, liegt außerhalb der Verantwortung der Postdienstleistungsunternehmer sowie der Thüringer Finanzverwaltung.

Das Verfahren der Thüringer Finanzverwaltung zur Übermittlung der SEPA-Informationen zum Lastschriftverfahren bei der Kfz-Steuer entspricht den datenschutzrechtlichen Bestimmungen.

10 Justiz

omino bianco in prigione
© diego 1012 – Fotolia.com

10.1 Datenschutz hinter Gittern – auch in einer Justizvollzugsanstalt gilt das Grundrecht auf informationelle Selbstbestimmung

Im Berichtszeitraum wurden von mehreren Gefangenen einer Thüringer Justizvollzugsanstalt (JVA) Anfragen und Beschwerden an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) herangetragen, die eine datenschutzrechtlichen Würdigung erforderten.
So war vom TLfDI zu prüfen, ob die Anfertigung von Lichtbildern der Gefangenen datenschutzrechtlich zulässig ist. Bei den konkret durch die Justizvollzuganstalt durchgeführten Maßnahmen handelte es sich jedoch nicht um erkennungsdienstliche Maßnahmen. Vielmehr erfolgte die Fertigung von Lichtbildern zu der betroffenen Person gemäß § 86 a Abs. 1 Satz 1 Strafvollzugsgesetz (StVollzG). Hiernach dürfen zur Aufrechterhaltung der Sicherheit und Ordnung der Anstalt Lichtbilder der Gefangenen aufgenommen und mit den Namen der Gefangenen sowie deren Geburtsdatum und -ort gespeichert werden. Ferner dürfen gemäß § 86 a Abs. 2 Nr. 1 StVollzG die Lichtbilder von Justizvollzugsbediensteten nur genutzt werden, wenn eine Überprüfung der Identität der Gefangenen im Rahmen ihrer Aufgabenwahrnehmung erforderlich ist. Da der Betroffene wegen eines Gerichtstermins von seiner Stammjustizvollzugsanstalt in eine andere Justizvollzugsanstalt überstellt wurde und er den Bediensteten/Transportbediensteten nicht persönlich bekannt war, war es erforderlich, digitale Lichtbilder zu fertigen. Nach Auskunft der Justizvollzugsanstalt wurden die mit einem Lichtbild bedruckte Terminmitteilung und das mit einem Originallichtbild versehene Personalblatt beim Rücktransport in die Stammjustizvollzugsanstalt übergeben und befinden sich dort in der Gefangenenpersonalakte.

Auch die bemängelte Videoüberwachung im Besucherbereich war datenschutzrechtlich zulässig. Jedoch war die Videoüberwachung nicht ausreichend kenntlich gemacht. Zwar waren die Videokameras im Besuchsbereich so installiert, dass jeder Gefangene und Besucher sie sehen konnte, es fehlte aber ein konkreter Hinweis darauf. Nachdem der TLfDI dies bemängelt hatte, wurde an der Tür, durch die die Gefangenen dem Besucherbereich zugeführt werden, und am Besuchereingang jeweils ein zusätzliches Hinweisschild angebracht, welche nun auf die Videoüberwachung hinweisen. Hierdurch ist jetzt für jeden Gefangenen und Besucher mehrmals deutlich erkennbar, dass im Besucherbereich eine Videoüberwachung stattfindet.
Weiterhin erkundigte sich der Gefangene über die datenschutzrechtliche Zulässigkeit der Überwachung der an Gerichte adressierten Post. Die Überwachung des Schriftwechsels, egal ob sie sich auf die Sichtkontrolle beschränkt oder die Inhaltskontrolle zulässt, ist immer mit der Verarbeitung personenbezogener Daten verbunden. Sie ist nur dann zulässig, wenn eine gesetzliche Grundlage hierzu besteht. § 29 Abs. 1 und 2 StVollzG nennt die Ausnahmen von der Überwachung des Schriftwechsels, wobei hier die ordentlichen Gerichte nicht genannt sind. Nach § 29 Abs. 3 StVollzG darf der übrige Schriftwechsel überwacht werden, soweit es aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erforderlich ist. Dies ist im Einzelfall von der überwachenden Justizvollzugsanstalt zu prüfen. Eine generelle Ausnahme der Überwachung der an Gerichte adressierten ausgehenden Post von Gefangenen besteht danach jedoch nicht. Die Rechtsprechung hat die generelle Anordnung der Überwachung besagter Post zwar als unverhältnismäßig eingestuft; dass dies jedoch im Einzelfall erforderlich und verhältnismäßig sein kann, wird nicht in Abrede gestellt. Daher ist es Sache des Gesetzgebers, hier Klarheit zu schaffen, sofern eine generelle Ausnahme für an Gerichte adressierte Post als zielführend angesehen wird.
Aufgrund der herangetragenen Anfragen wurde im Berichtszeitraum zudem eine der in Thüringen ansässigen Justizvollzugsanstalten durch den TLfDI kontrolliert, wobei der Vorgang im Berichtszeitraum noch nicht abgeschlossen werden konnte. Es zeigte sich aber, dass die Justizvollzugsanstalt sehr bemüht ist, den datenschutzrechtlichen Anforderungen zu entsprechen. So wurden bei der Kontrolle lediglich vereinzelte datenschutzrechtliche Mängel festgestellt. Es befanden 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 Hinweis auf die Arbeitsstätte in der Justizvollzugsanstalt. Für die Anbringung solcher auch teilweise sensibler Gesundheitsdaten und der Religionszugehörigkeit konnte eine Erforderlichkeit nicht dargelegt werden. Weiterhin zeigte sich, dass einzelne Gefangenendaten, die elektronisch gespeichert waren, jederzeit durch die Justizvollzugsanstalt wieder aufgerufen werden konnten. Die datenschutzgerechte Ausgestaltung ist derzeit noch nicht geregelt. Im Weiteren ist auch zu klären, wie die Überwachung der Telefonate der Gefangenen datenschutzkonform eingerichtet werden können.
Über den abschließenden Vorgang wird im kommenden Tätigkeitsbericht berichtet werden.

Das Grundrecht auf informationelle Selbstbestimmung ist das Recht des Einzelnen – auch eines Gefangenen –, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dieses Recht kann nur aufgrund eines Gesetzes oder seiner Einwilligung eingeschränkt werden. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil vom 15. Dezember 1983 erstmals aus der Garantie der Menschenwürde in Artikel 1 Grundgesetz (GG) in Verbindung mit der allgemeinen Handlungsfreiheit des Art. 2 GG das Grundrecht auf informationelle Selbstbestimmung abgeleitet. Seither hat das Bundesverfassungsgericht immer wieder den Schutz der Privatsphäre der Bürger stärken und den Gesetzgeber dahingehend berichtigen müssen.
Auch in die Verfassung des Freistaats Thüringen hat das Grundrecht auf informationelle Selbstbestimmung in Artikel 6 Abs. 2 Einzug gefunden.

10.2 Todeserklärung nach dem Verschollenheitsgesetz: Welche Daten dürfen in der Zeitung veröffentlicht werden?

Eine Bürgerin machte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darauf aufmerksam, dass im Verfahren der Todeserklärung nach dem Verschollenheitsgesetz (VerschG) Beschlüsse des zuständigen Amtsgerichts in

der Tagespresse veröffentlicht werden und dabei der Name und die Anschrift der Antragsteller genannt werden.
Das Thüringer Justizministerium teilte – nach Beteiligung der zuständigen Gerichte – mit, dass die Nennung der Anschrift des Antragstellers im Rahmen der Bekanntmachung des Aufgebots nach dem Verschollenheitsgesetz aus Klarstellungsgründen für erforderlich gehalten wird, um Verwechslungen zu vermeiden. Hinzu komme, dass das auf Bundesebene erstellte und bundesweit verwendete Formular die Angabe der Anschrift des Antragstellers vorsieht, sodass das praktizierte Verfahren einer bundeseinheitlichen Handhabung diene.
Aufgrund der bundesweiten Verwendung des Vordrucks hielt der TLfDI eine mit den anderen Landesdatenschutzbeauftragten abgestimmte Vorgehensweise für angezeigt, mit folgendem Ergebnis:
Nach § 19 Abs. 2 a VerschG ist in das bekanntzumachende Aufgebot insbesondere die „Bezeichnung des Antragstellers“ aufzunehmen. Hierzu ist es erforderlich, den Antragsteller auch in der Öffentlichkeit, an die sich das Aufgebot richtet, eindeutig und in identifizierbarer Weise zu bezeichnen, um Verwechslungen soweit wie möglich auszuschließen. Daher kann auch die Anschrift als nach § 19 Abs. 2 a VerschG erforderliches personenbezogenes Datum angesehen werden. Die „Bezeichnung“ umfasst in diesem Zusammenhang nicht zwingend ausschließlich den Namen des Antragstellers, wofür auch das Wort „insbesondere“ spricht.
Entscheidend ist in diesem Zusammenhang der Zweck des Aufgebots, Auskunft über den Verbleib des Verschollenen durch das Aufgebot zu erlangen. Dementsprechend wird – neben jedermann – im Übrigen auch der Verschollene durch das bekanntzumachende Aufgebot aufgefordert, sich innerhalb einer bestimmten Frist zu melden (§ 19 Abs. 2 b VerschG). Diese Meldung des Verschollenen kann auch gegenüber dem Antragsteller erfolgen, der vor der Entscheidung des Gerichts noch einmal angehört werden muss (§ 22 VerschG), denn § 19 Abs. 2 b VerschG regelt im Gegensatz zu § 19 Abs. 2 c VerschG gerade nicht, dass die Meldung gegenüber dem Gericht erfolgen muss. Die Nennung auch der Anschrift des Antragstellers räumt daher dem Verschollenen die Möglichkeit ein, sich statt beim Amtsgericht unmittelbar beim Antragsteller unter dessen bekanntgemachter Anschrift zu melden.

Für eine weitergehende Kontrolle des Amtsgerichts war der TLfDI nach § 2 Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) im vorliegenden Fall nicht befugt.

Die Kontrollkompetenz des TLfDI ist gemäß § 2 Abs. 6 ThürDSG bei Gerichten und dem Rechnungshof eingeschränkt. Der TLfDI ist demnach zur Kontrolle der Gerichte nur insoweit befugt, als es sich um reine Verwaltungsangelegenheiten handelt. Deren nicht auf Verwaltungsangelegenheiten bezogene Tätigkeiten sind im Hinblick auf die verfassungsrechtlich garantierte Unabhängigkeit der Richter von der Kontrolle ausgenommen. Der TLfDI ist insoweit nicht berechtigt, Ermittlungen anzustellen oder datenschutzrechtliche Bewertungen vorzunehmen.

10.3 Das Thüringer Justizvollzugsgesetzbuch – alles in Einem – alles gut?

Mitte des Jahres 2013 hatte das Kabinett den Referentenentwurf eines Thüringer Justizvollzugsgesetzbuchs (ThürJVollzGB) zur Anhörung freigegeben. Der mittlerweile verabschiedete Gesetzentwurf soll künftig die verfassungsrechtlich erforderliche gesetzliche Grundlage für den Vollzug der Freiheitsstrafe, der Jugendstrafe und der Untersuchungshaft im Freistaat Thüringen bilden. Dazu werden die vormals auf diesen Gebieten verschiedenen gesetzlichen Grundlagen in einem neu ausgerichteten Gesetz mit einheitlichen Rechtsbegriffen und Regelungen für den Justizvollzug des Freistaats Thüringen zusammengefasst. Das Thüringer Justizministerium bat dazu den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) um eine Stellungnahme aus datenschutzrechtlicher Sicht.
Der Gesetzentwurf sieht unter anderem vor, dass Akten zukünftig auch in elektronischer Form geführt werden, was zu höheren Risiken für den Datenschutz führt. Deshalb bedarf es aus Sicht des TLfDI bei der Einführung von elektronischen Akten deutlich höherer Anforderungen an die nach § 9 Thüringer Datenschutzgesetz zu treffenden technischen und organisatorischen Maßnahmen zum Datenschutz. Bei einer elektronischen Aktenführung muss gewährleistet sein, dass die gespeicherten personenbezogenen Daten nicht aktenübergreifend zusammengeführt und uneingeschränkt ausgewertet werden können. Dazu müssen auch technische Lösungen geschaffen werden, die eine

Auswertung über das gesetzlich geregelte Maß hinaus möglichst verhindern, zumindest aber erschweren. Dies kann zum Beispiel durch die Vergabe von Zugriffsrechten geschehen. Es muss gewährleistet sein, dass keine unberechtigten Personen Kenntnis vom Inhalt der Akten erlangen, die nicht in ihren Zuständigkeits- bzw. Aufgabenbereich fallen. Dies kann wiederum durch die Beschränkung von Zugriffsrechten oder durch eine Protokollierung der Zugriffe auf die Akten geschehen.

Bedenken bestehen beim TLfDI auch bezüglich der Erweiterung der möglichen erkennungsdienstlichen Maßnahmen auf die elektronische Erfassung jeglicher biometrischer Merkmale. In diesem Bereich ist der technische Fortschritt derzeit nicht abschätzbar. Bei der Verarbeitung weiterer biometrischer Merkmale – über Fingerabdrücke, Lichtbilder und Feststellungen äußerlicher körperlicher Merkmale hinaus – ist nicht auszuschließen, dass damit Erkenntnisse gewonnen werden können, die über die Identifizierung einer Person hinausgehen. Durch den TLfDI wird derzeit keine Notwendigkeit gesehen, eine solche breite Nutzung von biometrischen Merkmalen zu eröffnen. Auch die durch den Gesetzentwurf eröffnete Möglichkeit der Erhebung biometrischer Merkmale des Gesichts, der Augen, der Hände, der Stimme oder der Unterschrift von vollzugsfremden Personen bei ihrem Betreten des Anstaltsgeländes stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dieser Personen dar. Dem wird auch die in der Gesetzesbegründung aufgeführte Tatsache, dass die Erhebung biometrischer Merkmale nur erforderlich ist, um den Austausch von Gefangenen zu verhindern, nicht gerecht. Es kann beim Betreten der Anstalt gerade nicht abgeschätzt werden, ob diese Maßnahme bei dieser Person erforderlich ist. Die Gefahr besteht, dass jegliche vollzugfremde Personen von dieser Maßnahme zur Identitätsfeststellung „auf Vorrat“ betroffen wären. Dahingehend wäre eine datenschutzkonformere Ausgestaltung wünschenswert, bei dessen Umsetzung der TLfDI seine Hilfe anbietet.

Weitere Bedenken bestehen aus Sicht des TLfDI hinsichtlich der Daten von Gefangenen, die – mit Ausnahme von religiösen oder weltanschaulichen Bekenntnissen und Daten anlässlich einer ärztlichen Untersuchung – nach dem Gesetzesentwurf allgemein kenntlich gemacht werden dürfen, soweit dies für ein geordnetes Zusammenleben erforderlich ist. Unklar ist hierbei, welche Daten diesem Zweck unterfallen, da der Zweck im Gesetzentwurf einen bedenklich

weiten Anwendungsspielraum zulässt. Dadurch wäre es möglich, dass eine Vielzahl von personenbezogenen Daten der Gefangenen in der Anstalt offenbart werden könnten, sobald dies von der Anstaltsleitung für ein geordnetes Zusammenleben als erforderlich angesehen wird. Unklar ist auch, was unter den Begriffen „allgemein kenntlich“ zu verstehen ist. In der Gesetzesbegründung ist hierzu aufgeführt, dass solche Daten z. B. an der Haftraumtür kenntlich gemacht werden. Eine abschließende Aufzählung im Hinblick auf die Orte, an denen die Informationen kenntlich gemacht werden können, existiert nicht. Somit könnten die Daten z. B. auch an einem „schwarzen Brett“ veröffentlicht werden und wären für jegliche Personen, die sich im Anstaltsgebäude aufhalten würden, frei zugänglich. Dies stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der Gefangenen dar, zumal diese auch nicht (mit)entscheiden können, welche Daten von ihnen kenntlich gemacht werden.
Das parlamentarische Anhörungsverfahren zum Gesetzesentwurf, zu dem auch der TLfDI ein weiteres Mal Stellung nehmen wird, war zum Ende der Erstellung dieses Berichts noch nicht abgeschlossen.
Es bleibt abzuwarten, ob die datenschutzrechtlichen Erwägungen des TLfDI Eingang in den Inhalt des Gesetzentwurfs finden. Der TLfDI bietet jedoch weiterhin seine Unterstützung an.

Bei der Vorbereitung von Gesetzesentwürfen nimmt auch der TLfDI im Rahmen seiner Zuständigkeit Stellung zu den beabsichtigten Regelungen und erteilt Hinweise, die auf eine datenschutzkonforme Ausgestaltung der Gesetzesnormen hinwirken sollen. Im Rahmen seiner Stellungnahme zum Entwurf eines Thüringer Justizvollzugsgesetzbuchs wies der TLfDI insbesondere auf deutlich höhere Anforderungen an die technisch organisatorischen Maßnahmen bei der Einführung einer elektronischen Akte hin sowie auf eine datenschutzkonforme Ausgestaltung bezüglich der Erweiterung erkennungsdienstlicher Maßnahmen auf die Erfassung jeglicher biometrischer Merkmale.

10.4 Schutz des Erbrechts und der Verfahrensbeteiligungsrechte nichtehelicher und einzeladoptierter Kinder im Nachlassverfahren ("weiße Karteikarten")

Im Mai 2013 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ein Schreiben seines Amtskollegen aus Baden-Württemberg, der den von der Bundesnotarkammer erstellten Entwurf der Anlage „Datenschutzrechtliche Anforderungen“ zur Verwaltungsvereinbarung zwischen den Bundesländern und der Bundesnotarkammer über die Überführung der „weißen Karteikarten“ in das Zentrale Testamentsregister enthielt. Was verbirgt sich hinter dieser kompliziert klingenden Materie? Der Bundesgesetzgeber hatte mit Wirkung zum 29. März 2013 das Testamentsverzeichnisüberführungsgesetz (TVÜG) sowie weitere Gesetze durch das Gesetz zum Schutz des Erbrechts und der Verfahrensbeteiligungsrechte nichtehelicher und einzeladoptierter Kinder im Nachlassverfahren geändert. Gemäß § 9 Abs. 1 Satz 1 TVÜG sind die Bundesländer nunmehr verpflichtet, die bei den Standesämtern und dem Amtsgericht Schöneberg in Berlin vorhandenen Mitteilungen über ein Kind des Erblassers, mit dessen anderem Elternteil der Erblasser bei der Geburt nicht verheiratet war oder das er allein angenommen hat, in das von der Bundesnotarkammer geführte Zentrale Testamentsregister zu überführen. Diese Mitteilungen sind die so genannten weißen Karteikarten. Mit ihnen ordnen die Geburtsstandesämter nichteheliche und einzeladoptierte Kinder ihren Eltern zu und sichern im Erbfall ihre Beteiligung, indem sie nach dem Tod eines Elternteils von Amts wegen das Nachlassgericht informieren.
Die Bundesländer sind verpflichtet, der Bundesnotarkammer als Registerbehörde die in § 9 Abs. 1 Satz 2 TVÜG bezeichneten Daten in elektronischer, bei der Registerbehörde speicherfähiger Form zur Verfügung zu stellen. Die Bundesländer erfüllen diese genannte Verpflichtung mit Hilfe der Bundesnotarkammer im Wege der Organleihe. Gemäß § 9 Abs. 1 Satz 3 TVÜG dürfen die Bundesländer die Bundesnotarkammer damit betrauen, für sie die im Gesetz bestimmten Daten nach ihren Vorgaben zu erfassen und der Registerbehörde zur Verfügung zu stellen.
Die Bundesnotarkammer wiederum hatte die Überführung aller Testamentsverzeichnisse und der Hauptkartei für Testamente beim Amtsgericht Schöneberg in Berlin in das Zentrale Testamentsregister europaweit ausgeschrieben. Den Zuschlag für diese Aufgabe erhielt

ein privates Dienstleistungsunternehmen, das durch ein Subunternehmen in Rumänien die Erfassung der in Deutschland gescannten Karteikarten und so erzeugten Images vornimmt. Im Rahmen dieses Erfassungsvorgangs war die eingangs genannte Anlage „Datenschutzrechtliche Anforderung“ erforderlich, zu der der TLfDI gegenüber dem Datenschutzbeauftragten von Baden-Württemberg Stellung nahm. Dabei wies er unter anderem auf Folgendes hin:

- Die Feststellung in dem Entwurf der Anlage, dass die Metallbehälter und Rollcontainer, die zum Transport der weißen Karteikarten eingesetzt werden, der Deutschen Industrie Norm (DIN) 60529 entsprechen müssen, erschien dem TLfDI nicht ausreichend. Die Schutzart eines Gehäuses wird durch das Kennzeichen IP (Ingress Protection) und einer zweistelligen Kennziffer festgelegt, wobei die erste Ziffer den Schutz für Personen und Betriebsmittel und die zweite Ziffer den Schutz gegen Wasser angibt. Der TLfDI regte daher an, dass die Metallbehälter und Rollcontainer entsprechend der DIN 60529 mindestens der IP57 entsprechen müssten.
- Für den Teilprozess des Transports zum Verarbeitungsstandort des Dienstleistungsunternehmens bzw. seines Subunternehmens sollten sowohl für den Verarbeitungsstandort Berlin als auch für den Ausweichstandort Hamburg dieselben Voraussetzungen gelten: Dies betraf z. B. die Absicherung des Gebäudes, in dem die weißen Karteikarten entladen werden, mittels Rolltores, das erst nach Anmeldung oder mit Schlüssel geöffnet wird. Ferner war zu gewährleisten, dass die Rollcontainer mit ihrem Inhalt, den weißen Karteikarten, sowohl während des Transports als auch bei ihrer Entladung immer unter Aufsicht bleiben, damit kein unberechtigter Zugriff auf die Dokumente erfolgen konnte. Denn im Fall des Eintritts höherer Gewalt (unabwendbare Ereignisse, wie z. B. Naturkatastrophen) sollte laut der Anlage auf den Ausweich-Verarbeitungsstandort Hamburg ausgewichen werden.
- Für die Erfassung der Images in Rumänien waren dort gemäß der zu bewertenden Anlage Telearbeitsplätze oder Arbeitsplätze im Home-Office zwar als unzulässig definiert. Der TLfDI wies aber darauf hin, dass es in der Praxis eine Vielzahl von Fernwartungsverträgen in Form von Unterauf-

tragsverhältnissen gibt, sodass insoweit die Gefahr eines Datenabflusses trotz Verbots von Telearbeitsplätzen/Home-Office-Arbeitsplätzen bestehen könnte.

– Laut der Anlage sollte die Vernichtung der originalen Karteikarten mindestens nach der DIN 32757, Sicherheitsstufe 3 bzw.. nach neuer DIN 66399 Schutzklasse 2 (hoher Schutzbedarf für vertrauliche Daten), Sicherheitsstufe 3 erfolgen. Der TLfDI fordert hingegen bei der Vernichtung sensibler personenbezogener Daten stets eine höhere Sicherheitsstufe, als die Sicherheitsstufe 3 zu wählen. Er bat deshalb darum, für die Vernichtung der weißen Karteikarten mindestens die Sicherheitsstufe 4 anzusetzen.

Nachdem der Datenschutzbeauftragte von Baden-Württemberg die Anregungen des TLfDI und von anderen Landesdatenschutzbeauftragten zusammengefasst hatte, schickte er diese Stellungnahme zur Anlage 5 der genannten Verwaltungsvereinbarung an das Innenministerium von Baden-Württemberg. Daraufhin wurde die Anlage 5 nach Auskunft des dafür federführend zuständigen Innenministeriums von Baden-Württemberg noch einmal überarbeitet.

Sowohl § 9 BDSG als auch § 9 ThürDSG verlangen von öffentlichen Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, dass sie die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Bestimmungen von BDSG bzw. ThürDSG zu gewährleisten. Erforderlich sind die Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

10.5 Aktenklau

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte im Sommer 2012 der Presse entnommen, dass Ermittlungsakten der Staatsanwaltschaft Gera aus dem Kofferraum eines Autos gestohlen worden waren.

Aufgrund der Tatsache, dass staatsanwaltliche Ermittlungsakten naturgemäß eine Vielzahl an personenbezogenen Daten enthalten, wandte sich der TLfDI an die Staatsanwaltschaft Gera, um weitere Informationen über diesen Vorfall zu erhalten. Insbesondere interessierte den TLfDI, welche Regelungen beim Transport von Akten

bestehen und welche Maßnahmen zur Sicherstellung datenschutzrechtlicher Regelungen im Nachgang getroffen wurden.
Daraufhin äußerte sich die Staatsanwaltschaft Gera wie folgt:
Die sachbearbeitende Staatsanwältin habe Ende Juli 2012 den Verlust von Akten gemeldet, die sie zur weiteren Bearbeitung an ihren Wohnsitz nach Dienstende mitnehmen wollte. Sie habe die Akten, neben anderen persönlichen Gegenständen, in einem Nylonbeutel mit sich getragen und diesen in den Kofferraum ihres Privatfahrzeugs gelegt. Aus diesem seien die Akten letztlich entwendet worden, als sie ihre Heimfahrt an einem Einkaufsmarkt unterbrochen habe.
Nach § 5 der Thüringer Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften dürfen Beamte und Beschäftigte Akten nur mit Wissen des verantwortlichen Bediensteten aus den Diensträumen entfernen. Weitere konkretisierende gesetzliche bzw. behördeninterne Regelungen zum Transport von Akten bestünden nicht.
Der Transport von Akten durch Dezernenten der Staatsanwaltschaft finde zum einen in der Regel im Rahmen der Wahrnehmung des Sitzungsdienstes statt. Zum anderen sei aber auch die Bearbeitung von Verfahren nach Dienstschluss nicht verboten. Insbesondere im Hinblick auf die Personalsituation der Staatsanwaltschaft sei diese Verfahrensweise ausdrücklich geduldet.
Die Dezernenten der Staatsanwaltschaft Gera seien gehalten, die Sitzungsakten entweder mit dem eigenen Kraftfahrzeug oder unter Nutzung der öffentlichen Verkehrsmittel zu transportieren. Auf Dienstkraftwagen könne nicht zurückgegriffen werden, da es zu wenig gebe. Ein Transport durch die Justizwachtmeister zu den jeweiligen Gerichten sei nicht möglich, da die Dezernenten die Akten zur Vorbereitung der Verfahren benötigten. Zudem gäbe es auch nicht genügend Justizwachtmeister. Die Dezernenten seien in Fällen des Transports von Akten außerhalb der Dienstgebäude zu einem sorgfältigen Umgang mit den Akten angehalten. Sie seien insbesondere gehalten, die Akten vor Verlust zu schützen.
Nach dem Vorfall seien die Abteilungsleiter der Staatsanwaltschaft gebeten worden, die Dezernenten auf den sorgsamen Umgang mit den Akten beim Transport außer Haus hinzuweisen und sie zu sensibilisieren, alles Gebotene vorzunehmen, um die Akten vor Verlust zu schützen.

Wie der TLfDI im Ergebnis feststellen konnte, waren durchaus technische und vor allem organisatorische Maßnahmen getroffen worden, um den Verlust personenbezogener Daten bei der Staatsanwaltschaft zu vermeiden.
Der TLfDI wies aber unter anderem darauf hin, dass bei der Mitnahme von Akten zum Zwecke der Bearbeitung nach Dienstschluss zu Hause ebenfalls den datenschutzrechtlichen Vorschriften gegen unbefugten Zugriff bzw. gegen unbefugte Kenntnisnahme Rechnung zu tragen und ein Verschluss der Unterlagen erforderlich ist, z. B. gegenüber Familienangehörigen. Denn im häuslichen Bereich sind die sicherheitstechnischen Maßnahmen einer Staatsanwaltschaft, wie Gebäudesicherung und Zugangskontrollen etc., nicht gegeben.
Es wurde vom TLfDI letztlich angeregt, diesen Aspekt in den entsprechenden Belehrungen ebenfalls anzusprechen und dies nachzuholen, sofern eine solche Belehrung bisher nicht erfolgt sein sollte

§ 5 Abs. 5 der Thüringer Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften bestimmt, dass Beamte und Beschäftigte die Akten nur mit Wissen des verantwortlichen Bediensteten aus den Diensträumen entfernt werden. Damit steht und fällt das Recht auf informationelle Selbstbestimmung, wie großzügig ein Leitender Oberstaatsanwalt in seiner Behörde die Aktenmitnahme außerhalb seiner Behörde regelt. Aus Sicht des TLfDI ist es daher dringend erforderlich, diese Regelung sehr eng auszulegen. Im Falle einer Mitnahme von Akten außerhalb der Behörde hat eine Staatsanwältin / ein Staatsanwalt alle gebotenen und zumutbaren Maßnahmen in Anlehnung an die zur Telearbeit bestehenden Regelungen zu treffen, damit eine unbefugte Kenntnisnahme von personenbezogenen Daten aus den Akten ausgeschlossen ist. Als Beispiel ist hier die Aktenaufbewahrung zu Hause in einem abschließbaren Schrank zu nennen.
Ein Kommunikationsprozess zwischen Justiz und dem TLfDI ist bereits angestoßen.

11 Gesundheits- und Sozialdatenschutz

Patientenakte
© Doce Rabe Media 5 – Fotolia.com

11.1 OH KIS reloaded

Bereits in seinem 9. Tätigkeitsbericht hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) über die Orientierungshilfe Krankenhausinformationssysteme (OH KIS) informiert (siehe dort Punkt 11.1). Es handelt sich um eine OH, die die Unterarbeitsgruppe „Krankenhausinformationssysteme“ des Arbeitskreises „Gesundheit und Soziales“ der Datenschutzkonferenz erarbeitet hat, um bundesweit und trägerübergreifend ein einheitliches Verständnis der datenschutzrechtlichen Anforderungen an den Einsatz von Krankenhausinformationssystemen zu ermöglichen. Bereits beim Erlass der OH KIS stand fest, dass die technischen Anforderungen, Strukturen und Prozesse im Krankenhausbetrieb einem dynamischen Wandel unterworfen sind und die OH daher fortgeschrieben werden muss und soll. Dabei sollte der Dialog mit den Herstellern und Betreibern von Krankenhausinformationssystemen fortgeführt werden.
Im Berichtszeitraum tagte die Unterarbeitsgruppe, an der auch der TLfDI teilnahm, siebenmal, um über die inhaltliche Fortschreibung der OH zu beraten. In die Beratungen flossen die Erfahrungen des TLfDI ein, die dieser im Rahmen der von ihm durchgeführten Krankenhauskontrollen gemacht hatte. Hierzu wird auf den 9. Tätigkeitsbericht Punkt 11.1 verwiesen. Im Berichtszeitraum fanden in Thüringen drei gemeinsame Treffen von Vertretern des TLfDI, der Landeskrankenhausgesellschaft Thüringen e. V., Vertretern der kontrollierten Krankenhäuser und der Landesärztekammer statt. Ziel dieser Treffen war es, gemeinsam mit allen Beteiligten Lösungen für die Probleme zu erörtern, die sich anhand der durchgeführten Kontrollen im Hinblick auf die Durchführung der OH KIS ergeben hatten. Problematisch ist hierbei insbesondere, dass ein Teil der am

Markt angebotenen Software-Lösungen in technischer Hinsicht noch hinter den Anforderungen der OH KIS zurückbleiben. Außerdem konnten die Vertreter der Krankenhäuser darlegen, in welchen Bereichen die OH KIS vertretbaren Anforderungen aus der Praxis nicht gerecht wird.
Parallel hierzu stand die Unterarbeitsgruppe in intensivem Austausch mit der Deutschen Krankenhausgesellschaft. Die hier jeweils gewonnen Erkenntnisse flossen in eine überarbeitete Fassung der OH ein, die zum Ende des Berichtszeitraumes noch nicht fertiggestellt war, mit deren Veröffentlichung aber im Jahr 2014 zu rechnen ist. Nach Verabschiedung der neuen Fassung der OH KIS wird der TLfDI diese bei der Prüfung der Krankenhäuser in Thüringen heranziehen. Zur Umsetzung wird der enge Kontakt zur Landeskrankenhausgesellschaft weiterhin aufrechterhalten.

Die Orientierungshilfe Krankenhausinformationssysteme wurde aufgrund der in der Praxis gewonnenen Erfahrungen und dem engen Dialog mit der Deutschen Krankenhausgesellschaft sowie einigen Krankenhausgesellschaften fortgeschrieben.

11.2 Kooperation zwischen Jugendamt und Jobcenter

Das Thüringer Ministerium für Soziales, Familie und Gesundheit wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), damit dieser eine geplante Kooperationsvereinbarung zwischen einem Jugendamt und einem Jobcenter datenschutzrechtlich bewertet. Problematisch war hier eine Regelung, nach der das Jugendamt dem zuständigen Jobcenter automatisch mitteilen sollte, wenn Kinder aus einer Bedarfsgemeinschaft anderweitig untergebracht werden, etwa in einer Pflegefamilie. Besteht etwa eine Bedarfsgemeinschaft aus fünf Personen (Eltern und Kinder) und werden die Kinder untergebracht, ist dies für die Berechnung der Leistung nach dem Sozialgesetzbuch (SGB) II relevant. Durch die Unterbringung der Kinder ändert sich der Regelbedarf der Eltern um den Unterhalt der Kinder. Wenn die Eltern dem Jobcenter die Unterbringung nicht mitgeteilt haben, erhalten sie zunächst zu viel staatliche Zuwendungen und sind dann später Rückforderungsansprüchen und möglicherweise auch einem Ordnungswidrigkeitenverfahren ausgesetzt, weil sie leistungsrelevante Tatsachen nicht mitgeteilt haben. Das Jugendamt wehrte sich

zu Recht dagegen, sich zu einer derartigen Mitteilung gegenüber dem Jobcenter zu verpflichten. Nach seiner Auffassung würde die Mitteilung des Umstands der Unterbringung den Erfolg der Arbeit des Jugendamtes in Frage stellen. Ziel der Unterbringung ist es, die Kinder, sofern dies nach dem Kindeswohl möglich ist, perspektivisch wieder in die Familie zurückzuführen. Hierzu ist der Aufbau eines Vertrauensverhältnisses zu den Eltern erforderlich. Dieses Verhältnis würde gefährdet, wenn das Jugendamt das Jobcenter regelmäßig über die Unterbringung informiert. Nach den Vorschriften im SGB sollen sich die verantwortlichen Stellen gegenseitig Sozialdaten übermitteln, soweit dies zur ordnungsgemäßen Aufgabenwahrnehmung der beteiligten Behörden, insbesondere zur Bekämpfung von Leistungsmissbrauch und illegaler Beschäftigung erforderlich ist. Das bedeutet, dass eine Verpflichtung zu einer generellen Meldung an das Jobcenter unzulässig ist, da die gesetzliche Regelung vorsieht, dass es konkrete Anhaltspunkte für einen Leistungsmissbrauch geben muss. Weiterhin ist die Datenübermittlung für die Aufgabenwahrnehmung des Jugendamtes nicht erforderlich, sie gefährdet vielmehr die ordnungsgemäße Aufgabenerfüllung.
Der TLfDI unterbreitete den Beteiligten einen Kompromissvorschlag: Das Jugendamt soll bei der Beratung der betroffenen Eltern auf den Umstand hinweisen, dass die Tatsache der Unterbringung leistungsrelevant nach dem SGB II ist und dem Jobcenter mitgeteilt werden muss. In diesem Fall sind die Eltern informiert und müssen dann selbst entscheiden, ob sie eine entsprechende Mitteilung an das Jobcenter machen.

Übermittlungen von Sozialdaten zur Verhinderung von Leistungsmissbrauch setzen, sofern es keine spezialgesetzliche Regelung gibt, voraus, dass es konkrete Hinweise für das Vorliegen von Leistungsmissbrauch gibt. Es würde die Aufgabenerfüllung der Jugendämter gefährden, wenn diese die Unterbringung von Kindern automatisch an das zuständige Jobcenter melden.

11.3 Emergency Room auf Rädern: Videogaga 10

In Deutschland hat jedes Bundesland seine eigene Aufsichtsbehörde für den Datenschutz. Damit es auf diesem Wege nicht zu Wettbewerbsverzerrungen kommt, stehen diese Aufsichtsbehörden in einem stetigen und intensiven Informationsaustausch, an dem sich auch der

Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) beteiligt. Eine Art dieses Informationsaustausches sind so genannte Länderumfragen, in denen ein Bundesland ein spezifisches Problem darlegt und erfragt, wie in anderen Bundesländern damit umgegangen wird. In einem solchen Fall ist ein Bundesland an den TLfDI herangetreten und bat um Informationen, ob in Thüringen der Bereich rund um Rettungswagen videoüberwacht sei. Hintergrund sei das immer wiederkehrende Abhandenkommen von medizinischen Ausrüstungsgegenständen aus den Rettungswagen. Eine Rückfrage beim zuständigen Fachreferat des Thüringer Innenministeriums ergab jedoch, dass Videoüberwachung an Rettungswagen in Thüringen nicht durchgeführt wird.
Dies ist auch gut so, denn der TLfDI erachtet eine solche Überwachung für rechtswidrig. Einschlägige Erlaubnisnorm wäre mangels einer spezielleren Rechtsgrundlage § 6 b Bundesdatenschutzgesetz (BDSG). Dieser regelt die Zulässigkeit von Videoüberwachung in öffentlich zugänglichen Bereichen. Dies ist nur dann zulässig, wenn die Videoüberwachung zur Durchsetzung des Hausrechts oder für berechtigte Interessen zu konkret festgelegten Zwecken erforderlich ist und keine Anhaltspunkte bestehen, dass schützenswerte Interessen Betroffener überwiegen. Während die Ausübung eines Hausrechtes außerhalb des Rettungswagens nicht ausgeübt werden kann, wird die Videoüberwachung wohl zu berechtigten Interessen durchgeführt werden. Allerdings bestehen hier erhebliche Anhaltspunkte dafür, dass schützenswerte Interessen von Betroffenen überwiegen. Durch die Außenaufnahmen wird das Recht der übrigen Verkehrsteilnehmer auf informationelle Selbstbestimmung beeinträchtigt. Der Eingriff in das Grundrecht entfällt nicht dadurch, dass lediglich Verhaltensweisen im öffentlichen Raum erhoben werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begibt, Rechnung. Insoweit umfasst das Recht auf informationelle Selbstbestimmung auch das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden.

Bevor Videoüberwachungen eingerichtet werden, muss zwingend geprüft werden, ob diese den gesetzlichen Vorschriften entsprechen. Eine Videoüberwachung an Rettungswagen ist mit dem geltenden Recht nicht vereinbar.

11.4 Datenerhebung im Jobcenter des Landkreises Eichsfeld

Ein Kunde des Jobcenters des Landkreises Eichsfeld beschwerte sich beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) darüber, dass das Jobcenter alle sechs Monate Kopien seines Personalausweises, seines Versicherungsausweises, seiner Krankenversicherungskarte und seiner EC-Karte fertigt und zur Leistungsakte nimmt. Weiterhin legte der Beschwerdeführer eine Kopie des verwendeten Formulars „Bescheinigung der Unterkunftskosten“ vor. Da in dieser Bescheinigung, in der der Vermieter die Mietkosten bestätigen sollte, ein Hinweis auf § 67 a Abs. 4 Sozialgesetzbuch X (SGB X) enthalten war, handelte es sich um eine Übermittlung von Sozialdaten an den Vermieter. Dieser würde bei der Vorlage der Bescheinigung erfahren, dass der Mieter Leistungen nach dem SGB bezieht. Nach § 67 d Abs. 1 ist eine Übermittlung von Sozialdaten nur zulässig, soweit es dafür eine gesetzliche Übermittlungsbefugnis im SGB gibt. Eine solche liegt insoweit jedoch nicht vor.
Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis darf ausschließlich erfolgen zur Identitätsfeststellung oder nach Maßgabe der §§ 18 bis 20 Personalausweisgesetz. Hierzu wird auf den Punkt 3.48 des 1. Tätigkeitsberichts für den nichtöffentlichen Bereich verwiesen, der sich mit der Zulässigkeit der Fertigung von Personalausweiskopien näher beschäftigt. Verkürzt lässt sich sagen, dass eine Anfertigung der Kopie eines Personalausweises nur dann zulässig ist, wenn es hierfür eine spezielle gesetzliche Ermächtigung gibt. Zur Feststellung der Identität einer Person reicht es aus, wenn diese den Ausweis zur Identitätsfeststellung vorlegt und der Bearbeiter im Jobcenter die Identität vor Ort feststellt.
Das Jobcenter teilte auf Nachfrage mit, dass sich die Beschäftigten des Jobcenters den gültigen Pass oder Personalausweis ebenso wie die Krankenversicherungskarte und die Bankkarten vorlegen lassen. Nach einer internen Anweisung würden Ausweisdokumente, Krankenversicherungskarte, Bank- und Sparkassenkarten grundsätzlich

nicht zur Akte genommen. Es erfolge ein Aktenvermerk über die Ausweisung bzw. Vorlage der entsprechenden Dokumente. Nur wenn ein Kontoauszug eine Änderung der Leistungshöhe zur Folge habe oder weiterer Ermittlungsbedarf bestehe, würde eine Kopie zur Akte genommen. Der Leistungsberechtigte würde auf die Möglichkeit der Schwärzung bestimmter Passagen von Ausgabebuchungen hingewiesen.
Im Hinblick auf die Mietbescheinigung teilte das Jobcenter mit, dass die Verwendung der Bescheinigung freiwillig sei. Ihre Verwendung soll der Vereinfachung der Bearbeitung dienen. Dem Mieter stehe es jedoch frei, stattdessen den Mietvertrag vorzulegen. Die zur Verfügung gestellte Bescheinigung wurde dergestalt geändert, dass auf dem Papier an erster Stelle auf die Freiwilligkeit der nachstehend geforderten Angaben hingewiesen wird und anstelle dieser Bescheinigung auch der Mietvertrag vorgelegt werden kann. Damit verhält sich das Jobcenter nunmehr rechtskonform. Der Beschwerdeführer wurde hierüber informiert.

Die Fertigung von Personalausweiskopien ist nur zulässig, wenn es hierfür eine gesetzliche Grundlage gibt. Formulare, die das Jobcenter zur Vorlage bei dritten Stellen vorhält, dürfen, sofern sie verpflichtend zu verwenden sind, keinen Hinweis auf den Bezug von Leistungen nach dem SGB enthalten.

12 Wirtschaft, Arbeit, Bau und Verkehr

City on the construction helmet
© determined – Fotolia.com

12.1 Unklarheiten nicht nur beim Landesamt für Statistik – für welche Umsätze ist eine Steuerberaterin auskunftspflichtig?

Im Frühjahr 2013 erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Beschwerde einer Steuerberaterin darüber, dass sie mit Heranziehungsbescheid des Thüringer Landesamtes für Statistik (TLS) als Leiterin einer Steuerkanzlei aufgefordert worden sei, statistische Auskünfte zur Strukturerhebung im Dienstleistungsbereich (SiD) für das Berichtsjahr 2011 nach § 5 Abs. 1 Dienstleistungsstatistikgesetz (DlStG) zu erteilen. Die Steuerberaterin leitete als Partnerin einer bundesweit tätigen Partnerschaftsgesellschaft das Filialbüro in einer Ostthüringer Stadt und bezog daher umsatzsteuerbare Beteiligungsbezüge aus dieser Partnerschaftsgesellschaft. Aufgrund dessen war sie auch nach eigener Auffassung nicht in der Lage, für das Thüringer Filialbüro separat Auskünfte zu Umsatzerlösen, Materialaufwendungen und Beständen zu geben. Diese Auskünfte könne allein die Partnerschaftsgesellschaft geben. Diese Umstände hatte die Steuerberaterin bereits dem TLS ebenso zuvor per E-Mail mitgeteilt wie auch die Tatsache, dass ihr zuständiges Finanzamt die Korrektur der falschen Grundinformationen (statt Rechtsform „Freiberufler“ die Rechtsform „beteiligt“) vorgenommen habe. Offensichtlich waren die falschen Grundinformationen noch im Unternehmensregister gespeichert.
Der TLfDI wandte sich an das TLS und bat um dessen datenschutzrechtliche Stellungnahme in der Angelegenheit. Insbesondere interessierte den TLfDI dabei, wie das TLS den Begriff des Inhabers oder Leiters der Unternehmen oder Einrichtungen zur Ausübung einer freiberuflichen Tätigkeit in § 5 Abs. 1 DlStG auslegt. Fraglich war für den TLfDI in diesem Zusammenhang insbesondere, ob die

Steuerberaterin als Partnerin der Partnerschaftsgesellschaft oder als Leiterin des Filialbüros in Thüringen auskunftspflichtig sei.
Nachdem ein erstes Antwortschreiben des TLS nicht die Antworten auf die gestellten Fragen des TLfDI erbrachte, weil das Geheimhaltungsbedürfnis nach § 16 Bundesstatistikgesetz Anwendung fände, musste der TLfDI das TLS mit einem zweiten Schreiben erneut zur Auskunftserteilung über die aufgeworfenen Fragen auffordern. In diesem zweiten Schreiben wies der TLfDI auch auf § 38 Abs. 1 Satz 1 und 2 Nr. 1 Thüringer Datenschutzgesetz (ThürDSG) hin, wonach der TLfDI und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen sind und ihnen im Rahmen ihrer Kontrollbefugnis nach § 37 ThürDSG insbesondere Auskunft zu ihren Fragen zu gewähren ist.
Mit Schreiben vom Juni 2013 teilte das TLS schließlich seine Rechtsauffassung mit, dass die Steuerberaterin ausschließlich für ihre persönlich erzielten Umsätze aus der Beteiligung als Partnerin an der Partnerschaftsgesellschaft auskunftspflichtig sei. Für die nach wie vor bestehende Auskunftspflicht sei es nicht notwendig, eine Einzelsteuerpraxis zu führen. Denn sowohl die Einstufung als „sonstige selbstständig tätige Person“ als auch die Einstufung „Person mit Beteiligung an gewerblichen Personengesellschaften“ unterlägen der Berichtspflicht zur Dienstleistungsstatistik.
Diese Rechtsauffassung entsprach dem Anliegen der Steuerberaterin, nicht für das Filialbüro der Partnerschaftsgesellschaft separat auskunftspflichtig zu sein.
Ihre weiteren datenschutzrechtlichen Anfragen zu den Aufgaben und Befugnissen des Finanzamtes beantworte der TLfDI folgendermaßen:

- Zur Frage eines möglichen Widerspruchsrechts des Betroffenen gegenüber dem Finanzamt hinsichtlich einer Datenübermittlung wies der TLfDI darauf hin, dass die Abgabenordnung (AO) als spezialgesetzliche Ermächtigungsgrundlage weder eine Einwilligung in eine Datenübermittlung noch ein Widerspruchsrecht dagegen beinhalte. Demzufolge gibt es auch keine Pflicht des Finanzamtes, die an einen Dritten zu übermittelnden Daten dem Betroffenen etwa zu Korrekturzwecken vorzulegen.
- Die von der Steuerberaterin aufgeworfene Frage, ob das in § 30 AO enthaltene Steuergeheimnis einer Übermittlung

personenbezogener Daten an das TLS entgegenstehe, konnte der TLfDI unter Hinweis auf die Ausnahmeregelung von § 30 Abs. 4 Nr. 2 AO beantworten. Danach ist eine Offenbarung der dem Steuergeheimnis unterliegenden Daten zulässig, soweit sie durch Gesetz ausdrücklich zugelassen ist. Genau eine solche gesetzliche Ausnahmeerlaubnis findet sich für das Finanzamt in § 2 Statistikregistergesetz (StatRegG) in Verbindung mit § 1 Abs. 1 StatRegG. Danach ist es zulässig, dass das Finanzamt bestimmte, dem Grundsatz des Steuergeheimnisses unterliegende Daten an die statistischen Landesämter auf Anforderung übermittelt.

Steuerberater einer Partnerschaftsgesellschaft sind im Rahmen einer Strukturerhebung im Dienstleistungsbereich (SiD) ausschließlich für ihre persönlich erzielten Umsätze aus ihrer Beteiligung als Partner an der Partnerschaftsgesellschaft auskunftspflichtig. Sofern das Finanzamt oder das Landesamt für Statistik unzutreffende Angaben zu Grunde legt, empfiehlt sich folgende Vorgehensweise:
Der Betroffene sollte seine korrigierten Angaben an die Behörden nicht nur per E-Mail, sondern zur Sicherheit auch als Einschreiben mit Rückschein versenden. Dies gilt insbesondere im Hinblick auf die Heranziehung zu Strukturerhebungen im Dienstleistungsbereich, wenn Unklarheiten bei der Frage auftauchen, wer aufgrund eines Eintrags im Unternehmensregister wie weit berichtspflichtig ist. Im Streitfall hilft auch hier der TLfDI bei der Lösung des datenschutzrechtlichen Problems.

12.2 Fahrerlaubnis nur mit Gutachten?

Ein Bürger hat sich mit der Bitte um Prüfung eines Sachverhalts an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) gewandt. Er teilte mit, dass er in seiner Erwerbsfähigkeit gemindert sei. Er benötige einen PKW, um zu seiner Arbeitsstätte zu gelangen, könne aber nur ein Fahrzeug mit Automatikgetriebe bedienen. Seine Berufsgenossenschaft habe ihm mitgeteilt, dass er eine Eintragung in den Führerschein zum Führen eines Autos mit Automatikgetriebe bei der Fahrerlaubnisbehörde (FEB) Gotha vornehmen lassen müsse. Aufgrund dessen erhielt er bei der FEB Gotha einen Termin und bei dieser Gelegenheit wurde ein Gutachten über den Gesundheitszustand von ihm verlangt. Er bot

der FEB an, eine Zusammenfassung des Gesamtgutachtens zur Minderung der Erwerbsfähigkeit (MdE) vorzulegen. Seitens der FEB wurde dies nicht akzeptiert, vielmehr sei ihm nahegelegt worden, ein psychiatrisches Gutachten beizubringen. Daraufhin habe er das Gutachten übergeben, welches in Kopie zu den Akten genommen wurde. Er gehe davon aus, dass in dem Gesamtgutachten Sachverhalte zu seiner Person dokumentiert sind, die zur Beurteilung der Geeignetheit zum Führen von Kraftfahrzeugen nicht relevant sind. Die Bitte an den TLfDI war, zu prüfen, inwieweit er zur Herausgabe dieser persönlichen Unterlagen verpflichtet war.
Der TLfDI wandte sich an die Fahrerlaubnisbehörde Gotha und bat um Stellungnahme zu diesem Sachverhalt. Die FEB Gotha teilte mit, dass der Betroffene bei DEKRA e. V., Technische Prüfstelle für den Kraftfahrzeugverkehr ein Gutachten für Körperbehinderte gemäß §§ 11 und 46 Fahrerlaubnisverordnung (FeV) zum Führen von Kraftfahrzeugen zur Vorlage bei der Berufsgenossenschaft veranlasst hatte. In diesem werden Beschränkungen und Auflagen zur Erteilung/Verlängerung der Fahrerlaubnis vermerkt. Unter dem Punkt „Bemerkungen“ war ausgeführt, dass ein fachärztliches Gutachten nicht vorlag. Auf der Grundlage von § 2 Abs. 4 Straßenverkehrsgesetz in Verbindung mit §§ 11 und 46 Fahrerlaubnis-Verordnung habe die FEB Gotha ermitteln müssen, ob er zum Führen von Kraftfahrzeugen geeignet und befähigt ist und ob gegebenenfalls Beschränkungen für erforderlich gehalten werden. Zur Klärung der Eignungszweifel ist die Anordnung eines ärztlichen Gutachtens bei der Begutachtungsstelle für Fahreignung (BfF) oder eines amtlich anerkannten Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr beizubringen. Daraufhin sei vom Betroffenen auf ärztliche Unterlagen verwiesen worden, die Auskunft über die Fahreignung geben würden. Hätten diese Unterlagen zur Klärung der Eignungszweifel ausgereicht, so hätte auf ein kostenpflichtiges ärztliches Gutachten verzichtet werden können. Dies sei im Hinblick auf die Zusammenfassung aber nicht der Fall gewesen. Aus diesem Grund wurde mit Einverständnis des Betroffenen eine Kopie des Gesamtgutachtens zur Minderung der Erwerbsfähigkeit gefertigt. In die Fahrerlaubnisakte wurden nur entsprechende Seiten aus dem Gesamtgutachten, welche eignungsrelevant waren, abgelegt. Auf den Seiten, die als Nachweis dienen, sind darüber hinaus alle nicht relevanten Passagen geschwärzt worden.

Aus datenschutzrechtlicher Sicht ist festzustellen, dass die Fahrerlaubnisbehörde Eignungszweifel von Amts wegen klären muss. Die Kenntnis der Daten war zur Erfüllung der Aufgaben erforderlich. Liegt in diesen Fällen kein Gutachten vor, so muss ein kostenpflichtiges Gutachten von der Begutachtungsstelle für Fahreignung erstellt und dann der FEB übergeben werden. Es lag damit kein datenschutzrechtlicher Verstoß der FEB Gotha vor.

Auf der Grundlage von § 2 Abs. 4 Straßenverkehrsgesetz in Verbindung mit §§ 11 und 46 Fahrerlaubnis-Verordnung muss die Fahrerlaubnisbehörde von Amts wegen ermitteln, ob zum Führen von Kraftfahrzeugen die Eignung und Befähigung gegeben ist und ob Beschränkungen für erforderlich gehalten werden. Aus diesem Grund ist die Vorlage von Gutachten von der Begutachtungsstelle für Fahreignung zur Erfüllung dieser Aufgaben erforderlich.

12.3 Alles smart oder was ?

Entsprechend der Europäischen Richtlinie zu Energieeffizienz und Energiedienstleistungen (EDL 2006/32/EG) sind alle Mitgliedstaaten der Europäischen Union verpflichtet, intelligente Energienetze und -zähler einzuführen, die die Abrechnungen auf der Grundlage des tatsächlichen Verbrauchs durchführen und die Kunden in die Lage versetzen, ihren eigenen Energieverbrauch zu steuern. Der Stromverbrauch soll dann beispielsweise per Mobilfunk oder/und über das Internet an den jeweils zuständigen Energieversorger übermittelt werden. Die Gefahr, die von diesen intelligenten Stromzählern ausgeht, ist nicht zu unterschätzen. Über den Stromverbrauch lassen sich einige interessante Rückschlüsse ziehen. Ermittelbar ist nicht nur, wieviel Strom jemand zu Hause verbraucht, sondern mit hoher Wahrscheinlichkeit auch, welches Gerät wie lange betrieben wurde. Dies lässt sich nämlich unter Umständen aus der Stromverbrauchskurve entnehmen. Relativ konkrete Verbrauchs- und damit Verhaltensprofile lassen sich auf diese Weise erstellen. Unklar bleibt dabei, wer wann auf welche Daten Zugriff hat und wie Bürger sich vor dem Zugriff unberechtigter Dritter, beispielsweise bei Störungen, schützen können. Nicht nur das unberechtigte Ausspähen über das Internet erscheint möglich, sondern, da die intelligenten Stromzähler über kleine Computer verfügen, wird es eine Frage der Zeit sein, wann Kriminelle über das Internet auf den Stromzähler zugreifen und

mittels eines Computervirus den Stromverbrauch verringern oder erhöhen können.
Die Europäische Kommission hat am 9. März 2012 zur Vorbereitung für die Einführung dieser intelligenten Messsysteme (Smart Metering) Empfehlungen herausgegeben. Darin fordert die Kommission auch, den Schutz der Privatsphäre in vollem Umfang bei der Verarbeitung personenbezogener Daten zu gewährleisten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Düsseldorfer Kreis haben daraufhin im Juni 2012 eine „Orientierungshilfe datenschutzgerechtes Smart Metering“ erarbeitet. Diese befasst sich unter anderem mit den Anforderungen an die datenverarbeitenden Stellen, die Vermeidung des gläsernen Endverbrauchers (Letztverbrauchers), die Transparenz von Systemen für den Letztverbraucher und auch bei klar definierten Fällen von Störungen die Möglichkeit für ihn, die Kommunikation zu unterbinden. Die Orientierungshilfe ist auf den Internetseiten des TLfDI abrufbar unter:
http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oriemtierungshilfe_smart_metering.pdf
Auch das Bundesamt für die Informationssicherheit (BSI) hat aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten in Messsystemen sowie möglicher negativer Rückwirkungen auf die Energieversorgungssicherheit eingeschätzt, dass hohe Anforderungen an den Datenschutz und die Datensicherheit zu stellen sind. Nach Angaben des BSI machen bekannt gewordene Hackerangriffe auf intelligente Messsysteme, unter anderem in den USA, und neuere Gefährdungen, wie etwa der Computerwurm Stuxnet, der eben heimlich technische Prozesse überwachen und steuern kann, die Notwendigkeit für sichere Lösungen für die Einführung intelligenter Messsysteme in Deutschland deutlich. Um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure in Deutschland zu gewährleisten, hat das BSI ein Sicherheitsprofil für das Sicherheitsmodul eines Smart Meter Gateways (BSI-CC-PP-0073) und eine entsprechende Technische Richtlinie (BSI TR-03109) erarbeitet. Beide Dokumente sind abrufbar unter:
https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html .

Um zu verhindern, dass unter Zugrundelegung des Stromverbrauchs Profile über das Verhalten von Bürgerinnen und Bürgern im häuslichen Bereich erstellt werden können, sind die Orientierungshilfe der

Datenschutzkonferenz des Bundes und der Länder und das vom BSI erarbeitete Sicherheitsprofil und die Technische Richtlinie umzusetzen.

12.4 Section Control – Abschnittsgeschwindigkeits-Kontrolle auf Autobahnabschnitten bald auch in Thüringen?: Videogaga 11

Im Februar 2012 richtete das Thüringer Ministerium für Bau, Landesentwicklung und Verkehr (TMBLV) im Auftrag des Bundesministeriums für Verkehr (BMVBS) eine Anfrage an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI). Das TMBLV sollte in Erfahrung bringen, ob in Thüringen die Bereitschaft bestehe, an der Erarbeitung und Erprobung eines Modells zur abschnittweisen Geschwindigkeitsüberwachung – Projekt „Section Control“ – teilzunehmen. Hierzu wurde der TLfDI um eine Bewertung aus datenschutzrechtlicher Sicht gebeten.
Der Begriff „Section Control“ – Abschnittskontrolle bezeichnet ein System zur Überwachung von Tempolimits im Straßenverkehr. Die Abschnittskontrolle beruht auf dem an sich simplen Prinzip der Weg-Zeit-Rechnung: Die Fahrzeuge werden am Anfang und am Ende der kontrollierten Etappe erfasst. Anhand der Zeit, die beim Passieren verstrichen ist, kann darauf geschlossen werden, ob die Geschwindigkeitsbegrenzung eingehalten wurde oder nicht. Dies geschieht mit Hilfe von zwei Überkopfkontrollpunkten (Videokameras z. B. an Brücken). Das Fahrzeug wird sowohl beim ersten wie auch beim zweiten Kontrollpunkt fotografiert. Die Identifizierung der Fahrzeuge erfolgt anhand des Kfz-Kennzeichens mittels automatischer Nummernschilderkennung.
Nach § 4 Abs. 1 des Thüringer Datenschutzgesetzes ist die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Eine Einwilligung kommt wegen der Art des Einsatzes im öffentlichen Straßenverkehr nicht in Betracht. Daher bedarf die abschnittsbezogene Geschwindigkeitsmessung zur Verkehrsüberwachung durch Behörden einer Rechtsgrundlage. Auch das Ergebnis des 47. Verkehrsgerichtstags 2009 zu „Section Control“ stützt diese Rechtsauffassung. Hiernach „ist die zwischenzeitliche Datensammlung zweifellos ein Eingriff in die informationelle Selbstbestimmung und bedarf daher eines Gesetzes. Die Regelung muss hinreichend bestimmt, verhältnismäßig und „grundrechtsschonend“ sein. Da es

sich um Gefahrenabwehr handelt, wäre die Ermächtigungsnorm im Polizeirecht der Länder zu schaffen."
Die Bedenken gegen die Zulässigkeit des Verfahrens haben auch auf die Testphase Auswirkungen. Zwar gibt es für derartige Testphasen ein so genanntes „Forschungsprivileg", nach dem eine Datenverarbeitung auch zu Zwecken der wissenschaftlichen Forschung zulässig sein kann, § 20 Abs. 2 Nr. 9 ThürDSG. Dies setzt aber voraus, dass im Ergebnis des Modellversuches ein zulässiges Verfahren durchführbar wäre.
Gegen die Einführung von „Section Control" bestehen aus Sicht des TLfDI folgende Bedenken: Im Gegensatz zur herkömmlichen Geschwindigkeitsüberwachung wird demnach nicht die aktuelle Geschwindigkeit an einem ganz bestimmten Punkt, sondern die Durchschnittsgeschwindigkeit über eine längere Strecke mit einem Anfangs- und einem Endpunkt überwacht. Da an diesem Anfangspunkt nicht bekannt ist, welches Fahrzeug die erlaubte Geschwindigkeit durchschnittlich innerhalb der Messstrecke überschreiten wird, werden alle Fahrzeuge mit dem System erfasst und mindestens bis zum Endmesspunkt elektronisch gespeichert. Somit wird gegen alle die Strecke nutzenden Betroffenen ohne Anfangsverdacht innerhalb des Durchfahrens des Streckenabschnitts ermittelt und es werden deren personenbezogenen Daten für diesen Zeitraum gespeichert. Weiterhin ist darauf hinzuweisen, dass der Fahrzeugführer selbst mit dem Verfahren nicht ermittelt werden kann, weil nur die Kfz-Kennzeichen erfasst werden. Dies ermöglicht nur Rückschlüsse auf den Fahrzeughalter.
Wegen der dargestellten datenschutzrechtlichen Bedenken hat das TMBLV entschieden, dass sich Thüringen nicht an einem Modellversuch „Section Control" beteiligt.

Aus datenschutzrechtlicher Sicht ist die Durchführung eines Verfahrenstests nach dem Forschungsprivileg nur unter der Bedingung denkbar, dass im Ergebnis des Modellversuches ein zulässiges Verfahren durchführbar wäre.

12.5 Unzulässige Übermittlung von Daten durch die Industrie- und Handelskammer (IHK) an den Arbeitgeber

Die Weiterbildung von Beschäftigten wird von den Industrie- und Handelskammern (IHK) gefördert, da man sich hiervon Vorteile

sowohl für die Mitgliedsunternehmen als auch die dort tätigen Beschäftigten verspricht. Im vorliegenden Fall führte die vom Arbeitgeber nicht befürwortete Weiterbildung aber letztlich zur Kündigung eines Beschäftigten. Auslöser hierfür war die „freundschaftliche“ Korrespondenz zwischen einem Beschäftigten der IHK und dem Geschäftsführer desjenigen Betriebs, bei dem der weiterbildungsbeflissene Beschäftigte beschäftigt war. Die IHK informierte den Betrieb von der Teilnahme des Beschäftigten an einem Lehrgang sowie dessen Kurszeiten und den genauen Prüfungszeitpunkt. Die Übermittlung dieser personenbezogenen Daten des Betroffenen erfolgte, obwohl der IHK bekannt war, dass der Betrieb auf Bitte des Betroffenen über die Teilnahme an dem Lehrgang nicht informiert werden sollte. Die IHK versuchte ihr Verhalten vor dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit dem Hinweis auf § 22 Abs. 1 Nr. 2 Thüringer Datenschutzgesetz (ThürDSG) zu rechtfertigen, wonach das Unternehmen ein berechtigtes Interesse an der Kenntnis der Daten gehabt habe, während ein schutzwürdiges Interesse der Beschäftigten am Ausschluss der Übermittlung nicht habe festgestellt werden können. Es wurde auch darauf hingewiesen, dass man bei einem möglichen arbeitsgerichtlichen Verfahren ohnehin verpflichtet gewesen wäre, über die Lehrgangsteilnahme des Beschäftigten Auskunft zu geben. Der TLfDI teilte der IHK mit, dass bei einer sorgfältigen Prüfung der möglichen Konsequenzen für den Betroffenen sein schutzwürdiges Interesse wegen der drohenden Konsequenzen überwogen hätte. Außerdem kann man sich darüber hinaus nicht auf eine Auskunftspflicht vor Gericht berufen, solange ein Verfahren überhaupt nicht anhängig ist. Der TLfDI stellte gegenüber der IHK klar, dass die Datenübermittlung unzulässig war und forderte die Kammer auf, zukünftig bei Datenübermittlungen das schutzwürdige Interesse der Betroffenen mit größerer Sorgfalt zu erkunden. Bitter bleibt der Vorgang trotzdem, da die Feststellung des TLfDI nicht zu einer Rücknahme der Kündigung führte. Der Betrieb nutzte letztlich die Information, auch wenn sie auf unzulässige Weise übermittelt wurde.

Öffentliche Stellen sollten vor einer Übermittlung personenbezogener Daten an private Dritte insbesondere das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung prüfen. Diese Prüfung muss umso intensiver erfolgen, je folgenreicher die Übermittlung für den Betroffenen sein kann.

12.6 Datenschutz in Internetportalen des Deutschen Industrie- und Handelskammertags

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wurde darauf hingewiesen, dass auf den Internetseiten des Deutschen Industrie- und Handelskammertags (DIHK e. V.) ein Sachverständigenportal betrieben wird, wobei die Daten des Sachverständigen von den jeweiligen Industrie- und Handelskammern übermittelt worden seien. Es wurde festgestellt, dass unter der Internetadresse http://svv.ihk.de/content/home/home.ihk ein Portal betrieben wird, in dem man einen Suchbegriff sowie einen Ortsnamen eingeben kann. In der Folge wird man zu den bestehenden Treffern weitergeleitet. Im Impressum der Veröffentlichung ist als Verantwortlicher für den Inhalt der DIHK e. V. genannt. Realisiert wurde die Veröffentlichung ausweislich der Internetseite von der IHK-Gesellschaft für Informationsverarbeitung mbH (IHK-GfI mbH). Offensichtlich übermitteln die Industrie- und Handelskammern Daten der von der IHK öffentlich bestellten und vereidigten Sachverständigen an eine der genannten Stellen, um diese dann im Internet veröffentlichen zu lassen. Dabei handelt es sich um den Namen, Vornamen, akademischen Grad, das Sachgebiet, die Anschrift, sofern gewünscht die private Anschrift, Telefon, Fax und E-Mail-Adresse der Sachverständigen. Zu prüfen war, auf welche Weise die Daten der öffentlich bestellten Sachverständigen an den DIHK e. V. übermittelt wurde und ob es hierfür eine rechtliche Grundlage gab.
Der TLfDI wandte sich mit dieser Frage an die Industrie- und Handelskammern in Thüringen. Die Daten für die Sachverständigenlisten werden von den Industrie- und Handelskammern an die IHK-GfI mbH übermittelt. Mit dieser Gesellschaft besteht ein Vertrag zur Auftragsdatenverarbeitung, wohl aber nicht mit dem DIHK e. V., der nach dem Internetauftritt allerdings als datenschutzrechtlich verantwortliche Stelle verstanden werden muss. Gespräche, um zu einer datenschutzgerechten Lösung des Problems zu kommen, konnten im Berichtszeitraum nicht abgeschlossen werden. Über das Ergebnis wird im nächsten Tätigkeitsbericht berichtet werden.

Die Veröffentlichung von personenbezogenen Daten im Internet bedarf einer rechtlichen Grundlage. Hierbei muss transparent ge-

macht werden, welche die verantwortliche Stelle für die Datenverarbeitung ist.

12.7 Darf eine kommunale Stelle beliebige Daten aus den Datenbanken des amtlichen Vermessungswesens erhalten?

Eine Verwaltungsgemeinschaft wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit mit der Frage, ob die dort gespeicherten Daten aus dem automatisierten Liegenschaftsbuch (ALB) an den Bürgermeister einer der Mitgliedsgemeinden übermittelt werden dürfen.
Wie unter Punkt 5.21 bereits dargestellt wurde, kann nach § 18 Abs. 1 Thüringer Vermessungs- und Geoinformationsgesetz grundsätzlich jede Person oder Stelle die Datenbanken des amtlichen Vermessungswesens einsehen sowie Auskünfte und Ausgaben daraus enthalten. Allerdings steht der Anspruch auf Kenntnisnahme von Namen, Geburtsdaten und Anschriften sowie auf entsprechende Auskünfte und Ausgaben nur Personen und Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten darlegen und soweit überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Für die Bundes-, Landes- und Kommunalbehörden macht die Rechtsvorschrift aber eine Ausnahme: Diese müssen in Erfüllung ihrer Aufgaben kein berechtigtes Interesse darlegen. Für die anfragende Verwaltungsgemeinschaft heißt dies, dass die zur Aufgabenerfüllung der Mitgliedsgemeinde erforderlichen Daten an den Bürgermeister der Mitgliedsgemeinde einschließlich Namen, Geburtsdaten und die Anschriften übermittelt werden dürfen. Im vorliegenden Fall wäre etwa die Übermittlung der Namen, Geburtsdaten und Anschriften aus dem ALB nicht nur der Mitgliedsgemeinde, sondern aus der gesamten Verwaltungsgemeinschaft nicht erforderlich und damit unzulässig gewesen.

Eine Gemeinde darf die Liegenschaftsdaten nur in Erfüllung ihrer Aufgaben verarbeiten und nutzen.

12.8 Digitales Portemonnaie – oder bar?

Seit längerer Zeit beschäftigt die Geldinstitute, dass die Bürger so viel Geld in ihrem Portemonnaie herumtragen. Eine von der Bundesbank herausgegebene „Zahlungsverhaltensstudie 2011“ ergab, dass

die Befragten im Durchschnitt 103 € im Portemonnaie mit sich führen und 60 % der Befragten erst an der Ladenkasse die Entscheidung treffen, mit welchem Zahlungsinstrument (girocard, Kredtikarte oder bar) sie bezahlen wollen. Die Mehrheit zahle dabei lieber bar. Bei der Bezahlung in Cafés, Kneipen und für Fast Food entscheiden sich sogar 97 % für die Barzahlung. Vor diesem Hintergrund suchten die Banken und Sparkassen nach einem innovativen digitalen Zahlungsmittel für Kleinbeträge.

Banken und Sparkassen bieten seit einiger Zeit die Möglichkeit an, dass Kunden auf ihrer Zahlungskarte zusätzlich einen Geldbetrag von ca. 20 bis 200 € speichern können. Die Aufladung erfolgt in der Regel bei der Bank oder am Kassenautomaten. Ist die Karte geladen, können die Kunden durch Hineinstecken der Karte in das Lesegerät bzw. den Automaten des jeweiligen Händlers bezahlen. Diese Zahlungsweise findet man bspw. häufig bei der Nutzung im städtischen Nahverkehr oder an Zigarettenautomaten.

Neu ist der Trend, die Karten zusätzlich mit einem Funk-Chip (Near Field Communikation - NFC) zu versehen, sodass eine schnelle kontaktlose Bezahlung von Beträgen an entsprechenden Lesegeräten möglich ist. NFC basiert auf der radio-frequency identification Technologie (RFID), deren Funktionalität der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit bereits in seinem 6. Tätigkeitsbericht (TB) unter Punkt. 1.12 und im 7. TB unter Punkt 14.3 erläutert hat.

In der Regel werden bei diesen Zahlungsvorgängen eine eindeutige Identifikationsnummer, das Datum, die Uhrzeit, der Betrag und die Händlernummer unverschlüsselt gespeichert und können durch den Nutzer mit entsprechenden Lesegeräten eingesehen bzw. geprüft werden. Datenschutzrechtlich bedenklich ist dabei, dass auch unbefugte Dritte Zahlungsvorgänge kontaktlos auslösen oder auslesen könnten. Aber nicht nur Karten mit dieser NFC-Funktion sind auf dem Markt, sondern auch Mobilfunkhersteller haben den Trend des kontaktlosen Bezahlens für sich entdeckt und liefern zunehmend Smartphones mit NFC aus.

Die Europäische Kommission fordert von den Betreibern von RFID-Systemen die Durchführung von sogenannten Datenschutzfolgeabschätzungen (Privacy Impact Assessment – PIA). Die Arbeitsgruppe (AG) Kreditwirtschaft und der Arbeitskreis (AK) Technik der Datenschutzkonferenz des Bundes und der Länder nahmen dies zum Anlass, Vertreter der deutschen Kreditwirtschaft einzuladen und sich

die PIA‘s für verschiedene Verfahren der kontaktlosen Anwendung der Geldkarte erläutern zu lassen. Im Ergebnis wurde deutlich, dass es einer generellen Handreichung „Anforderungen an ein PIA aus Sicht einer Datenschutzaufsichtsinstanz“ bedarf, an der sich neben der Kreditwirtschaft auch alle anderen RFID-Betreiber orientieren können. Diese Handreichung wird derzeit vom AK Technik und der AG Kreditwirtschaft erarbeitet.

Das kontaktlose Bezahlen mit NFC-Funktion mit Geld- Kreditkarte oder Handy ist für den Anwender sehr praktisch. Da es aber datenschutzrechtliche Risiken birgt, müssen hinreichende Datenschutzfolgeabschätzungen (sog. PIA) durchgeführt und die dort vereinbarten Anforderungen beachtet werden.

12.9 Bargeldlose Bezahlfunktion nur mit ausreichender Information der Kunden

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wurde bekannt, dass die Sparkasse Mittelthüringen seit geraumer Zeit für die neue Bezahlfunktion für Kleinbeträge „girogo“ mittels der SparkassenCard wirbt.
Mit dem Deutschen Sparkassen- und Giroverband (DSGV) besteht Einvernehmen darüber, dass auf die Bezahlfunktion „girogo“ § 6 c Bundesdatenschutzgesetz (BDSG) anzuwenden ist. Das bedeutet, dass die Kunden in umfassender Weise aufzuklären sind. Dies gilt insbesondere in Bezug auf die Möglichkeit der Wahrnehmung ihrer Rechte. Auch müssen die Sparkassen dafür sorgen, dass Geräte oder Einrichtungen unentgeltlich zur Verfügung gestellt werden, an denen ihre Kunden das datenschutzrechtliche Auskunftsrecht wahrnehmen können. Der DSGV hat hierzu ein entsprechendes „Datenschutzmerkblatt girogo“ herausgegeben. Da nicht feststellbar war, wie die Sparkasse Mittelthüringen diesen Pflichten nachkommt, wurde sie hierzu um Stellungnahme gebeten.
Die Sparkasse Mittelthüringen teilte mit, dass das „Datenschutzmerkblatt girogo“ des DSGV zur Information von Karteninhabern bezüglich der Datenschutzaspekte von „girogo“ eingesetzt wird. Die Personen, die Kunden der Sparkasse mit einer EC-Karte sind, wurden über die Funktion „girogo“ mittels Kontoauszugsdrucker-Mitteilung informiert – mit der Möglichkeit, den geänderten Bedingungen zu widersprechen. Auf weitere Informationen auf der Home-

page sowie auf die Möglichkeit einer persönlichen Beratung in der Geschäftsstelle wurde hier ebenfalls verwiesen. Diese Vorgehensweise sei mit dem Sparkassen- und Giroverband Hessen-Thüringen abgestimmt. Im Rahmen von Kartenneubestellungen wird das „Datenschutzmerkblatt girogo“ an den Kunden ausgeben.
Hierzu teilte der TLfDI der Sparkasse Mittelthüringen mit, dass die Information mittels einer Kontoauszugsdrucker-Mitteilung nicht den gesetzlichen Anforderungen des § 6 c Abs. 1 Nr. 3 BDSG entspricht. Es wurde um Stellungnahme gebeten, warum an die Bestandskunden das „Datenschutzmerkblatt girogo“ nicht ausgehändigt wird.
Zwischenzeitlich haben die Arbeitskreise Technik und Kreditwirtschaft der Datenschutzaufsichtsbehörden des Bundes und der Länder über dieses Thema beraten. Durch den federführend zuständigen Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen wurde die abschließende Bewertung der Arbeitsgruppe Kreditwirtschaft zu Near Field Communication (NFC) Geldkarte „girogo“ an die Deutsche Kreditwirtschaft Sparkassen- und Giroverband mitgeteilt. Im Zusammenhang mit den Informationspflichten wird in diesem Schreiben dargelegt, dass die Karten ausgebenden Institute verpflichtet sind, sämtlichen Kunden die ausführlichen Hinweise zum Einsatz der SparkassenCard mit „girogo“ zugänglich zu machen haben.
Die Sparkasse Mittelthüringen wurde aufgefordert, ihren Informationspflichten nach § 6 c BDSG nachzukommen und allen Kunden die ausführlichen Hinweise des „Datenschutzmerkblatt girogo“ des Deutschen Sparkassen- und Giroverbands zum Einsatz der SparkassenCard mit „girogo“ zugänglich zu machen.

Bei der Einführung der bargeldlosen Bezahlfunktion der SparkassenCard „girogo“ sind alle Kunden über die Möglichkeit zur Wahrnehmung der Betroffenenrechte nach § 6 c Abs. 1 Nr. 3 BDSG mit dem „Datenschutzmerkblatt girogo“ des Deutschen Sparkassen- und Giroverbands zu unterrichten.

12.10 Meldungen zu Datenpannen

Soweit öffentliche Stellen in Thüringen am Wettbewerb teilnehmen, gelten für sie gemäß § 26 Thüringer Datenschutzgesetz die Bestimmungen des Bundesdatenschutzgesetzes (BDSG), mit Ausnahme des zweiten Abschnitts und des § 38. Insofern gilt der nachfolgend aus-

zugsweise sinngemäß wiedergegebene § 42 a BDSG auch für öffentlich-rechtliche Geldinstitute.
Stellt eine verantwortliche Stelle fest, dass bei ihr gespeicherte personenbezogene Daten im Sinne von § 42 a Satz 1 Nr. 1 bis Nr. 4 BDSG unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen der Betroffenen, hat sie dies unverzüglich der zuständigen Aufsichtsbehörde – in Thüringen also dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) – sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung des Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeigneten Maßnahme veröffentlicht werden müssen. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten.

Im Berichtszeitraum wurden dem TLfDI von öffentlich-rechtlichen Geldinstituten fünf Datenpannen gemeldet. Zwei Mal wurde mittels illegaler technischer Vorrichtungen für einen Kreditkartenbetrug, einer so genannten Skimming-Attacke, an Geldautomaten eine große Anzahl von Kundendaten (Kontonummer, Bankleitzahl, PIN) „ausgelesen“ – das Thema Skimming wird in einem gesonderten Beitrag

dieses Tätigkeitsberichts behandelt (siehe Punkt 12.11). In einem anderen Fall wurden Tonkassetten aus einem Gebäude und in einem weiteren Fall Akten mit Kundendaten aus einem Auto gestohlen. Einmal gingen Einschreibesendungen mit personenbezogenen Daten von Kunden beim Versand verloren. In allen fünf Fällen erfüllten die öffentlich-rechtlichen Stellen die Anforderungen aus § 42 a BDSG.

Soweit öffentliche Stellen am Wettbewerb teilnehmen, haben sie Datenpannen nach den Vorgaben des § 42a BDSG der zuständigen Aufsichtsbehörde und den Betroffenen mitzuteilen.

12.11 Skimming-Attacken sind zu melden!

Im Zusammenhang mit den bundesweit aufgetretenen Skimming-Attacken – über zwei derartige Fälle wurde in dem Beitrag dieses Tätigkeitsbericht zu den Meldepflichten der von Datenpannen betroffenen öffentlichen Wettbewerbsunternehmen berichtet (siehe Punkt 12.10) – stellt sich die Frage, ob Skimming-Attacken nach § 42 a Bundesdatenschutzgesetz (BDSG) zu melden sind.
Skimming ist eine Form von Betrug, bei der mittels illegaler technischer Vorrichtungen, die heimlich an Geldautomaten angebracht wurden, versucht wird, eine möglichst große Anzahl von Kundendaten (Kontonummer, Bankleitzahl, PIN) von Bankkunden unbemerkt „auszulesen“.
Vereinzelt wird die Auffassung geäußert, dass bei Skimming-Attacken, in denen aufgrund des bestehenden Versicherungsschutzes des Kreditinstitutes kein materieller Schaden entstanden ist, keine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen des Betroffenen (Kunden) droht und daher die Voraussetzungen der Meldepflicht nach § 42 a BDSG nicht gegeben sind.
Demgegenüber vertritt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) die Auffassung, dass auch bei einem bestehenden Versicherungsschutz im Falle von Skimming-Attacken die Voraussetzungen des § 42 a BDSG erfüllt sind. Nach herrschender Meinung (vgl. Simitis, BDSG, 7. Auflage, § 42 a, Rn. 9) zählen zu den schwerwiegenden Beeinträchtigungen der Rechte oder schutzwürdigen Interessen der Betroffenen neben materiellen Schäden auch (nichtversicherte) soziale Nachteile einschließlich Identitätsbetrug. Daher sollte von der ver-

antwortlichen Stelle kein zu enger Maßstab an die Gefahrenprognose anlegt und Skimming-Fälle auch bei bestehendem Versicherungsschutz nach § 42 a BDSG immer angezeigt werden.

Bei einem Abgreifen von Daten am Geldautomaten mittels Skimming liegen auch bei einem bestehenden Versicherungsschutz die Voraussetzungen des § 42 a BDSG vor.
Daher müssen Skimming-Fälle auch bei bestehendem Versicherungsschutz angezeigt werden.

13 Bildung, Wissenschaft und Forschung

Lehrerin zeigt Schülern etwas am Laptop
© contrastwerkstatt – Fotolia.com

13.1 AK Datenschutz und Bildung/ AG Datenschutz und Schule

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gründet Arbeitskreise, die sich mit speziellen datenschutzrechtlichen Themen beschäftigen. So auch den Arbeitskreis Datenschutz und Bildung, der sich weniger mit konkreten datenschutzrechtlichen Problemen als vielmehr mit der Frage beschäftigt, auf welchen Wegen Medienkompetenz und Datenschutzbewusstsein in die Bildungslandschaft getragen werden kann. Die Arbeitskreise wiederum gründen sogenannte Arbeitsgruppen, die sich mit spezielleren datenschutzrechtlichen Problematiken auseinander setzen. So hat der erwähnte Arbeitskreis Datenschutz und Bildung die Arbeitsgruppe Datenschutz und Schule gegründet, die konkrete datenschutzrechtliche Fragestellungen aus dem schulischen Bereich bearbeitet. Themen waren bisher unter anderem der Umgang mit sozialen Medien im Schulbereich, eLearning, die Verarbeitung von Schülerdaten auf privaten Endgeräten der Lehrkräfte und die Übermittlung von Schülerdaten per E-Mail. Da dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) sowohl die Lösung konkreter schulischer Datenschutzprobleme als auch die Vermittlung von Medienkompetenz in Schulen und auch Hochschulen ein besonderes Anliegen ist, wurde ihm 2013 die Leitung der Arbeitsgruppe Datenschutz und Schule übertragen. Diese Arbeitsgruppe tagt ein bis zweimal jährlich in Erfurt. Aufgrund einer guten Kooperation mit dem Thüringer Ministerium für Bildung Wissenschaft und Kultur, die unter anderem eine Abordnung eines Lehrers zur Behörde des TLfDI hervorbrachte, entstand unter den beteiligten Datenschutzbeauftragten der Länder offenbar der Eindruck, der TLfDI sei auch für den Vorsitz des Arbeitskreises Datenschutz und Bildung geeignet. Daher hat der rheinland-pfälzische Datenschutz-

beauftragte Edgar Wagner den Staffelstab an den TLfDI im Dezember 2013 übergeben. Der TLfDI betrachtet dies als große Ehre und Verpflichtung, ein Niveau anzustreben, das Kollege Wagner in Rheinland-Pfalz längst erreicht hat.

Datenschutzbewusstsein und Medienkompetenz fallen nicht vom Himmel. Die Datenschutzbeauftragten machen sich Gedanken, auf welchen Wegen diese Werte vermittelt werden können – Schülern, Lehrern, Eltern, aber auch Lehramtsstudenten. Daneben gilt es, konkrete Datenschutzprobleme im Schul- und Hochschulbereich zu lösen. Kein leichter Weg. Unterstützung seitens des Thüringer Ministeriums für Bildung, Wissenschaft und Kultur ist von Nöten – und zugesagt.

13.2 Behördliche Datenschutzbeauftragte an Schulen – ein Fall für die Nachhilfe

Bereits im letzten Tätigkeitsbericht (9. Tätigkeitsbericht unter Punkt 13.2) hatte der Thüringer Landesbeauftragte für den Datenschutz (TLfD) darüber informiert, dass aufgrund einer Änderung des § 10 a Abs. 6 Thüringer Datenschutzgesetz (ThürDSG) die Aufsichtsbehörde für die staatlichen Schulen einen ihrer Beschäftigten als Beauftragten für den Datenschutz (bDSB) bestellen kann. Hiervon hat das Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) auch umfassend Gebrauch gemacht und in jedem staatlichen Schulamt einen bDSB für alle staatlichen Schulen im jeweiligen Zuständigkeitsbereich bestimmt. Dies bedeutet konkret, dass nach der erfolgten Reduzierung der staatlichen Schulämter von ehemals elf auf nunmehr fünf, jeweils ein bDSB für alle Schulen in seinem Schulamtsbereich zuständig ist. Der TLfDI lud alle bDSB zu einem Gesprächstermin in seine Behörde ein. Zweck der Kontaktaufnahme war es, die schulischen bDSB miteinander ins Gespräch zu bringen und zu prüfen, ob sie gemäß § 10 a Abs. 1 Satz 5 ThürDSG über die notwendigen Fachkenntnisse verfügen und in keinem unüberwindbaren Interessenkonflikt mit sonstigen dienstlichen Aufgaben stehen. Aufgrund terminlicher Schwierigkeiten fanden zwei Termine statt, an denen jeweils auch ein Vertreter des TMBWK teilnahm.
In dem Termin erklärten die Vertreter der staatlichen Schulämter übereinstimmend, dass sie schriftlich für die Übernahme der Aufga-

ben des behördlichen Datenschutzbeauftragten für die staatlichen Schulen bestellt worden seien, ihnen für die Wahrnehmung dieser Aufgabe aber keine Arbeitszeit eingeräumt worden sei. Sie müssten vielmehr weiterhin die bisher bestehenden Aufgaben wahrnehmen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wies gegenüber dem TMBWK darauf hin, dass nach § 10 a Abs. 3 ThürDSG die datenverarbeitende Stelle den Beauftragten für den Datenschutz zur Erfüllung seiner Aufgaben in geeigneter Weise zu unterstützen hat. Hierzu gehört auch, dass dem behördlichen Beauftragten für den Datenschutz ausreichend Arbeitszeit zur Verfügung gestellt wird, damit dieser seine Aufgabe sinnvoll erfüllen kann. Aufgrund der Zuständigkeit der bDSB nach § 10 a Abs. 6 ThürDSG für jeweils mindestens 100 Schulen, können die bDSB ihre bisherigen Aufgaben nicht unverändert beibehalten. Eine ernsthafte Aufgabenerfüllung ist nur möglich, wenn mindestens 50 % der Arbeitszeit für diese Aufgabe zur Verfügung steht. Das TMBWK wurde gebeten, darauf hinzuwirken, dass die staatlichen Schulämter den bDSB durch Umstrukturierung der Aufgaben das erforderliche Zeitkontingent zur Verfügung stellen.

Nach § 10 a Abs. 1 Satz 3 ThürDSG darf zum bDSB nur bestellt werden, wer die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit hat. Dies war nach der bisherigen Einschätzung bei keinem der bestellten bDSB der Fall. Der TLfDI regte daher an, über das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien eine entsprechende Schulung der behördlichen Datenschutzbeauftragten zu initiieren.

Nach § 10 a Abs. 2 Satz 3 ThürDSG hat der behördliche Datenschutzbeauftragte die Aufgabe, bei der Freigabe automatisierter Verfahren nach § 34 Abs. 2 ThürDSG mitzuwirken, das Verfahrensverzeichnis nach § 10 ThürDSG zu führen, die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen und die bei der Verarbeitung oder Nutzung personenbezogener Daten tätigen Personen zu den einschlägigen datenschutzrechtlichen Vorschriften zu beraten. Das Gespräch mit den bDSB hat ergeben, dass an den wenigsten staatlichen Schulen Freigaben der entsprechenden Schulverwaltungssoftware erfolgt sind, die Schulen in der Regel keine Verfahrensverzeichnisse nach § 10 ThürDSG führen und auch Sicherheitskonzepte an den Schulen nicht existieren. Nach § 9 ThürDSG haben die öffentlichen Stellen, die selbst oder im Auf-

trag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind die Ausführung der datenschutzrechtlichen Bestimmungen zu gewährleisten. Die zu treffenden technischen und organisatorischen Maßnahmen sind auf Grundlage eines Sicherheitskonzepts zu ermitteln, § 9 Abs. 2 ThürDSG. Damit entspricht der Zustand an den staatlichen Schulen nicht den gesetzlichen Vorgaben des ThürDSG. Es sollte daher ein Fahrplan entwickelt werden, nach dem die gesetzlichen Anforderungen durch die bDSB abgearbeitet werden. Das TMBWK wurde auch gebeten, alle staatlichen Schulen in geeigneter Form darüber zu informieren, dass die bDSB der staatlichen Schulämter als Ansprechpartner und in beratender Funktion für die datenschutzrechtlichen Probleme an staatlichen Schulen zur Verfügung stehen.

Das TMBWK teilte daraufhin mit, dass die Einräumung eines angemessenen Zeitkontingents für die Erfüllung der Aufgaben als Datenschutzbeauftragte unter der derzeit gegebenen Personalsituation eine Herausforderung darstelle. Die Datenschutzbeauftragten seien zu den vom Thüringer Innenministerium angebotenen und im September 2013 stattfindenden Fortbildungslehrgang angelmeldet worden.

Uneinigkeit besteht des Weiteren im Hinblick auf die Zuständigkeit für die notwendige Erstellung der Verfahrensverzeichnisse und die datenschutzrechtlichen Freigaben.

Nach Auffassung des TMBWK sind hierfür die Landkreise und kreisfreien Städten als Träger der staatlichen Schulen nach § 13 Abs. 2 Thüringer Schulgesetz verantwortlich. Diese Ansicht teilt der TLfDI nicht. Die Schulträger haben gemäß § 3 Abs. 2 Thüringer Schulfinanzierungsgesetz den Sachaufwand und nach Absatz 3 den Aufwand für das Verwaltungs- und Hilfspersonal tragen. Man kann dies so zusammenfassen, dass die Schulträger die Infrastruktur zur „Durchführung von Schule“ finanzieren. Nach § 2 des Gesetzes über die Schulaufsicht hingegen hat das Land die Aufsicht über das gesamte Schulwesen. Diese Aufsicht umfasst die Gesamtheit der staatlichen Aufgaben zur inhaltlichen, organisatorischen und planerischen Gestaltung. Hierfür sprechen bereits die zahlreichen Bestimmungen im Thüringer Schulgesetz über die Befugnisse und Aufgaben des Schulleiters, etwa die Verantwortlichkeit für Schulbetrieb und Unterricht oder sein Weisungsrecht gegenüber den Lehrern. Auch stehen die Schüler, Eltern und Lehrer im Hinblick auf die Schule in einem Rechtsverhältnis zum Land. Aus daten-

schutzrechtlicher Sicht ist damit die Daten verarbeitende Stelle im Sinne von § 3 Abs. 5 ThürDSG nicht der Schulträger, sondern die Schule selbst bzw. das jeweils zuständige staatliche Schulamt als Aufsichtsbehörde. Der TLfDI befindet sich noch im Abstimmungsprozess mit dem TMBWK und wird sich weiter dafür einsetzen, dass an den Schulen in Thüringen datenschutzgerechte Zustände hergestellt werden.

Nach dem Gesetz hat die datenverarbeitende Stelle den Beauftragten für den Datenschutz zur Erfüllung seiner Aufgaben in geeigneter Weise zu unterstützen. Hierzu gehört auch, dass ihm das für seine Aufgabenerfüllung erforderliche Zeitkontingent zur Verfügung gestellt wird.

13.3 Modellprojekt „Grundschulen“ – Wer zahlt, will wissen wofür

Die Thüringer Grundschulen sollen auf Basis von Erprobungsmodellen nach § 12 des Thüringer Schulgesetzes weiterentwickelt werden. Hierfür hat die Landesregierung ein Rahmenkonzept entwickelt, das durch Einzelvereinbarungen mit den Schulträgern umgesetzt werden soll. Dabei sollen die Kooperationen zur Gestaltung von Betreuung, Erziehung und Bildung in gemeinsamer Verantwortung von Land und Kommune gestärkt werden und zu einer höheren Bildungsqualität in der Region führen. Die familienergänzende und unterrichtsunterstützende Betreuung der Grundschüler wird bisher in gemeinsamer Verantwortung von Land und kommunalen Schulträgern allerdings grundsätzlich mit getrennten Zuständigkeitsbereichen wahrgenommen. Das Land hat hierbei die alleinige Verantwortung für das Personal und die Schulträger für den jeweiligen Sachaufwand. Soweit öffentliche Schulträger an der Erprobung des Modellvorhabens der offenen Ganztagesschule teilnehmen, unterliegen die Erzieher und Erzieherinnen hinsichtlich der Erbringung ihrer Arbeitsleistung der Aufsicht des kommunalen Schulträgers, während das Land weiterhin die Finanzierung des Personals sicherstellt. Der Modellversuch sollte zunächst am 31. Dezember 2012 enden, wurde dann aber bis zum 31. Juli 2016 verlängert.
Da das Land das Erziehungspersonal finanziert, müssen die Schulträger nachweisen, welche Kosten für wen und wann tatsächlich entstanden sind. In diesem Zusammenhang wandte sich ein Schul-

träger an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Frage, wie oft und mit welchem Datenumfang er diese Nachweise an das für die Prüfung zuständige Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) übermitteln müsse. In einer Gesprächsrunde zur Problematik legte das TMBWK dar, dass zwar zukünftig eine pauschale Finanzierung des Erziehungspersonals geplant, für die Feststellung des genauen Finanzbedarfs aber während des Modellversuchs zunächst eine „Spitzabrechnung“ erforderlich sei. Das Land habe nicht nur die Kosten im Blick zu behalten, sondern müsse auch darauf achten, dass der Schulträger ausreichend Erziehungspersonal mit einem erforderlichen Zeitbudget den Schulen zur Verfügung stelle. Weiterhin kritisierte der TLfDI den nicht ausreichend geregelten Umgang mit den personenbezogenen Daten des Erziehungspersonals in der Vereinbarung mit dem Schulträger zur Durchführung des Modellversuchs. Das TMBWK räumte dieses Versäumnis ein, hielt aber die Änderung der Vereinbarung angesichts des baldigen Endes des Modellversuchs zum 31. Dezember 2012 für nicht mehr durchführbar. Weiterhin forderte der TLfDI die Löschung der Zwischennachweise nach Abschluss der Prüfung sowohl im TMBWK als auch in den Staatlichen Schulämtern, da diese Unterlagen bei den Schulträgern vorhanden sind und somit eine Prüfung der Zahlungsvorgänge durch den Landesrechnungshof gewährleistet ist.
Da zwischenzeitlich vom TMBWK die Verlängerung des Modellversuchs beschlossen wurde, besteht zwar weiterhin die Pflicht der Schulträger, die Nachweise quartalsweise zur Prüfung an das TMBWK zu übermitteln, der TLfDI konnte aber bewirken, dass die Vereinbarung und die Zwischennachweismuster überarbeitet wurden, sodass aus datenschutzrechtlicher Sicht hiergegen keine durchgreifenden Bedenken mehr bestehen. Nach Auskunft des TMBWK habe es auch seitens der teilnehmenden Schulträger keine Kritik mehr an dem Verfahren gegeben.

Personaldaten des Erziehungspersonals dürfen vom TMBWK zur Nachweisführung nur im unbedingt erforderlichen Umfang erhoben werden.

13.4 Der Datenschutz geht auf die Schule zu

Im digitalen Zeitalter ist Datenschutz in aller Munde, aber leider nicht im Bewusstsein aller. Dabei lebt das Grundrecht auf informationelle Selbstbestimmung auch vom Wissen und Handeln jedes Einzelnen von uns im Umgang mit seinen persönlichen Daten. Das klingt auf den ersten Blick einleuchtend. Im alltäglichen Umgang mit Email, Facebook und Co. liegen aber Gedanken darüber, was aus dem wird, was ich da von mir ins Netz gestellt habe, eher fern. Denn: „Ich habe ja nichts zu verbergen …".
Aber nicht erst seit PRISM ist klar, dass Datensammler – ob staatlich oder privat – allgegenwärtig sind und uns möglichst schattenfrei durchleuchten wollen. Privatsphäre ist ein hohes Gut. Gerade die Sensibilisierung unserer Kinder und Jugendlichen für diese Problematik sollte uns nicht gleichgültig sein. Sie sind es, die die Vorteile neuer Medien besonders intensiv ausschöpfen und dabei oft unbewusst und ungewollt Datenspuren hinterlassen. Hier müssen professionelle Datenschützer und Pädagogen gemeinsam Aufklärung anbieten und persönliche Handlungskompetenz bei den Schülerinnen und Schülern entwickeln helfen. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sieht sich in einer Handlungslinie mit den Kultusministern der Länder, die in ihrer Erklärung „Medienbildung in der Schule" auf der Kultusministerkonferenz 2012 betonten: *„Vor allem auf den Gebieten Datenschutz, Jugendschutz und Persönlichkeitsrecht, Urheber- und Lizenzrecht müssen Schülerinnen und Schüler, Lehrkräfte, Schulleitungen und Eltern sensibilisiert und unterstützt werden."* [1] Der TLfDI hat deshalb im Berichtszeitraum den Kontakt zum Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK) aufgenommen und wird von dort in der Weise unterstützt, dass ein Lehrer für den Zeitraum von zwei Jahren beim TLfDI tätig sein kann. Er wird die Schnittstelle zwischen dem TLfDI, den Schülerinnen und Schülern sowie den Lehrerinnen und Lehrern sein. Dort wird ab Klassenstufe 5 ein Kurs Medienkunde unterrichtet, in dem auch ein Lernbereich „Recht, Datensicherheit und Jugendmedienschutz" verankert ist. Der Kurs wird fächerintegrierend umgesetzt, das heißt im Rahmen der

[1] „Medienbildung in der Schule", Beschluss der Kultusministerkonferenz vom 8. März 2012

Unterrichtsfächer laut Stundentafel (Deutsch, Mathematik, Sozialkunde, Geschichte, …). Die Details zur Umsetzung legt die jeweilige Schule fest. Die Pädagogen sind für diese Unterrichtsfächer im Fächerkanon des jeweiligen Bildungsgangs ausgebildet, in der Regel aber nicht speziell für ein „Fach Medienkunde“. Insoweit besteht Unterstützungsbedarf durch medienpädagogische Fortbildungen, Medienempfehlungen zur Kursplanumsetzung sowie die Bereitstellung neuer Unterrichtsmodule. Besonders zum Bereich Datenschutz und Datensicherheit wurde dieser Bedarf gegenüber dem TLfDI bei seinen Schulbesuchen von Schülerinnen und Schülern und Lehrerinnen und Lehrern artikuliert. Hier gilt es für den TLfDI, in Umsetzung seines Beratungsauftrages nach § 40 Abs. 7 Thüringer Datenschutzgesetz tätig zu werden. Mit Hilfe des abgeordneten Lehrers wird es gelingen, vorhandene Unterrichtsmittelquellen zu den Inhalten des Lernbereiches „Recht, Datensicherheit, …“ nutzerfreundlich aufzubereiten, moderne Kommunikationswege für den Informationsaustausch zwischen Lehrern und TLfDI zu entwickeln sowie Unterrichtsmaterialien zu datenschutzrelevanten Fragen neu zu erstellen.

Erfreulicherweise sind im Internet heute schon Medien zum Thema Datenschutz und Datensicherheit eingestellt, die sich gut im Unterricht verwenden lassen. Die Anzahl der Quellen im deutschsprachigen Raum ist ebenso umfangreich wie vielfältig. Im Berichtszeitraum wurde beim TLfDI zunächst eine Datenbank entwickelt, die solche Unterrichtsmedien (Videos, Audiodateien, Broschüren, Beschreibung von Unterrichtsprojekten, etc.) aufnimmt und verlinkt. Sie werden durch einige Metainformationen für den Lehrer ergänzt. Jedem Mediendatensatz werden Schlagworte zugeordnet, die den Lehrern an den Schulen eine zielgerichtete Suche ermöglichen sollen. Ein Klick auf den eingefügten Link führt zum betreffenden Medienangebot im Internet. Die Datenbank wird inhaltlich und funktional ständig weiterentwickelt. Es ist Anspruch des TLfDI, für die Lehrkräfte in Thüringen ein praktikables Werkzeug für eine effiziente Vorbereitung des Medienkundeunterrichts anzubieten, mit dem die im Lernbereich „Recht, Datensicherheit und Jugendmedienschutz“ festgelegten Kompetenzziele der Schüler erreichbar sind. Die Datenbank wird demnächst zum Download sowie als webbasierte Variante auf der Internetseite des TLfDI verfügbar sein.

Parallel dazu werden im Rahmen der Kooperation zwischen dem TLfDI und dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) einige Unterrichtsmedien durch

die Gruppe der Medienkundefachberater mit Schülern erprobt werden. Bei besonderer Eignung und nach Klärung der Nutzungsrechte werden diese Medien dann in die Mediathek des Thüringer Schulportals eingestellt und kostenfrei für Thüringer Lehrkräfte abrufbar sein.
Schließlich ist geplant, das vorhandene Unterrichtsmittelspektrum durch ein eigenes Produkt des TLfDI zu bereichern. Nach derzeitigem Planungsstand wird eine Unterrichtseinheit zum Thema Videoüberwachung entstehen, die in der Klassenstufe 9/10 der Gymnasien zu Einsatz kommen kann. Darin eingeschlossen sind Entwicklung bzw. Bereitstellung der notwendigen Unterrichtsmaterialien wie Videosequenzen, Arbeitsblätter, Gesetzestexte usw. sowie Hintergrundmaterialien für die individuelle Unterrichtsvorbereitung des Lehrers. Hier wird also ein Paket aus mehreren Komponenten entstehen.
Auf den oben angesprochenen Fortbildungsbedarf reagiert der TLfDI zudem durch Veranstaltungsangebote für Lehrerinnen und Lehrer an Thüringer Schulen. Dabei ist irrelevant, ob diese Pädagogen aus staatlichen Schulen oder Schulen in freier Trägerschaft kommen. Im Berichtszeitraum wurden zwei Fortbildungen mit unterschiedlichem Schwerpunkt („Datenschutz im Schulalltag“ und „Sicherer Datentransfer durch Verschlüsselung“) durch den TLfDI angeregt und gemeinsam mit dem ThILLM konzipiert. Sie werden im April und Oktober 2014 stattfinden.

Der TLfDI kooperiert mit dem TMBWK: Ein Lehrer wurde ab 1. August 2013 für den Zeitraum von zwei Jahren zum TLfDI abgeordnet. Auch mit seiner Hilfe werden den Thüringer Schülerinnen und Schülern und Lehrerinnen und Lehrern bei der Sensibilisierung und Kompetenzentwicklung zu Fragen des Datenschutzes und der Datensicherheit nach Evaluierung seitens der Schülerinnen und Schüler geeignete Instrumente bereitgestellt.

13.5 Vertretungspläne für die Welt: Anforderungen an die Veröffentlichung von Vertretungsplänen im Internet durch Schulen

Immer wieder wenden sich Lehrkräfte an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Anfrage, ob die Veröffentlichung von Vertretungsplänen unter Nennung der Namen der Lehrkräfte und teilweise weiterer

Daten im Internet aus datenschutzrechtlicher Sicht zulässig ist. Der TLfDI geht davon aus, dass zwar eine solche Vertretungsliste im Schulgebäude selbst zur Aufgabenerfüllung der Schule ausgehängt werden darf, eine Erforderlichkeit für eine jedermann zugängliche Internetveröffentlichung aber nicht gegeben ist. So kann weltweit verfolgt werden, welche Lehrer wie oft für den Unterricht nicht zur Verfügung stehen. Eine namentliche Veröffentlichung von Lehrkräften im Internet stellt eine Übermittlung personenbezogener Daten an nicht näher bekannte private Stellen außerhalb der Schulöffentlichkeit dar. Dies ist nur unter den Voraussetzungen der §§ 21, 22 Thüringer Datenschutzgesetz (ThürDSG) zulässig, die aber hier nicht vorliegen. Insbesondere ist die Veröffentlichung im Internet nicht erforderlich, um schulische Aufgaben zu erfüllen. Wenn z. B. am nächsten Tag Stunden ausfallen, reicht die Information über die betroffenen Stunden in der jeweiligen Klasse. Wenn eine Stunde vertreten wird, so genügt der Hinweis darauf, welches Fach stattdessen stattfindet. Betroffene Lehrer können von der Schule direkt über eine Vertretungssituation informiert werden. Einige Schulen kommen auf die Idee, bei der Lehrerschaft um eine Einwilligung in die Internet-Übermittlung ihrer Namen zu ersuchen, da die zweifelsfreie Einwilligung des Betroffenen nach § 23 Abs. 2 Nr. 1 ThürDSG eine Übermittlung personenbezogener Daten grundsätzlich erlaubt. Gegen die Einwilligungslösung sprechen jedoch zwei Aspekte: Zum einen ist eine Einwilligung nach § 4 Abs. 2 ThürDSG die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen. Aufgrund des Beschäftigungsverhältnisses der Betroffenen mit der Daten verarbeitenden Stelle besteht ein Abhängigkeitsverhältnis, das eine Freiwilligkeit der abgegebenen Einwilligung zweifelhaft erscheinen lässt. Zum anderen ist im Falle einer Einwilligung die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dies zur Erfüllung anerkannter Zwecke erforderlich ist, wozu auch die Erforderlichkeit der Datenübermittlung zur Aufgabenerfüllung der Schule zählt (§ 4 Abs. 1 Satz 2 ThürDSG), welche hingegen – wie dargestellt – nicht gegeben ist. Der TLfDI wandte sich in der Sache an das TMBWK mit der Bitte den nachgeordneten Bereich nochmals ausdrücklich auf die gegebene Rechtslage hinzuweisen, was auch erfolgte.

Die Veröffentlichung von namentlichen Vertretungsplänen durch Schulen im Internet ist nicht erforderlich und damit nicht zulässig. Dies gilt auch bei einer vorherigen Einholung von Einwilligungen bei den Lehrkräften. Gegen eine Veröffentlichung von Vertretungslisten durch Aushang im Schulgebäude selbst, bestehen keine datenschutzrechtlichen Bedenken.

13.6 Toilettenszenen: Videogaga 12

Besorgte Eltern wandten sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilten mit, dass in der Staatlichen Grundschule Gera auf der Mädchentoilette Videokameras installiert sind. Sie baten den TLfDI, sich dieser Angelegenheit anzunehmen. Noch am gleichen Tag wurde Kontakt mit der Schulleitung dieser Schule aufgenommen und angefragt, ob in der dortigen Mädchentoilette Videokameras installiert worden seien. Die Schulleiterin teilte mit, dass man sich wegen Beschädigungen, Verschmutzungen, Toilettenpapierverbrauch etc. dazu entschlossen hätte, Kameraattrappen im Vorraum der Mädchentoilette zu installieren.
Aus datenschutzrechtlicher Sicht unterliegt dieser Einsatz von Videokameraattrappen den gleichen Voraussetzungen wie der Einsatz von „echten“ Videokameras. Zwar findet objektiv gesehen keine Verarbeitung personenbezogener Daten statt, allerdings weiß das der Betroffene nicht. Es liegt damit eine mit einer funktionstüchtigen Kamera vergleichbare Beeinträchtigung des Grundrechts der informationellen Selbstbestimmung des Betroffenen vor. Der Einsatz einer Kameraattrappe unterliegt somit grundsätzlich den gleichen Voraussetzungen wie der Einsatz echter Kameras. Die Videoüberwachung von höchstpersönlichen Bereichen der Privat- und Intimsphäre, z. B. Toiletten, Umkleidekabinen, Duschen, Saunas, ärztlichen Behandlungsräumen etc. ist generell als unverhältnismäßig und damit als unzulässig anzusehen. Das schutzwürdige Interesse des Betroffenen überwiegt hier stets. Weiterhin hat das Thüringer Ministerium für Bildung, Wissenschaft und Kultur als zuständige Aufsichtsbehörde den Einsatz von Videotechnik in Schulen ohnehin überall dort abgelehnt, wo Schüler sich zeitweise oder dauerhaft aufhalten.
In der Stellungnahme teilte die Staatliche Grundschule Gera mit, dass man dort nicht gewusst habe, dass Kameraattrappen dem Daten-

schutz unterworfen sind. Diese Attrappen wurden sofort nach der Kontaktaufnahme des TLfDI abgebaut.

Der Einsatz einer Kameraattrappe unterliegt grundsätzlich den gleichen Voraussetzungen wie der Einsatz echter Kameras. Die Videoüberwachung von höchstpersönlichen Bereichen der Privat- und Intimsphäre, z. B. Toiletten, Umkleidekabinen, Duschen, Saunas, ärztlichen Behandlungsräumen etc. ist generell als unverhältnismäßig und damit als unzulässig anzusehen.

13.7 Datenschutz geht zur Schule

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) erreichten Beschwerden über Mitarbeiter der Staatlichen Grundschule Bottendorf (GSB) im Kyffhäuserkreis. Inhalt der Beschwerden war zum einen, dass Mitarbeiter Informationen aus vertraulichen Gesprächen und E-Mails an Dritte weitergegeben hatten. Des Weiteren soll das Notenbuch öffentlich zugänglich gemacht worden sein. Außerdem wurden die Zeugnisse anhand einer Rangliste ausgegeben, die sich nach dem Notendurchschnitt der Schüler richtete. Nach einem ersten Anschreiben an die GSB antwortete das Staatliche Schulamt Nordthüringen. Diese Antwort war allerdings weder umfangreich noch aussagekräftig, weshalb eine zweite Stellungnahme mit dem Hinweis auf die Unterstützungspflicht nach § 38 Thüringer Datenschutzgesetz (ThürDSG) von der GSB gefordert wurde.
In der daraus folgenden ausführlichen Stellungnahme wurde allen Vorwürfen widersprochen und selbst Vorwürfe gegenüber dem Beschwerdeführer erhoben. Explizit wurde der Tatsache widersprochen, dass Inhalte aus Gesprächen oder E-Mails an Dritte weitergegeben wurden, wie auch, dass Zeugnisse nach einer Rangliste ausgegeben worden seien.
Kurz nachdem die Stellungnahme der GSB den TLfDI erreichte, wurde eine zweite Beschwerde bezüglich der GSB eingereicht. Diese nahm die bereits vorhandenen Beschwerden auf, konkretisierte diese und fügte neue Beschwerden hinzu. So wurde der Zeitraum, indem die Zeugnisse nach einer Rangliste ausgegeben wurden auf das Jahr 2011 datiert. Weiter wurde der Vorwurf erhoben, dass vertrauliche Informationen, unter anderem Krankheitsbilder von Lehrern wie auch Schülern, weitergegeben wurden. Auch sollen alle Noten nach

einem Test in der Klasse laut vorgelesen worden sein, ohne dass die Schüler sich dagegen hätten wehren können. Dieses Verhalten sei nach Beschwerde allerdings bereits eingestellt.
Da sich beide Aussagen gegenüberstehen ist eine zweifelsfreie Feststellung datenschutzrechtlicher Verstöße nicht möglich. Nichtsdestotrotz wurden die GSB wie auch das Nordthüringer Schulamt darauf hingewiesen, dass die dargestellten Praktiken Verstöße gegen das ThürDSG wie auch gegen § 57 Abs. 4 Thüringer Schulgesetz darstellen würden. Als Reaktion auf das Schreiben des TLfDI versprach das Nordthüringer Schulamt seinerseits eine Kontrolle der GSB sowie Beratungen der Lehrkräfte in Bezug auf den Datenschutz. Der TLfDI lässt sich über diese Kontrolle berichten und behält sich außerdem eine Kontrolle der GSB vor.

Kinder haben ebenso ein Recht auf Datenschutz wie Erwachsene. Auch wenn sie dieses noch nicht begreifen oder einfordern, sind ihre Daten gleichermaßen schützenswert. Der TLfDI unterstützt Schulen gern in ihren Bestrebungen, Datenschutz zu etablieren.

14 Entwicklungen der automatisierten Datenverarbeitung

apps et smarthpones – applications pour smartphones
© kotoyamagami – Fotolia.com

14.1 IPv4 goes to IPv6 – muss mein Kühlschrank das können?

PCs, die über das Internet oder in einem Netzwerk erreichbar sein wollen, benötigen eine sogenannte Internet Protocol-Adresse (IP-Adresse). Der derzeitige Standard hierfür ist IPv4.
So konnte weltweit mit dem IPv4-Standard ca. 4,2 Milliarden Geräten eine Adresse zugeordnet werden, die in technischen Systemen weiter verarbeitet wird.
Die IPv4-Adressen werden dabei beispielsweise PCs und anderen Geräten ständig zugewiesen (statische Zuweisung). Bei Nichtgebrauch können IP-Adressen auch einem neuen Gerät zugeordnet werden (dynamische Zuweisung).
Vom Letzteren wurde oft Gebrauch gemacht, weil die IP-Adressen nicht ausreichten oder aber auch, um bewusst nicht über die IP-Adresse auf das Gerät schlussfolgern zu können. Praktische Anwendung findet dieses Prinzip beispielsweise, um auf diese Weise anonym im Internet zu surfen.
Mit der weltweiten Zunahme von PCs, Tablets und Netzwerkkomponenten, wie Firewalls, Server und Router, die ständig mit der gleichen IP-Adresse über das Internet erreichbar sein sollen, ist dieser Adressbereich nun weitgehend ausgeschöpft.
Außerdem gibt es im privaten Bereich zunehmend Geräte, denen die Industrie eine statische IP-Adresse zuweisen möchte. So gibt es seitens der Industrie den Bedarf, Kühlschränke, Spielkonsolen, Rauchmelder, Smart-TVs, digitale Videorecorder, Waschmaschinen – kurz alle technischen Geräte, die mit modernen elektronischen Steuerungen arbeiten – den Kunden internetfähig anzubieten. Zweck dessen soll sein, dass Kunden, Hersteller, Betreiber oder aber auch vertraglich gebundene Firmen mit diesen technischen Geräten aus der Ferne über das Internet kommunizieren können sollen.

Aus diesem Grund wurde weltweit vereinbart, den möglichen Adressraum zu vergrößern.
So entstand der neue Internet-Protokoll-Standard – IPv6. Damit ist es aus heutiger Sicht möglich, jedem neuen technischen Gerät auf der Welt eine eindeutige IP-Adresse zuzuweisen.
Neben den vielen Vorzügen, welches dieser Internet-Protokoll-Standard mit sich bringt, birgt er aber auch Gefahren. Eine davon ist, dass die Industrie und/oder der Staat Bewegungsprofile bzw. Verhaltensmuster ohne Wissen der Kunden bzw. der Benutzer dieser Geräte erstellen könnten.
Aus diesem Grund hat die 84. Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder im November 2012 in ihrer Entschließung „Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller“ und der Arbeitskreis technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der gleichnamigen Orientierungshilfe eine Vielzahl von Hinweisen und Empfehlungen zum datenschutzgerechten Einsatz von IPv6 gegeben. Hierzu zählen die Gewährleistung einer sicheren und vertrauenswürdigen Ende-zu-Ende-Kommunikation, das Erstellen von Bewegungsprofilen bzw. Verhaltensmustern von Nutzern zu vermeiden, den Ortsbezug von Adressen zu verringern und den Einbau von benutzerfreundlichen Konfigurationsmöglichkeiten vorzusehen.
Sowohl die Entschließung als auch die Orientierungshilfe sind auf der Internetseite des TLfDI abrufbar unter: http://www.tlfdi.de.

Beim Einsatz von IPv6 sind personenbezogene Daten jeglicher Art in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen entsprechend der oben genannten Orientierungshilfe zu schützen.

14.2 Sind Sie mandantenfähig?

Zur Zentralisierung und Konsolidierung verteilter Datenverarbeitung sowie aus Kostengründen greifen Daten verarbeitende öffentliche und nicht-öffentliche Stellen zunehmend auf kooperative Betriebsmodelle zurück, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen. Technisch wird dies überwiegend durch Einrichtung von sogenannten „Mandanten“ in einer Softwarelösung umgesetzt.

Der Arbeitskreis technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb eine „Orientierungshilfe Mandantenfähigkeit“ erstellt, die neben den rechtlichen Grundlagen die ordnungsgemäße getrennte Verarbeitung personenbezogener Daten in einer gemeinsamen IT-Struktur beleuchtet.
Zum Nachweis einer ordnungsgemäßen Verfahrenstrennung ist es zunächst erforderlich,

- die rechtlichen Grundlagen – insbesondere auch zur Zulässigkeit der Datenübermittlungen zwischen Mandanten, wo diese vorgesehen sind – zu prüfen,
- die Revisionsfähigkeit der Übermittlungen zwischen den Mandanten,
- die Abgeschlossenheit der Transaktionen innerhalb der Mandanten und
- die Unabhängigkeit der Konfiguration nachzuweisen sowie
- die Beschränkungen der mandantenübergreifenden Verwaltung der Datenverarbeitung strikt umzusetzen.

Auf Basis dieser Vorüberlegungen ist dann das Datenschutz- und Sicherheitsmanagement auf diese besondere Form der Datenverarbeitung anzupassen.
Die Orientierungshilfe steht auf der Internetseite des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit zum Abruf bereit unter:
http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/oh_mandantenfaehigkeit.pdf

Bei der gemeinsamen Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten ist die Mandantenfähigkeit zu gewährleisten.

14.3 Wie sicher ist mein Passwort?

Anfang Oktober 2013 berichtete http://www.heise.de/ vom Einbruch Unbekannter in das Adobe-Netzwerk. Dort seien die Zugangsdaten von mindestens 150 Millionen Nutzern gestohlen worden. So hätten die Angreifer Zugriff auf die Accounts und verschlüsselten Passwörter gehabt. Allerdings waren die Passwörter von Adobe nicht ausreichend verschlüsselt worden, sodass die Angreifer diese entschlüssel-

ten und die beliebtesten 1000 Adobe-Passwörter im Internet veröffentlichten.
Der Software-Hersteller hatte nach Bekanntwerden des Lecks im o. g. Bericht alle Passwörter zurückgesetzt, die Inhaber der aktiven Accounts informiert und zur Vergabe eines neuen Passworts angehalten.
Neben der Meldung auf http://www.heise.de/hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) umgehend unter anderem das Thüringer Finanzministerium (TFM) auf diese Tatsache hingewiesen. Über das Computer Emergency Response Team der Bundesverwaltung (CERT-Bund – zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen) wurde an das TFM eine Liste mit allen kompromittierten Accounts versandt, die der Domain „thueringen.de“ zugeordnet waren. Nach Aussagen des TFM waren fast alle Ressorts des Freistaats Thüringen betroffen.
Aus gegebenem Anlass möchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit nochmals darauf hinweisen, grundsätzlich Passwörter nie mehrfach, also für mehrere Accounts, zu verwenden. Zum Schutz vertraulicher Dokumente, zum Verschlüsseln von Datenträgern oder aber für den Zugang zu Internetdiensten sollten nur solche Passwörter eingesetzt werden, die einem hohen Sicherheitsstandard genügen.
Die Sicherheit von gewählten Passwörtern steigt exponentiell mit der Anzahl der Zeichen und mit der Menge des Zeichensatzes. Optimale Passwörter bestehen aus zufällig gewählten Zeichenfolgen mit mehreren Bestandteilen, wie Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen. Auch sollten keine Vor- oder Nachnamen enthalten sein. Wenn für das Passwort alphanumerische Zeichen gewählt werden, sollte es mindestens 8 Zeichen lang sein (Maßnahme 2.11 Regelung des Passwortgebrauches der IT-Grundschutz-Kataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html).

Passwörter sollten nie für mehrere Accounts benutzt werden und der empfohlenen Maßnahme 2.11 der IT-Grundschutz-Kataloge des BSI genügen.

14.4 Clouds – schwere Wetter

IT-Dienstleistungen werden zunehmend unter Verwendung des Internet angeboten und vermarktet. Diese Verfahrensweise der Bereitstellung von z. B. Rechnerleistungen, Softwarediensten oder Speicherplatzkapazitäten über das Internet wird als Cloud Computing, also als Rechnen/Datenverarbeitung in der Wolke bezeichnet. Hinweise zu datenschutzkonformen Gestaltungsmöglichkeiten und zur Nutzung von Cloud-Computing wurden bereits im 8. Tätigkeitsbericht (TB) unter Punkt 14.7 sowie im 9. TB unter Punkt 14.1 gegeben mit Hinweisen zur Auftragsdatenverarbeitung. Im 9. TB zeichnete der TLfDI bereits das Bild dunkler aufziehender Wolken. Er wies darauf hin, dass Cloud-Lösungen nicht in jedem Fall geographische Grenzen kennen und dann die stattfindende Datenverarbeitung gerade nicht ortsgebunden erfolgt. Zudem können weitere Unterauftragsverhältnisse bestehen. Das jeweils anzuwendende Datenschutzrecht ist aber an den Ort der Verarbeitung gebunden, sodass bei Cloud-Computing eine Rechtsunsicherheit eintreten kann. Zudem ist im Zweifel nicht erkennbar, welche Geheim- und Sicherheitsdienste des jeweiligen Landes Zugriff auf welche Daten nehmen können oder sie gar beschlagnahmen dürfen.

Aus diesen Gründen sind, wenn personenbezogene Daten mit Cloud-Computing verarbeitet werden sollen, mit dem Cloud-Anbieter auch transparente, detaillierte und eindeutige vertragliche Regelungen zu treffen. Im Einzelnen sind das der tatsächliche Ort der Datenverarbeitung sowie die Benachrichtigung über eventuelle Ortswechsel, die Portabilität und Interoperabilität für den Fall, dass z. B. wegen Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen“ kann (9. TB, Punkt 14.1).

Angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der USA, einschließlich der Anti-Terror-Gesetze wie dem Patriot Act, der den Zugriff von amerikanischen Sicherheits- und Geheimdiensten auf Cloud-Daten von EU-Bürgern bei US-Firmen auch in Europa zulässt, weist der TLfDI darauf hin, dass die Wirtschaftlichkeit und Flexibilität, die durch Cloud-Computing erzielt werden können, nicht auf Kosten des Datenschutzes und der Datensicherheit gehen darf.

Deshalb sind derzeit aus datenschutzrechtlicher Sicht Private- bzw. Community-Clouds deutscher oder europäischer Anbieter vorzuzie-

hen, die zudem von vertrauenswürdigen Stellen zertifiziert sind. Personenbezogene Daten sind dabei nicht nur in der Cloud, sondern auch bei der Datenübertragung vor einem unberechtigten Zugriff dem Stand der Technik entsprechend durch sichere Verschlüsselungsverfahren zu schützen. Ein derzeit diskutiertes nationales oder europäisches Routing verringert nur die Wahrscheinlichkeit vor unberechtigtem Zugriff, wird ihn aber nicht verhindern können.

Der NSA-Skandal hat dem Vertrauen in sichere Cloud-Computing Dienste geschadet. Dies kann aber auch als Chance aufgefasst werden, denn das Bekanntwerden des NSA-Skandals könnte Projekte, die datenschutzgerechte Cloud-Computing Dienste entwickeln wollen, nun vorantreiben.

So hat bspw. das Bundesministerium für Wirtschaft und Energie (BMWi) gemeinsam mit Partnern aus der Wirtschaft und Wissenschaft bereits 2010 ein Aktionsprogramm „Cloud Computing“ sowie im November 2013 das Pilotprojekt „Datenschutz-Zertifizierung von Cloud-Diensten“ gestartet. Ziel ist es, geeignete Zertifizierungsverfahren für Cloud-Dienste zu entwickeln, um so ein hohes Datenschutzniveau für die Nutzer solcher Dienste sicherzustellen. Nach Einschätzung des BMWi ist es für den einzelnen Cloud-Nutzer nahezu unmöglich, die Rechtskonformität der Datenverarbeitung sowie die technischen und organisatorischen Vorkehrungen des Cloud-Anbieters eigenständig zu prüfen.

Nach Angaben des BMWi sind an dem Pilotprojekt alle maßgeblichen Akteure beteiligt, darunter mehrere Datenschutzbehörden, Anbieter und Anwender von Cloud-Diensten sowie Unternehmen aus den Bereichen der IT-Prüfung und IT-Rechtsberatung. Das Projekt soll im Frühjahr 2015 abgeschlossen werden. Man darf gespannt sein, inwieweit dabei die „Orientierungshilfe – Cloud Computing“ der Datenschutzbeauftragten des Bundes und der Länder (http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/orientierungshilfe_cloud_computing.pdf) und die „Sicherheitsempfehlungen für Cloud Computing Anbieter“ des Bundesamts für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile) Berücksichtigung finden.

Aber nicht nur hinsichtlich der Zertifizierung von Cloud-Anwendungen gibt es Bewegung. Einem Antwortschreiben der Eu-

ropäischen Kommission an den Bundesrat im Mai 2013 (BR-Drs. 455/13) ist unter anderem zu entnehmen, dass die Kommission hinsichtlich der Entwicklung von Verschlüsselungsverfahren eine Verschlüsselung für Daten auf dem Übermittlungsweg und bei der Speicherung sowie Verarbeitung für notwendig erachtet.

Die Wirtschaftlichkeit und Flexibilität, die durch Cloud-Computing erzielt werden kann, darf nicht auf Kosten des Datenschutzes und der Datensicherheit gehen. Deshalb sind derzeit aus datenschutzrechtlicher Sicht Private- bzw. Community-Clouds, von deutschen oder europäischen Anbietern vorzuziehen, die zudem von vertrauenswürdigen Stellen zertifiziert sind. Bei der Datenübermittlung, Speicherung und Nutzung der Daten sind dem Stand der Technik entsprechende Verschlüsselungsverfahren einzusetzen.

14.5 Ende-zu-Ende ist der Anfang!

In zahlreichen Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen werden personenbezogene Daten übertragen. Dabei kann die Vertraulichkeit, Integrität und Authentizität der Daten nur durch den Einsatz dem Stand der Technik entsprechender Verschlüsselungs- und Signaturverfahren gewährleistet werden (7. Tätigkeitsbericht, Punkt. 15.2). Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern. Bei einer Datenübertragung mit einer Ende-zu-Ende-Verschlüsselung können allerdings nur der Sender und Empfänger die Daten im Klartext lesen, also beispielsweise kein Provider dazwischen wie bei De-Mail (Punkt 2.4 dieses Berichts). Für die Ende-zu-Ende-Verschlüsselung bei E-Government-Verfahren steht mit dem Online Services Computer Interface (OSCI-Transport) ein bereits seit einigen Jahren bewährtes Datenübermittlungsprotokoll zur Verfügung. OSCI-Transport ist der vom Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich festgelegte jeweils geltende Standard für ein Datenübermittlungsprotokoll. So schreibt bereits die Verordnung über Personalausweise und den elektronischen Identitätsnachweis oder die Steueridentifikationsnummernverordnung die

Verwendung von OSCI-Transport in den jeweiligen Fachverfahren bei der Datenübermittlung zwischen den Behörden vor.
Aber auch die elektronische Datenübermittlung zwischen den Bürgern bzw. der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden.
Demzufolge hält die 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung im Oktober 2013 die verstärkte Gewährleistung sicherer elektronischer Kommunikationswege für unabdingbar. Da der IT-Planungsrat die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik koordiniert und fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards beschließt, wandte sich die 86. Konferenz mit ihrer Entschließung auch zum Teil an den IT-Planungsrat. Die Datenschutzbeauftragten des Bundes und der Länder halten den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen.
Die Datenschutzbeauftragten des Bundes und der Länder fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.
Der TLfDI wird bei Verfahren, die eine Datenübermittlung personenbezogener Daten vorsehen, weiter darauf drängen, dass diese nur verschlüsselt übertragen werden dürfen.
Die Entschließung „Sichere elektronische Kommunikation gewährleisten / Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“ kann in Anlage 20 oder im Internet nachgelesen werden unter:
http://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/enschliessungendk/entschlie__ung_sichere_elektronische_kommunikation.pdf

Die Datenschutzbeauftragten des Bundes und der Länder halten den Einsatz von Standards zur Ende-zu-Ende - Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen.

Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

14.6 Datenübermittlung Meldedaten an Kirchen und GEZ über Internet

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten unter anderem Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts-und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig. Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten verschlüsselt werden. Die Datenschutzbeauftragten des Bundes und der Länder mussten in der Vergangenheit jedoch feststellen, dass diese Anforderungen häufig missachtet werden. Aus diesem Grund forderten sie in der 84. Konferenz im November 2012 in ihrer Entschließung „Übermittlung von Meldedaten an öffentliche-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten“, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.
Des Weiteren wiesen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass mit dem Online Services Computer Interface (OSCI) bereits eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung steht (Punkt 14.5). So setzen beispielsweise die Meldeämter entsprechend der Ersten Bundesmeldedatenübermittlungsverordnung das Übermittlungsprotokoll OSCI-Transport für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein.

Aus diesem Grund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an die GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen umzusetzen.

Dies nahm der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit zum Anlass, das Thüringer Innenministerium (TIM) als zuständige Aufsichtsbehörde für den kommunalen Bereich um Umsetzung der Entschließung in den Meldebehörden zu bitten. Das TIM teilte daraufhin mit, dass die Datensicherheit bei der Datenübermittlung über das Internet durch den Einsatz von SSL/TLS (Secure Sockets Layer/ Transport Layer Security) mit gegenseitiger Authentifizierung von Sender und Empfänger in den Meldebehörden gewährleistet ist. Außerdem können die Daten auch mittels Datenträger oder PGP-verschlüsselter E-Mail den Empfängern zugestellt werden.
Inwieweit bei der Transportverschlüsselung mittels SSL/TLS der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im Oktober 2013 definierte Mindeststandard TLS 1.2 entspricht (https://www.bsi.bund.de/DE/Presse/Kurzmitteilungen/Kurzmit2013/Mindeststandard_TLS_1_2_Web-Seiten_des_BSI_13112013.html), wird vom TLfDI überprüft werden.

Die oben genannte Entschließung ist im Internet abrufbar unter:
http://www.tlfdi.de/imperia/md/content/datenschutz/entschliessungen/84_meldedatenuebermittlung.pdf

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich rechtliche Religionsgemeinschaften umzusetzen.

14.7 Das Multifunktionsgerät – ein unbekanntes Speichermedium

Die Vorteile von Multifunktionsgeräten im Vergleich zu klassischen Kopierern liegen auf der Hand:
Multifunktionsgeräte vereinen in sich Scanner, den automatischen Dokumenteneinzug – Automatic Document Feeder (ADF), Bildbearbeitungseinheit, Druck- sowie Sortier- und Heft-, Duplexeinheiten, Speichereinheiten, Netzwerk- und USB-Adapter, Router, Faxmodem, speicherprogrammierte Steuerungen (SPS) oder computergestützte Steuerung und Basis-Firmware.
Wer Multifunktionsgeräte nutzt, sollte wissen, dass jedes kopierte Dokument und die darin enthaltenen Daten im Gerät elektronisch gespeichert werden.
Diese Daten werden auf Knopfdruck (Start des Kopiervorgangs) automatisch auf interne Speichereinheiten, wie magnetische Festplatten oder Solid State Disks (SSD), geschrieben. Sie bleiben meist ein Geräteleben lang erhalten.
Tatsächlich haben alle bekannten Hersteller Vorsorge getroffen, dass Speicherbereiche gelöscht werden können. Nur gibt es diese Funktionalität – bzw. ein entsprechendes Security Kit (Sicherheitsoption) – nicht bei jedem Hersteller zum Nulltarif.
Insgesamt stehen die Gerätehersteller vor einer permanenten Optimierungsaufgabe. Mit der Entwicklung schneller und größerer Speichermedien steigen auch die Anforderungen an den Datenschutz und die Datensicherheit.
Auf welche Funktionalitäten beim Kauf oder beim Leasing insbesondere geachtet werden sollte, hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit auf seiner Internetseite veröffentlicht unter:
http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/pmtlfdi/130514_mulitfunktionsgeraet.pdf

Daten verarbeitende Stellen haben auch beim Leasing und/oder Kauf von Multifunktionsgeräten den Datenschutz sicherzustellen.

15 Technische Entwicklung in der Thüringer Landesverwaltung

3D Man Office © Spencer – Fotolia.com

15.1 Babyphone im Dienstzimmer: Wozu?

Bestimmte Hinweise nahm der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) zum Anlass, hinsichtlich der Telekommunikationsanlagen (TK-Anlagen) und ihrer Leistungsmerkmale in einer Pressemitteilung darauf hinzuweisen, dass Aufschaltfunktionen bei TK-Anlagen dazu führen können, dass bei geführten Telefonaten Dritte mithören und bei sogenannten Babyphon-Funktionen trotz aufgelegtem Telefonhörer Gespräche in demjenigen Raum, in dem sich der Telefonapparat befindet, mitgehört werden können.
Aus datenschutzrechtlicher Sicht stellt das Ab- oder Mithören von Telefongesprächen oder Gesprächen im Raum eine Erhebung personenbezogener Daten dar. Die Verarbeitung einschließlich Erhebung und Nutzung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Sofern von den in den Telefonen wohl marktüblich vorhandenen Abhörmöglichkeiten Gebrauch gemacht wird, stellt dies einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen (Beschäftigten und auch Dritte) dar.
Aus diesem Grund hinterfragte der TLfDI bei allen Ministerien und deren nachgeordneten Bereichen, bei der Thüringer Staatskanzlei und beim Thüringer Landtag die eingestellten Leistungsmerkmale der TK-Anlagen für deren Geschäftsbereiche. Insbesondere interessierte aus datenschutzrechtlicher Sicht, welche TK-Anlagen einschließlich der angeschlossenen Apparate das Aufschalten und/oder eine Raumüberwachung bei Nichtnutzung des Telefons (Babyphon-Funktion) technisch ermöglichen und inwieweit diese Leistungs-

merkmale aktiviert bzw. deaktiviert sind. Die datenschutzrechtliche Brisanz liegt beim „Aufschalten“ darin, dass während eines Telefongespräches sich ein Dritter zu-/aufschalten kann. Wird diese Funktion aktiv genutzt, wird in der Regel am Telefon optisch signalisiert, dass eine Aufschaltung durch Dritte erfolgte. Bei der Babyphon-Funktion ist datenschutzrechtlich bedenklich, dass unbemerkt eine Raumüberwachung erfolgen kann. Auch hier ist die Erkennbarkeit in der Regel durch ein optisches Signal (Lampe) gegeben. Der TLfDI empfiehlt den Behörden und Personalräten, nicht nur die notwendige Dienstvereinbarung entsprechend dem Personalvertretungsgesetz hinsichtlich der TK-Anlage und ihrer möglichen und tatsächlich aktivierten Leistungsmerkmale zu vereinbaren, sondern auch deren Einstellung regelmäßig vor Ort zu überprüfen.

Der TLfDI geht davon aus, dass aufgrund seiner Aktivitäten auch das Kabinett in seiner 137. Sitzung die IuK-Referenten der Ressorts beauftragte, die Funktionalitäten der Standard-Telefonanlagen zu erörtern.

Nach Kenntnisstand des TLfDI befinden sich derzeit 180 gekaufte und 37 gemietete TK-Anlagen in der Thüringer Landesverwaltung im Einsatz. Im Ergebnis wurde festgestellt, dass die Leistungsmerkmale „Aufschalten“ und die „Babyphon-Funktion“, teilweise technisch nicht möglich sind. Sofern diese Funktionen möglich sind, waren sie abgeschaltet bzw. wurden nach Mitteilung der zuständigen Stelle auf Grund der Initiative des TLfDI abgeschaltet.

Nach Angaben des Thüringer Innenministeriums (TIM) sind für den Bereich der Thüringer Polizei die Leistungsmerkmale „Aufschalten“ und die „Babyphonfunktion“ deaktiviert, die Funktion „Gesprächsaufzeichnungen“ aber teilweise verfügbar. Die Aufzeichnungen erfolgen nach Angaben des TIM nur in den Fällen des Notrufs und der Gefahrenabwehr bzw. der Strafverfolgung auf der Grundlage des Thüringer Gesetzes über die Aufgaben und Befugnisse über die Polizei bzw. der Strafprozessordnung.

Auch lassen nicht alle TK-Anlagen der Thüringer Landesverwaltung eine Protokollierung der geänderten Funktionalitäten zu bzw. die Funktion der Protokollierung war nicht immer eingeschaltet. Auswertungskonzepte – also wer wann die tatsächlich eingestellten Funktionalitäten bei der TK-Anlage überprüft – sind in seltenen Fällen vorhanden. Auch hier wird ein aktiveres Handeln der Personalräte notwendig sein, denn gemäß § 74 Abs. 2 Ziff. 11 Thüringer Personalvertretungsgesetz hat der Personalrat bei Einführung, An-

wendung, wesentlicher Änderung oder Erweiterung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen oder zu erfassen, ein Mitbestimmungsrecht.

Aufgrund der Bedeutsamkeit des Themas wandte sich der TLfDI auch zusätzlich an das TIM als oberste Aufsichtsbehörde der Kommunen mit der Bitte, diese über die datenschutzrechtlichen Gefahren zu informieren und die Funktionalitäten der TK-Anlagen zu klären. Zudem informierte der TLfDI auch die Thüringer Handwerkskammern und die Industrie- und Handelskammern Thüringens.

Hinsichtlich der neuen geplanten zentralen TK-Anlage für die Thüringer Landesverwaltung auf der Basis Voice over IP (VoIP), teilte das Thüringer Finanzministerium (TFM) mit, dass SIP-basierte (SIP: Session Initiation Protocol) Systeme zur Verfügung gestellt werden, bei dem die Funktion einer „ungewollten“ Raumüberwachung bei aufgelegtem Telefonhörer nicht möglich sei. Weiterhin teilte das TFM mit, dass das Leistungsmerkmal Babyphon-Funktion in der zentralen TK-Anlage nicht zur Verfügung stünde. Auch würden alle Updates durch das Thüringer Landesrechenzentrum sowie das TFM auf ihren Funktionsumfang und ihre Regelkonformität (sog. Compliance) untersucht. Die zur Anwendung kommenden Geräte seien dabei Standardgeräte, die in Kombination mit der installierten Firmware bei allen anzuschließenden Behörden und Einrichtungen zum Einsatz kommen.

Ferner teilte das TFM mit, dass alle innerhalb der zentralen Telefonanlage geführten Gespräche Ende-zu-Ende verschlüsselt werden. In den Voice-Rechenzentren werden lediglich die Sprachdaten ver- bzw. entschlüsselt, welche vom bzw. in das öffentliche Telefonnetz geleitet werden.

Es ist nicht vorgesehen, die Verschlüsselung in den Rechenzentren durch den Hersteller protokolltechnisch abschalten zu lassen. Sollte aus technischen Gründen eine Ende-zu-Ende Verschlüsselung nicht möglich sein, so wird die Telefonie-Verbindung trotzdem aufgebaut. Den Nutzern wird die unverschlüsselte Sprachverbindung durch ein durchgestrichenes bzw. offenes Schlosssymbol im Display ihres Telefons deutlich angezeigt.

Der TLfDI begrüßt, dass seinen Bedenken seitens des TFM Rechnung getragen wird, was nicht bedeutet, dass diese Thematik vom TLfDI als erledigt betrachtet wird.

Beim Betreiben von TK-Anlagen ist nicht nur entsprechend dem Personalvertretungsgesetz eine Dienstvereinbarung mit dem Personalrat zu schließen, die die möglichen und tatsächlich aktivierten Leistungsmerkmale definiert, sondern auch die regelmäßige Überprüfung vor Ort eingestellter und vereinbarter Leistungsmerkmale zu gewährleisten.

15.2 Unterrichtung über regelmäßige Datenübermittlungen infolge der Neuregelung von § 7 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG)

§ 7 Abs. 7 Thüringer Datenschutzgesetz (ThürDSG) wurde im Rahmen des Gesetzes zur Änderung des ThürDSG und anderer Vorschriften vom 20. Juli 2011 durch Beschluss des Thüringer Landtags vom 16. November 2011 eingefügt. Danach ist die Neufassung des ThürDSG am 9. Dezember 2011 in Kraft getreten.
Nach dem neu in das Gesetz eingefügten § 7 Abs. 7 ThürDSG sind die Absätze 1 bis 6 dieser Norm, darunter auch die Unterrichtungspflicht der verantwortlichen Stelle gegenüber dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nach § 7 Abs. 3 Satz 1 ThürDSG auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.
In diesem Zusammenhang stellt sich die Frage, ob § 7 Abs. 7 ThürDSG auch rückwirkend, das heißt auf „Altverfahren“, anzuwenden ist. Weder in den Übergansbestimmungen des § 43 a noch in der Begründung zum seinerzeitigen Gesetzentwurf (unter Nr. 4 des Gesetzentwurfs in der Drucksache 5/3086) finden sich Hinweise darauf, dass § 7 Abs. 7 ThürDSG auch rückwirkend Anwendung finden soll. Gegen eine Anwendung von § 7 Abs. 7 ThürDSG auf die Zeit vor seinem Inkrafttreten spricht auch, dass die Behörden ansonsten eine Flut von Formblättern zum Verfahrensverzeichnis ausfüllen und beim TLfDI einreichen müssten, ohne dass dies mit einen besonderem Erkenntnisgewinn des TLfDI verbunden wäre. Zudem war bereits mit der Novellierung des ThürDSG im Jahre 2001 das bis dahin bei der Aufsichtsbehörde zu führende, wenig effektive, Datenschutzregister als Verzeichnis der automatisierten Verfahren öffentlicher Stellen aufgegeben worden.
Nach Auffassung des TLfDI ist daher § 7 Abs. 7 ThürDSG nur für die regelmäßige Datenübermittlungen ab dem 9. Dezember 2011 anzuwenden.

§ 7 Abs. 7 ThürDSG ist nach Auffassung des TLfDI nur für die regelmäßige Datenübermittlungen ab dem 9. Dezember 2011 anzuwenden.

15.3 Einrichtung eines barrierefreien Notrufs für Menschen mit Behinderungen

Das Thüringer Innenministerium (TIM) wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) mit der Bitte, für folgendes Problem eine datenschutzgerechte Lösung zu finden: Menschen mit Behinderungen, insbesondere soweit sie gehörlos oder hörgeschädigt sind, haben auf Grund ihrer Behinderung ein zusätzliches Handicap, wenn sie in Notfällen über die für den nichtbehinderten Bürger verfügbaren Kommunikationsmittel um Hilfe bitten wollen. Durch die EU wurde 2009 in einer Konvention Verpflichtungen zur Unterstützung von Behinderten für die Mitgliedstaaten definiert. Nach Angaben des TIM ist eine wiederholte Forderung der Behindertenverbände in diesem Zusammenhang unter anderem die Einrichtung eines barrierefreien Notrufs, also eines ungehinderten Zugangs zu den Notrufabfragestellen.
Auch wenn nach der technischen Richtlinie Notruf (TR Notruf), der Verordnung über Notrufverbindungen – NotrufV (zuletzt geändert 2012) und § 108 Telekommunikationsgesetz (TKG) die Netzbetreiber und Mobilfunkanbieter beim Notruf verpflichtet sind, die Rufnummer des Anschlusses und die Standortdaten des Hilfesuchenden schon im Verbindungsaufbau zu übermitteln (siehe Punkt 4.4), so können Anrufende insbesondere soweit sie gehörlos oder hörgeschädigt sind, nicht in jedem Fall entsprechend kommunizieren. Da eine mögliche SMS-Lösung per Handy wegen der verzögerten Zustellung durch die Provider der zeitnahen Rettungshilfe entgegenwirkt, prüfte das TIM gemeinsam mit dem TLfDI die Nutzungsmöglichkeit des Sozialen Netzwerks "Twitter". Aus Sicht des TIM besteht für die in Thüringen ca. 1600 Gehörlosen und 8.000 bis 10.000 Hörgeschädigten der Vorteil bei der Nutzung von Twitter nicht nur darin, dass Hilfeersuchen (Notruf) in Echtzeit zugehen. Vielmehr kann dieser Dienst auch in einem offenen Bereich für die Warnung vor allgemeinen Gefahren (Warnung der Bevölkerung) genutzt werden.
Der TLfDI stimmte dem Verfahren unter folgenden Bedingungen zu:

- Werden Twitter-Plugins verwendet, ist auf die Übertragung von Nutzungsdaten an Twitter hinzuweisen und ein Link auf die (deutschsprachigen) Datenschutzrichtlinien von Twitter zu setzen.
- Mit Blick auf die Widerspruchsmöglichkeit nach § 15 Abs. 3 des Telemediengesetzes ist ein Hinweis vorzusehen, dass die Nutzer der Erfassung bzw. Speicherung von Cookies durch Twitter widersprechen bzw. entgegentreten können, indem ihnen die Möglichkeit eröffnet wird, das „Do not Track“-Plugin zu installieren.
- Solange die Reichweitenanalyse nicht auf allen Geräten verhindert werden kann, also das „Do not Track“-Plugin nicht auf allen verwendeten Geräten installiert werden kann, sind im Testbetrieb nur Geräte zu verwenden, die diese Installation ermöglichen. Dies schränkt derzeit die Nutzung von Smartphones ein.
- Twitter-Plugins oder der Zugang zum Twitter-Widget sind als Zwei-Schritt-Lösung zu implementieren, bei der Nutzungsdaten erst dann übertragen werden, wenn der Nutzer darüber unterrichtet wurde, etwa in Form eines Pop-Up-Fensters (1. Schritt) und durch eine bewusste und eindeutige Handlung („Klick“) dies akzeptiert (2. Schritt).

Zur Unterstützung von Menschen mit Behinderungen sind auch bei der Nutzung von Sozialen Netzwerken, wie Twitter, datenschutzrechtliche Vorgaben zu beachten.

15.4 Haushaltmanagementsystem – HAMASYS

HAMASYS steht für ein integriertes IT-Verfahren zur kompletten Abbildung des Haushaltskreislaufes in der Thüringer Landesverwaltung. Über dieses größte eGovernment-Projekt der Thüringer Landesverwaltung hatte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) bereits ausführlich in den letzten 4 Tätigkeitsberichten (TB) berichtet (6. TB Punkt 1.8.1; 7. TB Punkt 15.3; 8. TB Punkt 9.2 und 9. TB Punkt 9.1). Der TLfDI hat sich weiterhin der Problematik angenommen und mit dem Thüringer Finanzministerium (TFM) gemeinsam nach Lösungen gesucht, wie zukünftig das Verfahren HAMASYS datenschutzgerechter gestaltet werden kann.

So hat der TLfDI darauf hingewiesen, dass in jeder Rechnungslegung, Bescheiderteilung und parallel über das Internet Informationen zu HAMASYS und zur Widerspruchsmöglichkeit zwecks Nutzung der Partnerdaten durch andere Behörden hingewiesen werden muss.
Mit der Änderung des Thüringer Datenschutzgesetzes (ThürDSG) 2011 wurde auch das Betreiben von Verbundverfahren ermöglicht, nach dem mehrere Daten verarbeitende Stellen gemeinsam unter bestimmten Vorgaben personenbezogene Daten verarbeiten können (§ 7 a ThürDSG). Die Möglichkeit, HAMAYSYS als Verbunddatei im Sinne des § 7 a ThürDSG zu betreiben, wird derzeit vom TFM gemeinsam mit dem TLfDI rechtlich geprüft.

Gemäß § 7 a ThürDSG können mehrere Daten verarbeitende Stellen gemeinsam unter bestimmten Vorgaben personenbezogene Daten verarbeiten (§ 7 a ThürDSG).
Betroffene können ihre Rechte nach § 5 Abs. 1 Nr. 2 bis 4 und 7 ThürDSG gegenüber jeder der an dem Verbundverfahren beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der betroffenen Daten verantwortlich ist.

15.5 Projekt "Digitales Magazin des Freistaats Thüringen"

Im Juli 2012 trug das Thüringische Hauptstaatsarchiv Weimar (ThHStA) dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) das Projekt „Digitales Magazin des Freistaats Thüringen“ vor, das sich mit der ausführlichen Darstellung anzustrebender Prozesse und Arbeitsschritte der digitalen Archivierung beschäftigt und die Einführung einer Softwarelösung plant. Hierzu wurde der TLfDI beratend eingebunden.
Im Ergebnis wurde seitens des ThHStA eingeschätzt, dass die Verarbeitung von Daten im Digitalen Magazin mit dem Schutzbedarf „hoch“ einzustufen ist. Dies führte dazu, der Gewährleistung von Vertraulichkeit, Integrität und Authentizität dieser Daten besonderes Augenmerk zu widmen. So werden in dem Projekt zur Absicherung der Vertraulichkeit der Übertragungswege und zur Authentifizierung von Benutzern kryptographische Verfahren unterstützt.
Entsprechend dem Fach- und Organisationskonzept ist geplant, auf eine Verschlüsselung der Daten im Langzeitspeicher zu verzichten, um auch nach einem nicht auszuschließenden Schadensereignis

einen Datenverlust möglichst gering zu halten und die weitgehende Wiederherstellung der Archivdaten nicht zusätzlich zu erschweren. Auch wenn die Daten im Digitalen Magazin unverschlüsselt gespeichert werden, wird der Zugriff auf alle Daten durch eine dem aktuellen Stand der Technik entsprechende Zugriffskontrolle geschützt und geprüft, um den unbefugten Zugriff auf sensible Daten zu verhindern. Besonders gefährdete Bereiche des Digitalen Magazins, wie der Datentransfer (beispielsweise im Rahmen von Datenübernahmen) und der Nutzungsspeicher, in dem die Nutzungskopien dem Archivbenutzer bereitgestellt werden, sollen durch weitere kryptographische Verfahren, wie beispielsweise Verschlüsselungen, zusätzlich geschützt werden.
Dies begrüßt der TLfDI ausdrücklich, denn auch in einem „Digitalen Magazin“ muss die Vertraulichkeit hochsensibler personenbezogener Daten durch dem Stand der Technik entsprechende kryptografische Verfahren gewährleistet sein.
Hochsensible personenbezogene Daten sind personenbezogene Daten, bei deren Verarbeitung eine erhebliche Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung insofern zu erwarten ist, als dass durch einen Missbrauch der Daten der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. Es sind ferner solche personenbezogene Daten erfasst, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen oder deren unbefugte Kenntnis eine Gefahr für Leib, Leben oder die persönliche Freiheit des Betroffenen befürchten lässt (z. B. Sozial-; Gesundheits-; Steuer-; Personaldaten; Daten zu religiösen und politischen Anschauungen; Daten, die Berufs- und Geschäftsgeheimnisse sowie Fernmeldegeheimnisse betreffen).
Nähere Informationen zum Fach- und Organisationskonzept „Digitales Magazin des Freistaats Thüringen“ erhalten Interessierte unter:
http://www.thueringen.de/th2/staatsarchive/fachinformationen/digital/projekt/fachkonzept/ .

Beim Projekt „Digitales Magazin des Freistaats Thüringen“ müssen entsprechend dem Schutzbedarf der personenbezogenen Daten die Vertraulichkeit, Integrität und Authentizität sowohl während der Datenübernahme als auch während der Bereitstellung im Nutzungsspeicher gewährleistet sein. Dies erfordert den Einsatz von dem

Stand der Technik entsprechenden sicheren Verschlüsselungsverfahren.

16 Parlamentarische Anfragen gem. § 112 a Geschäftsordnung des Thüringer Landtags

16.1 Parlamentarische Anfragen gem. § 112 a Geschäftsordnung des Thüringer Landtags (Anfragen an den Datenschutzbeauftragten)

Mit der Novelle des Thüringer Datenschutzgesetzes (ThürDSG) im Jahr 2011 wurde die Regelung des § 40 Abs. 6 Satz 2 ThürDSG neu eingefügt. Danach hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) parlamentarische Anfragen, die den Datenschutz im Bereich seiner Kontrollbefugnis betreffen, zu beantworten. Im Berichtszeitraum erreichten den TLfDI neun parlamentarische Anfragen. Alle wurden innerhalb der nach § 112 a Abs. 4 Satz 1 der Geschäftsordnung des Thüringer Landtags gesetzten Sechs-Wochen-Frist beantwortet.
Mit folgenden Themen hatte der TLfDI sich im Rahmen der Beantwortung der parlamentarischen Anfragen zu befassen: Er musste dazu Stellung nehmen, ob die Regelungen des Telekommunikationsgesetzes zur Speicherung und Verwendung von Telekommunikationsdaten verfassungswidrig sind, er berichtete über die Aktenvernichtung im Landeskriminalamt und über die Sanktionsmöglichkeiten im öffentlichen Bereich. Es wurde dazu Bericht erstattet, unter welchen Voraussetzungen die Ermittlung des Übernachtungsgrundes durch Hoteliers in Thüringen zulässig ist, der TLfDI gab Auskunft zur Überwachung öffentlicher Plätze mittels Videotechnik in Thüringen, er legte dar, wie bei der Weitergabe von Daten eines Fahrzeugnutzers an den Fahrzeugvermieter durch die Polizei zu verfahren ist, nahm zum mangelhaften Datenschutz bei Apps Stellung, äußerte sich zu Datenschutz und Informationsfreiheit im Rahmen des SGB II und berichtete zum aktuellen Stand von angekündigten Prüfungen. Die Regelung des § 40 Abs. 6 Satz 2 ThürDSG hat sich bewährt. Der TLfDI steht dem Parlament mit Rat zur Seite und begrüßt diese enge Kooperation ausdrücklich! Die parlamentarischen Anfragen und entsprechenden Antworten des TLfDI finden Sie in den entsprechenden Landtagsdrucksachen, die im Anhang unter Anlage 24 bis 32 beigefügt sind.

Der TLfDI beantwortete im Berichtszeitraum fristgerecht neun parlamentarische Anfragen.

Anlagen

Anlage 1

Entschließung zwischen den Konferenzen 2011/2012

Schuldnerverzeichnis im Internet:
Anzeige von Schuldnerberatern nur im Rahmen der gesetzlich legitimierten Zwecke
(Umlaufentschließung vom 7. Februar 2012)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit

vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen

Anlage 2

Entschließung
der 83. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 21./22. März 2012 in Potsdam

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer **Datenschutz-Grundverordnung** enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittel-

bar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,

- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,

- die Förderung des Selbstdatenschutzes,

- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,

- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,

- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und

- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeili-**

chen und justiziellen Zusammenarbeit in Strafsachen in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

Anlage 3

Entschließung
der 83. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 21./22. März 2012 in Potsdam

Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.
Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

Anlage 4

Entschließung
der 83. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 21./22. März 2012 in Potsdam

Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder“ frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen

öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

Anlage 5

Entschließung zwischen den Konferenzen 2012

„Patientenrechte müssen umfassend gestärkt werden“
Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!
(Umlaufentschließung vom 23. Mai 2012)

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.

- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.

- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur

Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.

– Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.

– Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.

– Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

Anlage 6

Entschließung zwischen den Konferenzen 2012

Orientierungshilfe zum datenschutzgerechten Smart Metering
(Umlaufentschließung vom 27. Juni 2012)

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher

sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

Anlage 7

Entschließung zwischen den Konferenzen 2012

Melderecht datenschutzkonform gestalten!
(Umlaufentschließung vom 22. August 2012)

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adress-

buchverlage. Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.

– Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.
– Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.
– Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.
– Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.
– Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.
– Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu ver-

nachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

Anlage 8

Entschließung
der 84. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. November 2012 in Frankfurt (Oder)

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der **Datenschutz-Grundverordnung** an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden

Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.

- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.

- Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

Anlage 9

Entschließung
der 84. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. November 2012 in Frankfurt (Oder)

Einführung von IPv6
Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.

- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.

- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.

- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit

denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.

- Interface Identifier und Präfix sollten synchron gewechselt werden.

- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IPProtokollstack implementieren.

- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6- Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.

- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.

- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten.

Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6- Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfixes.

- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.

- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 - Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

Anlage 10

Entschließung
der 84. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. November 2012 in Frankfurt (Oder)

Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch

nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

Anlage 11

Entschließung
der 84. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. November 2012 in Frankfurt (Oder)

Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

Anlage 12

Entschließung zwischen den Konferenzen 2013

Beschäftigtendatenschutz nicht abbauen, sondern stärken!
(Umlaufentschließung vom 25. Januar 2013)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.

- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.

- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf

vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.

– Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.

– Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

Anlage 13

Entschließung
der 85. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 13./14. März 2013 in Bremerhaven

Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

Anlage 14

Entschließung
der 85. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 13./14. März 2013 in Bremerhaven

Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die

Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

Anlage 15

Entschließung
der 85. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 13./14. März 2013 in Bremerhaven

Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder

Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.

- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.

- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.

- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.

- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.

- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.

- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.

- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.

- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.

- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz- Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

Anlage 16

Erläuterungen

zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven „Europa muss den Datenschutz stärken“

- **Jedes personenbeziehbare Datum muss geschützt werden**

  Nach Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie z. B. IP-Adressen, Kenn-Nummern, Standortdaten ein.

- **Es darf keine grundrechtsfreien Räume geben**

  Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

- **Einwilligungen müssen ausdrücklich erteilt werden**

  Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer

eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäischen Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es – auch mit Blick auf Artikel 8 Abs. 2 der Grundrechtecharta – nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

- **Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern**

  Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch – in Anlehnung an Artikel 8 Abs. 2 der Grundrechtecharta – das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

- **Profilbildung muss beschränkt werden**

  Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung fin-

den. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

- **Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte**

  Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

- **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**

  Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

- **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**

  Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Art. 8 Abs. 3 der Grundrechtecharta und Art. 16 Abs. 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

- **Grundrechtsschutz braucht effektive Kontrollen**

  Die Sanktionen müssen – wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat – abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

- **Hoher Datenschutzstandard für ganz Europa**

  Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Rege-

lungen vor, die den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

Anlage 17

Entschließung
der 85. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 13./14. März 2013 in Bremerhaven

Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.

- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld

aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und –registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

Anlage 18

Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen

Anlage zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

- Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des BSI gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.

- Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.

- Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.

- Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.

- Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.

- Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.

Anlage 19

Entschließung zwischen den Konferenzen 2013

Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen
(Umlaufentschließung vom 5. September 2013)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u.a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die

Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.

- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.

- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.

- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

  Dazu gehört,

  - zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.
  - sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.
  - die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.

- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.

- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

Anlage 20

Entschließung
der 86. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 1./2. Oktober 2013 in Bremen

Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende- Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung "Sicherheit bei E-Government durch Nutzung des Standards OSCI" Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI-Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

Anlage 21

Entschließung
der 86. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 1./2. Oktober 2013 in Bremen

Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von "gläsernen Patientinnen und Patienten oder Versicherten" weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesund-

heitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

Anlage 22

Entschließung
der 86. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 1./2. Oktober 2013 in Bremen

Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung "Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU-Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz

gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizei und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

Anlage 23

Entschließung
der 86. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 1./2. Oktober 2013 in Bremen

Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt – wie repräsentative Studien belegen – mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz

der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.[2]

- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.[3]

- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z.B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.[4]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

---

[2] Siehe dazu die Entschließungen „Keine umfassende und anlasslose Überwachung durch
Nachrichtendienste! Zeit für Konsequenzen“ und „Handlungsbedarf zum Datenschutz im Bereich der
öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags“.

[3] Siehe dazu die heutige Entschließung "Stärkung des Datenschutzes im Sozial- und Gesundheitswesen".

[4] Siehe dazu die heutige Entschließung "Sichere elektronische Kommunikation gewährleisten – Ende-zu-
Ende-Verschlüsselung einsetzen und weiterentwickeln“.

Anlage 24

Anfrage 1 des Abgeordneten Bergner (FDP)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz
Thüringer Landtag Drucksache 5/4996 vom 17. September 2012

Regelung des Telekommunikationsgesetzes zur Speicherung und Verwendung von Telekommunikationsdaten teilweise verfassungswidrig?

Die **Anfrage 1** vom 1. August 2012 hat folgenden Wortlaut:

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom24. Januar 2012 (BVerfG - 1 BvR 12ggrc5, veröffentlicht am 24. Februar 2012) entschieden, dass mehrere Vorschriften des Telekommunikationsgesetzes (TKG) gegen das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger verstoßen und eine Eingrenzung der Datennutzung durch die Ermittler erfolgen muss. Diese Entscheidung hat auch Auswirkungen auf die Landesgesetzgebung.

Ich frage den Datenschutzbeauftragten:

1. Welche Auswirkungen hat der Beschluss vom 24. Januar 2012 auf Thüringen?
2. Auf welchen rechtlichen Grundlagen finden derzeit in Thüringen "manuelle Auskunftsverfahren" (§ 113 Abs. 1 Satz 1 TKG) statt?
3. Auf welchen rechtlichen Grundlagen findet derzeit in Thüringen die Identifizierung von dynamischen IP-Adressen statt?
4. Auf welchen rechtlichen Grundlagen findet derzeit in Thüringen die Abfrage von Daten der Zugangssicherung statt?
5. Erfolgen derzeit nach Auffassung des Thüringer Datenschutzbeauftragten, mangels einer Umsetzung des Beschlusses, Grundrechtsverletzungen bei Thüringer Bürgerinnen und Bürgern?

6. Müssen Rechtsgrundlagen in Thüringen angepasst und/oder geschaffen werden, um dem Beschluss des BVerfG zu entsprechen? Falls ja, welche?
7. Hat der Datenschutzbeauftragte Kenntnis darüber, ob eine Umsetzung des Beschlusses des BVerfG in Thüringen schon vor dem 30. Juni 2013 erfolgen soll? Falls ja, worauf stützt sich diese Kenntnis?
8. Welche Maßnahmen ergreift der Thüringer Datenschutzbeauftragte, um den Beschluss schnellstmöglich umzusetzen?

Der **Thüringer Landesbeauftragte für den Datenschutz** hat die Anfrage mit Schreiben vom 17. September 2012 wie folgt beantwortet:

Zu 1.:
Das Bundesverfassungsgericht hat mit Beschluss vom 24. Januar 2012 (1 BVR 1299105) entschieden, dass § 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes (TKG) vom 22. Juni 2004 mit Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes unvereinbar ist. Übergangsweise, längstens jedoch bis zum 30. Juni 2013, gilt die Vorschrift mit der Maßgabe fort, dass die dort genannten Daten nur erhoben werden dürfen, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Für einen Eingriff in das informationelle Selbstbestimmungsrecht bedarf es normenklarer Regelungen, die insbesondere dem Grundsatz der Verhältnismäßigkeit entsprechen.

Soweit sich die Verfassungsbeschwerde gegen § 113 Abs. 1 Satz 1 TKG gerichtet hat, wurde sie zurückgewiesen mit der Maßgabe, dass die Vorschrift in Übereinstimmung mit den Gründen der Entscheidung verfassungskonform auszulegen ist und damit nur in Verbindung mit qualifizierten Rechtsgrundlagen für den Datenabruf und nicht zur Zuordnung dynamischer IP-Adressen angewendet werden darf. Übergangsweise, längstens jedoch bis zum 30. Juni 2013, darf die Vorschrift auch unabhängig von diesen Maßgaben angewendet werden.
Der Beschluss hat somit auch für Thüringen die Auswirkung, dass Datenabrufe durch die Sicherheitsbehörden nur unter den vom Bundesverfassungsgericht genannten Voraussetzungen erfolgen dürfen.

Zu2:
Das manuelle Auskunftsverfahren gemäß § 113 Abs. 1 Satz 1 TKG betrifft die vom Diensteanbieter erhobenen und verwendeten Bestandsdaten nach § 95 TKG sowie die Daten, die nach § 111 TKG für Auskunftsersuchen der Sicherheitsbehörden vorzuhalten sind.
Im strafrechtlichen Ermittlungsverfahren können Auskunftsersuchen nach den strafprozessualen Regelungen (§ 100g Strafprozessordnung [StPO] oder der Generalklausel §§ 161,163 StPO) erfolgen.
Im Bereich der Gefahrenabwehr können Auskunftsersuchen nach den Vorschriften des Thüringer Polizeiaufgabengesetzes (PAG) erfolgen. In Betracht kommt die Generalermittlungsklausel nach § 31 Abs. 1 in Verbindung mit § 32 Abs. 1 Nr. 1 PAG.
Im Bereich des Verfassungsschutzes sind ebenfalls Auskunftsersuchen nach § 5 Abs. 4 Thüringer Verfassungsschutzgesetz möglich.
In Anbetracht der Übergangsregelung sind die Auskünfte noch auf der Grundlage der genannten Generalklauseln möglich.

Zu 3.:
Die Identifizierung der dynamischen IP-Adresse, die den Bestandsdaten zuzuordnen ist, ist nach dem Beschluss des Bundesverfassungsgerichts grundsätzlich nicht mehr auf der Grundlage der oben genannten Generalklauseln möglich, jedoch übergangsweise bis zum 30. Juni 2013 noch zugelassen .

Zu 4.:
Die Abfrage der Zugangscodes kann nach den Ausführungen des Bundesverfassungsgerichts (juris Rn. 184 ff.) bezogen auf das strafrechtliche Ermittlungsverfahren bereits unter der Voraussetzung des § 161 Abs. 1 StPO zulässig sein, auch wenn die mit der Abfrage erstrebte Nutzung der Daten an weitergehende Voraussetzungen gebunden wäre. Bei der Gefahrenabwehr kommt eine Abfrage auf der Grundlage der bereits genannten Generalklausel im Thüringer Polizeiaufgabengesetz – siehe oben Antwort zu Frage 2 – ebenfalls in Betracht. Erforderlich ist allerdings für eine effektive Strafverfolgung und Gefahrenabwehr lediglich, die Auskunftserteilung über die Zugangssicherungen an diejenigen Voraussetzungen zu binden, die bezogen auf den in der Abfragesituation konkret erstrebten Nutzungszweck – vgl. dazu BVerfG, juris, Rn. 184 f. – zu erfüllen sind. Dies ist in der Übergangszeit zu beachten.

Die praktische Verfahrensweise ist Gegenstand einer entsprechenden Anfrage des Thüringer Landesbeauftragten für den Datenschutz (TLfD) an das Thüringer Innenministerium und Thüringer Justizministerium.

Zu 5.:
Dem TLfD sind Grundrechtsverletzungen bei Thüringer Bürgerinnen und Bürgern mangels Umsetzung des Beschlusses nicht bekannt geworden. Es liegen derzeit keine diesbezüglichen Beschwerden oder Anfragen vor. Dessen ungeachtet ist die Beobachtung der Umsetzung der Bundesverfassungsgerichtsentscheidung durch die Sicherheitsbehörden vom TLfD hinterfragt worden. Antworten hierzu stehen noch aus. Soweit sich Maßnahmen auf die übergangsweise geltenden Rechtsgrundlagen stützen können, liegt zwar ein Grundrechtseingriff vor, der jedoch verfassungsrechtlich gerechtfertigt ist.

Zu 6.:
Die Schaffung normenklarer Befugnisnormen zur Rechtfertigung der thematisierten Abrufmöglichkeiten liegt im Aufgabenbereich des Parlaments bzw. der zuständigen Landesregierung. Für eine Unterstützung des Landtags steht der TLfD jederzeit zur Verfügung. Auch wird der TLfD – bei einer Beteiligung – zu gegebener Zeit zu entsprechenden Gesetzesvorhaben – selbstverständlich auch beratend – Stellung nehmen. Auf die Antwort zu Frage 1 wird zudem verwiesen.

Zu7.:
Hinsichtlich des Zeitpunkts einer gegebenenfalls erforderlichen Umsetzung des Beschlusses des Bundesverfassungsgerichts liegen dem TLfD derzeit noch keine Kenntnisse vor.

Zu 8.:
Die Sicherheitsbehörden wurden vom TLfD angeschrieben und um entsprechende Auskünfte zu den sich stellenden Problemen gebeten. In Auswertung der Antworten kann sich weiterer Handlungsbedarf für den TLfD ergeben. Soweit durch die Landesregierung oder das Parlament Gesetzesänderungsbedarf gesehen wird, weil sonst zumindest nach Ablauf der Übergangsfrist bestimmte Datenabrufe nicht mehr möglich wären, stehe ich gerne unterstützend zur Verfü-

gung. Sollte der Gesetzesänderungsbedarf nicht erkannt werden, wird der TLfD hierauf hinweisen.

Anlage 25

Anfrage 2 des Abgeordneten Meyer (BÜNDNIS 90/DIE GRÜNEN)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz
Thüringer Landtag Drucksache 5/5136 vom 18. Oktober 2012

Aktenvernichtung im Landeskriminalamt

Die **Anfrage 2** vom 3. September 2012 hat folgenden Wortlaut:

Innenminister Geibert hat die Vernichtung von Akten der Soko "Rechte Gewalt" im Landeskriminalamt verteidigt. Wie etwa der MDR berichtete, hätten die Akten laut Geibert entsprechend der Vorschriften nach einigen Jahren vernichtet werden müssen.

Nach einem Bericht der Thüringer Allgemeinen vom 3. August 2012 beabsichtigt der Thüringer Datenschutzbeauftragte, die Aktenverwaltung im Geschäftsbereich des Innenministeriums einer Prüfung zu unterziehen. Seine Behörde habe sich eingeschaltet, um herauszufinden, was konkret mit den Akten passiert sei. Er hat sich ferner skeptisch gezeigt, dass bei den vernichteten Akten die erforderlichen Aufbewahrungsfristen abgelaufen seien. Vor einem solchen Schritt sei zu prüfen, ob das Löschen Interessen Dritter berühre. So stünde das Beweisinteresse des NSU-Untersuchungsausschusses dem Vernichten der Akten entgegen. Zudem müssten in Thüringen Akten vor einer endgültigen Vernichtung dem Staatsarchiv angeboten werden.

Ich frage den Datenschutzbeauftragten:

1. Welche konkreten Schritte hat der Datenschutzbeauftragte gegenüber dem Innenministerium und dem Landeskriminalamt unternommen? Wie ist der Stand der Prüfungen?
2. Mit welchen konkreten Rechtsvorschriften hat das Innenministerium bzw. das Landeskriminalamt die Aktenvernichtung begründet?
3. Wie bewertet der Datenschutzbeauftragte die Begründung des Innenministers zu der Aktenvernichtung?

4. Sofern die Aktenvernichtung auf internen Verwaltungsvorschriften beruht, reichen diese aus oder bedarf es einer materiell-gesetzlichen Regelung?
5. Können die vom Innenminister zur Rechtfertigung angegebenen Rechtsvorschriften das Thüringer Archivgesetz verdrängen? Welche datenschutzrechtlichen Rechtsfolgen hätte ein Verstoß gegen das Archivgesetz?

Der **Thüringer Landesbeauftragte für den Datenschutz** hat die Anfrage mit Schreiben vom 18. Oktober 2012 wie folgt beantwortet:

Zu 1.:
Nachdem Ende Juli 2012 bekannt geworden war, dass Akten der Sonderkommission Rechte Gewalt nicht auffindbar waren, hat der Thüringer Landesbeauftragte für den Datenschutz (TLfD) mit Schreiben vom 27. Juli 2012 Fragen an das Thüringer Innenministerium (TIM) gerichtet. Dies umfasste auch die Frage, auf welcher konkreten Rechtsgrundlage und nach welcher konkreten Aufbewahrungsfrist gegebenenfalls eine Löschung vorgenommen wurde und ob die Unterlagen vor der Löschung dem zuständigen Archiv zur Übernahme angeboten wurden. Nach der Stellungnahme des TIM nach Beteiligung des Thüringer Landeskriminalamts (TLKA) vom 11. Oktober 2012 haben die Recherchen dazu geführt, dass noch Unterlagen im Aktenbestand des TLKA sowohl in Papier als auch in elektronischer Form vorhanden sind. Zu weiteren Unterlagen bzw. Ermittlungsverfahren war ein polizeilicher Aktenrückhalt wegen Ablaufs der Aufbewahrungsfristen nicht mehr vorhanden. Zu den Aussonderungsfristen und zur Archivanbietung verweise ich auf die Antwort zu Frage 5.
Die Organisationsakte der Sonderkommission im TIM ist nach den Ausführungen vermutlich ausgesondert worden. Ich habe nochmals differenziert zu vorhandenen Akten im TIM und ob diese vor einer Löschung durch das TIM dem zuständigen Staatsarchiv zur Übernahme angeboten wurden, nachgefragt. Eine Antwort stand bis Redaktionsschluss noch aus.

Zu 2.:
Ermittlungsakten mit bekannten Tätern unterliegen den Aufbewahrungs- und Löschfristen nach § 2 der Thüringer Verordnung der Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolP-

rüffristVO) sowie der Dienstanweisung Kriminalaktennachweis (DA KAN).
Akten zu Ermittlungsverfahren mit unbekannten Tätern werden so lange aufbewahrt, bis die Verfolgungsverjährung für das zu Grunde liegende Delikt eintritt. Dies ist unproblematisch, da das Verfahren keine Beschuldigtendaten enthält.
Die Organisationsakte der Sonderkommission Rechte Gewalt stellte allgemeines Schriftgut dar, welches einer Aufbewahrungsfrist von zwei Jahren nach der Richtlinie zum Umgang mit dienstlichem Schriftgut sowie zur Akten- und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei vom 1. April 2004 (RLAktenThürPol) unterlag. Insoweit ist eine Aussonderung der Akte nach Ablauf der Aussonderungsprüffrist zum 31. Dezember 2004 anzunehmen.
Die Aussonderungslisten unterliegen ebenfalls einer Aussonderungsprüffrist von zwei Jahren der Richtlinie zum Umgang mit dienstlichem Schriftgut sowie zur Akten- und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei.

Zu 3.:
Die endgültige Begründung des Innenministeriums hinsichtlich der Behandlung der Organisationsakte Sonderkommission Rechte Gewalt steht – wie erwähnt, siehe Antwort zu Frage 1 am Ende – noch aus.
Die Behandlung dieser Akte im Thüringer Landeskriminalamt entspricht nach derzeitigem Kenntnisstand den rechtlichen Vorschriften.

Zu 4.:
Eine umfassende materiell-gesetzliche Regelung zu Löschfristen wäre wünschenswert, jedoch ist diese nicht zuletzt wegen der Differenzierungen und des Umfangs einer Rechtsverordnung vorbehalten (§ 45 Abs. 2 Satz 2 Thüringer Polizeiaufgabengesetz [ThürPAG]).

Zu 5.:
Nach § 45 Abs. 5 ThürPAG können die zu löschenden Datenträger bzw. die zu vernichtenden Unterlagen dem Staatsarchiv zur Übernahme übergeben werden, soweit archivrechtliche Regelungen dies vorsehen. Dies ist durch §§ 3 und 11 Thüringer Archivgesetz (ThürArchivG) umgesetzt. Danach sind grundsätzlich alle Unterla-

gen anzubieten. Die Einstufung, ob die Unterlagen archivwürdig sind und übernommen werden, obliegt grundsätzlich dem Archiv (§ 12 ThürArchivG). Es können jedoch Vereinbarungen getroffen werden, die ein Bewertungsverfahren durch die Stelle (hier: TLKA) selbst festlegen (§ 13 ThürArchivG). Dies ist im Bereich des TLKA für Akten der Polizei gemäß § 13 Abs. 1 ThürArchivG bereits im August 2002 erfolgt. Das TIM hat mitgeteilt, dass diese Vereinbarung durch das TLKA eingehalten wurde. Ich habe auch nach Rücksprache mit dem Thüringer Hauptstaatsarchiv keine Anhaltspunkte dafür, dass dem nicht so wäre. Insoweit erübrigt sich die Frage, ob die vom Innenminister zur Rechtfertigung angegebenen Rechtsvorschriften des Thüringer Archivgesetzes verdrängen.

Sowohl das Thüringer Datenschutzgesetz (ThürDSG) als auch das Thüringer Polizeiaufgabengesetz enthalten die Vorschrift, dass Unterlagen vor ihrer Löschung dem Archiv anzubieten sind. Sollte dem nicht nachgekommen werden, ist dies als Verstoß auch gegen datenschutzrechtliche Vorschriften zu bewerten, was nach § 39 ThürDSG beanstandet werden kann.

Anlage 26

Anfrage 3 des Abgeordneten Meyer (BÜNDNIS 90/DIE GRÜNEN)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz
Thüringer Landtag Drucksache 5/5143 vom 19. Oktober 2012

Sanktionsmöglichkeiten im öffentlichen Bereich

Die **Anfrage 3** vom 20. September 2012 hat folgenden Wortlaut:

Auf der Internetseite des Thüringer Landesbeauftragten für den Datenschutz (TLfD) findet sich eine Pressemeldung vom 24. Juni 2012, wonach der TLfD mehr Sanktionsmöglichkeiten für Kontrollen der öffentlichen Verwaltung fordere. Derzeit habe er kaum ein Druckmittel in der Hand. Der TLfD wird wie folgt zitiert: "Bei Beanstandungen bin ich auf die Mithilfe der Aufsichtsbehörden wie dem Landesverwaltungsamt angewiesen." Die Zusammenarbeit laufe aber bisweilen ins Leere. Bei Prüfungen im Bereich der Privatwirtschaft könne er auch Bußgelder in Höhe von bis zu 300 000 Euro verhängen.

In einem Artikel der Zeitschrift der Südthüringer Wirtschaft, auf der Internetseite des TLfD veröffentlicht, wird der TLfD dahingehend zitiert, er wolle von der Möglichkeit, im nichtöffentlichen Bereich mit dem eisernen Besen Ordnung zu schaffen, keinen Gebrauch machen. Hingegen wird der TLfD in einem Artikel der Thüringer Allgemeine vom 9. Juni 2012 (ebenfalls auf der Internetseite des TLfD) hinsichtlich der Übernahme der Kontrolle über den nichtöffentlichen Bereich wie folgt zitiert: "Wir fangen praktisch bei null an." Danach habe sich bis zum Aufgabenwechsel das Landesverwaltungsamt um den nichtöffentlichen Bereich "mit der geballten Kraft einer Dreiviertelstelle" gekümmert.

Ich frage den Datenschutzbeauftragten:

1. Wie wird derzeit die vom Landesverwaltungsamt übernommene Kontrolle des nichtöffentlichen Bereichs personell und organisatorisch sichergestellt?

2. Welche Defizite bestehen und bestanden bei der datenschutzrechtlichen Kontrolle des nichtöffentlichen Bereichs in Thüringen?
3. Weshalb fordert der TLfD Sanktionsmöglichkeiten für den öffentlichen Bereich und damit zusätzliche Aufgaben, wenn er gleichzeitig für den nichtöffentlichen Bereich "bei null anfange" und von den dortigen Sanktionsmöglichkeiten keinen Gebrauch machen wolle?
4. Welche konkreten Beanstandungen des TLfD liegen vor, bei denen die "Zusammenarbeit mit den Aufsichtsbehörden" wie dem Landesverwaltungsamt ins Leere lief?
5. Welche obersten Landesbehörden haben Beanstandungen des TLfD ignoriert und in welchen Fällen?
6. Hat sich der TLfD in den unter Frage 4 fallenden Vorgängen an das Innenministerium oder andere oberste Aufsichtsbehörden zwecks Abhilfe gewandt? Wenn ja, mit welchen Resultaten? Wenn nein, warum nicht?

Der **Thüringer Landesbeauftragte für den Datenschutz** hat die Anfrage mit Schreiben vom 19. Oktober 2012 wie folgt beantwortet:

Zu 1.:
Die Sicherstellung der Aufsicht über den nichtöffentlichen Bereich stellt sich in personeller und organisatorischer Hinsicht als äußerst schwierig dar. Bis zum jetzigen Zeitpunkt wurde dem Landesbeauftragten für den Datenschutz für den nichtöffentlichen Bereich lediglich eine Stelle des gehobenen Dienstes A10 neu zur Verfügung gestellt. Da mit einer derartigen personellen Ausstattung eine wirksame Aufsicht über den nichtöffentlichen Bereich nicht zu bewältigen ist, werden die anstehenden Aufgaben von allen Mitarbeitern des Landesbeauftragten für den Datenschutz neben ihren bisherigen Aufgaben mit wahrgenommen. Die Zuordnung erfolgt korrespondierend zu der bisherigen Aufgabenwahrnehmung im öffentlichen Bereich. Da sich die Zahl der Eingaben insgesamt erheblich vergrößert hat, steht die Arbeitskraft der Behörde nicht mehr in gleicher Weise für die Kontrolle des öffentlichen Bereichs zur Verfügung wie vor dem Aufgabenzuwachs. Dadurch haben sich leider die Bearbeitungszeiten von Eingaben insgesamt, also auch im öffentlichen Bereich, erheblich verlängert und anlassunabhängige Kontrollen sind – wenn überhaupt – nur noch in sehr eingeschränktem Maße möglich.

Der Haushaltsentwurf 2013/2014 sieht für den Landesbeauftragten für den Datenschutz drei neue Stellen (1 mD/1 gD/1 hD) vor. Dies wird die personelle Situation zwar entspannen. Um wirklich effektive Arbeit leisten zu können, sind jedoch mindestens noch zwei weitere Stellen erforderlich. Da nach dem derzeit im parlamentarischen Verfahren befindlichen Thüringer Informationsfreiheitsgesetz (Drucksache 5/4986) künftig die Aufgabe des Landesbeauftragten für die Informationsfreiheit von dem Landesbeauftragten für den Datenschutz wahrgenommen werden soll, ist die Forderung nach mehr Personal noch nachdrücklicher zu stellen, wenn die Qualität und Quantität der Erledigung der vielfältigen Aufgaben nicht leiden soll.

Zu 2.:
Bei der Aufsicht über den nichtöffentlichen Bereich herrschte und herrscht ein dramatischer Personalmangel. Bis zum 9. Dezember 2012 war das Landesverwaltungsamt für die Wahrnehmung dieser Aufgabe zuständig. Dort standen insgesamt nur 0,85 Vollbeschäftigteneinheiten für die Kontrolle des gesamten nichtöffentlichen Bereichs in Thüringen zur Verfügung. Es gab und gibt aufgrund dessen nur wenige Kontrollen vor Ort. Datenschutzrechtliche Anordnungen nach § 38 Abs. 5 Bundesdatenschutzgesetz wurden bislang nicht erlassen und auch die Zahl der Bußgeldbescheide bewegte sich jährlich im niedrigen einstelligen Bereich. Aufklärungsarbeit in Form von allgemeinen Informationen, Flyern, Broschüren oder Schulungsangeboten gab es bislang nicht in ausreichender Weise. Hier versucht der Landesbeauftragte für den Datenschutz derzeit mit seinen begrenzten Mitteln, Boden wiedergutzumachen, um das Datenschutzbewusstsein im nichtöffentlichen Bereich zu stärken.

Zu 3.:
Das Datenschutzbewusstsein ist im öffentlichen Bereich durch die bisherige (Aufklärungs-)Arbeit des Landesbeauftragten für den Datenschutz gestiegen und insgesamt gesehen durchaus zufriedenstellend. Hierzu beigetragen haben die Veröffentlichungen im Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die stetige Kommunikation mit den zuständigen Stellen. Die Mehrzahl der der Kontrolle des Landesbeauftragten für den Datenschutz unterliegenden öffentlichen Stellen bezieht diesen entweder vorab in

anstehende datenschutzrechtliche Entscheidungen mit ein oder ist bei einem Einschreiten bemüht, rechtskonforme Zustände herzustellen. Dies gilt aber leider nicht für alle öffentlichen Stellen. Einige verantwortliche Stellen – und in einigen Fällen auch die zuständigen Aufsichtsbehörden – teilen die Rechtsauffassung des Landesbeauftragten für den Datenschutz nicht und kommen seinen Forderungen nicht nach. In diesem Fall der Rechtsunsicherheit für die Betroffenen besteht – anders als im nichtöffentlichen Bereich – nicht die Möglichkeit, einen Anordnungs- oder Bußgeldbescheid zu erlassen, der dann der gerichtlichen Prüfung unterliegt. Außerdem ist die Auseinandersetzung mit den Aufsichtsbehörden in strittigen Fällen mit einem hohen zeitlichen Aufwand verbunden.
Der Landesbeauftragte für den Datenschutz beabsichtigt nicht, im nichtöffentlichen Bereich von seinen Sanktionsmöglichkeiten keinen Gebrauch zu machen. Sofern dies erforderlich ist, wird er mit den ihm zur Verfügung stehenden Mitteln das geltende Datenschutzrecht durchsetzen. Die seiner Aufsicht unterliegenden Stellen sollen aber vor der Durchführung von anlasslosen Kontrollen über die datenschutzrechtlichen Anforderungen informiert werden. Angesichts der bisherigen Abstinenz der Datenschutzaufsicht erscheint dies geboten. In zeitnahem Anschluss daran wird von den Sanktionsmöglichkeiten natürlich Gebrauch gemacht werden.

Zu 4.:
Vorbemerkung:
Die in dem Einleitungstext der Anfrage zitierte Auffassung, dass die Zusammenarbeit bisweilen ins Leere laufe, darf nicht allein im Zusammenhang mit Beanstandungen gesehen werden. Insgesamt ist das vom Thüringer Datenschutzgesetz vorgesehene Beanstandungsverfahren schwerfällig. Da das dem Landesbeauftragten für den Datenschutz zur Verfügung stehende schärfste Schwert die Beanstandung ist, wird von ihr nur Gebrauch gemacht, wenn eine öffentliche Stelle sich nach zähen Verhandlungen und dem Ringen um tragfähige Kompromisse nicht bereit zeigt, den Forderungen des Landesbeauftragten für den Datenschutz nachzukommen. In diesem Fall spricht der Landesbeauftragte für den Datenschutz eine Beanstandung aus. Wird die Beanstandung nicht innerhalb der gesetzten Frist behoben, fordert er von der Aufsichtsbehörde binnen angemessener Frist geeignete Maßnahmen. Hier ist also im Verfahren nochmals das Verstreichen zweier weiterer Fristen erforderlich. Zudem sind mitunter

weitere mühsame Verhandlungen mit den Aufsichtsbehörden vonnöten. Mit dem Erlass eines Bescheides wäre hingegen ein rechtssicherer Zustand oftmals schneller zu schaffen und die öffentliche Stelle hätte im gerichtlichen Verfahren die Möglichkeit, die Rechtsauffassung des Landesbeauftragten für den Datenschutz durch eine weitere unabhängige Stelle prüfen zu lassen. In der geplanten EU-Datenschutz-Grundverordnung sind die angemessenen Sanktionsmöglichkeiten für den öffentlichen und den nichtöffentlichen Bereich identisch.

Dies vorangestellt werden nun die in jüngerer Zeit betroffenen Beanstandungen benannt:

a) Beanstandung der Verwaltungsgemeinschaft (VG) Rennsteig wegen unzulässiger Datenerhebung in Zusammenhang mit der Fremdenverkehrssatzung
Aufsichtsbehörde: Landratsamt Ilm-Kreis
b) Beanstandung der Gemeinde Ichtershausen wegen unzulässiger Videoüberwachung im Freibad
Aufsichtsbehörde: Landratsamt Ilm-Kreis
c) Beanstandung der Stadt Stadtilm wegen mangelnder Unterstützung des Landesbeauftragten für den Datenschutz
Aufsichtsbehörde: Landratsamt Ilm-Kreis
d) Beanstandung der Stadt Stadtlengsfeld wegen mangelnder Unterstützung des Landesbeauftragten für den Datenschutz
Aufsichtsbehörde: Landratsamt Wartburgkreis
e) Beanstandung der Stadt Ruhla wegen Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten
Aufsichtsbehörde: Landratsamt Wartburgkreis
f) Beanstandung der Stadt Schkölen wegen mangelnder Unterstützung des Landesbeauftragten für den Datenschutz
Aufsichtsbehörde: Landratsamt Saale-Holzland-Kreis
g) Beanstandung der Stadt Jena wegen der Veröffentlichung von Personaldaten im Internet
Aufsichtsbehörde: Thüringer Landesverwaltungsamt

Zu 5.:
Beanstandungen oberster Landesbehörden haben diese bislang nicht ignoriert.

Zu 6.:

a) Der Landesbeauftragte für den Datenschutz hat sich, nachdem das Landesverwaltungsamt zwar einen datenschutzrechtlichen Verstoß gesehen hat, aber nicht aufsichtlich tätig werden wollte, an das Innenministerium gewandt. Hierzu wird zunächst auf die Veröffentlichungen des Landesbeauftragten für den Datenschutz im 8. Tätigkeitsbericht (Nummer 5.7) und im 9. Tätigkeitsbericht (Nummer 5.8) verwiesen. Das Innenministerium teilte mit, dass die zuständige Rechtsaufsichtsbehörde die Entscheidung über die Einleitung rechtsaufsichtlicher Maßnahmen nach pflichtgemäßem Ermessen getroffen habe. Außerdem sei die Datenerhebung mittlerweile eingestellt worden. Dies wird der Landesbeauftragte für den Datenschutz in einer neuerlichen Kontrolle in Kürze überprüfen.

b) Nein; zum einen ist die nächsthöhere zuständige Aufsichtsbehörde zunächst das Landesverwaltungsamt, zum anderen ist der Landesbeauftragte noch im Dialog mit der zuständigen Aufsichtsbehörde, da deren Führung gewechselt hat.

c) Nein; zum einen ist die nächsthöhere zuständige Aufsichtsbehörde zunächst das Landesverwaltungsamt, zum anderen zeigte sich im weiteren Verlauf die Stadt Stadtilm kooperativ. An der Umsetzung der Forderungen wird gearbeitet.

d) Nein; zum einen ist die nächsthöhere zuständige Aufsichtsbehörde zunächst das Landesverwaltungsamt, zum anderen zeigte sich im weiteren Verlauf die Stadt Stadtlengsfeld kooperativ; die Kontrolle ist mittlerweile abgeschlossen

e) Nein; zum einen ist die nächsthöhere zuständige Aufsichtsbehörde zunächst das Landesverwaltungsamt, zum anderen zeigte sich im weiteren Verlauf die Stadt Ruhla kooperativ. An der Umsetzung der Forderungen wird gearbeitet.

f) Nein; zum einen ist die nächsthöhere zuständige Aufsichtsbehörde zunächst das Landesverwaltungsamt, zum anderen ist die Stadt Schkölen mittlerweile Mitglied der VG Heideland-Elstertal-Schkölen.

g) Ja; das Innenministerium folgte der differenzierenden Auffassung des Landesbeauftragten für den Datenschutz nicht. Hierzu wird auf die Veröffentlichungen des Landesbeauftragten für den Datenschutz im 8. Tätigkeitsbericht (Nummer 5.3, S. 39) verwiesen. Das Innenministerium geht indes generell davon aus, dass die Veröffentlichung von Kontaktdaten behördlicher Mitarbeiter im Internet grundsätzlich keiner Rechtsgrundlage bedarf.

Anlage 27

Anfrage 4 des Abgeordneten Bergner (FDP)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz
Thüringer Landtag Drucksache 5/5454 vom 9. Januar 2013

Angabe des Übernachtungsgrundes für Gäste in Thüringen

Die **Anfrage 4** vom 27. November 2012 hat folgenden Wortlaut:

Das Bundesverwaltungsgericht (BVerwG) in Leipzig urteilte am 11. Juli 2012, dass Kommunen keine pauschale Bettensteuer auf Hotelübernachtungen erheben dürfen. In den Urteilen wird klargelegt, dass es einen Unterschied zwischen privaten und berufsbedingten Übernachtungen gibt. Von Touristen dürfe die Abgabe als sogenannte Aufwandsteuer verlangt werden, von Geschäftsreisenden nicht (Az.: BVerwG 9 CN 1.11 und 9 CN 2.11). Aufgrund der Entscheidungen planen mehrere Kommunen, ihre Satzungen rückwirkend rechtskonform auszugestalten. Der Übernachtungsgrund der Gäste soll nach einem Pressebericht vom 27. November 2012 (Thüringer Allgemeine) durch Fragebögen oder durch das Vorzeigen eines Dienstreiseantrags ermittelt werden.

Ich frage den Datenschutzbeauftragten:

1. Ist eine solche Ermittlung des Übernachtungsgrundes durch einen Hotelier datenschutzrechtlich zulässig? Wie begründet der Thüringer Datenschutzbeauftragte seine diesbezügliche Meinung?
2. Falls die Ermittlung des Übernachtungsgrundes datenschutzrechtlich zulässig ist, welche Rechtsgrundlage kommt hierfür in Betracht?
3. Falls die Ermittlung solcher Daten nicht zulässig ist, ist die Erhebung einer Bettensteuer unter der Einhaltung des Urteils des BVerwG nach Ansicht des Thüringer Datenschutzbeauftragten noch möglich? Wie begründet der Thüringer Datenschutzbeauftragte seine diesbezügliche Meinung?
4. Wenn die Ermittlung der Übernachtungsdaten zulässig sein sollte, ist die Ausweitung der Datenerhebung auf den Über-

nachtungsgrund im Sinne der Datensparsamkeit wünschenswert?

Der **Thüringer Landesbeauftragte für den Datenschutz** hat die Anfrage mit Schreiben vom 17. Dezember 2012 (Eingang: 9. Januar 2013) wie folgt beantwortet:

Zu 1. bis 4.:
Für die Frage nach der Zulässigkeit der Datenerhebung ist zunächst entscheidend, ob der Hotelier als öffentliche Stelle oder als nichtöffentliche Stelle tätig wird. Zwar handelt es sich bei einem Hotelinhaber in aller Regel um eine Person des privaten Rechts, auf die die Bestimmungen des Bundesdatenschutzgesetzes Anwendung finden. Die Erhebung des Übernachtungsgrundes durch die Hoteliers erfolgt aber nicht in deren eigenem geschäftlichen Interesse, sondern die Daten werden für die jeweilige Gemeinde bzw. Stadt im Rahmen der Erhebung gemeindlicher Steuern erhoben. Daher gelten die Bestimmungen des Thüringer Datenschutzgesetzes (ThürDSG). Nach § 4 Abs. 1 Satz 1 ThürDSG ist die Erhebung personenbezogener Daten durch öffentliche Stellen zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.

Eine Erlaubnisnorm für die Datenerhebung findet sich im kommunalen Steuerrecht. Nach § 5 Abs. 1 Thüringer Kommunalabgabengesetz (ThürKAG) dürfen die Gemeinden örtliche Verbrauchs- und Aufwandssteuern erheben, solange und soweit diese nicht bundesrechtlich geregelten Steuern gleichartig sind. Rechtsgrundlage für die zur Steuerfestsetzung erforderliche Datenerhebung ist eine gemeindliche Satzung, die die Voraussetzungen der §§ 2, 1 Abs. 1 ThürKAG erfüllt. Nach § 6 ThürKAG kann die Steuersatzung Dritte, die zwar nicht Steuerschuldner sind, aber in engen wirtschaftlichen Beziehungen zum Steuergegenstand oder zu einem Sachverhalt stehen, an den die Steuerpflicht oder der Steuergegenstand anknüpft, verpflichten, die Steuer zu kassieren, abzuführen und Nachweis darüber zu führen. Diese Voraussetzungen treffen auf den Inhaber eines Hotels zu, in dem der Steuerpflichtige übernachtet.

Die Datenerhebung durch den Inhaber des Hotels ist zulässig, wenn die Kommune aufgrund einer gültigen gemeindlichen Satzung eine sogenannte "Bettensteuer" auf nicht dienstliche Übernachtungen von

Hotelgästen erhebt und die Hotelinhaber in der Satzung verpflichtet werden, die Steuer zu kassieren, abzuführen und Nachweis darüber zu führen.

Eine derartige satzungsrechtliche Ermächtigung kann sich aber nur innerhalb der vom Thüringer Kommunalabgabengesetz vorgegebenen Grenzen bewegen. Die Prüfung der Steuerpflicht an sich muss Aufgabe der steuererhebenden Stelle, also der Gemeinde, bleiben. Der Hotelbetrieb darf vom Steuerpflichtigen nur die Steuer abkassieren und abführen und über diese Umstände Nachweis führen. Zur Feststellung der Steuerpflicht ist es ausreichend, wenn der Gast Angaben dazu machen muss, ob er aus dienstlichem oder privatem Anlass in der Beherbergungsstätte übernachtet. Die Prüfung des Vorliegens der Tatbestandsvoraussetzungen im Einzelnen obliegt dann der steuererhebenden Stelle. Das bedeutet, dass der Inhaber des Hotels seinen Gast nur fragen darf, ob er dienstlich oder privat bei ihm übernachtet. Eine derartige Datenerhebung entspricht auch dem Grundsatz der Datensparsamkeit.

Eine weitere Datenerhebung, beispielsweise die Erhebung von Anschriften der Arbeitgeber oder die Frage nach dem konkreten Grund des Besuches, ist unzulässig; für sie gibt es keine von § 6 ThürKAG gedeckte satzungsrechtliche Rechtsrundlage.

Anlage 28

Anfrage 5 der Abgeordneten König (DIE LINKE)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit
Thüringer Landtag Drucksache 5/6439 vom 31. Juli 2013

Überwachung öffentlicher Plätze mittels Videotechnik

Die **Anfrage 5** vom 27. Juni 2013 hat folgenden Wortlaut:

Die Rechtsanwaltskammer Thüringen zeigt sich laut einer Meldung des MDR bereits jetzt besorgt über das Ausmaß der Überwachung öffentlicher Plätze mittels Videoaufzeichnung. Von solchen Maßnahmen sind nicht nur die öffentlichen Plätze als solche, sondern auch Zugänge zu Arztpraxen, Anwaltskanzleien und andere sensible Bereiche, die einem gewissen Schutz unterliegen sollten, betroffen. Insbesondere stellt die Anwaltskammer fest, dass die Kamerasysteme keine Straftaten verhinderten und kaum abschreckende Wirkung entfalten würden.
Erst kürzlich ist die Überwachung des Bahnhofsvorplatzes in Erfurt durch eine Kameraanlage am Intercity-Hotel bekannt geworden. Andere Installationen von Videoüberwachungssystemen stießen auch in Thüringen auf breiten Widerstand der Bevölkerung und betroffener Berufsgeheimnisträger. Auch Datenschützer weisen immer wieder auf Probleme mit Videoüberwachung hin. In seinem Tätigkeitsbericht 2010/2011 beurteilt der Thüringer Landesbeauftragte für den Datenschutz das Verfahren der Videobeobachtung gegenüber der Videoaufzeichnung als weniger bedenklich hinsichtlich des Eingriffs in die informationelle Selbstbestimmung.

Ich frage den Datenschutzbeauftragten:

1. In wie vielen und welchen Fällen sowie mit jeweils welchem Ergebnis wurden Anlagen zur Videoüberwachung öffentlicher Plätze durch den Thüringer Landesbeauftragten für den Datenschutz seit 2011 auf ihre datenschutzrechtliche Zulässigkeit geprüft?

2. In wie vielen der unter Frage 1 genannten Fällen haben Arztpraxen, Anwaltskanzleien, Partei- und Abgeordnetenbüros, Büros von Gewerkschaften und Sozialverbänden, Journalistenbüros und Redaktionen oder sonstige berufsmäßige Geheimnisträger ihren Hauptzugang auf den mittels Videotechnik überwachten Plätzen, Straßenabschnitten etc.?

3. In welchen Abständen werden Installationen zur Videoüberwachung durch den Thüringer Landesbeauftragten für den Datenschutz auf ihre Übereinstimmung mit den Datenschutzgesetzen überprüft?

4. In welcher Form und unter welchen Voraussetzungen erfolgt eine datenschutzrechtliche Prüfung durch den Thüringer Landesbeauftragten für den Datenschutz bei der Installation nichtstationärer und zeitlich begrenzt eingesetzter Videokameras auf öffentlichen Plätzen?

Der **Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit** hat die Anfrage mit Schreiben vom 31. Juli 2013 wie folgt beantwortet:

Zu 1.:
Die vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) in dem von Ihnen genannten Zeitraum kontrollierten zahlreichen Videoüberwachungsanlagen haben keinen öffentlichen Platz überwacht.
Die noch nicht abgeschlossene Kontrolle der Kameraanlage am Intercity-Hotel Erfurt hat ergeben, dass es sich hierbei nicht um eine Überwachung eines öffentlichen Platzes handelt.
Soweit sich die Anfrage auf die in der kleinen Anfrage der Abgeordneten Frau Renner (DIE LINKE) an das Thüringer Innenministerium vom 16. Mai 2013 erwähnte Kamera der Polizei bezieht, verweisen wir insoweit auf die Antwort des Thüringer Innenministeriums vom 10. Juni 2013 (Drucksache 5/6352). Wie auch in dieser Antwort bereits erwähnt, hatte der TLfDI von der Installation keine Kenntnis. Laut Antwort des Thüringer Innenministeriums ist die Kamera bereits wieder deinstalliert.

Zu 2.:

Siehe Antwort zu 1

Zu 3.:
Es gibt keine Festlegungen, denen eine Regelmäßigkeit für Überprüfungen entnommen werden kann. Der TLfDI führt vielmehr Kontrollen im eigenen Ermessen durch. Diese werden zumeist ausgelöst, indem Mitarbeiter des TLfDI derartige Installationen feststellen oder sich Dritte über eine solche Videoüberwachung beschweren. Solche durchgreifenden Beschwerden zu einer Videoüberwachung von öffentlichen Plätzen liegen dem TLfDI derzeit nicht vor.

Zu 4.:
Soweit dem TLfDI derartige mobile, kurzfristig eingerichtete Videoüberwachungsanlagen bekannt werden, unterscheidet sich die datenschutzrechtliche Prüfung nicht von der bei immobilen Kameras. Grundsätzlich ist hierbei der öffentliche vom nicht-öffentlichen Bereich zu unterscheiden. Die Zulässigkeit einer Videoüberwachung öffentlicher Plätze durch nicht-öffentliche Stellen richtet sich nach § 6b BDSG. Nur unter den dort aufgeführten abschließenden Voraussetzungen ist eine solche Videoüberwachung zulässig.

Im öffentlichen Bereich richtet sich die Zulässigkeit einer solchen Videoüberwachung öffentlicher Plätze zunächst nach § 25 a Thüringer Datenschutzgesetz (ThürDSG). Wird die Videoüberwachung zur Erfüllung ordnungsbehördlicher Zwecke durchgeführt, ist die Spezialnorm des § 26 Nr. 1 OBG zu beachten.

Sowohl im öffentlichen wie auch nicht-öffentlichen Bereich ist allerdings Voraussetzung für eine Prüfung, dass durch die Videoüberwachungsanlage personenbezogene oder personenbeziehbare Daten erhoben werden. Das ist zum Beispiel nicht der Fall, wenn die entsprechenden Kameras so unscharf eingestellt werden, dass einzelne Personen oder sonstige Merkmale nicht mehr identifizierbar sind. Die Erhebung personenbezogener Daten kann des Weiteren durch Verpixelung oder Ausblendung ausgeschlossen werden.

Abschließend sei die Bemerkung gestattet, dass aus Sicht des TLfDI die Videoüberwachung durch nicht-öffentliche Stellen überproportional zunimmt und das derzeit vorherrschende Problem darstellt. Während es im Jahr 2012 noch knapp unter 90 Kameras waren, die

dem TLfDI bekannt gemacht wurden, wurde dieser Wert bereits Mitte des Jahres 2013 mit 107 Kameras deutlich übertroffen. Es ist von einer hohen Dunkelziffer auszugehen. Hierbei handelt es sich häufig um Unternehmen, die zu verschiedenen Zwecken sowohl in als auch um das Betriebsgelände herum Videoüberwachungsanlagen betreiben und diese auch zur Arbeitnehmerüberwachung nutzen.
Einen weiteren Problembereich stellt die teilweise Aufnahme des öffentlichen Verkehrsraums dar, also die partielle Aufnahme von Fußwegen oder Straßen durch Private. Ein Großteil dieser im nicht-öffentlichen Bereich betriebenen Kameras erweist sich als datenschutzrechtswidrig.

Anlage 29

Anfrage 6 des Abgeordneten Bergner (FDP)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit
Thüringer Landtag Drucksache 5/6713 vom 7. Oktober 2013

Mangelhafter Datenschutz bei Apps

Die **Kleine Anfrage 6** vom 23. August 2013 hat folgenden Wortlaut:

Das Bayerische Landesamt für Datenschutzaufsicht hat im Mai 2013 im Rahmen einer internationalen Prüfungsaktion 30 Apps bayerischer Anbieter überprüft und dabei erhebliche Mängel bei der Information über den Umgang mit Daten festgestellt.

Ich frage den Datenschutzbeauftragten:

1. Hat Thüringen durch den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) an der internationalen Prüfungsaktion teilgenommen? Falls nein, warum nicht?

2. Falls Frage 1 mit Ja beantwortet wird, wie viele und welche Apps aus Thüringen wurden dabei kontrolliert?

3. Falls Frage 1 mit Ja beantwortet wird, welche Ergebnisse konnten bei den Apps hinsichtlich der Datenschutzerklärung durch den TLfDI festgestellt werden?

4. Falls Frage 1 mit Ja beantwortet wird, welche Schlussfolgerungen bzw. Folgen zieht der TLfDI aus den Ergebnissen?

5. Falls Frage 1 mit Ja beantwortet wird, wurden Bußgelder aufgrund mangelhafter Datenschutzerklärungen verhängt? Falls ja, wie viele und in welcher Höhe?

6. Wurden durch den TLfDI andere Prüfungsaktionen von Apps durchgeführt? Wenn nein, warum nicht?

7. Falls Frage 6 mit Ja beantwortet wird, mit welchem Ergebnis? Wurden Bußgelder verhängt?

8. Sollen in Zukunft Prüfungen von Apps durch den TLfDI erfolgen? Falls ja, wann? Falls nein, warum nicht?

Der **Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit** hat die Anfrage namens der Landesregierung mit Schreiben vom 7. Oktober 2013 wie folgt beantwortet:

Zu 1.:
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat nicht an der Prüfaktion teilgenommen. Jeder Landesbeauftragte für den Datenschutz ist nur für die Unternehmen zuständig, die in seinem Land ihren Sitz haben. Dementsprechend hatte auch das Bayerische Landesamt für Datenschutzaufsicht nur Betreiber von Apps überprüft, die in Bayern ansässig sind. Da die Landesdatenschutzbeauftragten bei der Wahrnehmung ihres Amtes unabhängig sind, sprechen sie sich in aller Regel nicht über ihre Kontrollmaßnahmen ab. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat in diesem Jahr andere Prüfschwerpunkte gesetzt.

Zu 2. bis 5.:
entfällt

Zu 6.:
Es wird auf die Antwort zu Frage 1 verwiesen.

Zu 7.:
entfällt

Zu 8.:
Aktuell sind derartige Prüfungen nicht vorgesehen. Eingaben über in Thüringen ansässige Betreiber von Apps liegen nicht vor. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit verfügt verglichen mit dem Umfang seiner Aufgaben über eine sehr dünne Personaldecke. Daher werden schwerpunktmäßig Kontrollen nicht allseits, sondern in den neuralgischen Bereichen

durchgeführt; als solche sind App-Betreiber derzeit noch nicht identifiziert worden.

Anlage 30

Anfrage 7 der Abgeordneten König (DIE LINKE)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz
Thüringer Landtag Drucksache 5/6923 vom 18. November 2013

Weitergabe von Daten eines Fahrzeugnutzers an den Fahrzeugvermieter durch die Polizei

Die **Anfrage 7** vom 27. September 2012 hat folgenden Wortlaut:

Am 24. Mai 2013 demonstrierten in Eisenach etwa 250 Menschen gegen den Burschentag der "Deutschen Burschenschaft", der am gleichen Wochenende in Eisenach stattfand. Es wurde bekannt, dass das als Lautsprecherfahrzeug genutzte Fahrzeug nach der Demonstration von Polizeikräften mit Verweis auf das fehlende Blinkersetzen bei einem Abbiegevorgang angehalten und umfangreich kontrolliert wurde. Neben einem verhängten Bußgeld in Höhe von 25 Euro wegen "unzureichender Ladungssicherung" hätten die Beamten die aus der Halterabfrage neugewonnen Daten weiterverwertet und das entsprechende Mietunternehmen kontaktiert, um es darüber in Kenntnis zu setzen, dass der gemietete Wagen als Lautsprecherfahrzeug auf einer Demonstration eingesetzt wurde.
Diesen Vorgang thematisierte die Fragestellerin in der Kleinen Anfrage 3180, die mit Schreiben vom 20. September 2013 durch die Landesregierung beantwortet wurde (vgl. Drucksache 5/6673).
Die Landesregierung bestätigte grundsätzlich den Vorgang. Zur erfragten Rechtsgrundlage der Übermittlung von Daten teilte die Landesregierung mit:

"Das Mietunternehmen als Halter des Fahrzeuges wurde von dem kontrollierenden Polizeibeamten der Landespolizeiinspektion Gotha telefonisch über den Sachverhalt informiert. ... Die Polizeibeamten bezweckten mit der Information an das Mietunternehmen, dieses als Eigentümer des Wagens (eines Transporters) in die Lage zu versetzen, eine eingehende Prüfung auf Beschädigung vorzunehmen. Eine verspätete Feststellung von Schäden durch den Vermieter hätte die Durchsetzung berechtigter Rechtsansprüche wesentlich erschweren oder sogar unmöglich machen können. Aus diesem Grund wurde der

Vermieter des Fahrzeuges über die Kontrolle (ohne die Weitergabe von Personendaten) und über die Art und Weise der Anbringung von Gegenständen auf dem Dach des Transporters informiert. Rechtsgrundlage der Mitteilung bildet § 2 Abs. 2 in Verbindung mit § 12 Abs. 1 Polizeiaufgabengesetz (Schutz privater Rechte)."

Erst durch die Weitergabe der Information durch die Polizei wurde somit gegenüber der Autovermietung eine dieser bis dato unbekannten Verknüpfung des namentlich bekannten Anmieters mit der Demonstration in Eisenach hergestellt.

Ich frage den Datenschutzbeauftragten:

1. Welche Rechtsgrundlagen kommen nach Auffassung des Datenschutzbeauftragten für die durch die Landesregierung eingeräumte Übermittlung von Daten an eine nichtöffentliche Stelle in oben geschildertem Sachverhalt grundsätzlich in Frage und wie begründet der Datenschutzbeauftragte seine Auffassung?
2. Liegen jeweils für die in Frage kommenden Rechtsgrundlagen die formellen und materiellen Voraussetzungen für die durch die Landesregierung eingeräumte Übermittlung von Daten an eine nichtöffentliche Stelle in oben geschildertem Sachverhalt vor und wie begründet der Datenschutzbeauftragte seine Auffassung?
3. Wie beurteilt der Datenschutzbeauftragte die durch die Landesregierung genannte Grundlage in § 2 Abs. 2 Thüringer Polizeiaufgabengesetz (PAG) vor dem Hintergrund, dass ausweislich der Antwort der Landesregierung gar kein Schaden erkennbar und in der Folge auch kein Recht daraus ableitbar gewesen ist und sich eine auf § 2 Abs. 2 PAG beziehende Datenübermittlung lediglich auf die Mutmaßung einer Nichtausschließbarkeit eines Schadens stützte; wie begründet der Datenschutzbeauftragte seine Auffassung?
4. Teilt der Datenschutzbeauftragte im Übrigen die im Kommentar (Eber/Seel Boorberg Verlag, 6. Auflage, 2012) zu § 2 Abs. 2 PAG niedergelegte Rechtsauffassung, dass es sich hierbei nicht um eine Befugnis, sondern lediglich um eine Aufgabe handelt und die Datenübermittlung sich folg-

lich auf eine andere Befugnisnorm stützen muss (die die Landesregierung aber auf entsprechende Anfrage nicht genannt hat); wie begründet der Datenschutzbeauftragte seine Auffassung?

5. Kann der Datenschutzbeauftragte eine (konkrete) Gefahr für die öffentliche Sicherheit oder Ordnung im geschilderten Sachverhalt erkennen, die Voraussetzung für die Anwendbarkeit der von der Landesregierung als weitere Rechtsgrundlage benannten Generalklausel in § 12 Abs. 1 PAG für die Datenübermittlung ist; wie begründet er seine Auffassung?

Der **Thüringer Landesbeauftragte für den Datenschutz** hat die Anfrage mit Schreiben vom 18. November 2013 wie folgt beantwortet:

Zu 1.:
Als Rechtsgrundlage für die Übermittlung der Daten kommt ausschließlich § 41 Abs. 3 Satz 2 in Verbindung mit § 41 Abs. 3 Satz 1 Nr. 3, 2. Variante Thüringer Polizeiaufgabengesetz (ThürPAG) in Betracht.
Dies ergibt sich aus der Subsidiarität der allgemeinen Regelungen des Thüringer Datenschutzgesetzes gegenüber den bereichsspezifischen Datenschutznormen der §§ 31 bis 47 ThürPAG. Lediglich soweit in diesen Vorschriften keine besonderen Regelungen getroffen worden sind, kommt für den Bereich der polizeilichen Gefahrenabwehr das Thüringer Datenschutzgesetz (ThürDSG) zur Anwendung (vgl. § 2 Abs. 3 Satz 1 ThürDSG). In § 41 Abs. 3 Satz 2 ThürPAG findet sich eine solche besondere Regelung.
Zudem ist § 12 ThürPAG gegenüber den Normen der §§ 13 bis 47 ThürPAG subsidiär (vgl. § 12 Abs. 1 ThürPAG).

Zu 2.:
Ja; die formellen Voraussetzungen waren hier erfüllt.

Die materiellen Voraussetzungen für die Übermittlung der Daten lagen im zu beurteilenden Sachverhalt vor, da die tatbestandlichen Voraussetzungen von § 41 Abs. 3 Satz 2 in Verbindung mit Abs. 3 Satz 1 Nr. 3., 2. Variante ThürPAG erfüllt waren, die Maß-

nahme verhältnismäßig war und Ermessensfehler nicht ersichtlich sind.

Zunächst handelte es sich bei den übermittelten Informationen um personenbezogene Daten im Sinne von § 41 Abs. 3 Satz 2 ThürPAG. Als solche werden Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person bezeichnet. Eine Person ist bestimmbar, wenn ihre Identität mit Hilfe anderer verfügbarer Daten oder durch besondere äußere Umstände festgestellt werden kann. Die Angaben über die Nutzung des gemieteten Fahrzeugs als Lautsprecherfahrzeug auf einer Demonstration, die polizeiliche Kontrolle des Mietwagens und die Art und Weise der Anbringung von Gegenständen auf dem Dach des Transporters sind sachliche Verhältnisse einer bestimmbaren Person. Diese Sachverhalte sind auch ohne die Weitergabe der Personendaten konkret der anmietenden Person zuzuordnen, da das Mietwagenunternehmen den Bezug mit Hilfe der Fahrzeugdaten herstellen konnte.

Unter das Tatbestandsmerkmal der schutzwürdigen Belange einzelner fällt auch der Schutz privater Rechte (siehe dazu die Begründung zu § 41 ThürPAG aus dem Gesetzentwurf der Landesregierung in der Drucksache 1/1025, S. 40).

Vorliegend war das Eigentumsrecht des Mietunternehmens am Mietwagen aus Artikel 14 Abs. 1 Grundgesetz (GG), Artikel 34 Abs. 1 der Verfassung des Freistaats Thüringen hier zumindest tangiert. Dies ergibt sich aus dem zu Grunde zu legenden Sachverhalt, wonach die den Mietwagen kontrollierenden Polizeibeamten vor Beginn der Versammlung beobachtet hatten, wie auf dem Dach des Mietwagens eine so genannte "Euro-Palette" und ein Lautsprecher darauf befestigt wurden und dafür mindestens eine Person das Dach des Fahrzeuges betrat.

Eine darüber hinausgehende (abstrakte oder konkrete, vgl. § 54 Nr. 3 Ordnungsbehördengesetz - OBG -) Gefahr ist für die Annahme von schutzwürdigen Belangen nicht erforderlich. Dies ergibt sich aus einem Vergleich des Wortlauts von § 41 Abs. 3 Satz 1 Nr. 2 ThürPAG mit dem Wortlaut von § 41 Abs. 3 Satz 1 Nr. 3 ThürPAG: Hätte der Gesetzgeber in § 41 Abs. 3 Satz 1 Nr. 3 ThürPAG das Vorliegen einer Gefahr als

Tatbestandsmerkmal vorausgesetzt, so hätte er dies, wie im Fall von § 41 Abs. 3 Satz 1 Nr. 2 ThürPAG geschehen, in die genannte Regelung aufgenommen. Das ist aber nicht der Fall.

Die Übermittlung der genannten personenbezogenen Daten an das Mietunternehmen war hier erforderlich, da keine andere, gleich geeignete Maßnahme, die weniger belastend gewesen wäre, ersichtlich ist. Hätte der Polizeibeamte die Daten über die Art und Weise der Anbringung von Gegenständen nicht übermittelt, hätten mögliche Schäden am Dach des Fahrzeuges nicht gesichtet werden können. Zudem ist die Maßnahme verhältnismäßig im engeren Sinne, da hier das Recht auf informationelle Selbstbestimmung aus Artikel 2 Abs. 1 GG in Verbindung mit Artikel 1 Abs. 1 GG, Artikel 6 Abs. 2 der Verfassung des Freistaats Thüringen gegenüber der Eigentumsgarantie aus Artikel 14 Abs. 1 GG, Artikel 34 Abs. 1 der Verfassung des Freistaats Thüringen zurücktreten muss. Die dem Vermieter übermittelten Daten betrafen lediglich die "Sozialsphäre" des Anmietenden, da zumindest die Nutzung als Lautsprecherfahrzeug, das Anbringen der Europalette und das Betreten des Daches öffentlich durchgeführt wurde und somit ohnehin von jedem, der sich vor Ort befand, bemerkbar war.
Fehler bei der Ermessensausübung sind nicht ersichtlich.

Zu 3.:
Es wird auf die Antwort zur Frage 1 verwiesen. Als Rechtsgrundlage für das genannte Handeln der Polizei ist ausschließlich § 41 Abs. 3 Satz 2 ThürPAG in Verbindung mit § 41 Abs. 3 Satz 1 Nr. 3, 2. Variante ThürPAG zu Grunde zu legen.

Zu 4.:
Ja; es wird auf die Antworten zu Fragen 1 und 2 verwiesen.

Zu 5.:
Der Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit vermag in dem zu Grunde zu legenden Sachverhalt, wie er in der Antwort der Landesregierung in der Drucksache 5/6673 auf die Kleine Anfrage 3180 der Fragestellerin geschildert worden ist, noch keine konkrete Gefahr für die öffentliche Sicherheit oder Ordnung zu erkennen.

Eine konkrete Gefahr liegt gemäß § 54 Nr. 3 Buchst. a OBG vor, wenn eine Sachlage besteht, bei der im einzelnen Falle die hinreichende Wahrscheinlichkeit besteht, dass bei ungehindertem Fortgang in absehbarer Zeit ein Schaden für die öffentliche Sicherheit und Ordnung eintreten wird.
Laut Antwort der Landesregierung auf die Frage 8 der Kleinen Anfrage 3180 konnte es im hier zu beurteilenden Sachverhalt "nicht ausgeschlossen werden", dass der Wagen aufgrund der Befestigung der Europalette und des Lautsprechers auf dem Dach des Mietfahrzeugs beschädigt wurde.
Diese Angaben reichen indes für die hinreichend wahrscheinliche Annahme eines Schadens in überschaubarer Zukunft nicht aus. Zu verlangen ist vielmehr, dass neben den geschilderten Beobachtungen der Polizeibeamten mindestens ein weiteres Indiz für einen Schadenseintritt am Mietfahrzeug vorliegt.

Anlage 31

Anfrage 8 der Abgeordneten Leukefeld (DIE LINKE)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit
Thüringer Landtag Drucksache 5/7180 vom 15. Januar 2014

Datenschutz und Informationsfreiheit im Rahmen des SGB II

Die **Anfrage 8** vom 26. November 2013 hat folgenden Wortlaut:

Die in Thüringen für die Leistungen nach dem Zweiten Buch Sozialgesetzbuch (SGB II) zuständigen kommunalen Träger und die gemäß § 6 a SGB II zugelassenen kommunalen Träger erheben gemäß § 51 b Abs. 1 SGB II laufend die für die Durchführung der Grundsicherung für Arbeitsuchende erforderlichen Daten und übermitteln diese gemäß den Regelungen nach § 51 b Abs. 4 SGB II an die Bundesagentur für Arbeit. Gemäß § 52 SGB II überprüfen die zugelassenen kommunalen Träger in Thüringen Personen, die Leistungen nach dem SGB II beziehen im Wege des automatisierten Datenabgleichs. Seit dem Inkrafttreten des SGB II gab es fortgesetzt und wiederholt auch aus datenschutzrechtlichen Erwägungen heraus Kritik an der Ausgestaltung der Kontroll- und Durchgriffsrechte. So wurden unter anderem die umfassenden Auskunftspflichten im Beantragungsverfahren, die von vielen als "Durchleuchtung" empfunden wurden, aber auch die Praxis von überprüfenden Hausbesuchen hinterfragt. Gerade letzteres wird von vielen Betroffenen als ein Verstoß gegen Artikel 13 des Grundgesetzes bzw. Artikel 8 der Verfassung des Freistaats Thüringen ("Unverletzlichkeit der Wohnung") erlebt. Im Rahmen der derzeitigen Bemühungen mittels einer Bund-Länder-Arbeitsgruppe zu einer Rechtsvereinfachung im SGB II zu gelangen, hat die Bundesagentur für Arbeit eine Reihe eigener Reformvorschläge präsentiert (PEG 21 - II-8400, siehe Anlage). Dabei werden zahlreiche weitere Kontrollmechanismen in Form von Datenabgleichen eingefordert. Zugleich halten sich Arbeitsagenturen und Jobcenter ausgesprochen bedeckt, wenn es um eine transparente Außendarstellung geht. So sind zahlreiche Fälle belegt, bei denen erst juristische Verfahren (u. a. Verwaltungsgericht Leipzig Az.: 5 K 981/11 - Zugänglichkeit von Telefondaten nach dem Informationsfreiheitsgesetz für von Leistungsberechtigten mandatierte Anwälte) oder starker

politischer Druck Jobcenter dazu bewegten im Rahmen des Informationsfreiheitsgesetzes ihren Verpflichtungen nachzukommen.

Ich frage den Datenschutzbeauftragten:

1. Wie beurteilen Sie aus datenschutzrechtlicher Sicht die zur Zeit bestehenden Möglichkeiten der Thüringer Behörden die Überlassung und Vorlage von Informationen und Unterlagen zu verlangen sowie die bestehenden Durchgriffs- und Kontrollmöglichkeiten, die jeweils im Rahmen des SGB II implementiert wurden?

2. Inwiefern gibt es bei bzw. für die zuständigen Thüringer Behörden Festlegungen, z. B. in Form von Ausführungsbestimmungen oder Verwaltungsvorschriften und wie werden diese datenschutzrechtlich überprüft?

3. Inwiefern gab es in der Vergangenheit in Thüringen aus datenschutzrechtlicher Sicht Beschwerden bzw. Beanstandungen hinsichtlich der Umsetzung des SGB II durch Thüringer Behörden? Welche Konsequenzen wurden von den verschiedenen Beteiligten gegebenenfalls aus den Beschwerden bzw. Beanstandungen gezogen?

4. Wie beurteilen Sie aus datenschutzrechtlicher Sicht die von den Thüringer Behörden anzuwendenden Vorschriften zum automatischen Datenabgleich bzw. zur Überprüfung von Daten (vgl. §§ 52, 52 a SGB II) sowie die Möglichkeit der Abfrage von Kontendaten der Antragstellerinnen und Antragsteller bzw. Bezieherinnen und Bezieher durch die bzw. bei der sogenannten "Kontenevidenzzentrale" gemäß § 93 Abs. 8 Satz 1 Nr. 1 Abgabenordnung?

5. In welcher Art und Weise beabsichtigt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit die weitere Diskussion und Umsetzung der in der Bund-Länder-Arbeitsgruppe von der Bundesagentur für Arbeit präsentierten Änderungsvorschläge zu begleiten?

6. Wie beurteilen Sie aus datenschutzrechtlicher Sicht mit Blick auf die Funktion der Thüringer Behörden bei der Wahrnehmung ihrer Aufgaben nach dem SGB II folgende Reformvorschläge der Bundesagentur für Arbeit:

   a) Erhöhung des bisher quartalsweise durchgeführten automatisierten Datenabgleichs auf eine monatliche Frequenz,
   b) Ausweitung des Datenabgleichs zu absolvierten Beschäftigungszeiten vor dem SGB-II-Leistungsbezug,
   c) Erweiterung des Datenabgleichs um Vermögensanlagen bei Versicherungsunternehmen,
   d) Möglichkeit eines Datenabgleichs mit den Grundbuchämtern,
   e) Ausweitung der Datenabgleiche auf alle Mitglieder einer Bedarfsgemeinschaft, unabhängig von deren tatsächlichen Leistungsbezug,
   f) Kooperation mit dem Bundeszentralamt für Steuern zur Überprüfung von E-COMMERCE-Aktivitäten?

7. Welche Schlussfolgerungen ergeben sich aus Ihrer Sicht aus dem eingangs aufgeführten Urteil des Verwaltungsgerichts Leipzig für die Praxis der Thüringer Jobcenter?

Der **Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit** hat die Anfrage mit Schreiben vom 15. Januar 2014 wie folgt beantwortet:

Vorbemerkung:

Im gesetzlichen Regelfall sind die Bundesanstalt für Arbeit (BA) und die jeweilige Kommune Leistungsträger der Grundsicherungsleistungen nach dem SGB II. Sie bilden eine gemeinsame Einrichtung nach § 44 b SGB II, die nach § 6 d SGB II die Bezeichnung Jobcenter führt. Seit dem 1. Januar 2011 ist die datenschutzrechtliche Zuständigkeit für alle Jobcenter grundsätzlich auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) übergegangen, § 50 Abs. 4 Satz 3 SGB II. Im Gesetz wird den Kommunen die Option eingeräumt, alle Aufgaben nach dem SGB II eigenständig wahrzunehmen (so genannte zugelassene kommunale

Träger - Optionskommunen – gemäß § 6 a bis 6 c SGB II). Von dieser Möglichkeit haben in Thüringen folgende Kommunen Gebrauch gemacht: Landkreis Eichsfeld, Stadt Jena sowie ab dem 1. Januar 2012 Landkreis Greiz und Landkreis Schmalkalden-Meiningen. Lediglich für die Jobcenter in diesen vier Optionskommunen besteht eine datenschutzrechtliche Zuständigkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Zu 1.:
Das SGB enthält sowohl im zweiten auch als im zehnten Buch datenschutzrechtliche Bestimmungen. Diese Bestimmungen sind, wie auch der erwähnte § 51 b SGB II, von dem Grundsatz geprägt, dass nur die Daten erhoben und verarbeitet werden dürfen, die für die gesetzliche Aufgabenerfüllung erforderlich sind. Die Übermittlung von Sozialdaten ist nur bei Vorliegen einer gesetzlichen Ermächtigungsgrundlage aus dem SGB zulässig, § 67 d Abs. 1 SBG X.
Nach § 51 b Abs. 1 SGB II in Verbindung mit der Verordnung zur Erhebung der Daten nach § 51 b des zweiten Buches Sozialgesetzbuch werden umfassende Daten erhoben, die alle wichtigen privaten Lebensumstände des Leistungsberechtigten und seiner Bedarfsgemeinschaft einschließen. Hierbei handelt es sich nach Auffassung des TLfDI um einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen. In § 51 b Abs. 3 SGB II werden die Zwecke benannt, zu denen die Daten verarbeitet und genutzt werden dürfen. Durch die Begrenzung der Zwecke erfährt dann auch die Intensität des staatlichen Eingriffs eine gewisse Beschränkung, sodass die Regelung als noch hinnehmbar angesehen werden kann. Eine Nutzung und Verwendung für andere als die in § 51 b Abs. 3 SGB II genannten Zwecke ist unzulässig.

Zu 2.:
Ausführungsbestimmungen oder Verwaltungsvorschriften zu den von Ihnen benannten gesetzlichen Bestimmungen sind dem TLfDI nicht bekannt. Die Nachfrage bei einer Thüringer Optionskommune ergab, dass in diesem Bereich keine Verwaltungsvorschriften für Thüringer Behörden existieren.

Zu 3.:

Es gab in der Vergangenheit Beschwerden zur Umsetzung des SGB II durch Thüringer Behörden. Hierzu hat der TLfDI jeweils in seinen Tätigkeitsberichten informiert. In jüngster Zeit wurden keine Beanstandungen ausgesprochen. Die Beschwerden betrafen Fälle, in denen Daten unzulässigerweise erhoben wurden. Die Angelegenheit konnte jeweils mit dem Jobcenter geklärt werden. Der TLfDI hat im Jahr 2013 eine zweitägige Informationsveranstaltung im Jobcenter der Stadt Jena durchgeführt. Weitere Fortbildungsveranstaltungen sind vorgesehen, soweit die personelle Situation beim TLfDI dies zulässt.

Zu 4.:
Die Befugnis zum automatischen Datenabgleich nach § 52 SGB II soll die missbräuchliche Inanspruchnahme von Arbeitslosengeld II vermeiden helfen. Der Datenabgleich ist nur für Angaben vorgesehen, zu denen der Leistungsempfänger bei Antragstellung oder bei einer erheblichen Veränderung der Verhältnisse verpflichtet ist. Die Daten unterliegen nach Absatz 3 der Regelung einer strengen Zweckbindung und sind bei nichtabweichenden Feststellungen unverzüglich zu löschen. Hierbei handelt es sich nach Auffassung des TLfDI um einen sehr starken Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen. Es wird vom Regelungskonzept des § 67 ff. SGB X abgewichen, weil die Vorschrift die regelmäßige Abfrage von Daten zum beherrschenden Prinzip erhebt und von einer einzelfallbezogenen Feststellung von Verdachtsmomenten absieht. Diese Tendenz wird durch die neu eingeführte vierteljährliche Abfrage infolge des Gesetzes zur Fortentwicklung der Grundsicherung für Arbeitsuchende noch verstärkt. Die Vorschrift ist daher als sehr einschneidende Ausnahme vom Sozialgeheimnis restriktiv auszulegen.
Im Gegensatz zu § 52 sieht § 52 a SGB II keinen regelmäßigen Datenabgleich vor. Die Aufkunftseinholung wird davon abhängig gemacht, dass dies zur Bekämpfung von Leistungsmissbrauch im Einzelfall erforderlich ist. Der mit dieser Regelung verbundene Eingriff ist daher nicht so erheblich wie derjenige durch § 52 SGB II. Das Jobcenter wird durch spezielle Normen im SGB II ermächtigt, Daten, die bei anderen Behörden oder Dritten vorliegen, direkt dort zu erheben. So darf das Jobcenter zur Vermeidung von Leistungsmissbrauch Auskünfte beim zentralen Fahrzeugregister oder bei dem Melde- und dem Ausländerzentralregister einholen,

§ 52 a Abs. 1 SGB II. Auskunftspflichtig gegenüber dem Jobcenter sind außerdem der Arbeitgeber und andere Personen, die dem Antragsteller Leistungen gewähren oder schulden sowie Dritte, die für den Antragsteller Guthaben führen oder Vermögensgegenstände verwahren, §§ 57 bis 60 SGB II. Aus datenschutzrechtlicher Sicht wird diese gesetzliche Regelung, in der von dem Grundsatz der Datenerhebung beim Betroffenen abgewichen wird, kritisch gesehen. Allerdings möchte der Antragsteller nach SGB II staatliche Leistungen erhalten. Diese dürfen ihm nur bei Vorliegen der gesetzlichen Voraussetzungen gewährt werden. Sollte in diesem Bereich der Grundsatz der Datenerhebung beim Betroffenen aufrechterhalten werden, würde dies bedeuten, dass der Antragsteller alle erforderlichen Informationen beizubringen hätte. Sofern er dem nicht nachkommt, müsste der Antrag auf Leistungsgewährung abgelehnt werden. Demgegenüber stellt die gesetzliche Regelung im SGB II eine Verfahrenserleichterung dar, durch die allerdings stärker in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen eingegriffen wird.

Zu 5.:
Der TLfDI ist nicht Mitglied in der Bund-Länder-Arbeitsgruppe zu einer Rechtsvereinfachung im SGB II. Vorgesehene Änderungen im SGB II werden in aller Regel durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) begleitet. Inhaltlich werden die Reformvorschläge in dem Arbeitskreis Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erörtert, in der auch der TLfDI Mitglied ist. Die BfDI bringt die dort gefundene Rechtsauffassung in die Verhandlungen mit ein. Der TLfDI wird die Änderungsvorschläge der BA für die Tagesordnung der Frühjahrssitzung des Arbeitskreise Gesundheit und Soziales anmelden.

Zu 6.:
Die Erhöhung des bisher quartalsweise durchgeführten automatisierten Datenabgleichs auf eine monatliche Frequenz ist aus den unter Nummer 4 genannten Gründen abzulehnen.
Die Ausweitung des Datenabgleichs zu absolvierten Beschäftigungszeiten vor dem SGB II – Leistungsbezug wird kritisch gesehen, da die Fälle, in denen es zu einem Zufluss von Einnahmen innerhalb des SGB-Zeitraums aufgrund vorhergegangener Beschäftigungsverhält-

nisse gekommen sein könnte, gering sein dürften. Sofern im Einzelfall Verdachtsmomente für einen Leistungsmissbrauch bestehen, gibt es auch die Möglichkeit, Daten beim Arbeitgeber zu erheben.
Die Erweiterung des Datenabgleichs um Vermögensanlagen bei Versicherungsunternehmen wird als nicht erforderlich angesehen. Es findet bereits ein Abgleich mit Daten nach § 45 d Abs. 1 Einkommensteuergesetz (EStG) statt, bei dem die Kapitalerträge ermittelt werden. Es ist nicht ersichtlich, dass die Vermögensanlagen, die durch § 45 EStG nicht erfasst werden, erheblich sind. Weniger kritisch wird die Erweiterung des Datenabgleichs um Daten der Grundbuchämter gesehen, da es derzeit offenbar keine Möglichkeit gibt, das Vorhandensein von Immobilienvermögen festzustellen. Die Ausweitung der Datenabgleiche auf alle Mitglieder der Bedarfsgemeinschaft, unabhängig von deren tatsächlichem Leistungsbezug, ist abzulehnen. Die Zugehörigkeit zu einer Bedarfsgemeinschaft besteht auch dann, wenn der Partner aufgrund seines eigenen Einkommens nicht hilfebedürftig ist. Dieser hat keinen Antrag auf Leistung gestellt. Nur wenn gesetzliche Leistungen bezogen werden sollen, rechtfertigt sich wie bereits in der Antwort zu Frage 4 dargelegt, der mit § 52 Abs. 1 SGB II verbundene starke Eingriff in Grundrechte. Hier soll aber vom Grundsatz der Datenerhebung beim Betroffenen abgewichen werden, ohne dass dieser eine staatliche Leistung überhaupt in Anspruch nehmen will. Gegen einen automatisierten Datenabgleich, ob und welche Daten im Bundeszentralamt für Steuern aus der Beobachtung elektronisch angelegter Dienstleistungen nach § 5 Abs. 1 Nr. 17 des Finanzverwaltungsgesetzes vorliegen, bestehen keine grundlegenden datenschutzrechtlichen Bedenken. Die Daten liegen im Bundeszentralamt für Steuern ohnehin vor und der Abgleich dient dazu, Leistungsmissbrauch zu verhindern. Andernfalls müssten die Thüringer Behörden selbst Daten erheben. Hierzu sind sie aufgrund ihrer personellen und sachlichen Ausstattung nicht in der Lage. Außerdem würden in diesem Fall Daten doppelt vorgehalten werden, was dem Grundsatz der Datensparsamkeit widerspricht.

Zu 7.:
Auch die Telekommunikation mit dem Bürger ist Teil der staatlichen Aufgabe. Die telefonische Erreichbarkeit ist Ausdruck eines modernen staatlichen Selbstverständnisses gerade auch in Bereichen, wo es um die soziale Existenz geht (VG Leipzig, Urteil vom

10. Januar 2013 – 5 K 981/11 -, juris). Die Jobcenter sind vor diesem Hintergrund gehalten, ihre Außenwirkung möglichst transparent und bürgerfreundlich zu gestalten. Nach § 50 Abs. IV S. 2 SGB II richtet sich der Anspruch auf Zugang zu amtlichen Informationen nach dem Informationsfreiheitsgesetz des Bundes. Soweit es sich um öffentliche Stellen im Sinne des Thüringer Informationsfreiheitsgesetzes handelt, ist das Thüringer Informationsfreiheitsgesetz jeweils daraufhin zu überprüfen, ob die dem vorliegenden Urteil zugrundeliegenden Erwägungen analog gelten.

Anlage 32

Anfrage 9 des Abgeordneten Fiedler (CDU)
und die Antwort des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit
Thüringer Landtag Drucksache 5/7181 vom 15. Januar 2014

Aktueller Sachstand von angekündigten Prüfungen

Die **Anfrage 9** vom 3. Dezember 2013 hat folgenden Wortlaut:

Im Hinblick auf die Einhaltung bestehender datenschutzrechtlicher Bestimmungen hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) seit dem Beginn des Jahres 2013 in diversen Pressmittelungen die rechtliche Prüfung und Würdigung unterschiedlicher Vorgänge im Freistaat angekündigt. Der jeweiligen Pressemitteilung lagen die nachfolgenden Sachverhalte zugrunde:

1. Ausweislich der Berichterstattung der Thüringer Allgemeinen vom 11. Januar 2013 hat der TLfDI die datenschutzrechtliche Prüfung der Vorgehensweise des Thüringer Antikorruptionsbeauftragten im Zusammenhang mit dem Verkauf der E.ON-Aktien an Thüringer Kommunen angekündigt.
2. Laut Thüringischer Landeszeitung vom 12. Januar 2013 sowie anderer Medien kündigte der TLfDI eine umfassende Prüfung der Telefonanlagen der gesamten Landesverwaltung im Hinblick auf deren Abhörsicherheit an.
3. Die Thüringer Allgemeine berichtete am 25. Januar 2013, dass der TLfDI beabsichtigt, eine datenschutzrechtliche Prüfung durchzuführen, aufgrund von internen Observationsmaßnahmen von Polizeibeamten in verschiedenen Thüringer Polizeidienststellen.
4. Ausweislich eines Berichts der Thüringischen Landeszeitung vom 9. Juli 2013 kündigte der TLfDI eine datenschutzrechtliche Prüfung aufgrund des Einsatzes einer Kameradrohne in Heilbad Heiligenstadt an.
5. Die Südthüringer Zeitung berichtete mit Datum vom 17. Juli 2013, dass der TLfDI beabsichtigt, eine bundeswei-

te Prüfung der Gepflogenheiten zur Aktenlagerung durchzuführen.

Ich frage den Datenschutzbeauftragten:

1. In welchem Prüf- bzw. Bearbeitungsstadium befinden sich die oben unter den Punkten 1 bis 5 aufgeführten Sachverhalte (bitte für jeden Punkt einzeln darstellen)?

2. Wann ist hinsichtlich der oben unter den Punkten 1 bis 5 aufgeführten Sachverhalte mit einem Abschlussbericht bzw. einer abschließenden Stellungnahme seitens des TLfDI zu rechnen (bitte für jeden Punkt einzeln aufführen)?

3. Welche konkreten Maßnahmen und Recherchen wurden seitens des TLfDI hinsichtlich der oben unter den Punkten 1 bis 5 aufgeführten Sachverhalte angestrengt, um die mutmaßlichen datenschutzrechtlichen Verstöße zu hinterfragen und rechtlich zu würdigen?

Der **Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit** hat die Anfrage mit Schreiben vom 15. Januar 2014 wie folgt beantwortet:

Zu 1.:
Zu Punkt 1:
Der Vorgang ist abgeschlossen.

Zu Punkt 2:
Der Vorgang ist abgeschlossen.

Zu Punkt 3:
Der Vorgang ist sowohl hinsichtlich der Landespolizeiinspektion (LPI) Jena als auch hinsichtlich der Kriminalpolizeiinspektion (KPI) Mühlhausen abgeschlossen.

Zu Punkt 4:
Der Vorgang ist abgeschlossen.

Zu Punkt 5:

Der Vorgang ist noch nicht abgeschlossen, sondern als fortwährende Aufgabe – nicht nur des TLfDI – zu begreifen.

Zu 2.:
Zu Punkt 1:
Siehe dazu die Antwort zu Frage 3.

Zu Punkt 2:
Ein Abschlussbericht bzw. eine abschließende Stellungnahme seitens des TLfDI ist nicht geplant. Die Ergebnisse finden Eingang in die gesetzlich vorgeschriebenen Tätigkeitsberichte.

Zu Punkt 3:
Siehe dazu die Antwort zu Frage 3.

Zu Punkt 4:
Siehe dazu die Antwort zu Frage 3.

Zu Punkt 5:
Siehe dazu die Antwort zu Frage 3.

Zu 3.:
Zu Punkt 1:
Da im Rahmen der Korruptionsbekämpfung in der Regel auch personenbezogene Daten von Bediensteten verarbeitet werden, ging der TLfDI zunächst davon aus, dass auch der Bericht des unter Punkt 1 der Anfrage 9 genannten Antikorruptionsbeauftragte des Thüringer Innenministeriums (TIM) Personenbezug aufwies. In einem ersten Schreiben des TLfDI vom Januar 2013 wurde das TIM daher um Stellungnahme gebeten, auf welcher Rechtsgrundlage der genannte Bericht angefertigt und dem Thüringer Landesverwaltungsamt übermittelt wurde.
Aufgrund widersprüchlicher Aussagen des TIM zur Rechtsgrundlage des angefertigten Berichts des Antikorruptionsbeauftragten forderte der TLfDI in einem zweiten Schreiben vom April 2013 das TIM erneut auf, eine einheitliche Rechtsauffassung zu dieser Rechtsfrage mitzuteilen. Nachdem das TIM dieser Aufforderung im Mai 2013 nachgekommen war, bat der TLfDI um Übersendung des Berichts des Antikorruptionsbeauftragten des TIM sowie um Mitteilung, auf welcher Rechtsgrundlage in diesem Zusammenhang personenbezo-

gene Daten an das Thüringer Landesverwaltungsamt übermittelt wurden. Nach abschließender Prüfung des zur Verfügung gestellten Berichts durch den TLfDI wurde dem TIM im Juni 2013 mitgeteilt, dass der Vorgang datenschutzrechtlich nicht zu beanstanden ist.

Zu Punkt 2:
Zum Zeitpunkt der Pressemeldung im Januar 2013 waren nach Kenntnisstand des TLfDI 180 gekaufte und 37 gemietete Telekommunikationsanlagen (TK-Anlagen) in der Thüringer Landesverwaltung im Einsatz.
Mit Schreiben vom Januar 2013 wandte sich der TLfDI an das Thüringer Finanzministerium (TFM) mit der Bitte um Mitteilung, um welche TK-Anlagen es sich dabei handelt und welche Leistungsmerkmale die jeweiligen TK-Anlagen aufweisen und welche Leistungsmerkmale davon tatsächlich freigeschaltet bzw. deaktiviert wurden. Insbesondere interessierte aus datenschutzrechtlicher Sicht, welche Anlagen das Aufschalten (mit Signal oder auch ohne Signal) und/oder eine Raumüberwachung bei Nichtnutzung des Telefons (Babyphonfunktion) technisch ermöglichen und inwiefern diese aktiviert bzw. deaktiviert sind.
Ebenfalls mit Schreiben vom Januar 2013 teilte das TFM dem TLfDI mit, dass die Unterlagen hinsichtlich der bestehenden TK-Anlagen und ihrer Leistungsmerkmale seit 2004 nicht mehr im TFM vorhanden seien, sondern sich beim nun zuständigen Bauministerium befänden. Eine im Zusammenhang mit der Bestandsaufnahme zum Ausschreibungsverfahren EiCoNeD bestehende Übersicht der vorhandenen TK-Anlagen mit Stand 2010 konnte dem TLfDI aber zugeleitet werden.
Mit weiteren Schreiben vom Januar 2013 wandte sich der TLfDI daraufhin an alle Ministerien, die Thüringer Staatskanzlei und den Thüringer Landtag, mit der Bitte, in ihrem/seinem Geschäftsbereich die Leistungsmerkmale der TK-Anlagen zu überprüfen. Daraufhin gingen dem TLfDI im Zeitraum von Ende Februar bis Ende April 2013 die Antworten mit den abgefragten Informationen aus den Ressorts, der Staatskanzlei und dem Thüringer Landtag ein.
Nach heutigem Kenntnisstand des TLfDI sind die Leistungsmerkmale Aufschalten/Babyphon-Funktion Bestandteil der Standard-Herstellersoftware und bei neuen TK-Anlagen durchaus marktüblich. Diese Merkmale müssen – wenn sie vorhanden und nicht erwünscht sind – in der TK-Anlage deaktiviert werden.

Bei den TK-Anlagen der Thüringer Landesverwaltung, die zum Teil sehr stark veraltet sind, wurde im Ergebnis durch den TLfDI festgestellt, dass die Leistungsmerkmale "Aufschalten“ und die "Babyphonfunktion“ teilweise technisch nicht möglich sind, bzw. wenn sie möglich sind, abgeschaltet waren bzw. auf Grund der Anfrage des TLfDI deaktiviert wurden.

Zu Punkt 3:
Aufgrund von Pressemeldungen Ende des Jahres 2012 und Anfang des Jahres 2013 gab es Hinweise darauf, dass möglicherweise rechtswidrige Beobachtungsmaßnahmen gegenüber Polizeibeamten der KPI Mühlhausen durchgeführt wurden. Hintergrund dafür war, dass diese Beamte Dienstfahrzeuge für private Zwecke genutzt haben sollten. Da es sich bei den Observationsmaßnahmen um die Erhebung personenbezogener Daten mit besonderen oder heimlichen Mitteln handelte, bat der TLfDI zunächst im Januar 2013 das Thüringer Landeskriminalamt um Stellungnahme zum Sachverhalt, insbesondere um Angabe, auf welcher Rechtsgrundlage diese Mittel eingesetzt wurden. Zusätzlich nahm der TLfDI selbst kurzfristig Anfang 2013 Einsicht in die Unterlagen der zuständigen Staatsanwaltschaft, um die Rechtmäßigkeit der gewählten Ermittlungsmaßnahmen datenschutzrechtlich zu überprüfen. Aus den Ermittlungsunterlagen ergab sich, dass für vier Beschuldigte eine richterliche Anordnung vorlag und damit eine rechtliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung gegeben war. Somit war die Observation dieser Beschuldigten datenschutzrechtlich nicht zu beanstanden.
Darüber hinaus wurden aber im Zuge der Observationsmaßnahmen auch drei weitere Polizeibeamte observiert, ohne dass diese Observationsmaßnahmen auf eine rechtliche Grundlage gestützt werden konnten.

Weitere Observationsmaßnahmen sollen auch gegenüber Polizeibeamten der LPI Jena stattgefunden haben. Hintergrund dafür war auch hier der Vorwurf, dass zwei Beamte Dienstfahrzeuge für private Zwecke genutzt haben sollen. Da es sich bei den Maßnahmen um die Erhebung personenbezogener Daten mit besonderen oder heimlichen Mitteln handelte, nahm der TLfDI im Januar 2013 Einsicht in die Unterlagen der zuständigen Staatsanwaltschaft, um die Rechtmäßig-

keit der gewählten Ermittlungsmaßnahmen datenschutzrechtlich zu überprüfen.

Die datenschutzrechtliche Prüfung ergab, dass für die zwei beschuldigten Beamten richterliche bzw. staatsanwaltschaftliche Anordnungen vorlagen und damit eine rechtliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung gegeben war. Damit waren diese Observationen nicht zu beanstanden. Anhand der Ermittlungsunterlagen konnte jedoch auch festgestellt werden, dass im Rahmen der Ermittlungen gegen die zwei Beschuldigten auch vier weitere Beamte observiert wurden. Dabei konnte lediglich die Observation von zwei der vier Beamten auf eine rechtliche Grundlage gestützt werden. Eine rechtliche Grundlage für die Observation der zwei anderen Beamten konnte hingegen nicht festgestellt werden. Der TLfDI musste im Ergebnis bei beiden Sachverhalten davon ausgehen, dass – im Rahmen der zulässigen durchgeführten längerfristigen Observationen – grundsätzlich alle Personen, die die Dienstfahrzeuge nutzten, observiert wurden. Die konkreten Verdachtsmomente beschränkten sich indes nur auf die in den richterlichen Anordnungen erwähnten Zielpersonen. Diese erhebliche datenschutzrechtliche Verletzung hat der TLfDI jeweils förmlich nach § 39 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet. Der TLfDI hat ferner die zuständigen Stellen aufgefordert, für die Zukunft darauf hinzuwirken, dass solche datenschutzrechtlichen Verstöße im Rahmen der Verarbeitung und Nutzung personenbezogener Daten unterbleiben.

Zu Punkt 4:
Aufgrund der Beschwerde eines Bürgers aus dem Heilbad Heiligenstadt recherchierte der TLfDI im Amtsblatt der Stadt mit der Nr. 13/2013 vom 27. Juni 2013. Dem Amtsblatt war zu entnehmen, dass die Stadtverwaltung des Heilbads Heiligenstadt beabsichtigte, eine ferngesteuerte Drohne mit acht Propellerarmen einzusetzen, die während eines Fluges mit einer Auflösung von 36 Megapixeln Videos aufnehmen oder Fotografien anfertigen kann. Die Drohne sollte vielfältig genutzt werden, so z. B. auch zur Inspektion für Neubaugebiete und zur Aufnahme von Veranstaltungen. Der TLfDI forderte die Stadtverwaltung daher Anfang Juli 2013 auf, mitzuteilen, zu welchem Zweck die drohnengestützten Bildaufnahmen, insbesondere von Neubaugebieten und Veranstaltungen, angefertigt werden sollen

und auf welcher Rechtsgrundlage diese Maßnahmen beruhen. Zugleich bat der TLfDI um Auskunft darüber, welche technisch-organisatorischen Maßnahmen in diesem Zusammenhang von der Stadt geplant seien, um bei den beabsichtigten Einsatzszenarien datenschutzrechtliche Bestimmungen einzuhalten. Schließlich bat der TLfDI um die Vorlage von bestehenden Regelungen (Dienstanweisungen) im Zusammenhang mit dem Einsatz der Drohne.
Mit Schreiben vom Juli 2013 teilte der Bürgermeister des Heilbads Heiligenstadt dem TLfDI mit, dass die Stadt keine Kameradrohne besitze und auch nicht beabsichtige, eine solche anzuschaffen. Ebenso wenig solle eine solche Drohne von der Stadt angemietet werden.
Im Ergebnis war somit – trotz gegenteiliger Informationen aus dem Amtsblatt – noch kein Verstoß gegen datenschutzrechtliche Vorschriften festzustellen.

Zu Punkt 5:
Der TLfDI hatte aufgrund des entdeckten Aktenlagers in Immelborn am 29. Oktober 2013 zu einem Runden Tisch eingeladen. Teilnehmer waren Thüringer Unternehmen, deren Kerngeschäft die Aktenaufbewahrung und -vernichtung ist. Es wurde eine fachliche Diskussion zum datenschutzgerechten Umgang mit Akten geführt, und der TLfDI konnte sich einen Überblick über die branchenspezifischen Probleme verschaffen. Im Anschluss daran gelang es ihm, Vertreter von großen Archivierungsdienstleistern aus der Branche und von Seiten der betrieblichen Datenschutzbeauftragten an einen weiteren Runden Tisch zu bitten, um dort zu erörtern, wie konzeptionell ein "zweiter Fall Immelborn“ verhindert werden kann. Dieser Termin fand am 5. Dezember 2013 in Erfurt statt.
Als Ziel kristallisierte sich bei dieser Beratung heraus, dass es zur Konkretisierung unpräziser gesetzlicher Vorgaben dringend einer "Orientierungshilfe Aktenaufbewahrung" bedarf. Sie soll einerseits Archivierungsdienstleistern, andererseits aber auch Unternehmen, die diese Dienstleister beauftragen wollen, eine Richtschnur an die Hand geben, auf welche Weise die rechtlichen Vorgaben einzuhalten sind und wie sich Auftraggeber (vorab) von der Einhaltung dieser Vorgaben überzeugen können. Die gemeinsam erarbeitete Orientierungshilfe soll sodann mit dem zuständigen Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgestimmt werden, um so die bundesweite Anwendung der Orientierungshilfe zu gewährleisten. Der Runde Tisch wird in regelmäßigen

Abständen zusammenkommen, um die Orientierungshilfe zu erarbeiten.

Anlage 33

Pressemitteilung
vom 5. März 2012

Nutzung der LKA-Akten zur Aufklärung der Neonazi-Morde nicht bestritten

Meldungen des Mitteldeutschen Rundfunks vom 4. März 2012 zur Aktenprüfung im Fall der Neonazi-Mordserie haben in der Öffentlichkeit für Irritationen gesorgt. Der MDR hatte berichtet, dass der Thüringer Landesbeauftragte für den Datenschutz die Einhaltung der Aufbewahrungsfristen für Akten des Thüringer Landeskriminalamts prüfen wird. Darunter seien auch die 24 Aktenordner, die derzeit beim Generalbundesanwalt zur Aufklärung der Morde des sog. Zwickauer Terrortrios ausgewertet werden. „Wir haben Hinweise darauf erhalten, dass Unterlagen zu abgeschlossenen strafrechtlichen Ermittlungen nicht ordnungsgemäß geprüft und jeweils über deren weitere Aufbewahrung oder Vernichtung beim Landeskriminalamt nicht entschieden worden sei," erklärt der Thüringer Landesbeauftragte für den Datenschutz, Dr. Lutz Hasse. „Dies betreffe auch die Unterlagen zu dem Neonazi-Trio.“

Das hat der Thüringer Landesbeauftragte für den Datenschutz zum Anlass genommen, beim Thüringer Landeskriminalamt Auskünfte zur Einhaltung der gesetzlichen Aufbewahrungsfristen sowohl bei den 24 Aktenordnern als auch bei allen anderen abgeschlossenen Ermittlungsverfahren einzuholen. Hasse legt aber Wert auf die bereits in seinem Statement gegenüber dem MDR abgegebene Feststellung, dass mögliche Verletzungen der Prüf- und Aussonderungsvorschriften keine Auswirkungen auf die datenschutzrechtliche Zulässigkeit der Nutzung dieser Unterlagen zur Aufklärung der Neonazi-Morde haben. „Werden die Daten zur Behebung einer bestehenden Beweisnot benötigt, dann dürfen und müssen die Daten hierfür weiter aufbewahrt werden, auch wenn die Prüf- und Aufbewahrungsfristen bereits abgelaufen wären“, so Hasse weiter. „Datenschutz ist also auch hier kein Täterschutz!“

Anlage 34

Pressemitteilung
vom 27. März 2012

Konferenz der Datenschutzbeauftragten in Potsdam fordert ein modernes Datenschutzrecht für Europa

Unter Vorsitz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg tagte am 21. und 22. März 2012 die 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Potsdam.
Im Mittelpunkt der Konferenz stand die Forderung der Datenschützer nach einem modernen Datenschutzrecht in Europa. Die Konferenz unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der EU zu modernisieren und zu harmonisieren und fordert, für alle Mitgliedstaaten ein möglichst hohes Datenschutzniveau festzuschreiben.
Die Vizepräsidentin der Europäischen Kommission und Justizkommissarin Viviane Reding stellte auf der Konferenz den Entwurf für eine **Europäische Datenschutz-Grundverordnung** vor. Die geplanten Neuregelungen zum Einsatz datenschutzfreundlicher Technologien, zu wirksamen Sanktionsbefugnissen sowie verstärkten Datenschutzrechten gegenüber länderübergreifend tätigen Unternehmen können nach Auffassung der Datenschutzbeauftragten zu einer wesentlichen Weiterentwicklung des Datenschutzrechts führen. Darüber hinaus halten die Konferenzteilnehmer aber weitere Schritte, wie etwa eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen und die anonyme und pseudonyme Nutzung digital angebotener Dienste für zwingend erforderlich. Für besonders problematisch hält die Konferenz die im Entwurf vorgesehenen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte. Die Datenschutzbeauftragten fordern, diese auf das unbedingt erforderliche Maß zu reduzieren und die für den Grundrechtsschutz wesentlichen Punkte in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten zu regeln.
Als besonders bedeutsam zur Gewährleistung eines wirksamen Grundrechtsschutzes wurde von den Datenschutzbeauftragten die Ergänzung des zurzeit auf europäischer Ebene beratenen Entwurfs einer **Europäischen Ermittlungsanordnung** in Strafsachen hervor-

gehoben. Dieser sieht trotz eines fehlenden einheitlichen Schutzstandards in den Mitgliedsstaaten vor, Eingriffsentscheidungen der Strafverfolgungsbehörden dieser Staaten gegenseitig anzuerkennen. Dies führt zu Problemen, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Europäische Ermittlungsanordnung muss deshalb in ein Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung integriert werden, um bei grenzüberschreitender Strafverfolgung im vereinten Europa den Grundrechtsschutz der Betroffenen zu gewährleisten.
Die Datenschutzbeauftragten berieten auf der Konferenz zum Thema „**Öffentlich geförderte Forschungsprojekte** zur Entdeckung abweichenden Verhaltens im öffentlichen Raum“, mittels derer menschliche Bewegungs- und Verhaltensmuster ausgewertet werden können, mit dem Ziel, eine mögliche Gewaltbereitschaft o. a. Bedrohungen frühzeitig zu erkennen. Bei dieser Mustererkennung menschlichen Verhaltens besteht aber die große Gefahr, dass diese präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der Betroffenen verletzen könnte. Der Appell der Konferenz richtet sich deshalb an die öffentlichen Stellen des Bundes, der Länder und die der EU mit der Forderung, zur Verhinderung von Datenschutzverstößen bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Forschungsvorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in die Entscheidung einzubeziehen.

Die auf der Konferenz gefassten Entschließungen sind auf der Internetseite des TLfD http://www.thueringen.de/datenschutz/veroeffentlichungen/entschliessungen_datenschutzkonferenz/83/ abrufbar.

Anlage 35

Pressemitteilung
vom 16. Mai 2012

Warnung vor fingierten Anrufen einer „Datenschutzzentrale“

Der Thüringer Landesbeauftragte für den Datenschutz hat Kenntnis über Telefonanrufe einer sogenannten „Datenschutzzentrale Düsseldorf“ erlangt, die ihn zu folgender Warnung veranlasst:
Die Anrufer geben vor, Mitarbeiter der „Datenschutzzentrale Düsseldorf“ zu sein und rufen unter einer Düsseldorfer Nummer an, unter der bei Rückruf allerdings niemand zu erreichen ist. Es wird behauptet, die Angerufenen hätten an einem Gewinnspiel teilgenommen.

Eine „Datenschutzzentrale Düsseldorf“ existiert jedoch nicht. Es ist auch nicht üblich, dass sich die regulären Aufsichts- und Kontrollbehörden für den Datenschutz mit Bürgern ohne vorherigen schriftlichen Kontakt telefonisch in Verbindung setzen, um diese zu beraten. Die erwähnten verdächtigen Anrufe dienen denn auch regelmäßig missbräuchlichen Zwecken. Vorgetäuscht wird, die persönlichen Daten der Betroffenen schützen und die angebliche Teilnahme an einem Gewinnspiel beenden zu wollen. Dabei werden die Bürger oftmals nach den Bankverbindungsdaten befragt, um Geld von ihren Konten abzubuchen oder es werden „günstigere Vertragskonditionen“ angeboten.

Der Thüringer Landesbeauftragte für den Datenschutz warnt davor, persönliche Daten, insbesondere Anschrift und Kontoverbindung, an unseriöse Anrufer herauszugeben. Falls durch ein solches Telefonat bereits ein Vertrag zustande gekommen sein sollte, kann der Betroffene von seinem Widerspruchsrecht Gebrauch machen und die Löschung seiner Daten fordern. Da dieses telefonisch nicht möglich sein wird, müssen die Kontaktdaten etwaigen späteren Vertragsunterlagen entnommen werden. Es wird zudem empfohlen, nach einem derartigen Anruf die Bewegungen auf dem Konto zu kontrollieren, um gegebenenfalls einer unberechtigten Lastschrift rechtzeitig widersprechen zu können.

Gibt es Verdachtsmomente für ein strafbares Verhalten, sollten die Strafverfolgungsbehörden (örtliche Polizeidienststelle oder Staatsanwaltschaft) informiert werden. Hilfe bei der Vertragsrücknahme bieten Verbraucherzentralen an. Die Bundesnetzagentur informiert auf ihrer Internetseite über unerlaubte Telefonwerbung und Rufnummernmissbrauch.

Rückfragen beantworten die Mitarbeiter des Thüringer Landesbeauftragten für den Datenschutz gern.

Anlage 36

Pressemitteilung
vom 18. Mai 2012

Der Thüringer Landesbeauftragte für den Datenschutz und die Landeskrankenhausgesellschaft Thüringen e. V. treffen sich am 22.05.2012 mit Vertretern der Krankenhäuser zum Informationsaustausch „Umsetzung der Orientierungshilfe Krankenhausinformationssysteme“

Am kommenden Dienstag wird auf Initiative des Thüringer Landesbeauftragten für den Datenschutz (TLfD) eine gemeinsame Informationsveranstaltung des TLfD und der Landeskrankenhausgesellschaft Thüringen e. V. (LKHG) zur Umsetzung der „Orientierungshilfe zur datenschutzkonformen Gestaltung und Nutzung von Krankenhausinformationssystemen (KIS)“ stattfinden. Im Rahmen dieser Veranstaltung wird der TLfD den Vertretern von voraussichtlich 27 Thüringer Krankenhäusern am Vormittag sowohl den Inhalt der „Orientierungshilfe KIS“ vorstellen als auch Informationen über die Ergebnisse der im Jahr 2011 durchgeführten Prüfungen der Krankenhausinformationssysteme geben. Am Nachmittag des 22. Mai 2012 werden Vertreter der LKHG zu den Anforderungen der „Orientierungshilfe KIS“ und deren Umsetzung- aus Krankenhausträgersicht- referieren. Die Tagung soll insbesondere auch Gelegenheit bieten, Streitpunkte zu erörtern.

Zeit: Dienstag, 22. Mai 2012, 10.00 Uhr bis 16:00 Uhr

Ort: Thüringer Landtag, Jürgen-Fuchs-Straße 1, 99096 Erfurt, Raum F 125 a

In Thüringer Krankenhäusern wird flächendeckend Informationstechnologie zur Verarbeitung von Patientendaten und die Dokumentation ärztlichen Handelns genutzt. Menschen, die medizinische Hilfe in Krankenhäusern in Anspruch nehmen wollen, möchten dies aber mit der Gewissheit tun, dass mit ihren personenbezogenen- zumeist sensiblen- Gesundheitsdaten, die für eine umfassende Behandlung erhoben und verarbeitet werden, datenschutzkonform umgegangen wird.

Die Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben unter Mitarbeit von Datenschutzbeauftragten der Evangelischen und Katholischen Kirche in Deutschland sowie Vertretern der Krankenhäuser und der Softwarebranche eine „Orientierungshilfe zur datenschutzkonformen Gestaltung und Nutzung von Krankenhausinformationssystemen“ mit sowohl rechtlichen als auch technischen Hinweisen erarbeitet, die auf der 81. Konferenz am 16./17. März 2011 Zustimmung erfahren hat. Die Orientierungshilfe benennt die sich aus den geltenden datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergebenden Anforderungen und beschreibt die Maßnahmen für die technische Umsetzung.

Der Thüringer Landesbeauftragte für den Datenschutz hat die Verabschiedung der Orientierungshilfe zum Anlass genommen, im Jahr 2011 eine Überprüfung einer repräsentativen Auswahl von Krankenhäusern nach diesem neuen Maßstab vorzunehmen.
"Optimale Patientenversorgung muss immer auch mit optimalem Schutz der Patientendaten einhergehen“, fordert der seit 1. März 2012 amtierende Datenschutzbeauftragte Dr. Lutz Hasse. Nach seiner Meinung steht der Datenschutz einem Einsatz von Informationstechnologie in Krankenhäusern nicht entgegen; vielmehr ist gemeinsam mit den Krankenhäusern ein Weg zu finden und zu gehen, der gerade in diesem sensiblen Bereich zu einem rechtskonformen Schutz der Patientendaten führt. Darüber zu wachen, dass die Nutzung von Krankenhausinformationssystemen datenschutzkonform erfolgt, versteht er als eine seiner wichtigsten Aufgaben. „Ich verbinde die Informationsveranstaltung mit dem Angebot an die Vertreter der Krankenhäuser, im Dialog zu praktikablen Lösungen zu gelangen“, betont er im Vorfeld.

Für Anfragen vor und nach der Veranstaltung, zu denen die Medienvertreter herzlich eingeladen sind, stehen die Veranstaltungsteilnehmer gern zur Verfügung.

Anlage 37

Pressemitteilung
vom 8. Juni 2012

Vorstellung des 9. Tätigkeitsberichts des TLfD

Anlässlich der heutigen Vorstellung des 9. Berichtes über die Tätigkeit des Thüringer Landesbeauftragten für den Datenschutz für den Berichtszeitraum 2010/2011 erklärt der amtierende Datenschutzbeauftragte Dr. Lutz Hasse vorab:

„Der vorliegende 9. Tätigkeitsbericht ist in seiner ursprünglichen Fassung von meinem Amtsvorgänger gefertigt worden. Da der Bericht allerdings vom Amtsinhaber dem Landtag und der Landesregierung zu erstatten und zu verantworten ist (§ 40 Abs. 1 ThürDSG), habe ich im für erforderlich erachteten Umfang vereinzelt Änderungen nicht Sinn entstellender Art vorgenommen, die nicht zuletzt der Erwärmung des datenschutzrechtlichen Klimas dienen sollen.“

Der Bericht enthält auf 198 Seiten einen Überblick über die Tätigkeitsschwerpunkte in den Jahren 2010 und 2011.

Der TLfD hat im Berichtszeitraum wieder zwei repräsentative Vor-Ort-Kontrollen durchgeführt. Auf der Grundlage einer landesweiten Umfrage wurde in insgesamt elf Schwimmbädern der Einsatz von Videoüberwachungstechnik kontrolliert (5.5). „In einigen Fällen mussten zum Teil erhebliche Verstöße gegen den Datenschutz festgestellt werden. Im gravierendsten Fall betraf dies die Anfertigung von Videoaufnahmen in der Sauna.“ Diese Kontrollen sind derzeit noch nicht abgeschlossen. „Derzeit steht meine Behörde mit den Betreibern in Kontakt, um Lösungen zur Beseitigung der festgestellten Mängel zu finden“, so Hasse weiter. In zwei Fällen musste allerdings eine formelle Beanstandung nach § 39 ThürDSG ausgesprochen werden, weil Betreiber sich geweigert hatten, die vom TLfD geforderten Maßnahmen umzusetzen. Hier wird mithilfe der zuständigen Rechtsaufsichtsbehörden das Datenschutzrecht durchzusetzen sein. Um künftig Querelen zu vermeiden, erarbeitet der TLfD in Kooperation mit dem Bundesverband Öffentlicher Bäder e.V. eine

Richtlinie, die den Bäderbetreibern Antworten auf die datenschutzrechtlichen Konfliktfälle geben soll.
Die andere Querschnittskontrolle hatte die Prüfung des datenschutzgerechten Umgangs mit Patientendaten in Krankenhausinformationssystemen (11.1) zum Gegenstand. Hierzu hatten die Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen und Katholischen Kirche in Deutschland sowie Vertretern der Krankenhäuser und der Softwarebranche eine „Orientierungshilfe zur datenschutzkonformen Gestaltung und Nutzung von Krankenhausinformationssystemen (KIS)“ mit sowohl rechtlichen als auch technischen Hinweisen erarbeitet, die auf der 81. Datenschutzkonferenz am 16./17. März 2011 Zustimmung erfahren hat. Die Verabschiedung dieser Orientierungshilfe hat der TLfD zum Anlass genommen, im Jahr 2011 eine Überprüfung von 6 Krankenhäusern vorzunehmen. Auch diese Kontrollen sind noch nicht abgeschlossen. Das grundsätzliche Problem besteht darin, dass es sich dabei um sehr sensible personenbezogene Daten handelt, auf die nicht mehr Krankenhausmitarbeiter Zugriff haben sollen, als unbedingt erforderlich ist. Andererseits darf man nicht verkennen, dass Ärzte und Pflegekräfte das Recht auf die bestmögliche Information über den Patienten beanspruchen, um diesen optimal behandeln zu können. "Optimale Patientenversorgung muss aber immer auch mit optimalem Schutz der Patientendaten einhergehen“, forderte Dr. Lutz Hasse bereits am 22. Mai 2012 auf der gemeinsamen Informationsveranstaltung des TLfD und der Landeskrankenhausgesellschaft Thüringen e. V. zur Umsetzung dieser Orientierungshilfe „KIS“. Weiter dazu Dr. Hasse: „Ich betone immer wieder: Datenschutz steht einem Einsatz von Informationstechnologie in Krankenhäusern nicht entgegen; gemeinsam mit den Krankenhäusern ist allerdings ein Weg zu finden und zu gehen, der gerade in diesem datenschutzrechtlich sensiblen Bereich zu einem rechtskonformen Schutz der Patientendaten führt.“ Die Krankenhäuser stehen dem Angebot des TLfD, gemeinsam zu tragfähigen Lösungen zu gelangen, ausgesprochen offen gegenüber. Infolge dessen wurde bislang auch keine formelle Beanstandung seitens des TLfD ausgesprochen.

Die Aufarbeitung der Kontrollen der Kommunen 2008 und 2009 (8. Tätigkeitsbericht des TLfD) hat im Berichtszeitraum nochmals

enorme Kapazitäten gebunden und gestaltete sich teilweise sehr mühsam. Wegen mangelhafter bzw. zögerlicher Beseitigung der datenschutzrechtlichen Defizite mussten daher nochmals fünf Kommunen vom TLfD beanstandet werden. Eine weitere Beanstandung wurde wegen offenkundig unzulässiger Forderung der Verwaltungsgemeinschaft Rennsteig an einen Unternehmer zur Angabe seines Jahresumsatzes zwecks Fremdenverkehrsabgabenberechnung ausgesprochen – ein besonders krasser Fall, der noch Folgen nach sich ziehen wird. Schließlich musste die Polizeidirektion Nordhausen wegen einer unzulässigen Zuverlässigkeitsprüfung beanstandet werden. „Im Berichtszeitraum wurden insgesamt elf Beanstandungen ausgesprochen“, resümiert Dr. Hasse.

Große Bedeutung für die Datenschutzentwicklung hatte im Berichtszeitraum die Novellierung des Thüringer Datenschutzgesetzes. Infolge der vom Europäischen Gerichtshof in seinem Urteil vom 9. März 2010 geforderten völligen Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden im nicht-öffentlichen Bereich sind die Aufgaben der bisherigen Aufsichtsbehörde (Landesverwaltungsamt) zum 9. Dezember 2011 auf den TLfD übergegangen; indes wurde diese Aufgabenübertragung bis zum Redaktionsschluss personell nicht untersetzt. „Ich habe jedoch Grund zu der Annahme, dass sich diese ungute Personalsituation den neuen Aufgaben entsprechend entspannen wird“, gibt sich Dr. Hasse zuversichtlich.

Themenschwerpunkte im zurückliegenden Berichtszeitraum waren weiterhin die datenschutzrechtliche Begleitung der zum Stichtag 9. Mai 2011 durchgeführten Volkszählung (Zensus) in Thüringen, die Prüfung der datenschutzkonformen Umsetzung des Bildungspakets, aber auch bekannte Themen wie Videoüberwachung allgemein, Datenschutz im Bereich der Medizin oder bei der Verarbeitung von Personal- und Sozialdaten standen wiederholt auf der Tagesordnung des TLfD.

Weiterhin zunehmend waren im Berichtszeitraum die Beratungen der öffentlichen Stellen und des Gesetzgebers in datenschutzrechtlichen Fragen.

Aufgrund von Beschwerden der Bürger hat der TLfD in den vergangen Jahren wiederum eine Vielzahl von Hinweisen auf datenschutz-

rechtliche Mängel erhalten, denen in jedem Einzelfall nachgegangen wurde. Die Hinweise der Bürger bleiben mithin eine unverzichtbare Hilfe, Datenmissstände aufzudecken.

Die Zahl der Beschwerden belegt nach Meinung des Datenschutzbeauftragten das stetig wachsende Interesse der Bürgerinnen und Bürger am Schutz ihrer personenbezogenen Daten – sei es bei privaten oder bei öffentlichen Stellen. Zunehmend sind sie zu Recht nicht damit einverstanden, in ihrem Alltag registriert und überwacht zu werden. „Ich finde es gut, dass sich die Menschen auf ihr Grundrecht der informationellen Selbstbestimmung besinnen und dies auch mit ihren Beschwerden zum Ausdruck bringen“- so Dr. Hasse.

Anlage 38

Pressemitteilung
vom 14. Juni 2012

In's Netz gegangen – Facebook Sachstand & Hinweise

Gegründet wurde Facebook im Februar 2004. Das Prinzip des Sozialen Netzwerkes klingt einfach. Nutzer, die dem Netzwerk beitreten, kommunizieren untereinander, tauschen Informationen über ihr Leben aus. Facebook vermarktet diese Informationen. Jeder scheint von dem System etwas zu haben. Es ist „cool", dabei zu sein. Im Mai 012 ging Facebook an die Börse. Der Wert eines Nutzerprofiles beträgt ca. 107 $; über 900 Millionen Nutzer sind registriert (Der Spiegel 19/2012).
Die Mahnungen der Datenschützer an die Nutzer, nur mit Bedacht Informationen von sich preiszugeben, verhallen in der Cloud.

Solche Datenmengen wecken Begehrlichkeiten von Dritten, für die sie gar nicht gedacht waren. Längst kann nicht mehr ausgeschlossen werden, dass bspw. Personalabteilungen von Firmen vor einer Einstellung einer Person sich über diese in Facebook informieren.
Die aktuelle Diskussion, dass nun auch die Schufa plant(e), Daten in diesem und anderen Sozialen Netzwerken abzuschöpfen, lässt wohl nur ansatzweise das Ausmaß erkennen, in welches Überwachungsgeflecht sich der Nutzer durch seine Teilnahme an Facebook begibt.

Und nicht nur das. Facebook sammelt auch Daten bei jedem Besuch seiner Fanpage-Seiten und beim Klick des „Gefällt mir"- Buttons von Nicht-Facebook-Mitgliedern. Dem Begehren der Datenschützer, diese Verfahrensweise offen zu legen, kam Facebook bisher nur eingeschränkt nach. Auf Grund der Intransparenz von Facebook hegen die Datenschützer Bedenken. Dies hat zu einer bundesweiten Debatte geführt, deren Sachstand der TLfD auf seiner Webseite kurz umrissen hat; dort gibt der TLfD auch **Hinweise und Tipps** für Mitglieder und Nicht-Mitglieder von Facebook
(http://www.thueringen.de/imperia/md/content/datenschutz/themen/medien/facebook.pdf).

Anlage 39

Pressemitteilung
vom 29. Juni 2012

Orientierungshilfe zum datenschutzgerechten Smart Metering

Der Thüringer Landesbeauftragte für den Datenschutz, Dr. Lutz Hasse, informiert nachfolgend über die Mitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27.06.2012 zur „Orientierungshilfe zum datenschutzgerechten Smart Metering“ sowie in den Anlagen über die von der Konferenz zum Thema verabschiedete Entschließung und die entsprechende Orientierungshilfe:

Presseinformation der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Entschließung und eine ergänzende Orientierungshilfe mit Hinweisen zum datenschutzgerechten Betrieb der neuen intelligenten Zähler für den Energieverbrauch in Häusern und Wohnungen – der so genannten Smart Meter – verabschiedet.

Mit der Novellierung des Energiewirtschaftsgesetzes im Jahr 2011 wurde in Deutschland der Startschuss gegeben, um Smart Meter einzuführen, die detaillierte Verbrauchsdaten aufzeichnen und eine Übermittlung dieser an externe Marktteilnehmer ermöglichen. Die detaillierte Erfassung und Übermittlung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch eine langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff können sich massive Verletzungen der Privatsphäre der Betroffenen ergeben.

Die Datenschutzbeauftragten begrüßen die im Energiewirtschaftsgesetz getroffenen Datenschutzregelungen, weisen aber nachdrücklich darauf hin, dass die Regelungen weiter konkretisiert und detailliert

ausgestaltet werden müssen. Um die Privatsphäre der Verbraucherinnen und Verbraucher auch beim Einsatz der modernen Messtechnik wahren zu können, den Betroffenen die Souveränität über ihre Daten zu gewähren und ihnen die Möglichkeit zur Intervention zu geben, sind neben den gesetzlichen Vorgaben umfangreiche technische und organisatorische Maßnahmen und Regelungen erforderlich.

Die Orientierungshilfe gibt Hilfestellung zur datenschutzgerechten Konzeption der technischen Systeme für das Smart Metering. Es wird erläutert, wie die zentralen Forderungen des Datenschutzes nach Zweckbindung, Datensparsamkeit und Erforderlichkeit berücksichtigt werden können. Dabei wird die gesamte Prozesskette der Verarbeitung personenbezogener Daten betrachtet. Diese reicht vom Messen von Strommengen mittels Zählern über die Verarbeitung im Smart Meter bis zur weiteren Nutzung durch die an der Energielieferung, -verteilung und -abrechnung beteiligten Stellen. In der Orientierungshilfe werden verschiedene Anwendungsfälle dargestellt, analysiert und datenschutzrechtlich bewertet.

Die in der Entschließung und der Orientierungshilfe genannten Anforderungen und Empfehlungen für das Smart Metering sind in einer noch zu erlassenen Rechtsverordnung festzuschreiben.
Die Orientierungshilfe wird nächste Woche im Internetangebot des Landesbeauftragten veröffentlicht werden.

Anlagen

- Entschließung zum datenschutzgerechten Smart Metering (http://www.thueringen.de/datenschutz/veroeffentlichungen/entschliessungen_datenschutzkonferenz/zwischen_den_konferenzen/2012/)

- Orientierungshilfe datenschutzgerechtes Smart Metering (http://www.thueringen.de/datenschutz/veroeffentlichungen/orientierungshilfen/)

Anlage 40

Pressemitteilung
vom 6. Juli 2012

Missachtung des Datenschutzes im "Gesetz zur Fortentwicklung des Meldewesens" stoppen

Nach der vom Bundestag am 29. Juni 2012 in zweiter Lesung beschlossenen Regelung im "Gesetz zur Fortentwicklung des Meldewesens" dürfen Melderegisterauskünfte für Zwecke der Werbung oder des Adresshandels“ an Firmen auch erteilt werden, wenn die betroffene Person gegen die Übermittlung für jeweils diesen Zweck Widerspruch eingelegt hat und zwar dann, wenn die Daten ausschließlich zur Bestätigung oder Berichtigung bereits vorhandener Daten verwendet werden.

Die Einführung dieser Ausnahme vom Verbot der Übermittlung bei Widerspruch hätte gravierende Auswirkungen für die betroffenen Bürgerinnen und Bürger und die Meldebehörden. Bislang und nach dem ursprünglichen Entwurf konnten sich Auskunfteien und Adresshändler keine Adressen aus dem Melderegister ohne vorherige Einwilligung des Betroffenen beschaffen.

Mit der anstehenden Änderung würde nunmehr eine (vermeintlich) nicht korrekte Adresse ausreichen und schon könnten sich Adresshändler die geprüften aktuellen Adressen aus dem Melderegister zur Bestätigung oder Berichtigung ihrer Adress-Altbestände besorgen. Adresshändler könnten diese neuen Adressen in Folge auch weiter veräußern.
Dazu der Thüringer Landesdatenschutzbeauftragte Dr. Lutz Hasse: „Mit dieser Änderung würden den Bürgerinnen und Bürgern alle Rechte aus der Hand geschlagen, selbstbestimmt zu entscheiden, ob Firmen für Zwecke der Werbung und des Adresshandels ihre personenbezogenen Daten erhalten dürfen. Um diese den Datenschutz missachtende Regelung im Gesetz zu stoppen, werde ich mich umgehend an die Fraktionen des Thüringer Landtags mit der Bitte um Unterstützung meines datenschutzrechtlichen Anliegens wenden.

Anlage 41

Pressemitteilung
vom 9. Juli 2012

Patrick Kurth (FDP) und das neue Bundesmeldegesetz

Herr Kurth (FDP) verbittet sich in einer Pressemitteilung die Kritik des TLfD am neuen Bundesmeldegesetz und empfiehlt dem TLfD einen Blick in das aktuelle Thüringer Landesmeldegesetz und meint, erst mit dem neuen Bundesrecht könnten Bürgerinnen und Bürger die Datenweitergabe zu Werbezwecken und Adresshandel unterbinden.

Diese Ansicht des Herrn Kurth ist rechtsirrig.

Aktuelle Rechtslage

Nach § 31 Thüringer Meldegesetz (ThürMeldeG) *darf* die Meldebehörde Personen Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften einzelner bestimmter Einwohner erteilen (einfache Melderegisterauskunft). Weiter ist im Thüringer Meldegesetz (§ 7 ThürMeldeG) geregelt, dass schutzwürdige Interessen der Betroffenen durch die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nicht beeinträchtigt werden dürfen. Schutzwürdige Interessen werden insbesondere beeinträchtigt, wenn die Erhebung, Verarbeitung oder Nutzung, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, den Betroffenen unverhältnismäßig belastet. Die Prüfung, ob schutzwürdige Interessen der Betroffenen beeinträchtigt werden, *entfällt*, wenn die Erhebung, Verarbeitung oder Nutzung *durch Rechtsvorschrift* vorgeschrieben ist (sog. *Mussvorschrift*). Eine solche Vorschrift ist nach dem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 21. Juni 2006 (6C 05.05) *nicht* der § 31 ThürMeldeG, denn diese Norm wird vom Gericht als Ermessensnorm und eben nicht als Mussvorschrift qualifiziert (Die Entscheidung des BVerwG bezieht sich auf die hamburgische Rechtslage, die jedoch der thüringischen Rechtslage entspricht).
Folglich, so das BVerwG, sind § 31 und § 7 ThürMeldeG im Kontext zu lesen. Diese Vorschriften verlangten daher eine Interessen-

abwägung, bei der das Interesse des Betroffenen an der Geheimhaltung seiner Daten gegen das Interesse der Meldebehörde oder eines Dritten an der Erhebung, Verarbeitung oder Nutzung abzuwägen ist. Mithin darf – so das Gericht präzisierend – eine Meldebehörde eine einfache Melderegisterauskunft nicht erteilen, wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird und der Betroffene einer Weitergabe seiner Daten für solche Zwecke zuvor ausdrücklich widersprochen hat. Dieses Widerspruchsrecht ergibt sich aus den erwähnten §§ 31, 7 ThürMeldeG.

Jeder Bürger und jede Bürgerin in Thüringen kann somit derzeit bei der Meldebehörde Widerspruch gegen die Preisgabe der Daten für Zwecke der Direktwerbung einlegen. Diese Rechtsposition zerschellt indes an der geplanten Regelung des Bundes.

Es bleibt also dabei: Die geplante Neuregelung im Bundesrecht stellt eine signifikante Verschlechterung der Rechtsposition der Thüringer Bürger und Bürgerinnen dar. Das neue Recht schlägt den Bürgerinnen und Bürgern die bisherigen Rechte aus der Hand!

Für weitere Auskünfte stehe ich gern zur Verfügung, natürlich auch Herrn Kurth (FDP).

Anlage 42

Pressemitteilung
vom 14. Juli 2012

Gemeinsame Presseerklärung des Bundestagsabgeordneten Patrick Kurth (FDP) und des Thüringer Landesdatenschutzbeauftragten Dr. Lutz Hasse zum neuen Melderecht

Der Thüringer Landesdatenschutzbeauftragte Dr. Lutz Hasse und der Bundestagsabgeordnete Patrick Kurth (FDP) sind heute zu einem Arbeitsgespräch zum vom Bundestag verabschiedeten Gesetz zur Fortentwicklung des Meldewesens zusammengetroffen. Im Anschluss an das Gespräch erklären Kurth und Hasse:

„Einigkeit besteht darin, dass das verabschiedete Gesetz so nicht in Kraft treten sollte. Die optimale Lösung wäre die Einführung einer Einwilligungslösung, was die Weitergabe von Daten durch die Meldeämter an Adresshändler angeht. Alternativ wäre die im Bundesgesetz eingeführte Widerspruchslösung nur dann akzeptabel, wenn die das Widerspruchsrecht zunichte machende Klausel zur Berichtigung bereits vorhandener Daten gestrichen wird. Keine Einigkeit besteht bei der Bewertung des beschlossenen Gesetzes hinsichtlich der Datenschutzlage in Thüringen. Während der Datenschutzbeauftragte Dr. Lutz Hasse von einer signifikanten Verschlechterung der Rechtsposition der Thüringer Bürgerinnen und Bürger ausgeht, sieht der Bundestagsabgeordnete Patrick Kurth einen Fortschritt zur derzeitigen Gesetzeslage. Die unterschiedliche Auffassung ist jedoch dann hinfällig, wenn das Gesetz im Vermittlungsausschuss noch entsprechend geändert wird. Die Ergebnisse des Vermittlungsverfahrens werden dann konkret bewertet.“

Anlage 43

Pressemitteilung
vom 17. Juli 2012

TLfD meets Facebook

Auf Wunsch von Dr. Gunnar Bender, dem Director Public Policy der Facebook Germany GmbH, traf dieser heute mit dem Thüringer Landesbeauftragten für den Datenschutz zu einem Gespräch zusammen, das einem ersten Kennenlernen diente.

In angenehmer und sachlicher Atmosphäre wurden zunächst die gegensätzlichen Standpunkte ausgetauscht.

Ziel künftiger Treffen soll indes sein, die vielfältigen Ursachen der bestehenden Kontroversen zu ergründen. Auf diese Weise kann zum einen der Blick für „die andere Seite“ geschärft werden, zum anderen kann hierbei unter Umständen Potenzial zu Tage treten, das Bewegung in die teilweise festgefahrene Diskussion bringt.

Dieser Weg erscheint arbeitsreich, im Sinne des Datenschutzes, aber allemal lohnend!

Anlage 44

Pressemitteilung
vom 18. Juli 2012

Grünes Licht für Solarkataster in Erfurt

Alle Bürger Erfurts können sich demnächst im Internet mit wenigen Mausklicks darüber informieren, welche Dachflächen der Landeshauptstadt sich für die Nutzung einer Solaranlage eignen. Hierfür werden die Dachflächen von Luftbildaufnahmen der Stadt je nach Eignungsgrad mit unterschiedlichen Farben belegt.

Der Thüringer Landesbeauftragte für den Datenschutz hat sich nach reiflicher Überlegung aller aus datenschutzrechtlicher Sicht zu beachtenden Argumente und unter Berücksichtigung des von ihm sowohl beim Thüringer Ministerium für Wirtschaft, Arbeit und Technologie als auch beim Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz eingeholten fachlichen Rats entschlossen, sich einer Veröffentlichung eines Solar-/Dachflächenkatasters nicht mehr entgegenzustellen.

Bei der vom Thüringer Umweltinformationsgesetz geforderten Abwägung zwischen der Unterrichtung der Öffentlichkeit über Umweltinformationen und dem Schutz privater Belange überwiegt nach Einschätzung des Thüringer Landesbeauftragten für den Datenschutz das öffentliche Interesse. Er legt dabei besonderen Wert auf die Feststellung, dass die Verwirklichung des Umweltschutzzieles für den Staat nach Art. 31 Thüringer Verfassung und Art. 20a des Grundgesetzes Verfassungsrang besitzt. Dem gegenüber tritt hier der relativ geringe Eingriff in das Recht der informationellen Selbstbestimmung des Betroffenen zurück, zumal nach dessen Widerspruch dieser Eingriff gänzlich entfällt.

Denn die Zustimmung zur Veröffentlichung des Solarkatasters durch die Stadt Erfurt ist zur Wahrung der Rechte der Betroffenen davon abhängig, dass jedem Eigentümer vor der Veröffentlichung rechtzeitig die Möglichkeit des Widerspruchs eingeräumt wird. Über die Verfahrensweise wird die Stadt Erfurt auf geeignete Weise informieren.

Der Thüringer Landesbeauftragte für den Datenschutz geht davon aus, dass auch andere Thüringer Städte auf das „Erfurter Modell“ zurückgreifen werden.

Anlage 45

Pressemitteilung
vom 19. September 2012

Sicherheitshinweis des BSI !!!
„Kritische Schwachstelle im Internet Explorer“

Der Thüringer Landesbeauftragte für den Datenschutz, Dr. Lutz Hasse, weist auf folgende Warnung des BSI (Bundesamt für Sicherheit in der Informationstechnik) vom 18. September 2012 hin:

„PC-Nutzer, die den Internet Explorer in den Versionen 7, 8 oder 9 verwenden, sollten derzeit einen alternativen Browser nutzen, um ins Internet zu gehen. Der Grund ist eine bisher unbekannte, kritische Schwachstelle im Internetbrowser von Microsoft, die möglicherweise von Online-Kriminellen für Angriffe ausgenutzt werden kann. Da der entsprechende Angriffscode im Internet frei verfügbar ist, muss von einer breitflächigen Nutzung ausgegangen werden. Somit steht Online-Kriminellen quasi die Tür zum Rechner der Nutzer offen und sie können jegliche Schadsoftware auf die Rechner aufspielen – je nachdem, welche Zwecke sie verfolgen.

Um die Schwachstelle auszunutzen, reicht es aus, den Internetnutzer auf eine präparierte Webseite zu locken. Beim Anzeigen dieser Webseite kann dann durch Ausnutzen der Schwachstelle beliebiger Schadcode auf dem betroffenen System mit den Rechten des Nutzers ausgeführt werden. Angreifer können somit beispielsweise Transaktionsdaten ausspähen, den E-Mailverkehr mitlesen, den Rechner kapern und zu einem Teil eines Botnetzes machen oder den Rechner sperren, um einen Geldbetrag zu erpressen. Nutzer des Internet Explorers in Versionen 7, 8 und 9 können sich quasi im Vorbeisurfen diesen Schadcode einfangen und ihren Rechner infizieren.

Ein Sicherheitsupdate von Microsoft ist derzeit nicht verfügbar. Daher empfiehlt das BSI allen Nutzern des Internet Explorers, so lange einen alternativen Browser für die Internetnutzung zu verwenden, bis der Hersteller ein Sicherheitsupdate zur Verfügung gestellt hat Das BSI steht bezüglich einer Lösung zur Schließung der

Schwachstelle mit Microsoft in Verbindung. Sobald die Sicherheitslücke geschlossen ist, wird das BSI darüber informieren.“

Anlage 46

Pressemitteilung
vom 20.September 2012

Sicherheitsupdate für kritische Schwachstelle im Internet Explorer für Freitagabend, den 21. September 2012, angekündigt

Am 19. September 2012 wies der Thüringer Landesbeauftragte für den Datenschutz, Dr. Lutz Hasse, darauf hin, dass das BSI (Bundesamt für Sicherheit in der Informationstechnik) wegen einer bisher unbekannten, kritischen Schwachstelle im Internet Explorer in den Versionen 7, 8 oder 9 solange die Nutzung eines alternativen Browsers empfiehlt, bis ein entsprechendes Sicherheitsupdate von Microsoft zur Verfügung steht.

Nach Angaben des BSI (20.09.2012) stellt Microsoft derzeit ein Fixit Tool als temporäre Gegenmaßnahme zum Download zur Verfügung. *„Damit wird die Schwachstelle zwar nicht geschlossen, kann aber dazu beitragen, die Ausnutzung der Schwachstelle zu erschweren. Microsoft hat angekündigt, am Freitagabend, den 21. September 2012, ein Sicherheitsupdate bereit zu stellen, das die Sicherheitslücke schließt.*

Das BSI empfiehlt Anwendern des Internet Explorers, sowohl das Fixit Tool als auch das für morgen angekündigte Sicherheitsupdate zu installieren.“

Anlage 47

Pressemitteilung
vom 27. September 2012

Besseres Datenschutzbewusstsein bei Schülern
Kooperation TLfD – Thillm

Der Thüringer Landesbeauftragte für den Datenschutz, Herr Dr. Lutz Hasse, hat mit dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (Thillm) einen Kooperationsvertrag für einen Zeitraum von sechs Jahren geschlossen. Die Unterzeichnung erfolgte im Rahmen der Fachtagung des Medienkompetenznetzwerks Thüringen am 26. September 2012.
Es ist dem Thüringer Landesbeauftragten für den Datenschutz ein wichtiges Anliegen, gerade die datenschutzrechtlichen Kompetenzen von Schülerinnen und Schülern zu stärken. Insbesondere diese jungen Menschen sind es, die mit den neuen Medien täglich in Berührung kommen und viel zu oft unbefangen persönliche Daten preisgeben, ohne sich über die möglichen Folgen bewusst zu sein und ohne ihre tatsächlichen und rechtlichen Möglichkeiten zu kennen.
Nach dem Kooperationsvertrag liegen die inhaltlichen Schwerpunkte der Zusammenarbeit darin, Lehrerinnen und Lehrern speziell über rechtliche Grundlagen und aktuelle datenschutzrechtliche Problemstellungen aus der Schulwelt zu informieren, damit sie als Multiplikatoren Datenschutzrecht als Teilmenge der Medienkompetenz an die Schülerinnen und Schüler, aber auch die Lehrerkolleginnen und Lehrerkollegen herantragen können. Gemeinsam mit dem Thillm sollen mit der Evaluation des Unterrichtsfaches Medienkunde etwaige Defizite behoben werden, etwa durch Erstellung von Unterrichtsmaterialien speziell für Thüringen unter Mitwirkung erfahrener Pädagoginnen und Pädagogen. Aber auch die Lehrerausbildung könnte um ein Modul „Medienkompetenz“ ergänzt werden.
Daneben möchte der Thüringer Landesbeauftragte sein Engagement „vor Ort“ in den Schulen fortsetzen und Lehrerinnen und Lehrern, Eltern und Schülerinnen und Schülern beratend zur Seite stehen. Die hierbei bereits gewonnenen Erfahrungen ermutigen dazu, diesen Weg des lebendigen Dialogs weiter zu beschreiten (im Rahmen der personellen Möglichkeiten des TLfD).

Den Text der Kooperationsvereinbarung finden Sie unter http://www.thueringen.de/imperia/md/content/datenschutz/veroeffentlichungen/kooperationsvertrag.pdf

Anlage 48

Pressemitteilung
vom 15. Oktober 2012

Thüringer Landesamt für Verfassungsschutz:
Datenlöschung rechtswidrig

Das Thüringer Landesamt für Verfassungsschutz (TLfV) sah sich in seiner Pressemitteilung vom 12. Oktober 2012 zu folgenden Mitteilungen veranlasst:

Das TLfV meint, vor Löschung personenbezogener Daten/Akten hätten diese dem Thüringer Hauptstaatsarchiv nicht angeboten werden müssen. Der insoweit vom Thüringer Landesbeauftragten für den Datenschutz (TLfD) vorgeworfene Rechtsverstoß sei unberechtigt. Zudem sei die Zuständigkeit des TLfD für solche Feststellungen zweifelhaft.

Diese Rechtsirrtümer bedürfen der Klarstellung:

- **Alle** in § 3 Thüringer Archivgesetz (ThürArchivG) genannten **Behörden**, also auch das TLfV, sind gemäß § 11 ThürArchivG verpflichtet, sämtliche Unterlagen vor der Löschung dem **Staatsarchiv** zur Übernahme anzubieten. **Nur dort** wird darüber entschieden, welche dieser Unterlagen nicht archivwürdig sind und mithin gelöscht werden können. Mit seiner Pressemitteilung räumt das TLfV indes ein, diese Rechtslage zu ignorieren und rechtswidrigerweise die Unterlagen zu löschen und gelöscht zu haben.

- Dass das Thüringer Verfassungsschutzgesetz Vorschriften zur Löschung enthält – worauf das TLfV zutreffend hinweist – ist unstrittig. Ebenso unstrittig ist allerdings der Umstand, dass das Verfassungsschutzgesetz kein Eremitendasein führt, sondern im Kontext zu anderen Gesetzen steht. Und so lassen denn der bereits erwähnte **§ 3 als auch § 11 ThürArchivG** (s. Anlage) überhaupt keinen Zweifel daran, dass das TLfV **auch der Geheimhaltung unterlie-**

gende Unterlagen dem Staatsarchiv vor deren Löschung anzubieten hat.

- Der TLfD ist nach **Artikel 69 Thüringer Verfassung** berufen, das Recht auf Schutz der personenbezogenen Daten zu wahren. Damit fällt es in die Zuständigkeit des TLfD, bei der Datenverarbeitung darauf zu achten, dass Löschvorschriften eingehalten werden. Dazu zählt auch, dass eine Löschung personenbezogener Daten unterbleibt, wenn diese vom Staatsarchiv als archivwürdig angesehen werden – was natürlich voraussetzt, dass diese Daten dem Staatsarchiv überhaupt zur Prüfung der Archivwürdigkeit angeboten werden.

Nicht nur rechtlich bitter ist, dass das TLfV meint, seine Rechtsirrtümer in den Fokus der Öffentlichkeit rücken zu müssen. Es ist aber auch unverständlich, da das TLfV in seiner Pressemitteilung selbst anführt, mit dem Staatsarchiv in Kontakt treten zu wollen. Letzteres macht aber nur Sinn, wenn das ThürArchivG Anwendung finden soll, was das TLfV indes zuvor bestreitet.

Wenn das TLfV sich nunmehr doch noch dazu durchringen sollte, das Thüringer Archivrecht künftig einzuhalten zu wollen, was diesseits empfohlen wird, sollte es Unterlagen solange aufbewahren, bis das Staatsarchiv sie übernehmen kann. Eine vorherige rechtswidrige Löschung scheidet somit weiterhin aus.

Anlage

Thüringer Gesetz über die Sicherung und Nutzung von Archivgut (Thüringer Archivgesetz - ThürArchivG)Vom 23. April 1992
(letzte Änderung: § 16 geändert durch Artikel 4 des Gesetzes vom 16. Juli 2008 (GVBl. S. 243, 244))

Auszug:

§ 3
Archivgut des Landes und des Bundes

(1) Als öffentliches Archivgut des Landes werden alle archivwürdigen Unterlagen bestimmt, die bei den Verfassungsorganen, Behör-

den, Gerichten und sonstigen Stellen des Landes Thüringen, bei deren Funktions- und Rechtsvorgängern sowie bei sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen entstanden sind und von den thüringischen Staatsarchiven nach Maßgabe dieses Gesetzes archiviert werden.
(2) Die in Wahrnehmung staatlicher Aufgaben entstandenen Unterlagen der SED, übrigen Parteien und Massenorganisationen der ehemaligen DDR sowie der mit ihnen verbundenen Organisationen und juristischen Personen, soweit sie bei einem Organisationsteil angefallen sind, der auf staatlicher Ebene Funktionsvorgänger des Landes oder einer kleineren Einheit war, werden wie Archivgut des Landes behandelt. Dies gilt, sobald die in Satz 1 genannten Unterlagen in den staatlichen Archiven des Landes Thüringen archiviert werden.
(3) Werden von den zuständigen Staatsarchiven Unterlagen nachgeordneter Stellen des Bundes übernommen, so gelten sie als öffentliches Archivgut des Landes im Sinne dieses Gesetzes, soweit bundesrechtlich nicht anders bestimmt ist. Für die Benutzung solcher Unterlagen gelten die Bestimmungen des Bundesarchivgesetzes entsprechend.

§ 11
Aussonderung und Anbietung von Archivgut

(1) Die in § 3 Abs. 1 und § 4 Abs. 1 genannten öffentlichen Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind und deren Aufbewahrungsfristen abgelaufen sind, auszusondern und dem zuständigen Archiv zur Übernahme anzubieten, sofern bundesrechtlich nicht anders bestimmt ist. Dies sollte im Regelfall 30 Jahre nach Schließung der Unterlagen erfolgen. Die in § 3 Abs. 2 genannten Stellen sind verpflichtet, die dort genannten Unterlagen den Staatsarchiven unverzüglich vollständig anzubieten und sie auf Anforderung herauszugeben.
(2) Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind. Unberührt bleiben gesetzliche Vorschriften über die Löschung oder Vernichtung unzulässig erhobener oder verarbeiteter Daten oder Unterlagen.
(3) Die in § 3 Abs. 1 und § 4 Abs. 1 genannten öffentlichen Stellen dürfen Unterlagen nur vernichten oder Daten nur löschen, wenn das

zuständige öffentliche Archiv die Übernahme abgelehnt oder nicht innerhalb eines Jahres über die Archivwürdigkeit angebotener Unterlagen entschieden hat.
(4) Von dem Anbieten und Vorlegen von Unterlagen kann im Einvernehmen mit dem zuständigen Archiv abgesehen werden, wenn diese wegen ihres offensichtlich geringen Quellenwertes nicht archivwürdig sind.
(5) Ausgesonderte Unterlagen sind im Regelfall zu vernichten, sofern kein Grund zu der Annahme besteht, dass durch die Vernichtung schutzwürdige Belange von Betroffenen beeinträchtigt werden.
(6) Die in § 3 Abs. 1 und § 4 Abs. 1 genannten öffentlichen Stellen sind verpflichtet, ein Exemplar der von ihnen herausgegebenen Druckschriften dem zuständigen öffentlichen Archiv zur Verfügung zu stellen.

Anlage 49

Pressemitteilung
vom 19. Oktober 2012

Datenschutztagung zu sozialen Netzwerken

Der Thüringer Landesbeauftragte für den Datenschutz, Dr. Lutz Hasse veranstaltet in Kooperation mit dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien, der Thüringer Verbraucherzentrale und der Landesarbeitsgemeinschaft Kinder- und Jugendschutz e. V. am 4. Dezember 2012 im Festsaal des Rathauses der Stadt Erfurt das Symposium:

„Soziale“ Netzwerke? Meine Daten! Mein Leben! – Dein Geschäft!

Adressaten der Veranstaltung sind insbesondere Schüler, Lehrer, Sozialarbeiter, Schuldnerberater, Verbraucherverbände: sie sollen für das Thema Datenschutz in sozialen Netzwerken sensibilisiert werden.

Soziale Kommunikation zwischen Jugendlichen findet heute größtenteils über soziale Netzwerke im Internet statt; der Datenschutz bleibt dabei oft auf der Strecke. Gerade junge Menschen geben Daten von sich preis, ohne sich über die Konsequenzen im Klaren zu sein. Den erwachsenen Ansprechpartnern fehlt es oftmals an ausreichendem Wissen über die Datennutzung dieser Unternehmen. Die Tagung soll die Hintergründe von sozialen Netzwerken verdeutlichen, die damit verbundenen Probleme näher beleuchten und Lösungsmöglichkeiten aufzeigen.

Vorträge über die datenschutzrechtlichen Grundlagen, spezielle datenschutzrechtliche Probleme bei Facebook sowie Cybercrime und Datenmissbrauch stehen auf dem Programm. Spezifische Themenbereiche können dann mit Experten am Nachmittag in Workshops bearbeitet werden.

Die Teilnahme an der Tagung ist kostenlos. Bei Interesse wenden Sie sich bitte an die Verbraucherzentrale Thüringen. Weitere Informationen finden Sie unter:
http://www.thueringen.de/imperia/md/content/datenschutz/themen/medien/flyer_informationsveranstaltung_04.12.2012.pdf

Anlage 50

Pressemitteilung
vom 23. November 2012

Unabhängigkeit des Thüringer Landesbeauftragten für den Datenschutz (TLfD) wird vom Thüringer Generalstaatsanwalt in Frage gestellt

In seiner Pressemitteilung vom 16.11.2012 (Anlage), die der TLfD erst jüngst aufspüren konnte, lässt sich der Thüringer Generalstaatsanwalt zu folgender Aussage hinreißen:

„Soweit in der Presse der Thüringer Datenschutzbeauftragte mit den Worten zitiert wird, er „fürchte, dass sich im Laufe der Untersuchungen Rechtsverstöße ergeben werden“, halte ich eine solche Äußerung vor seiner Kontrolle für nur schwer vereinbar mit der Unabhängigkeit seines Amtes. In diesem Zusammenhang ist darauf hinzuweisen, dass für die Staatsanwaltschaft – ebenso wie für die Strafgerichte – die Strafprozessordnung maßgeblich ist.“

Aufgrund dieser tatsächlichen und juristischen Fehleinschätzung sind folgende Hinweise an den Thüringer Generalstaatsanwalt angezeigt:

1. Der TLfD bezieht seine Informationen nicht allein durch Akteneinsicht, sondern aus diversen Quellennetzen.
2. Die verfassungsrechtlich garantierte Unabhängigkeit gestattet daher dem TLfD, seine rechtliche Einschätzung von Sachverhalten jederzeit zu veröffentlichen.
3. Den untauglichen Versuch zu starten, über diese verfassungsrechtliche Position des TLfD zu befinden, liegt weit jenseits der Kompetenz des Thüringer Generalstaatsanwalts.
4. Die Feststellung des Thüringer Generalstaatsanwalts, für die Staatsanwaltschaft gelte die Strafprozessordnung, ist frei von Einwänden. Allerdings steht die Staatsanwaltschaft nicht außerhalb der übrigen Rechtsordnung und ist mithin auch dem Datenschutzrecht unterworfen. Diese Sichtweise sich zeitnah anzueignen, wird dem Thüringer Generalstaatsanwalt angeraten.

5. Hier ist nicht bekannt, welche Motivation den Thüringer Generalstaatsanwalt bewogen hat, die Integrität des Verfassungsorgans TLfD in Zweifel zu ziehen, ohne sich offenbar im konkreten Fall zuvor einem näheren Aktenstudium zu unterziehen. Dieses nachzuholen, wird dem Thüringer Generalstaatsanwalt diesseits dringend empfohlen.
6. Bei Fragen im Zusammenhang mit der normativen Koexistenz von Strafprozessordnung und Datenschutzrecht bietet der TLfD hiermit selbstverständlich gern seine Unterstützung an.

1 Anlage

Pressemitteilung der Thüringer Generalstaatsanwaltschaft, Der Generalstaatsanwalt vom 16. November 2012

Thüringer Generalstaatsanwalt weist Diffamierung der Staatsanwaltschaft zurück

Ich begrüße es sehr, dass in dem Ermittlungsverfahren gegen einen Thüringer Polizeibeamten wegen der Verletzung des Dienstgeheimnisses und eine besonderen Geheimhaltungspflicht (§ 353b StGB) durch ein Gericht überprüft werden soll, ob das Vorgehen der Ermittlungsbehörden rechtlich zulässig war. Damit kommt die Sache vor die Justiz, wo sie hingehört.
Den Vorwurf der Abgeordneten des Thüringer Landtages Martin Renner, „dass Polizei und Staatsanwaltschaft beliebige Ermittlungsverfahren dazu missbrauchen, Informationsnetzwerke und Kommunikationsinhalte von Abgeordneten auszuforschen“ (Pressemeldung der Fraktion DIE LINKE vom 15.11.12), weise ich hingegen entschieden zurück.
Die Unterstellung, den Ermittlungsmaßnahmen der Staatsanwaltschaft lägen unsachliche Motive zugrunde, ist nicht akzeptabel. Diese Äußerung ist nicht nur ein die Thüringer Staatsanwältinnen und Staatsanwälte pauschal herabwürdigendes Unwerturteil, vielmehr wird damit faktisch auch der Staatsanwaltschaft insgesamt Rechtsbeugung vorgeworden. Dieser Vorwurf ist absurd.
Entsprechendes gilt für die in der Presse zitierte Äußerung des Fraktionsvorsitzenden Bodo Ramelow, „die zuständige Staatsanwaltschaft Meiningen habe ‚wohl ein Rad ab‘“.

Soweit in der Presse der Thüringer Datenschutzbeauftragte mit den Worten zitiert wird, er „fürchte, dass sich im Laufe der Untersuchungen Rechtsverstöße ergeben werden“, halte ich eine solche Äußerung vor deiner Kontrolle für nur schwer vereinbar mit der Unabhängigkeit seines Amtes.
In diesem Zusammenhang ist darauf hinzuweisen, dass für die Staatsanwaltschaft – ebenso wie für die Strafgerichte – die Strafprozessordnung maßgeblich ist.

Hartmut Reibold

Anlage 51

Pressemitteilung
vom 28. November 2012

„Soziale“ Netzwerke?
Meine Daten! Mein Leben! – Dein Geschäft!

Unter diesem Titel veranstaltet der Thüringer Landesbeauftragte für den Datenschutz, Dr. Lutz Hasse, in Kooperation mit dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien, der Thüringer Verbraucherzentrale und der Landesarbeitsgemeinschaft Kinder- und Jugendschutz e. V. am 4. Dezember 2012 im Rathaus der Stadt Erfurt ein Symposium zu den Möglichkeiten, aber auch den Gefahren sozialer Netzwerke.

Fast einhundertfünfzig Teilnehmer haben sich bereits angemeldet. Vor allem Schüler und Lehrer, aber auch Thüringer Polizeibeamte sowie Mitarbeiter von Jugendschutzeinrichtungen wollen sich dort auch mit den verschiedenen Hintergründen der Nutzung sozialer Netzwerke auseinandersetzen. Sie erwarten unter anderem spannende Vorträge über die datenschutzrechtlichen Probleme speziell bei Facebook, den Umgang mit Cybercrime sowie die (spezifischen) Verhaltensweisen im Netz. Am Nachmittag besteht dann Gelegenheit, sich mit der Materie in Workshops vertieft auseinanderzusetzen. Schüler des Albert-Schweitzer-Gymnasiums stellen beispielsweise ihre „Facebook-Welt“ vor; eine Mitarbeiterin des Projektes „Medienwelten in der Familie“ beleuchtet die aus sozialen Netzwerken resultierenden Anforderungen an die pädagogische Arbeit und es gibt die Gelegenheit, sich über Gegenmaßnahmen bei Cybermobbing auszutauschen.

Herr Staatssekretär Prof. Dr. Roland Merten wird die Veranstaltung um 10.00 Uhr mit einem Grußwort eröffnen. Vertreter der Medien sind herzlich willkommen!

Gleichzeitig findet am 4. Dezember 2012 ab 16.00 Uhr die – nicht öffentliche – achte Sitzung des Arbeitskreises „Datenschutz und Bildung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in den Räumen des Rathauses der Stadt Erfurt statt;

diese Veranstaltung wird am 5. Dezember 2012 enden. Die Teilnehmer des Arbeitskreises können die Gelegenheit nutzen, zunächst an dem Symposium teilzunehmen, um sich im Anschluss daran weiteren Fragen der Medienkompetenz im Bildungsbereich zuzuwenden.

Anlage 52

Pressemitteilung
vom 5. Dezember 2012

Volles Haus!

Am 4. Dezember 2012 veranstaltete der Thüringer Landesbeauftragte für den Datenschutz (TLfD), Herr Dr. Lutz Hasse, in Kooperation mit dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien, der Thüringer Verbraucherzentrale und der Landesarbeitsgemeinschaft Kinder- und Jugendschutz e. V im Rathaus der Stadt Erfurt ein Symposium unter dem Titel "„Soziale" Netzwerke? Meine Daten! Mein Leben! – Dein Geschäft!". Der große Festsaal war mit mehr als einhundertfünfzig Teilnehmern aus verschiedenen Bereichen (Lehrern, Schülern, Polizeibeamten, Jugendarbeitern) bis auf den letzten Platz belegt. Die spannenden und zugleich hochkarätigen Vorträge zu verschieden Themen rund um soziale Netzwerke werden in Kürze auf der Homepage des TLfD bereitgestellt werden. Bewegt haben die Besucher insbesondere die Ausführungen einer Mitarbeiterin des LKA dazu, wie leicht es ist, sich sozialer Netzwerke zum Zweck krimineller Machenschaften zu bedienen. Einer der nachmittäglichen Höhepunkte war ein von Schülern des Albert-Schweitzer-Gymnasiums geleiteter Workshop. Hier konnten die Teilnehmer „life" miterleben, wie Jugendliche über Facebook kommunizieren, warum dieses Netzwerk eine so große Faszination ausübt und wie schnell sich private Informationen ohne Zutun des Betroffenen über das Netz verbreiten.
Im Anschluss an die Veranstaltung tagte der Arbeitskreis „Datenschutz und Bildung" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Dieser gründete die Arbeitsgruppe „Schuldatenschutz", die unter Vorsitz des Thüringer Landesbeauftragten für den Datenschutz künftig regelmäßig in Erfurt tagen wird. Aufgabe dieser Arbeitsgruppe wird es sein, aktuelle Probleme des Datenschutzes in Schulen aufzugreifen und zu lösen. Beeindruckt waren die Teilnehmer des Arbeitskreises vom Interesse und der Offenheit des Staatssekretärs Prof. Dr. Roland Merten, der sich über den intensiven Kontakt zwischen Kultusministerium und TLfD sehr erfreut zeigte und gemeinsamen Vorhaben volle Unterstützung zusagte.

Anlage 53

Pressemitteilung
vom 21. Dezember 2012

Nicht jedes Mittel ist Recht!

Laut Presseinformation des mdr vom 20. Dezember 2012 wurde gegen Polizeibeamte wegen des Verdachts des Betrugs und der Untreue ermittelt, weil diese Dienstfahrzeuge für private Zwecke genutzt haben sollen. Die Rede ist von monatelanger Observation, Telekommunikationsüberwachungsmaßnahmen und der verdeckten Spiegelung von Computerdaten, die nach der Strafprozessordnung nur unter engen Voraussetzungen zulässig sind. Die Polizeigewerkschaften haben sich zwischenzeitlich ebenfalls zu Wort gemeldet und auf die Möglichkeiten der Telekommunikationsüberwachung und auf bereits stattgefundene Durchsuchungen von E-Mail Postfächern, sogar bei Personalräten hingewiesen.
Besorgnis erregend ist zudem die Information, dass die Telefontechnik über eine Mithörfunktion verfügen soll.
Keine Frage, auch Polizeibeamtinnen und Polizeibeamte, die die Staatsgewalt verkörpern, haben sich an die geltenden Rechtsvorschriften zu halten. Auch sie dürfen selbstverständlich nicht gegen Gesetze und Dienstvorschriften verstoßen. Jedoch sind auch im Polizeibereich strafprozessuale Maßnahmen gegen Beschäftigte ebenso wie interne Ermittlungen als Grundrechtseingriffe am Maßstab der Rechtmäßigkeit und der Verhältnismäßigkeit zu messen.
Da der Einsatz von heimlichen Ermittlungsmaßnahmen immer mit tiefgreifenden Eingriffen in das informationelle Selbstbestimmungsrecht der Betroffenen einhergeht und daher an strenge Voraussetzungen gebunden ist, wird der TLfD in Wahrnehmung seiner verfassungsrechtlich verankerten unabhängigen Prüfkompetenz die laut gewordenen Vorwürfe gegen die Ermittler einer datenschutzrechtlichen Überprüfung unterziehen und rasch Einsicht in die betreffenden Ermittlungsakten nehmen.
Sollte sich herausstellen, dass bei den Ermittlungen gegen die Polizeibeamtinnen und Polizeibeamten über das Ziel hinausgeschossen wurde, wird dies der TLfD in der Angelegenheit gerecht werdender Weise bewerten und entsprechende Forderungen stellen, damit das

Grundrecht der informationellen Selbstbestimmung auch bei polizeiinternen Maßnahmen endlich Beachtung findet.

Anlage 54

Pressemitteilung
vom 14. Januar 2013

BIG BROTHER – STANDARD

Die in meiner Pressemitteilung „Nicht jedes Mittel ist Recht“ vom 21. Dezember 2012 geäußerte Befürchtung hat sich inzwischen leider bewahrheitet:
Die Telefonanlagen in der Thüringer Polizei verfügen laut Auskunft des Thüringer Innenministeriums über folgende fragwürdige Funktionen

- die sog. Aufschaltfunktion: geführte Telefonate können von Dritten mitgehört werden;
- die sog. Babyfonfunktion: trotz aufgelegtem Telefonhörer können die Gespräche in demjenigen Raum, in dem sich der Telefonapparat befindet, mitgehört werden.

Was viele spaßhaft vermuteten, aber bislang kaum jemand wusste oder wahr haben wollte, ist nun für alle schockierender Ernst geworden: Ohne eigene Kenntnis und ohne Möglichkeit der eigenen Einflussnahme können bisher Aufschalt- und Babyfonfunktionen aktiviert werden. Man muss also als um den Datenschutz Bemühter nicht mehr in die Ferne des Internets schweifen, wenn die Gefahren 30 Zentimeter entfernt auf dem Schreibtisch im Telefonapparat lauern können.

Dass diese Funktionen zum „marktüblichen“ Standard der Telefonanlagen zählen sollen, macht es eher schlimmer.
Zu besorgen ist, dass sich diese Funktionen nicht auf die Telefonanlagen der Thüringer Polizei oder des Thüringer Innenministeriums beschränken, sondern sich auf Telefonanlagen der gesamten Landesverwaltung erstrecken, einschließlich der Kommunalverwaltung. Doch dessen nicht genug: Nicht unwahrscheinlich ist, dass auch Telefonanlagen in Unternehmen über derartige Funktionen verfügen. Und das wohl nicht nur in Thüringen.
Ob die fragwürdigen Funktionen aktiviert oder deaktiviert sind bzw. waren, wird im Detail zu prüfen sein. Ebenso sind sämtliche Standorte solcher Anlagen zu ermitteln.

Des Weiteren müssen technische und rechtliche Sicherungsmechanismen kontrolliert, intensiviert bzw. eingeführt werden, um das offene Tor des Missbrauchs möglichst dicht zu schließen. Das gilt auch für (Fern-)Wartungsarbeiten.
Nicht zuletzt müssen Personal- und Betriebsräte entsprechende Vereinbarungen mit dem Dienstherren bzw. den Arbeitgebern treffen.
Der TLfDI wird zu seinen Prüfungserkenntnissen fortlaufend berichten.

Der TLfDI bittet die Bürgerinnen und Bürger um Mithilfe bei der Aufklärung dieser prekären Situation!

Für weitere Fragen stehen Ihnen Frau Böhlke (Leiterin Referat Technik) unter der Telefonnummer 0361-3771931 und Frau Rühlemann (Geschäftszimmer des TLfDI) unter der Telefonnummer 0361-3771900 zur Verfügung. Sie können sich auch per E-Mail an poststelle@datenschutz.thueringen.de wenden.

Anlage 55

Pressemitteilung
vom 18. Januar 2013

Toilettenpapier endlos – Fehlende Unterstützung durch das Thüringer Landeskriminalamt (TLKA)

Jüngsten Berichten und Nachweisen des MDR zufolge verfügt das TLKA über eine juristische Stellungnahme aus eigenem Hause zur längerfristigen verdeckten Observationsmaßnahme wegen Diebstahls von Toilettenpapier.

In dieser Stellungnahme wird die Rechtswidrigkeit dieser Maßnahme festgestellt.

Unterlagen in dieser Angelegenheit – einschließlich der genannten Stellungnahme – hat der TLfDI beim TLKA mehr als einmal angefordert. Eine Übersendung der vom MDR veröffentlichten juristischen Stellungnahme erfolgte indes nicht.

Mit Befremden nimmt der TLfDI diese fehlende Unterstützung seitens des TLKA zur Kenntnis und wird hierauf entsprechend reagieren

Anlage 56

Pressemitteilung
vom 15. März 2013

85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Unter Vorsitz der Landesbeauftragten für Datenschutz und Informationsfreiheit Bremen tagte am 13. und 14. März 2013 die 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Bremerhaven.
Die Konferenz hat sich erneut für die Stärkung des Datenschutzes auf europäischer Ebene eingesetzt. Bereits im vergangenen Jahr hatte die EU-Kommission den Entwurf einer Datenschutz-Grundverordnung vorgelegt. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen aber die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten. Die Konferenz wendet sich mit der an das Europäische Parlament, den Rat und die Kommission gerichteten **Entschließung "Europa muss den Datenschutz stärken"** gegen alle Änderungsvorschläge, deren Umsetzung das Grundrecht auf Datenschutz schwächen würde.

Angesichts zunehmender Bedeutung sozialer Netzwerke hat die Datenschutzkonferenz deren Betreiber auf ihre Verpflichtung hingewiesen, die Einhaltung datenschutzrechtlicher Anforderungen zu gewährleisten. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird. Die Konferenz hat daher den Gesetzgeber in ihrer **Entschließung "Soziale Netzwerke brauchen Leitplanken"** nachdrücklich aufgefordert, die noch bestehenden Gesetzeslücken schnell zu schließen. Die Datenschutzbeauftragten haben zur Unterstützung der Betreiber sozialer Netzwerke und der die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutz- gerechten Gestaltung und Nutzung der Angebote eine **Orientierungshilfe „Soziale Netzwerke“** vorgelegt.

In allen Bundesländern werden Daten über Krebserkrankungen in Krebsregistern In allen Bundesländern werden Daten über Krebser-

krankungen in Krebsregistern gespeichert, um diese Daten der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Die Datenschutzbeauftragten sind der Auffassung, dass das vor ca. 20 Jahren entwickelte und gegenwärtig noch genutzte Verfahren für die Pseudonymisierung von Krebsregisterdaten den erforderlichen Schutz dieser höchst sensiblen Daten der Betroffenen nicht mehr in ausreichendem Maße gewährleistet. Sie fordern deshalb mit der **Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern"** die zuständigen Fachaufsichtsbehörden der Länder auf, Rahmenbedingungen für eine dem heutigen Stand der Technik angemessene Pseudonymisierung zu schaffen.

Die Konferenz hat zudem eine engere Zusammenarbeit mit der Koordinierungsstelle für IT-Standards (KoSIT) vereinbart. Die KoSIT koordiniert und erstellt im Auftrag des IT-Planungsrates des Bundes und der Länder IT-Standards für die öffentlichen Verwaltungen.

Die auf der Konferenz gefassten Entschließungen und die Orientierungshilfe sind auf der Internetseite des TLfDI http://www.thueringen.de/datenschutz abrufbar.

Anlage 57

Pressemitteilung
vom 20.März 2013

Cyber-Attacke: gefälschte Rechnungsmahnungen

Seit einigen Wochen werden deutsche Nutzer per E-Mail mit gefälschten Rechnungsmahnungen attackiert, die Trojaner enthalten. Von Sicherheitsexperten wird für den 21. März 2013 und den 4. April 2013 ein erhöhtes Aufkommen dieser Mails erwartet. Neben der Aufforderung, die Rechnung zu begleichen, wird auch eine angebliche Rechnungskopie in Form einer pdf-Anlage mit versendet.
Da der in der Rechnungskopie versteckte Trojaner nicht in jedem Fall vom Antivirenprogramm entdeckt werden kann, möchte der TLfDI folgende Hinweise geben:

- Bevor Sie eine Mail mit einer Aufforderung zum Bezahlen einer Rechnung öffnen, überlegen Sie bitte, ob Sie überhaupt eine Bestellung ausgelöst haben.
- Sofern Sie die Mail öffnen und Ihnen weiterhin Absender und Inhalt unklar bleiben sollte, öffnen Sie die **Anlage** bitte **nicht**.
- Aktualisieren Sie Ihre Adobe-, Java- und Anti-Virenprogramme!
- Führen Sie nach einem Update des Anti-Virenprogramms häufiger eine Virensuche durch. Das neue Update kann so unter Umständen Schadsoftware finden, welche sich bereits auf Ihren PC eingenistet hat und zuvor nicht erkannt werden konnte.
- Nutzen Sie regelmäßig die Rubrik „Wie mache ich meinen PC sicher“ auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

Der TLfDI wird über die weitere Entwicklung informieren.

Anlage 58

Pressemitteilung
vom 9. April 2013

Staatsanwaltschaft Meiningen nicht gehindert, unzulässig erhobene und gespeicherte Daten zu löschen

Im Ermittlungsverfahren der Staatsanwaltschaft Meiningen wegen des Verdachts der Verletzung eines Dienstgeheimnisses durch Weiterleitung von geheimhaltungsbedürftigen polizeilichen Unterlagen zum Papstbesuch in Thüringen an Medienvertreter wurde bekannt, dass unter anderem auch personenbezogene Daten der Landtagsabgeordneten Frau Renner verarbeitet wurden, indem deren Mail vom Handy des Beschuldigten ausgedruckt und in der Ermittlungsakte festgehalten (gespeichert) wurde.

Nach Prüfung des Sachverhalts kam der TLfDI zu dem Ergebnis, dass die Verarbeitung der personenbezogenen Daten der Landtagsabgeordneten in mehrfacher Hinsicht unzulässig war.
Diese datenschutzrechtlichen Verstöße beanstandete der TLfDI mit Schreiben vom 1. März 2013 förmlich gegenüber der Staatsanwaltschaft Meiningen und der KPI Suhl und forderte dazu auf, die Mail der Landtagsabgeordneten aus den Ermittlungsunterlagen zu entfernen und zu löschen. Der TLfDI hat mit Fristsetzung die Umsetzung der Beanstandung gefordert. Dieser ist die Staatsanwaltschaft Meiningen bis zum jetzigen Zeitpunkt nicht nachgekommen. Sie verweist in ihrer Presseinformation vom 8. April 2013 auf ein laufendes gerichtliches Verfahren, dessen Ausgang – ihrer Auffassung nach – abzuwarten sei, bevor sie die Löschung der Mail der Landtagsabgeordneten vornehmen kann.
Der TLfDI weist darauf hin, dass die Staatsanwaltschaft Meiningen unabhängig von einem gerichtlichen Verfahren eigenständig entscheiden kann, ob sie der Rechtsauffassung des TLfDI folgt. Dazu muss sie nicht den Ausgang des gerichtlichen Verfahrens abwarten. Eine Pflicht der Staatsanwaltschaft, einen Verstoß gegen das Datenschutzrecht für die Dauer eines laufenden Gerichtsverfahrens zu perpetuieren, ist aus Sicht des TLfDI nicht erkennbar.

In diesem Zusammenhang weist der TLfDI darauf hin, dass die Staatsanwaltschaft Meiningen wegen fehlender Unterstützung erneut durch den TLfDI beanstandet werden kann.

Anlage 59

Pressemitteilung
vom 25. April 2013

Neue Homepage – Datenschutz in Bewegung

Der neue Internetauftritt des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist ab sofort unter www.tlfdi.de abrufbar. Die Website präsentiert sich nicht nur unter einer neuen Webadresse, sondern auch in einem lebendigen Layout. Die Seite soll künftig wichtige Informationen rund um das Thema Datenschutz und Informationsfreiheit besser in Szene setzen, um auf diese Weise den Zugang attraktiver zu gestalten. So bietet beispielsweise der Schnelleinstieg „DATENSCHUTZ FÜR WEN“ direkten Zugriff auf ausgewählte Themen für Bürger, Unternehmen und Behörden. Die aktuellen Datenschutznews sind auf der Startseite hinterlegt. Weiterhin ist durch die neue Navigation ein schneller Überblick über alle Kernbereiche der Arbeitsaufgaben des TLfDI möglich. Die Seite soll nun vor allem auch junge Nutzer ansprechen und somit animieren, sich mit dem Thema Datenschutz in der Schule, in sozialen Netzwerken oder bei Unternehmen/Firmen auch anhand von Videoclips auseinander zu setzen. Der neue Aufgabenbereich der Informationsfreiheit ist ebenfalls eingebunden.
Zeitnah werden via Homepage des TLfDI Diskussionsforen und Blogs für Bürger, Krankenhäuser, Schulen, Unternehmen und Kommunen zur Verfügung stehen. Hier kann der TLfDI mit allen (datenschutz-/informationsfreiheitsrechtlichen) Anliegen bombardiert werden.

Natürlich wird die Homepage fortlaufend weiterentwickelt; konstruktive Verbesserungsvorschläge richten Sie bitte an
poststelle@datenschutz.thueringen.de
– damit wir nicht einrosten ;-)

Anlage 60

Pressemitteilung
vom 25. April 2013

Datenschutz im Klassenzimmer gestärkt!

Am 24. Und 25. April 2013 trafen sich die für Schuldatenschutz zuständigen Vertreter der Landesdatenschutzbeauftragten unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zur ersten Sitzung der Arbeitsgruppe „Datenschutz und Schule“. Die Arbeitsgruppe wurde auf Initiative des TLfDI ins Leben gerufen, um mit vereinten Kräften den Datenschutz an Schulen zu verbessern. Die Arbeitsgruppe wird jährlich beim TLfDI tagen, um spezielle datenschutzrechtliche Probleme im Schulbereich gemeinsam zu lösen. Nach Ansicht des TLfDI ist der fachliche Austausch in diesem Bereich unerlässlich. Der technische Fortschritt macht auch vor Schulen nicht Halt. Die pädagogische Arbeit wird zunehmend durch neue Techniken unterstützt. Als Stichworte seien das E-Learning über das Internet, das elektronisches Klassenbuch, elektronische Kommunikationsmöglichkeiten, soziale Medien und die Verwendung von Chipkarten genannt. Diese Hilfsmittel kommen oft zum Einsatz, ohne dass die Beteiligten sich der damit verbundenen datenschutzrechtlichen Gefahren bewusst sind oder darauf irgendeinen Einfluss hätten.
Die Sitzung in Erfurt gab den Vertretern der Datenschutzbeauftragten der Länder die Gelegenheit zum intensiven fachlichen Austausch. So konnten neue Impulse für die datenschutzrechtliche Begleitung der Schulen gewonnen werden. Als erste Maßnahme wird die Arbeitsgruppe „Datenschutz und Schule“ eine Orientierungshilfe zu Anforderungen an datenschutzgerechtes E-Learning entwickeln.
Der TLfDI wird über die erzielten Ergebnisse auf seiner Homepage unter dem Thema „Schule“ berichten und sich damit an die, die es angeht, wenden.

Anlage 61

Pressemitteilung
vom 26. April 2013

Gefahr für Steuergeheimnis und Sozialdaten

Seit dem 3. Mai 2011 ist das De-Mail-Gesetz in Kraft. Es regelt, dass mit sogenannten De-Mail-Diensten (z. B. Versenden von De-Mails oder das Ablegen von wichtigen Dokumenten in einem sogenannten De-Safe) ein sicherer, vertraulicher und nachweisbarer Geschäftsverkehr für jedermann im Internet gewährleistet werden soll.

Doch diese Vertraulichkeit lässt zu wünschen übrig. Die teilnehmenden akkreditierten Diensteanbieter sind nach dem Gesetz gezwungen, durch geeignete Maßnahmen sicherzustellen, dass nach Eingang einer Nachricht diese unmittelbar auf Schadsoftware zu prüfen ist. Dies bedeutet, dass dort jede De-Mail für einen kurzen Moment automatisch *entschlüsselt und geprüft* wird, bevor sie weitergeleitet oder für den Abruf gespeichert wird. Beruhigt wird der Nutzer damit, dass die Diensteanbieter durch eine vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Technischen Richtlinie (BSI TR 01201) i. V. m.§ 18 De-Mail-Gesetz verpflichtet wurden, die Entschlüsselung ausschließlich zur Prüfung auf Schadsoftware durchzuführen und durch geeignete Maßnahmen sicherzustellen, dass für Unbefugte keine Möglichkeit besteht, den Nachrichteninhalt zur Kenntnis zu nehmen. Der Begriff des Unbefugten wird jedoch nicht näher bestimmt. Derjenige, der heute noch unbefugt ist, kann morgen schon zu einem Befugten werden!
Manche glauben gar, diese gesetzlich vorgeschriebene kurzzeitige Entschlüsselung der Daten in den Klartext könnte sich zu einer Schnittstelle für Ermittlungsbehörden entwickeln.

Aus datenschutzrechtlicher Sicht wird den Bürgern, den Unternehmen und der Verwaltung mit De-Mail keine vertrauliche Kommunikationsmöglichkeit für das Internet ermöglicht.
Das De-Mail-Gesetz erlaubt zwar, zusätzlich eine Ende-zu-Ende Verschlüsselung einzusetzen, allerdings muss sich der Nutzer darum selbst kümmern und der Empfänger muss diese auch handhaben können.

2011 hat der Gesetzgeber noch erkannt, dass mit De-Mail keinesfalls die Vertraulichkeit der Daten gewährleistet wird. So wurde in der Begründung zum De-Mail-Gesetz extra darauf hingewiesen, dass im Bereich des § 30 Abgabenordnung (AO) – Steuergeheimnis – eine Übermittlung von Nachrichten per De-Mail von der Behörde zu Steuerpflichtigen ausscheide. Mit dem derzeit im Bundesrat vorliegenden Gesetzentwurf zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (BT DS 17/11473) will der Bund nun auch den elektronischen Versand von besonders sensiblen Daten, wie bspw. Sozial- und Steuerdaten, per De-Mail zulassen. Dies geschieht, in dem er das Öffnen und Prüfen der De- Mails beim Diensteanbieter nunmehr per Gesetz als unkritisch einstuft – ein bemerkenswertes Vorgehen:
In § 30 AO und § 87 AO soll die Klausel aufgenommen werden, dass der Vorgang bei den Diensteanbietern (Entschlüsseln und Prüfen von Daten, die auch dem Steuergeheimnis unterliegen) nun doch keine unbefugte Offenbarung, Verwertung und kein unbefugter Abruf von dem Steuergeheimnis unterliegenden Daten sei und nicht gegen das Verschlüsselungsgebot verstoßen werde.
Doch weiter:
Die Datenübermittlung von Sozialdaten ist im Zehnten Buch Sozialgesetzbuch (SGB X) in der Anlage zum SGB X geregelt. Werden Sozialdaten automatisiert verarbeitet oder genutzt, sind insbesondere dem *Stand der Technik* entsprechende Verschlüsselungsverfahren einzusetzen. Eine dem Stand der Technik entsprechende Ende-zu-Ende Verschlüsselung ist daher zwingend vorgeschrieben.
Der Gesetzgeber will nunmehr jedoch in § 67 Abs. 6 Satz 2 Nr. 3 Zehntes Buch Sozialgesetzbuch (SGB X) vorsehen, dass das Übermitteln einer De-Mail zum Diensteanbieter kraft Gesetzes gar keine Übermittlung sei – ebenfalls bemerkenswert. Die beabsichtigte Folge wäre, dass der bisher vorgeschriebene Einsatz von dem Stand der Technik entsprechenden Verschlüsselungsverfahren ausgehebelt werden würde und bei der Datenübermittlung von Sozialdaten mittels De-Mail keine Ende-zu-Ende Verschlüsselung mehr erfolgen muss.

Seltsam: Der Gesetzgeber weist in seiner Gesetzesbegründung selbst darauf hin, dass es in bestimmten Konstellationen erforderlich werden könne, die Ende-zu-Ende-Verschlüsselung zusätzlich zur De-

Mail zu verwenden und die Empfehlungen der Beauftragten für den Datenschutz des Bundes und der Länder zu beachten.

Den Bürgern ist daher dringend anzuraten, genau zu prüfen, ob sie De-Mail nutzen möchten und inwieweit sie ihre De-Mail-Adresse in öffentlichen Verzeichnissen für alle Verfahren der Behörden zugänglich machen oder den Zugang weiterhin gegenüber jeder Behörde einzeln erklären wollen.

Wenn Sie sensible Daten tatsächlich vertraulich versenden möchten, müssen Sie diese selbst mit Zusatzsoftware vor dem Versand verschlüsseln. Entsprechende Software wird speziell vom Bundesamt für Sicherheit in der Informationstechnik für die Ende-zu-Ende-Verschlüsselung bei der Nutzung von De-Mail empfohlen:
https://www.bsi.bund.de/BSIFB/DE/SicherheitImNetz/KommunikationUeberInternet/DeMail/VorteileundFunktionen/EndezuEndeVerschluesselung/EndezuEndeVerschluesselung.html

Anlage 62

Pressemitteilung
vom 14. Mai 2013

Multifunktionsgerät: Das unbekannte Speichermedium!

In heutigen Büros werden Drucker und Kopierer zunehmend durch Multifunktionsgeräte (auch „Kombi- oder Mehrzweckgeräte“, „All in One“) ersetzt.
Die Vorteile dieser Geräte im Vergleich zu klassischen Kopierern liegen auf der Hand:
Multifunktionsgeräte vereinen in sich Scanner, den automatischen Dokumenteneinzug – Automatic Document Feeder (ADF), Bildbearbeitungseinheit, Druck- sowie Sortier- und Heft-, Duplexeinheiten, Speichereinheiten, Netzwerk- und USB-Adapter, Router, Faxmodem, speicherprogrammierte Steuerungen (SPS) oder computergestützte Steuerung und Basis-Firmware.

Wer Multifunktionsgeräte nutzt, sollte wissen, dass jedes kopierte Dokument und die darin enthaltenen Daten im Gerät elektronisch gespeichert werden.

Diese werden auf Knopfdruck (Start des Kopiervorgangs) automatisch auf interne Speichereinheiten, wie magnetische Festplatten oder Solid State Disks (SSD), geschrieben und bleiben meist ein Geräteleben lang erhalten.

Gerade bei Leasing- oder Miet-Geräten ist es kaum nachvollziehbar, wie diese Geräte später durch zwischengeschaltete Vertriebsstellen weiter veräußert bzw. umgesetzt werden. In Presse und bei Fachtests wurde mehrfach darauf aufmerksam gemacht, dass manches Gerät die komplette Historie (~.log-Dateien) sowie alle kopierten/gescannten Dokumente auf-bewahrt.

Aussagen der Gerätehersteller dazu sind widersprüchlich, tendenziell jedoch beruhigend. Manche Händler argumentieren: Keiner hätte je Kenntnis erhalten, dass von seinen Multifunktionsgeräten schon Geheimnisse gestohlen worden seien. Der Käufer hätte sich beim

Kauf des Gerätes ausschließlich im Billigsektor orientiert und dabei ausdrücklich auf Sicherheit verzichtet.
Viele Dokumentationen verschleiern im Kleingedruckten, dass bei Multifunktionsgeräten explizit Datenschutzerfordernisse zu beachten und durch geeignete Maßnahmen umzusetzen sind.

Tatsächlich haben jedoch alle bekannten Hersteller Vorsorge getroffen, dass Speicherbereiche gelöscht werden können. Nur gibt es diese Funktionalität bzw. ein entsprechendes Security Kit (Sicherheitsoption) nicht bei jedem Hersteller zum Nulltarif.

Was bedeutet das nun praktisch für die Nutzung von Multifunktionsgeräten verantwortende Stellen?

- Fragen Sie den Hersteller/Verkäufer/Leasingeber/Vermieter Ihrer Wahl, ob Speicherbereiche tatsächlich gelöscht werden und ob es dazu integrierte Funktionalitäten (Sicherheitsoptionen) gibt.
- Achten Sie darauf, dass die Löschung der Daten nicht nur vorgetäuscht wird, weil das Gerät nur den Verweis auf die Ablage der zu kopierenden Daten auf dem Speichermedium des Gerätes löscht – zugunsten der Kopiergeschwindigkeit.
- Dazu sollten Sie vor Aufstellen des Gerätes sowie Freigabe für die Nutzer in die technische Dokumentation sehen und einen technisch verantwortlichen Mitarbeiter mit der Umsetzung der o. a. Erfordernisse gemäß § 9 ThürDSG bzw. § 9 BDSG (technische und organisatorische Maßnahmen) beauftragen.
- Nutzen Sie die ggfs. als Sonderfunktion beschriebene periodische physische Löschung der Daten auf den eingebauten Speichermedien.
- Eine gute Lösung ist die Realisierung des Speichermediums als sogenannte RAM-Disks, die ihren gesamten Inhalt „vergessen“, sobald sie von der Stromversorgung getrennt werden. Hier ist die Netztrennung durch den Aus-Schalter für die Datenlöschung ausreichend – und beansprucht nicht viel Zeit in Ihren betrieblichen Abläufen.
- Ziehen Sie Geräte vor, die die aufgezeichneten Daten sicher verschlüsseln.

- Nehmen Sie den Umgang mit Multifunktionsgeräten in Ihr Sicherheitskonzept auf und treffen Sie entsprechende technisch-organisatorische Maßnahmen.
- Wer ein Gerät mit Common Criteria Zertifizierung nach ISO 15408 betreibt, kann sich sicher sein, dass er über den aktuellen technischen Stand verfügt.
- Hersteller bieten für ältere Geräte, die nicht die heutigen Standards erfüllen, ggfs. Sicherheitskits an, die Ihnen beim Lösen der entsprechenden Datenschutzprobleme helfen können. Fragen Sie in diesem Falle beim jeweiligen Hersteller nach, wenn Sie ein solches Gerät betreiben.

Insgesamt stehen die Gerätehersteller vor einer permanenten Optimierungsaufgabe. Mit der Entwicklung schneller und größerer Speichermedien steigen auch die Anforderungen an den Datenschutz und die Datensicherheit.

Anlage 63

Pressemitteilung
vom 23. Mai 2013

Gefällt Dir mein Spiel?

Sie weiß, was Du spielst, wo Du surfst, mit wem Du gerade in skype Kontakt hast, welchen Film Du siehst, welches Video Dir gefällt.
Sie reagiert auf Deine Stimme, sieht Deine Gesten und kann Deinen Herzschlag hören!!!
Sie erkennt, wenn Du Dein Gewicht von einem Fuß auf den anderen verlagerst und kann auf die kleinsten Bewegungen des Handgelenkes reagieren.
Sie sieht Dich auch, wenn Du glaubst, sie schläft.
Du hast eine Beziehung mit ihr. Du bist nicht mehr allein. Sie ist Deine Nummer Eins.

Die Rede ist allerdings nicht von Deiner Traum-Frau, sondern von der Microsoft an-gekündigten Xbox One.
Microsoft selbst verspricht den Käufern der Xbox One eine wahre Beziehung zu dem Gerät und eine Steuerung durch wahre Emotionen.
Doch wer steuert eigentlich wen? Microsoft selbst sagt „Wir haben nun die menschliche Kontrolle für ein menschliches Erlebnis“.
Aber will das tatsächlich jeder, in dieser Intensität und für immer?
Um der jeweiligen Person z. B. das am Vortag Erlebte wieder anzuzeigen und ähnliche Produkte wie Filme und Spiele anzubieten, werden Unmengen von Daten pro Nutzer gespeichert – wo auch immer. In Verbindung mit dem für die Spiele notwendigen Microsoft Account können die gesammelten Daten auch konkreten Personen zugeordnet und umfangreiche Persönlichkeitsprofile gebildet werden. Dies wird Begehrlichkeiten wecken, nicht nur für die Film- und Werbungsindustrie. Auch die Konsole selbst könnte, da sie quasi die Tür zum Wohnzimmer oder Kinderzimmer darstellt, ein begehrtes Zielobjekt für Cyberkriminelle und Sicherheitsbehörden werden.

Aus datenschutzrechtlicher Sicht bedarf es hinsichtlich der Nutzung der Xbox One von Microsoft noch umfassender Informationen, bspw. wann welche Dienste eine Internetverbindung aufbauen, wel-

che Daten nur auf der Konsole gespeichert werden, welche Daten wann und wie an Microsoft und weitere Dienstanbieter übermittelt werden und wie bspw. der Nutzer seine Daten auf den 300.000 Servern, die Microsoft dafür bereitstellen will, löschen kann.
Interessant wird auch sein, ob und wie Microsoft das unbemerkte Einschalten der Kamera und des Mikrofons durch Cyberkriminelle verhindern können wird. Denn selbst wenn der Käufer die Vertragsbedingungen und technischen Anleitungen gelesen hat, muss er Microsoft vertrauen. Da nützt es auch nur bedingt etwas, wenn er das Gerät – wie bei der Webcam – nach Gebrauch vom Netz nimmt.
Der TLfDI erwartet, dass hier seitens Microsoft eine umfassende Aufklärung des Käufers erfolgt.

Die Datenschutzbeauftragten jedenfalls sind alarmiert.

Weitere Informationen finden Sie z. B. unter:

http://www.stern.de/digital/spiele/xbox-one-und-kinect-microsofts-guckloch-inswohnzimmer-2014672.html

http://www.spiegel.de/netzwelt/games/microsoft-konsole-xbox-one-kinect-kameraschafft-datenschutz-probleme-a-900397.html

http://www.computerbild.de/artikel/cbs-News-Hardware-Xbox-One-7753883.html

Anlage 64

Pressemitteilung
vom 23. Mai 2013

Nur mit Fingerabdruck zum Arbeitsplatz ?

Auf dem Markt werden vermehrt Zeiterfassungssysteme angeboten, die biometrische Daten der Beschäftigten nutzen. Insbesondere sogenannte Fingerprint-Zeiterfassungssysteme kommen zur Anwendung.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) weist darauf hin, dass die Erhebung, Speicherung und Verwendung biometrischer Daten Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer darstellen, die datenschutzrechtlich nicht gerechtfertigt sind. Für die Zeiterfassung gibt es andere, datenschutzgerechtere Lösungen. In der Regel ist daher die Verwendung biometrischer Merkmale zu diesem Zweck nicht erforderlich, daher nicht verhältnismäßig und mithin nach § 32 Abs. 1 Satz 1 BDSG unzulässig.

„Nur in besonderen Einzelfällen kann eine biometrische Zutritts- oder Zugriffskontrolle am Arbeitsplatz unter strengen Voraussetzungen zulässig sein“, so der TLfDI, Dr. Lutz Hasse. Er empfiehlt den Arbeitgeberinnen und Arbeitgebern vor dem Einsatz von derartigen Systemen die Lektüre der „Hinweise zur biometrischen Datenerfassung am Arbeitsplatz“, die unter folgendem Link veröffentlicht sind:

http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/hinweis_biometrischen_datenerfassung_am_arbeitsplatz.pdf

Anlage 65

Pressemitteilung
vom 24. Mai 2013

Polizei, Staatsanwaltschaften, Verfassungsschutz: Aufbewahrungsfristen von personenbezogenen Daten & dienstlichem Schriftgut

In der Vergangenheit haben den TLfDI vielfach die komplexen und mitunter recht undurchsichtigen „Regelungslandschaften“ der Aufbewahrungs- und Prüffristen bei den erwähnten öffentlichen Stellen beschäftigt. Diverse Fragestellungen sowohl seitens dieser öffentlichen Stellen selbst als auch seitens der Thüringer Bürgerinnen und Bürger werden an den TLfDI herangetragen, mit denen die unterschiedlichen Aufbewahrungsfristen personenbezogener Daten und dienstlichem Schriftgut, insbesondere bei dem Thüringer Landesamt für Verfassungsschutz, der Thüringer Polizei sowie in den Thüringer Staatsanwaltschaften hinterfragt werden. Vor diesem Hintergrund ist vom TLfDI ein Leitfaden über die entsprechenden Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut unter Beachtung der archivrechtlichen Bestimmungen erarbeitet worden, der ab sofort auf der Internetseite des TLfDI abrufbar ist.

http://www.tlfdi.de/imperia/md/content/datenschutz/veroeffentlichungen/hinweistlfd_synopse.pdf

Anlage 66

Pressemitteilung
vom 6. Juni 2013

Bundesgerichtshof: Überwachung mit GPS-Empfängern durch Private grundsätzlich strafbar

In der Pressemitteilung des 1. Strafsenats des Bundesgerichtshofs (BGH) vom 4. Juni 2013 (1 StR 32/13) bestätigt der BGH, dass die heimliche Überwachung von "Zielpersonen" mittels eines GPS-Empfängers wegen mehrerer Verstöße gegen das Bundesdatenschutzgesetz grundsätzlich strafbar ist.
Nur ausnahmsweise könne das Vorliegen eines starken berechtigten Interesses (etwa in notwehrähnlichen Situationen) ein solches Vorgehen rechtfertigen.
Dem Verfahren lag eine Überwachung durch eine Detektei zu Grunde. Zur Erfüllung ihres Auftrags bedienten sich die Angeklagten in großem Umfang der GPS-Technik (Global Positioning System), indem sie einen GPS-Empfänger unbemerkt an den Fahrzeugen der Zielpersonen anbrachten. Dadurch konnten sie feststellen, wann und wo sich das jeweilige Fahrzeug aufhielt. Auf diese Weise erstellten sie Bewegungsprofile der Zielpersonen.
Der Landesdatenschutzbeauftragte Dr. Lutz Hasse befürwortet diese Stärkung des Datenschutzes und wird derartige Fälle als Ordnungswidrigkeit verfolgen bzw. an die zuständige Staatsanwaltschaft zur Strafverfolgung abgeben.

Link zur Pressemitteilung des BGH: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2013&Sort=3&nr=64248&pos=2&anz=97

Anlage 67

Pressemitteilung
vom 10. Juli 2013

PRISM + TEMPORA
Was Sie tun können, um Ihre Individualität und Privatsphäre vor Geheimdienstattacken besser schützen zu können:

- Ziehen Sie bei der Auswahl von Internet-Diensten deutsche Angebote den Angeboten aus Drittländern vor. Hier ist das „schärfere“ europäische Datenschutzrecht auf Ihrer Seite!
- Nutzen Sie Internetangebote, bei denen Ihre Daten nur in geringem Umfang erhoben werden, wie z. B. die der TU Dresden (http://tu-dresden.de/).
- Verwenden Sie beim Surfen Anonymisierungsdienste, auch hier verweisen wir auf die o. g. Website der TU Dresden.
- Verwenden Sie statt Klarnamen Pseudonyme beim Surfen. Dies ist im Telemediengesetz rechtlich ausdrücklich vorgesehen.
- Lesen Sie vor der regelmäßigen Nutzung von Internetangeboten sorgfältig die Nutzungs- und die Datenschutzbestimmungen. Lehnen Sie diese im Zweifelsfall ab und weichen auf alternative Angebote aus.
- Verwenden Sie gleichzeitig mehrere Browser, mehrere E-Mail-Accounts oder mehrere sonstige Identitäten. Damit erschweren Sie sogenannte Profilbildungen erheblich.
- Verzichten Sie – wenn nicht für Sie nachvollziehbare Sicherheitsmechanismen beschrieben sind – auf die Verwendung von Cloud-Computing. Hier gibt es noch erhebliche Lücken, bei denen Datenmissbrauch stattfinden kann.
- Nutzen Sie bei der Datenspeicherung – in jedem Falle in der Cloud, aber auch anderswo – zu Ihrer eigenen Sicherheit Verschlüsselungsmechanismen. Dies ist sowohl bei Dateien als auch bei E-Mails eine zusätzliche Hürde, die der potenzielle Angreifer auf Ihre Daten zu überwinden hat.
- Setzen Sie Tracking-Blocker ein und löschen Sie regelmäßig die Cookies in Ihrem Browser. Dies lässt sich in den meisten Fällen automatisieren und in der Konfiguration Ihrer Programme (z. B. Internet-Browser) einstellen.

Die dünne Schutzhülle des Rechtsstaats darf durch die entfesselten Erosionskräfte der Geheimdienste nicht weiter zerstört werden.

Nicht aufgeben, kämpfen – Wir schaffen das!

Anlage 68

Pressemitteilung
vom 16. Juli 2013

SPRENGSÄTZE

Der Tipp kam aus der Bevölkerung: In Immelborn würden in einem Gebäude Patientenakten verwahrt – das Gebäude sei jedoch nicht sicher, da Fenster eingeworfen wären und die Tür aufgebrochen sei.
Fenster und Türen wurden daraufhin von der Feuerwehr unverzüglich gesichert.
Die gestrige Augenscheineinnahme sprengte indes die Vorstellungskraft selbst des TLfDI: In drei Geschossen auf 3:000 m^2 Fläche werden ca. eine Viertel Million Akten gelagert. In Regalen, Kisten und sonstigen Behältern. Allerdings ist vieles umgestürzt, sodass nicht wenige der Akten auf dem Boden verstreut sind. Vandalismus ist nicht auszuschließen. Ein Verantwortlicher ist derzeit nicht erreichbar.
Nach Sichtung der Aktenberge werden diese abgetragen, indem die Unterlagen – größtenteils sensible Daten von Rechtsanwälten, Insolvenzverwaltern, Personalabteilungen, Ärzten etc. – an diese zurückgeführt werden.
Angesicht der Vielzahl der Akten ist hierzu die Amtshilfe anderer Behörden notwendig.

Diese Katastrophe wirft Fragen auf:

- Wie lange dauern diese Missstände bereits an und wer hat von diesen gewusst?
- Gibt es in Thüringen weitere Lagerstätten dieser Art und wie erfährt der TLfDI von ihnen?
- Wie stellt sich diese Problematik in anderen Bundesländern dar?
- Muss das Datenschutzrecht etwa im Hinblick auf Kontroll- und Meldepflichten nachgebessert werden, damit sich dergleichen nicht wiederholt?

Deutlich wird hier leider, dass der Rechtsstaat ohne wirksame Kontrollmechanismen nur schwerlich funktioniert.

Der TLfDI, Dr. Lutz Hasse: „Dieser Vorfall wird Kräfte zur Aufarbeitung binden, aber sicherlich auch Energien freisetzen, um solche Desaster in Zukunft zu vermeiden. Zusätzliche Sorge bereiten mir allerdings die – noch unkonkreten – Hinweise, dass in Thüringen mit weiteren Sprengsätzen zu rechnen ist… “

Anlage 69

Pressemitteilung
vom 24. Juli 2013

Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten

Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013

Angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency (NSA), weist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf die Befugnisse hin, die den Aufsichtsbehörden beim internationalen Datenverkehr zwischen Unternehmen in Deutschland und Drittstaaten nach dem Bundesdatenschutzgesetz und der europäischen Datenschutzrichtlinie bereits jetzt zustehen.

Die Europäische Kommission hat in mehreren Entscheidungen Grundsätze des "sicheren Hafens" (Safe Harbor) zum Datentransfer in die USA (2000) und Standardvertragsklauseln zum Datentransfer auch in andere Drittstaaten (2004 und 2010) festgelegt. Die Beachtung dieser Vorgaben soll gewährleisten, dass personenbezogene Daten, die in die USA oder andere Drittstaaten übermittelt werden, dort einem angemessenen Datenschutzniveau unterliegen. Allerdings hat die Kommission stets betont, dass die nationalen Aufsichtsbehörden die Datenübermittlung dorthin aussetzen können, wenn eine "hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind.

Dieser Fall ist jetzt eingetreten. Die Grundsätze in den Kommissionsentscheidungen sind mit hoher Wahrscheinlichkeit verletzt, weil die NSA und andere ausländische Geheimdienste nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden.

Zwar enthält die Safe-Harbor-Vereinbarung eine Regelung, die die Geltung der Grundsätze des "sicheren Hafens“ begrenzt, sofern es die nationale Sicherheit erfordert oder Gesetze solche Ermächtigungen vorsehen. Im Hinblick auf das Ziel eines wirksamen Schutzes der Privatsphäre soll jedoch von diesen Eingriffsbefugnissen nur im Rahmen des tatsächlich Erforderlichen und nicht exzessiv Gebrauch gemacht werden. Ein umfassender und anlassloser Zugriff auf personenbezogene Daten kann daher durch Erwägungen zur nationalen Sicherheit in einer demokratischen Gesellschaft nicht gerechtfertigt werden. Auch bei Datenübermittlungen in die USA aufgrund der Standardverträge muss der Datenimporteur zusichern, dass seines Wissens in seinem Land keine Rechtsvorschriften bestehen, die die Garantien aus den Klauseln in gravierender Weise beeinträchtigen. Eine solche Generalermächtigung scheint in den USA zu bestehen; denn nur so lässt sich erklären, dass der US-amerikanische Geheimdienst auf personenbezogene Daten, die aufgrund der Standardverträge übermittelt werden, mit hoher Wahrscheinlichkeit routinemäßig zugreift.

Deshalb fordert die Konferenz die Bundesregierung auf, plausibel darzulegen, dass der unbeschränkte Zugriff ausländischer Nachrichtendienste auf die personenbezogenen Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt wird. Bevor dies nicht sichergestellt ist, werden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten (zum Beispiel auch zur Nutzung bestimmter Cloud-Dienste) erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind.

Schließlich fordert die Konferenz die Europäische Kommission auf, ihre Entscheidungen zu Safe Harbor und zu den Standardverträgen vor dem Hintergrund der exzessiven Überwachungstätigkeit ausländischer Geheimdienste bis auf weiteres zu suspendieren.

Die diesjährige Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Doktor Imke Sommer, sagte hierzu: „Wirtschaftsunternehmen, die personenbezogene Daten in die USA übermitteln, tragen für diese Daten die Verantwortung. Wie alle Menschen in Deutschland müssen auch sie deshalb ein Interesse

daran haben, dass personenbezogene Datenflüsse von Geheimdiensten nicht im großen Stil anlasslos überwacht werden.“

Anlage 70

Pressemitteilung
vom 25. Juli 2013

prism: Miteinander reden – nicht übereinander

Um die bereits bestehenden Kontakte zum Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, und zur datenschutzpolitischen Sprecherin der SPD-Fraktion Frau Dorothea Marx MdL, aufzufrischen, hat der amerikanische Generalkonsul Mark J. Powell am 23. Juli die Einladung von Frau Marx und Dr. Hasse zu einem Gedankenaustausch angenommen.

In offener und konstruktiver Atmosphäre wurden am Dienstag aktuelle Fragestellungen diskutiert. Natürlich kam auch die Prism-Problematik zur Sprache. Unterschiedliche Standpunkte wurden hierbei beleuchtet, um den Ursachen für die verschiedenen Sichtweisen auf den Grund zu gehen. Generalkonsul Powell brachte zum Ausdruck, er sei erfreut über den lebendigen Meinungsaustausch, die erörterten Argumente seien gewichtig; die Bedeutung von Datenschutz und Schutz der Privatsphäre dürfe nicht übergangen werden.
Der Generalkonsul machte auf die Rede von Robert S. Litt, Chefjustitiar des amerikanischen Nationalen Geheimdienstkoordinators am Brookings Institute am 19. Juli aufmerksam (http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection).

Das Gespräch wurde von allen Beteiligten als richtungsweisend eingestuft, sodass der Dialog um Datenschutz, Freiheit und Sicherheit fortgesetzt werden soll.

Anlage 71

Pressemitteilung
vom 29. Juli 2013

Lehrer in facebook & Co.?
NEIN!

Ein großes Anliegen des TLfDI ist, dass Schülerinnen und Schüler in den Schulen Medienkompetenz erlangen und auch Lehrer sich diesem Thema stellen. Aus diesem Grund wird demnächst, Dank Unterstützung des Thüringer Ministeriums für Bildung, Wissenschaft und Kultur, ein Lehrer zum TLfDI abgeordnet, um mit dem TLfDI Unterrichtsmaterialien für das Fach Medienkunde zu erstellen.

Grundsätzlich muss man unterscheiden, ob Lehrer den Schülern den sachkundigen Umgang mit sozialen Netzwerken vermitteln oder ob sie als Lehrer mit Schülern in sozialen Netzwerken kommunizieren, etwa Hausaufgaben verteilen, Ergebnisse von Arbeiten, Unterrichtsausfälle, Lob und Tadel mitteilen.
Die Nutzung sozialer Netzwerke für die Übermittlung solcher personenbezogenen Daten muss zunächst den Anforderungen des § 9 Thüringer Datenschutzgesetz gerecht werden. Die öffentlichen Stellen haben hierfür alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind um die Ausführungen der Bestimmungen des Thüringer Datenschutzgesetzes zu gewährleisten. Hierzu zählt insbesondere die Vertraulichkeit der übermittelten personenbezogenen Daten und die Transparenz des genutzten Verfahrens sicherzustellen.
Diese Kriterien können aber viele der gebräuchlichen sozialen Netzwerke nicht erfüllen. Denn bei der Nutzung von sozialen Netzwerken wie bspw. Facebook und Google for Education werden die Daten nicht unter der alleinigen Kontrolle der Schule verarbeitet.

Die Server, auf denen diese Netzwerke betrieben werden, liegen außerhalb Deutschlands bzw. des EU-Raumes. Der dortige Datenschutzstandard ist zumeist nicht mit demjenigen in Deutschland und der EU vergleichbar. Zudem unterliegen diese Server nicht der Kontrolle der Datenschutzbeauftragten oder vergleichbarer Institutionen. Die Schulen und somit auch die Lehrer können mithin derzeit nicht

dafür Sorge tragen, dass sowohl die Verkehrs- und Inhaltsdaten der Lehrer und der Schüler vertraulich bleiben.
Im Ergebnis stellt daher jegliche dienstliche Kommunikation, die personenbezogene Daten beinhaltet, mittels solcher sozialen Netzwerke sowohl zwischen Lehrkräften und Schülern als auch der Lehrkräfte untereinander einen **Verstoß gegen das Thüringer Datenschutzgesetz** dar.
Irrelevant ist, ob der Lehrer dabei von der Schule oder von zu Hause aus tätig wird.
Datenschutzrechtliche **Alternativen** bilden Netzwerke, die dezentral bei den Schulen selbst eingerichtet oder deren Server ausschließlich in Deutschland betrieben werden; sie sind im Internet zu finden.
Zudem ist zu bedenken, dass Schüler, die bislang auf die Nutzung sozialer Netzwerke wie Facebook verzichtet haben, **faktisch gezwungen** werden könnten, sich hieran zu beteiligen, um keine Nachteile infolge verspäteter oder unvollständiger schulischer Informationen zu erleiden.
Schulen und Lehrer sollten angesichts der dargelegten Argumente keinen derartigen Druck ausüben.

Der TLfDI wird die Einhaltung des Thüringer Datenschutzgesetzes durch Schulen und Lehrer überwachen und steht für Rückfragen gern zur Verfügung.

Anlage 72

Pressemitteilung
vom 31. Juli 2013

**Persönlichkeitsrechte– auch im Internet –
keine Frage …des Alters!**

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit und die Verbraucherzentrale Thüringen laden zu einer Kooperationsveranstaltung am

**Montag, dem 30. September 2013, 10:00 Uhr,
in das Erfurter Rathaus Großer Festsaal, Fischmarkt 1 nach
99084 Erfurt**

ein.
Das Internet entwickelt sich mehr und mehr zu einem Teil unseres täglichen Lebens. Gerade für Menschen in fortgeschrittenem Alter bietet das Internet Chancen, den Alltag zu erleichtern, Kontakte zu pflegen und Informationen zu beschaffen, die auf anderem Weg nicht zu erreichen wären. Wenn da nicht die Spamfluten, aggressive Werbungen oder der Adresshandel wären, die ihnen den Umgang erschweren. Die Verbraucherzentrale und der Datenschutzbeauftragte sind hierfür die richtigen Ansprechpartner. Die Veranstaltung soll den **Seniorinnen und Senioren** in Vorträgen und Workshops ihre Rechte aufzeigen. Außerdem erhalten die Teilnehmer die Gelegenheit, sich mit den Chancen und Gefahren sozialer Netzwerke für „Silver Surfer“ vertraut zu machen; zudem werden wir ausführlich darüber informieren, wie man mit dem sehr begehrtem Gut der persönlichen Daten im Internet richtig umgeht.

Als Gäste werden wir die Ministerin für Soziales, Familie und Gesundheit, Frau Heike Taubert begrüßen können, die auch das Grußwort sprechen wird, und Frau Michaela Zinke vom Bundesverband der Verbraucherzentrale.

Weitere Informationen finden Sie unter → www.tlfdi.de

Anlage 73

Pressemitteilung
vom 5. September 2013

Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013

Keine umfassende und anlasslose Überwachung durch Nachrichtendienste – Zeit für Konsequenzen

Unter dem Motto "Zeit für Konsequenzen" haben heute die Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2013 und Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, Dr. Imke Sommer, und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, in der Bundespressekonferenz zur Überwachung der elektronischen Kommunikation durch ausländische Nachrichtendienste Stellung genommen.

Sie stellten dabei die gleichnamige Entschließung der Datenschutzkonferenz vor. Schon die bisherigen Erkenntnisse ließen den Schluss zu, dass die Aktivitäten u. a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinausliefen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden seien. Deshalb fordern die Datenschutzbeauftragten von Bund und Ländern die Regierungen und Parlamente des Bundes und der Länder auf, nationales, europäisches und internationales Recht zu ändern, verfassungswidrige nachrichtendienstliche Kooperationen abzustellen, die Kontrolle der Nachrichtendienste zu intensivieren, Initiativen zum Schutz der informationellen Selbstbestimmung und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme zu starten, völkerrechtliche Abkommen wie das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehrs auf den Prüfstand zu stellen und auch innerhalb der Europäischen Union sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung der Europäischen Grundrechtecharta erfolgt.

Dr. Imke Sommer sagte hierzu: "Wir müssen aufpassen, dass sich nicht angesichts des Ausmaßes der bekannt gewordenen Überwachung bei uns allen und auch bei denjenigen, die Abwehrmaßnahmen treffen müssen, Resignation breit macht. Parlamente und Regierungen haben alle Mittel in der Hand, sich schützend vor die Grundrechte der Menschen in der Bundesrepublik Deutschland zu stellen und verfassungswidrige Situationen zu beenden. Davon müssen sie jetzt Gebrauch machen!"

Anlage 74

Pressemitteilung
vom 9. September 2013

PRISM + TEMPORA + XKEYSCORE
Teil II

Nach jüngsten Presseinformationen verfügen die amerikanischen und britischen Geheimdienste über die Fähigkeit, selbst verschlüsselte Botschaften nahezu in Echtzeit zu entschlüsseln. Zudem ist diesen Informationen zu entnehmen, dass Software, also auch Verschlüsselungssoftware, mit „Hintertürchen“ für Geheimdienste infiziert ist. Dennoch: Jetzt ist nicht die Zeit, an der Gefährdung des Rechtsstaats zu verzweifeln, sondern es müssen mangels erkennbarer Schutzmaßnahmen der „Verantwortlichen“ eigene Schutzvorkehrungen getroffen werden.
Bereits im ersten Teil der Pressemitteilung PRISM + TEMPORA vom 10. Juli habe ich aufgezeigt, wie Sie Ihre Individualität und Privatsphäre vor Geheimdienstattacken besser schützen können.
Heute eine neue Alternative, um dem Überwachungswahn zu entkommen: **PRISM BREAK!** Wir haben uns die Seite für Sie angeschaut:
prism-break.org ist eine Webseite des Interface-Designers (Schnittstellendesigner) Peng Zhong. Sie zeigt in 24 Kategorien Softwarealternativen zu proprietären (herstellergebundenen) Programmen, Betriebssystemen und Online-Anwendungen. Die Möglichkeit, dass Geheimdienste Hintertüren in diese Software eingebaut haben, ist zwar nicht ausgeschlossen, soll aber laut PRISM BREAK reduziert sein. Mit diesen Softwareangeboten wird der Schutz jedenfalls verbessert, sodass u. a. auch die Stiftung Datenschutz PRISM BREAK in ihren Praxistipps empfiehlt. Leider sind die Zeiten, in denen eine gewisse Sicherheit im Netz zugesagt werden konnte, vergangen. Trotzdem können Alternativprogramme Bausteine für den Schutzschild Ihrer Privatsphäre sein. Diese Chance sollten Sie nutzen!
Verlassen Sie sich auf sich und nicht mehr auf die sogenannten Verantwortlichen – Betreiben Sie Selbstschutz!
Nicht aufgeben, kämpfen – Wir schaffen das!

Anlage 75

Pressemitteilung
vom 2. Oktober 2013

Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 2. Oktober 2013

86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1. und 2. Oktober 2013 in Bremen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert auf ihrer 86. Tagung in Bremen an alle Akteurinnen und Akteure der 18. Legislaturperiode, sich für die Stärkung des Datenschutzes auf nationaler, europäischer und internationaler Ebene einzusetzen. Angesichts der anlasslosen und umfassenden internationalen Überwachungsaktivitäten von Nachrichtendiensten fordern die Datenschutzbeauftragten von dem Bundesgesetzgeber und der neuen Bundesregierung wirksame Maßnahmen zum Schutz der Vertraulichkeit der Kommunikation und der Privatsphäre. Wenn hier nicht entschieden gegengesteuert wird, ist zu befürchten, dass wir uns an eine allgegenwärtige Überwachung gewöhnen und damit rechtsstaatliche Garantien dauerhaft außer Kraft gesetzt werden.

Mit ihrer Entschließung "Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!" fordern die Datenschutzbeauftragten des Bundes und der Länder eine Weiterentwicklung des Datenschutzrechts auf nationaler und internationaler Ebene. Von besonderer Bedeutung ist auch ein europäischer Datenschutz auf hohem Niveau. Die Datenschutzkonferenz nimmt dabei zu den drei besonders bedeutsamen Bereichen öffentliche Sicherheit, Gesundheitsdatenschutz und Vertraulichkeit der elektronischen Kommunikation in gesonderten Entschließungen Stellung.

In ihrer Entschließung zur öffentlichen Sicherheit betont die Datenschutzkonferenz "Handlungsbedarf" für diesen besonders eingriffsintensiven Bereich. Sie fordert eine rechtsstaatlich transparente Kontrolle der Nachrichtendienste im nationalen wie im internationalen Rahmen. Darüber hinaus müssen diesen Behörden, deren Tätigkeit tief in die Grundrechte der Bürgerinnen und Bürger eingreift, enge

Grenzen gesetzt werden. Auch für Grundrechtseingriffe anderer Sicherheitsbehörden sind wirksame Beschränkungen erforderlich.

Mit der Entschließung zur "Stärkung des Datenschutzes im Sozial- und Gesundheitswesen" fordert die Konferenz angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenden Risiken für die informationelle Selbstbestimmungen die Stärkung der Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten.

In ihrer Entschließung "Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln" setzt sich die Konferenz für die Förderung der Vertraulichkeit und Integrität elektronischer Kommunikation ein. Sie fordert, dass der öffentliche Bereich mit gutem Beispiel vorangeht und die Ende-zu-Ende-Verschlüsselung unter Verwendung des in Bremen entwickelten Standards OSCI-Transport flächendeckend einsetzt.

Die Konferenz hatte sich an die Konferenz der Ministerpräsidentinnen und Ministerpräsidenten gewandt, und ihre Mitarbeit dabei angeboten, bei den Betreibern sozialer Netzwerke auf eine Rechtmäßigkeit der Anwendungen hinzuwirken. Die Konferenz der Ministerpräsidentinnen und Ministerpräsidenten hat diese Anregung aufgenommen.

Die derzeitige Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit, Dr. Imke Sommer, sagte zum Thema Datenschutz in der 18. Legislaturperiode: "Nicht das Ob, sondern nur noch das Wie des künftigen Schutzes der Datenschutzgrundrechte gegen alle ihnen drohenden Angriffe von privaten wie öffentlichen, von inländischen wie ausländischen Stellen muss Thema der anstehenden Koalitionsverhandlungen werden!"

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, erklärte: "In der neuen Legislaturperiode haben die Bundesregierung und der Bundestag die Chance für einen Neuanfang im Datenschutz. Die Bürgerinnen und Bürger erwarten

zu Recht, dass sie gegen den Datenhunger von Unternehmen und gegen überbordende Überwachungsaktivitäten geschützt werden."

Der Vorsitzende der Datenschutzkonferenz im kommenden Jahr, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar, erklärt: "Die nächste Zeit wird darüber entscheiden, ob sich die Herrschaft des Rechts und damit auch die Grundrechte gegenüber den Geheimdiensten durchsetzen werden lassen. Eine dauerhafte Überwachung unserer Informations- und Kommunikationsbeziehungen ist nicht akzeptabel. Nicht der digitale Untertan, sondern der mündige Bürger muss das zentrale Leitbild des demokratischen Rechtsstaats bleiben."

Anlage 76

Pressemitteilung
vom 29. Oktober 2013

IT-Systeme der Landesverwaltung sicher?

Der Thüringer Allgemeinen war am 26. Oktober 2013 zu entnehmen, dass laut zuständigem Thüringer Finanzministerium die IT-Systeme der Thüringer Landesverwaltung ständig auf mögliche Schwachstellen überprüft würden und derzeit kein Grund vorliege, die Sicherheit dieser Systeme aktuell zu erhöhen.
Insoweit stellt sich allerdings die Frage, welcher Schutz überhaupt ausreichend ist, wenn Geheimdienste verschiedener Staaten Telefongespräche und E-Mails von Bürgern, Parlamentariern, Unternehmen und Behörden erfassen, ohne dass nationale Sicherheitsbehörden dies in diesem Ausmaß erkennen bzw. dieses verhindern konnten/können.
Wie wir wissen, findet Schadsoftware ihren Weg entweder über zentrale Zugänge oder durch angeschlossene Einzelgeräte. Auch Computersysteme der Landesverwaltung bleiben davon grundsätzlich nicht verschont.
Um das Ausmaß der heimlichen Überwachung einzuschränken, möchte der TLfDI nochmals an Behörden, aber auch Unternehmen appellieren,

- personenbezogene Daten nur verschlüsselt zu übertragen,
- personenbezogene Daten – soweit möglich – verschlüsselt zu speichern,
- nur Cloud-Dienste zu nutzen, deren Server in Deutschland stehen (http://www.tlfdi.de/imperia/md/content/datenschutz/orientierungshilfe/orientierungshilfe_cloud_computing.pdf),
- auf den Einsatz von „Bring Your Own Device“ (BYOD-Einsatz privater Geräte in Behörden/Unternehmen) zu verzichten und nur firmen- bzw. behördeninterne Geräte zuzulassen, die auch zentral administriert werden können,
- aktuelle Virenscanner auch auf mobilen Endgeräten einzusetzen,
- die erhältlichen (!) Telefone ohne „Babyphone-Funktion“ einzusetzen,

– eingestellte Leistungsmerkmale der Telefonanlagen regelmäßig auf Erforderlichkeit und evtl. ungewünschte Veränderungen zu überprüfen.

Anlage 77

Pressemitteilung
vom 18. November 2013

Sitzung des Deutschen Bundestags zu den Abhöraktivitäten der NSA:
Bundesdatenschutzbeauftragter legt Bericht vor.

Anlässlich der Sitzung des Deutschen Bundestags zu den Abhöraktivitäten des US-amerikanischen Nachrichtendienstes NSA und den Auswirkungen auf Deutschland und die transatlantischen Beziehungen hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar den Abgeordneten des Deutschen Bundestags einen Bericht vorgelegt, der den Abgeordneten des Deutschen Bundestags Anhaltspunkte für mögliche Entscheidungen und Weichenstellungen liefern soll.

Die Kernaussagen des Berichts lauten:

- Grundrechtsschutz und Sicherheit müssen insbesondere im Bereich der Nachrichtendienste in einem ausgewogenen Verhältnis stehen. Dies setzt eine effektive und lückenlose unabhängige Kontrolle nachrichtendienstlicher Tätigkeiten voraus.

- Die berichteten anlasslosen Massendatenerhebungen sind schnell, umfassend, detailliert und – soweit rechtlich zulässig – auch öffentlich aufzuklären.

- Strukturelle und/oder regelungstechnische Defizite sind unverzüglich und nachhaltig zu beseitigen – auf nationaler wie internationaler Ebene.

- Die Zusammenarbeit deutscher mit ausländischen Nachrichtendiensten darf nicht dazu führen, durch Aufgabenteilung nationale (verfassungs-)rechtliche Beschränkungen für ihre Tätigkeit zu umgehen („Befugnis-Hopping“).

- Aufgrund der Gesetzgebungs- und Kontrollkompetenz des Deutschen Bundestages über die Nachrichtendienste des Bundes ist eine engere Kooperation der parlamentarisch bestellten Kontrollorgane und die Beseitigung bestehender Kontrolldefizite dringend erforderlich.

Der vollständige Bericht kann unter http://dip21.bundestag.de/dip21/btd/18/000/1800059.pdf abgerufen werden.

Anlage 78

Pressemitteilung
vom 20. Dezember 2013

Datenschutzbeauftragter hat Anspruch auf Amtshilfe

Erfreut zeigt sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse, dass die Landtagsverwaltung in einem Gutachten zum Aktenfund in Immelborn einen Anspruch auf Amtshilfe des TLfDI gegenüber der Thüringer Polizei anmahnt. „Allerdings hätte ich mir gewünscht, dass die Landtagsverwaltung in ihrer gutachterlichen Stellungnahme auch die konkreten Umstände des Einzelfalls gleich mit prüft“, sagte Hasse am Freitag in Erfurt.

So lässt das Gutachten die Frage unbeantwortet, ob die Polizei zumindest dann, wenn gerichtlicherseits ein Amtshilfeanspruch des TLfDI abgelehnt werden sollte, nach § 3 Thüringer Polizeiaufgabengesetz allein zuständig wird.
Unabhängig davon finden in dieser Angelegenheit Verhandlungen zwischen dem TLfDI und dem Thüringer Innenministerium bereits statt.

Sollte das Thüringer Innenministerium dem Amtshilfeersuchen nicht stattgeben, wird der Datenschutzbeauftragte den verwaltungsgerichtlichen Klageweg beschreiten. „Auf diesen Weg verweist mich das Landtagsgutachten ausdrücklich. In der Zwischenzeit machen wir natürlich weiter: 10.000 Akten sind bereits zurückgeführt, mehr als 80.000 Akten sind registriert und warten auf ihre Abholung. In den „Chaos-Abteilungen“ des Gebäudes in Immelborn benötigen wir aber Stromgeneratoren und auch schwereres technisches Gerät, um rechtskonforme Zustände herstellen zu können. Da ist Hilfe erforderlich, die uns – von wem auch immer – gewährt werden wird“, so Hasse abschließend.

Abkürzungsverzeichnis

Abkürzung	Bedeutung
a. F.	alte Fassung
Abs.	Absatz
ADF	Automatic Document Feeder (automatischer Dokumenteneinzug)
AG	Arbeitsgruppe
AK	Arbeitskreis
ALB	Automatisiertes Liegenschaftsbuch
AO	Abgabenordnung
Art.	Artikel
ATDG	Antiterrordateigesetz
AufenthG	Aufenthaltsgesetz
AuslG	Ausländergesetz
bDSB	behördlicher Datenschutzbeauftragter
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfF	Begutachtungsstelle für Fahreignung
BGH	Bundesgerichtshof
BMJ	Bundesministerium der Justiz
BMVBS	Bundesministerium für Verkehr
BMWi	Bundesministerium für Wirtschaft und Energie
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamt für die Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BtM	Betäubungsmittel
BtmG	Betäubungsmittelgesetz
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
CERT-Bund	Computer Emergency Response Team der Bundesverwaltung
DA KAN	Dienstanweisung Kriminalaktennachweis
DIHK e. V.	Deutscher Industrie- und Handelskammertags e. V.
DIN	Deutsche Industrienorm
DlStG	Dienstleistungsstatistikgesetz
DMS	Dokumentenmanagementsystem

DPolG	Deutsche Polizeigewerkschaft
DSGV	Deutscher Sparkassen- und Giroverband
ED-Behandlung	Erkennungsdienstliche Behandlung
ED-Maßnahme	Erkennungsdienstliche Maßnahme
ELS	Einsatzleitsystem
EU	Europäische Union
FEB	Fahrerlaubnisbehörde
FeV	Fahrerlaubnisverordnung
Findus	Fallinformation durchsuchen mit System
GCHQ	The Government Communications Headquarters
GdP	Gewerkschaft der Polizei
GewO	Gewerbeordnung
GG	Grundgesetz
GPS	Global Positioning System
GSB	Grundschule Bottendorf
I. V. m.	in Verbindung mit
IGVP	Integrationsverfahren Polizei
IHK	Industrie- und Handelskammer
IHK-GfI mbH	IHK-Gesellschaft für Informationsverarbeitung mbH
INPOL	Informationssystem der Polizei
INPOL BUND	bundesweites Informationssystem der Polizei
IP	Ingress Protection
IP-Adressen	Internetprotokoll-Adressen
IT-SiKo	IT-Sicherheitskonzept
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
Kfz-Steuer	Kraftfahrzeugsteuer
KIS	Krankenhausinformationssystem
KIV Thüringen	Kommunale Informationsverarbeitung Thüringen
KoSIT	Koordinierungsstelle für IT-Standards
KPI	Kriminalpolizeiinspektion
LDI Nordrhein-Westfalen	Landesbeauftragter für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen
LKA	Landeskriminalamt
LKHG	Landeskrankenhausgesellschaft
LPD	Landespolizeidirektion
LPI	Landespolizeiinspektion
LVwG	Landesverwaltungsgericht

MdE	Minderung der Erwerbsfähigkeit
MDR	Mitteldeutscher Rundfunk
MiStra	Anordnung über Mitteilung in Strafsachen
MZG	Mikrozensusgesetz
NFC	Near Field Communication
NotrufV	Verordnung über Notrufverbindungen
NSA	National Secutity Agency
NSU	Nationalsozialistischer Untergrund
NWR	Nationales Waffenregister
NWRG	Nationales Waffenregistergesetz
OH KIS	Orientierungshilfe Krankenhausinformationssysteme
OSCI	Online Services Computer Interface
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PAG	Polizeiaufgabengesetz
PD	Polizeidirektion
PI	Polizeiinspektion
PIA	Privacy Impact Assessment
PostG	Postgesetz
PPS-Richtlinie	Richtlinien für die Führung polizeilicher personenbezogener Sammlungen
PUAG	Gesetz zur Regelung es Rechts der Untersuchungsausschüsse des Deutschen Bundestages
Rdnr.	Randnummer
RFID	radio-frequency identification
RLAktenThürPol	Richtlinie zum Umgang mit dienstlichem Schriftgut sowie zur Akten- und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei
SARS	Syborg Auskunft- und Recherchesystem
SchufFV-E	Schuldnerverzeichnisführungsverordnung
SDÜ	Schenger Durchführungsübereinkommen
SEPA	Single Euro Payments Area
SGB	Sozialgesetzbuch
SiD	Strukturerhebung im Dienstleistungsbereich
SIP	Session Initiation Protocol
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengener Informationssystem

SPS	speicherprogrammierte Steuerungen
SSD	Solid State Disks
SSL	Secure Sockets Layer
StatRegG	Statistikregistergesetz
Steuer-ID	Steuer-Identifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVollzG	Strafvollzugsgesetz
TB	Tätigkeitsbericht
TFM	Thüringer Finanzministerium
ThHStA	Thüringisches Hauptstaatsarchiv
ThILLM	Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien
ThürArchivG	Thüringer Archivgesetz
ThürBG	Thüringer Beamtengesetz
ThürDG	Thüringer Disziplinargesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürGGO	gemeinsame Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen
ThürIFG	Thüringer Informationsfreiheitsgesetz
ThürJVollzGB	Thüringer Justizvollzugsgesetzbuch
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKO	Thüringer Kommunalordnung
ThürMeldeG	Thüringer Meldegesetz
ThürMeldeVO	Thüringer Meldeverordnung
ThürPAG	Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei
ThürPolPrüffristVO	Thüringer Verordnung über die Prüffristen bei vollzugspolizeilicher Datenspeicherung
ThürRettG	Thüringer Rettungsdienstgesetz
ThürStatG	Thüringer Statistikgesetz
ThürUAG	Thüringer Untersuchungsausschussgesetz
ThürVBl	Thüringer Verwaltungsblätter
ThürVerf	Thüringer Verfassung
ThürVerfGH	Thüringer Verfassungsgerichtshof
ThürVSG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TierGefG	Thüringer Gesetz zum Schutz der Bevölkerung vor Tiergefahren

TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TK-Anlagen	Telekommunikations-Anlagen
TKG	Telekommunikationsgesetz
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLfV	Thüringer Landesamt für Verfassungsschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLKA	Thüringer Landeskriminalamt
TLS	Thüringer Landesamt für Statistik
TLS	Transport Layer Security
TLVermGeo	Thüringer Landesamt für Vermessung und Geoinformation
TMBLV	Thüringer Ministerium für Bau, Landesentwicklung und Verkehr
TMBWK	Thüringer Ministerium für Bildung, Wissenschaft und Kultur
TR Notruf	Technische Richtlinie Notruf
TSK	Thüringer Staatskanzlei
TVÜG	Testamentsverzeichnisüberführungsgesetz
VerfThür	Verfassung des Freistaats Thüringen
VerschG	Verschollenheitsgesetz
VG	Verwaltungsgemeinschaft
VoIP	Voice over IP
WaffG	Waffengesetz
ZensG 2011	Zensusgesetz 2011

Sachregister

§ 100 a StPO	4.5
§ 100 g StPO	4.5
Abgaben	2.4; 5.10; 5.20; 9.1; 9.2; 9.4; 9.5; Anlage 31; Anlage 37; Anlage 61
Abgabenordnung	2.4; 5.10; 9.2; 9.4; 9.5; Anlage 31; Anlage 61
Abgeordnete	7.13; 7.19; 7.20; Anlage 24; Anlage 25; Anlage 26; Anlage 27; Anlage 28; Anlage 29; Anlage 30; Anlage 31; Anlage 32; Anlage 42; Anlage 50; Anlage 58; Anlage 77
Abordnung	13.1; 13.4; Anlage 71
Abstammung	5.8; 5.15
Abwehr von Einbrüchen	7.10; 14.3
Adoption	9.1; 10.4; 14.6; Anlage 10
Adresshandel	2.10; Anlage 7; Anlage 40; Anlage 41; Anlage 42; Anlage 72
Adressmittlungsverfahren	5.9; 5.14
Akteneinsicht	5.26; 7.3; 9.5; Anlage 34; Anlage 50
Aktensammelcontainer	7.1
Aktenvernichtung	7.1; 7.7; 7.8; 7.9; 8.1; Anlage 25
Alkoholabhängigkeit	6.4
Amtlicher Vater	5.7
Amtsblatt	5.19; 5.22; 5.24; Anlage 32
Amtsgericht	7.3; 7.4; 10.2; 10.4
Anerkannte Zwecke	5.10; 5.31; 6.1; 7.17
Anfangsverdacht	7.3; 7.4; 12.4
Anfertigung von Bildaufzeichnungen	7.22; 10.1; Anlage 37
Antikorruptionsbeauftragte	5.16; Anlage 32
Antiterrordatei	2.2; Anlage 22
Anwohner	7.10
Anzeigeerstatter	5.26
App	16.1; Anlage 29

Arbeitgeber	5.5; 5.10; 5.18; 6.3; 6.6; 9.2; 12.5; Anlage 12; Anlage 27; Anlage 31; Anlage 54; Anlage 64
Arbeitsgruppe Datenschutz und Schule	13.1
Arbeitsgruppe Zensus	2.5
Arbeitskreis Datenschutz und Bildung	13.1
Arbeitsunfähigkeitsbescheinigung	6.8
Arbeitszeiterfassung	6.7
Archiv	2.3; 5.6; 5.15; 7.8; 7.15; 8.1; 15.5; Anlage 5; Anlage 25; Anlage 32; Anlage 48; Anlage 65
Archivanbietung	8.1; Anlage 25
Archivgesetz	7.15; 8.1; Anlage 25; Anlage 48
Archivrecht	7.15; Anlage 25; Anlage 65
Archivvereinbarung	8.1
Artikel 29-Datenschutzgruppe	3.2; 4.1
Arzt	5.12; 6.4; 6.8; 10.3; 11.1; 12.2; 13.6; Anlage 5; Anlage 21; Anlage 28; Anlage 36; Anlage 37; Anlage 68
Aufbewahrungsfrist	A.1; 7.7; 7.8; 7.9; 7.15; Anlage 25; Anlage 33; Anlage 48; Anlage 65
Aufbewahrungsrichtlinie	7.14; 7.15
Aufenthaltsgesetz	3.3; 7.11
Aufgebot	10.2
Auflösung	Anlage 32
Auftragsdatenverarbeitung	5.6; 6.5; 12.6
Aufzeichnung	5.3; 5.6; 5.18; 5.22; 5.27; 7.6; 7.10; 7.13; 7.18; 7.20; 7.22; 15.1; Anlage 4; Anlage 28; Anlage 39
Auskunftsersuchen	5.11; Anlage 24
Auskunftserteilung	5.11; 5.26; 7.13; 7.19; 8.2; 12.1; Anlage 24
Auskunftssperre	5.11
Auskunftsverweigerung	5.10; 8.2
Ausländerbehörde	7.11
Außenbewirtschaftungszeiten	5.32

Aussonderung 7.7; 7.8; 7.12; 7.14; 7.15; Anlage 25; Anlage 33; Anlage 48
Aussonderungsprüffrist 7.8; 7.12; Anlage 25
Austausch von Gefangenen 10.3
Authentisierung 9.2
Automatisiertes Liegenschaftsbuch 12.7
Automatisiertes Verfahren 6.5
Babyphonfunktion 15.1; Anlage 32
Bagatellbeträge 2.8
Bargeldlose Zahlung 12.9
Bauaufsicht 5.32
Beamte A.1; 5.7; 6.4; 6.7; 7.2; 7.3; 7.4; 7.6; 7.12; 7.20; 7.21; 7.22; 7.23; 10.5; Anlage 30; Anlage 32; Anlage 50; Anlage 51; Anlage 52; Anlage 53
Beanstandung A.1; 3.3; 5.1; 5.5; 5.10; 5.14; 5.16; 5.17; 5.18; 5.19; 5.20; 5.25; 5.28; 6.1; 7.1; 7.2; 7.3; 7.4; 7.16; 7.18; 7.20; 7.21; 8.1; 8.2; Anlage 25; Anlage 26; Anlage 31; Anlage 32; Anlage 37; Anlage 58
Befragung 2.6; 5.14; 5.23; 5.25; 5.31; 6.2; 7.8; 12.8; Anlage 21; Anlage 35
Beginn der Prüffrist 7.8; 7.16
Begrüßungsveranstaltung 5.9
Begutachtungsstelle 12.2
Beherbergungsbetrieb 5.10
Behördlicher Datenschutzbeauftragter (bDSB) 2.1; 5.2; 5.17; 7.1; 13.2
Beihilfe 6.5
Belehrung 5.5;7.12; 10.5
Beratung 2.2; 2.10; 3.2; 5.1; 5.2; 5.16; 6.7; 7.13; 7.15; 9.2; 11.1; 11.2; 12.9; 13.2; 13.4; 13.7; 14.4; 15.5; Anlage 2; Anlage 3; Anlage 7; Anlage 12; Anlage 24; Anlage 32; Anlage 34; Anlage 35; Anlage 37; Anlage 47; Anlage 49
Beratungspflicht 5.2

Berechtigtes Interesse	5.6; 5.21; 11.3; 12.5; 12.7
Berichterstattung	5.27; Anlage 17; Anlage 32
Beschäftigte	2.2; 2.6; 5.1; 5.4; 5.5; 5.6; 5.15; 5.16; 5.17; 5.18; 5.23; 6.1; 6.2; 6.3; 6.4; 6.6; 6.7; 7.2; 7.18; 10.5; 11.4; 12.5; 13.2; 15.1; Anlage 2; Anlage 8; Anlage 12; Anlage 16; Anlage 26; Anlage 28; Anlage 53; Anlage 64;
Beschäftigtendatenschutz	6.1; 6.3; Anlage 8; Anlage 12
Besonders geschützte Daten	5.17; 6.8
Bestandsdatenabfrage	7.13; 7.19
Bestandsdatenspeicherung	7.13
Betäubungsmittelgesetz (BtmG)	7.7
Betriebsvereinbarung	5.6
Betriebsversammlung	5.18
Betrug	7.3; 7.8; 12.10; 12.11; Anlage 53
Bettensteuer	5.10; Anlage 27
Bewegungsprofile	7.23; 14.1; Anlage 66
Big Data	2.2
Bildaufzeichnung	7.13
Bildübertragung	7.6
Bildungszentrum der Thüringer Polizei	A.1; 7.1; 7.2
Biometrische Merkmale	6.6; 10.3; Anlage 64
Booz Allen Hamilton	2.2
BOS-Digitalfunk	7.23
Broschüre	7.15; 13.4
Bundesamt für die Sicherheit in der Informationstechnik (BSI)	2.2; 12.3; 14.3; 14.4; 14.6; Anlage 6; Anlage 10; Anlage 18; Anlage 45; Anlage 46; Anlage 57; Anlage 61;
Bundesland	2.7; 4.5; 7.6; 10.4; 11.3; Anlage 1; Anlage 56; Anlage 68
Bundesmeldegesetz	Anlage 41
Bundesnetzagentur	4.4; 7.21; Anlage 35
Bundesnotarkammer	10.4

Bundesrat	2.8; 2.10; 3.2; 7.13; 14.4; Anlage 7; Anlage 61
Bundesverfassungsgerichtsentscheidung	2.6; 7.6; 7.13; 7.19; 7.21; Anlage 2; Anlage 8; Anlage 19; Anlage 23; Anlage 24
Bundesverwaltungsgerichtsentscheidung	2.10; 6.1; 7.2; Anlage 27; Anlage 41
Bundeszentralregister	7.8; 7.17
Bürgerbefragung	5.14; 5.31
Bürgermeister	5.9; 5.19; 5.24; 5.25; 5.28; 5.32; 9.4; 12.7; Anlage 32;
Bußgeld	5.26; 5.33; Anlage 15; Anlage 16; Anlage 26; Anlage 29; Anlage 30;
Bußgeldverfahren	5.26; 5.33
Chipkarte	6.6; Anlage 60
Cloud Computing	2.1; 2.2; 14.4; Anlage 67; Anlage 76
Cloud-Dienste	14.4; Anlage 21; Anlage 69; Anlage 76
Community-Cloud	14.4
Computer	2.2; 2.9; 7.2; 9.2; 12.3; 14.3; 14.5; 14.6; 14.7; Anlage 10; Anlage 20; Anlage 53; Anlage 62; Anlage 63; Anlage 76
Cookies	4.1; 4.3; 15.3; Anlage 14; Anlage 67
DA KAN	7.14; Anlage 25
Datenerhebung	A.1; 2.2; 2.6; 5.10; 5.13; 5.19; 5.25; 5.31; 7.17; 7.23; 11.4; Anlage 3; Anlage 12; Anlage 26; Anlage 27; Anlage 32; Anlage 34; Anlage 77
Datenlöschung	6.5; 7.16; Anlage 48; Anlage 62
Datenpanne	12.10
Datenschutz und Schule	13.1; Anlage 60
Datenschutzbeauftragter	A.Vorwort; 2.1; 2.2; 2.5; 2.7; 2.8; 2.9; 2.10; 4.1; 4.2; 4.3; 5.1; 5.2;

	5.5;5.17; 6.1; 7.2; 7.6; 7.13; 9.5; 10.2; 10.4; 12.3; 13.1; 13.2; 14.1; 14.2; 14.4; 14.5; 14.6; Anlage 1; Anlage 2; Anlage 3; Anlage 4; Anlage 5; Anlage 6; Anlage 7; Anlage 8; Anlage 9; Anlage 10; Anlage 11; Anlage 12; Anlage 13; Anlage 14; Anlage 15; Anlage 16; Anlage 17; Anlage 19; Anlage 20; Anlage 21; Anlage 22; Anlage 23; Anlage 24; Anlage 25; Anlage 26; Anlage 27; Anlage 28; Anlage 29; Anlage 30; Anlage 31; Anlage 32; Anlage 34; Anlage 36; Anlage 37; Anlage 39; Anlage 40; Anlage 42; Anlage 50; Anlage 51; Anlage 52; Anlage 56; Anlage 60; Anlage 63; Anlage 66; Anlage 69; Anlage 71; Anlage 72; Anlage 73; Anlage 75; Anlage 77; Anlage 78
Datenschutzbewusstsein	13.1; Anlage 26; Anlage 47
Datenschutzerklärung	4.3; 7.17; Anlage 29
Datenschutzmerkblatt	12.9
Datenschutzniveau	3.1; 5.27; 6.1; Anlage 2; Anlage 8; Anlage 12; Anlage 15; Anlage 56; Anlage 69
Datenschutzregister	15.2
Datenschutzrichtlinie 95/46/EG	3.1; 3.2; Anlage 16
Datenspeicherung	7.5; 7.7; 7.8; 7.12; 7.13; 7.14; 7.15; 7.16; 7.23; 9.1; Anlage 6; Anlage 22; Anlage 25; Anlage 67
Datenübermittlung	2.2; 2.4; 2.9; 5.7; 5.9; 5.21; 5.24; 5.27; 5.30; 9.2; 9.4; 11.2; 12.1; 12.5; 14.2; 14.4; 14.5; 14.6; 15.2; Anlage 10; Anlage 11; Anlage 20; Anlage 21; Anlage 30; Anlage 61; Anlage 69
Datenverarbeitung im Auftrag	5.6; 9.6

De-Mail 2.4; 14.5; Anlage 61
Deutsche Gesellschaft für Bäderwesen e. V. 5.3
Deutsche Kreditwirtschaft 12.8; 12.9
Diebstahl 5.3; 5.18; 7.8; 7.12; 7.18; 9.2; Anlage 55
Diebstahl von Akten 10.5
Dienstanweisung 5.4; 5.7; 5.18; 7.14; 7.15; Anlage 25
Dienstaufsicht 2.1; 5.5
Dienstherr 6.4; 6.8; 7.2; Anlage 54
Dienstleistungsstatistikgesetz (DlStG) 12.1
Dienstliche Dateien 7.2
Dienstliche Kraftfahrzeuge 7.4
Dienstliches Schriftgut A.1; 7.14; 7.15; Anlage 65
Dienstvereinbarung 7.2; 7.23; 15.1
Dienstvorgesetzter 5.5; 7.2
Dienstzeit 7.3; 7.4
Digitales Magazin Thüringen 15.5
Digitalfunkgeräte 7.23
DIHK e. V. 12.6
DIN 32757 10.4
DIN 60529 10.4
Dokumentation 5.4; 5.5; 7.21; 7.22; Anlage 5; Anlage 62;
Dokumentenmanagementsysteme (DMS) 6.2
Doppeltürenmodell 7.19
Dritte Geldwäscherichtlinie (2005/60/EG) 2.8
Drohne 5.19; Anlage 32
Drucker 12.9: Anlage 62
Durchsuchung 7.2; 7.7; 7.14; 7.19; 7.20; 7.21; Anlage 53
Düsseldorfer Kreis 5.3; 12.3
DVD 5.18
Dynamische Internetprotokoll-Adresse; dynamische IP-Adresse 7.13; 7.19; Anlage 24
E.ON 5.16; Anlage 32

E-Call; eCall-Dienst	3.2; 4.4
Eckpunktepapier	2.5; Anlage 2
E-Geld	2.8
E-Government	2.4; 14.5; 14.6; Anlage 10; Anlage 20
E-Government-Gesetz	2.4
Eheschließung	5.8
Eilanordnung	4.5
Einkommensteuer	9.2; Anlage 31
Einsatzbefehl	7.20; 7.21; 7.22
Einschreibesendungen	12.10
Einwilligung	2.10; 3.2; 4.1; 4.4; 5.9; 5.10; 5.12; 5.15; 5.23; 5.24; 5.25; 5.26; 5.27; 5.31; 6.1; 6.6; 6.7; 7.12; 7.17; 10.1; 12.1; 12.4; 13.5; Anlage 2; Anlage 7; Anlage 8; Anlage 12; Anlage 15; Anlage 17; Anlage 42
Einwohnerversammlung	7.10
Einzelangaben für kommunalstatistische Zwecke	5.4
eLearning	13.1
Elster	9.2; Anlage 26
Eltern	5.24; 7.12; 9.1; 10.4; 11.2; 13.1; 13.2; 13.4; 13.6; Anlage 47
E-Mail	2.2; 5.8; 5.29; 5.30; 7.2; 7.20; 12.1; 12.6; 13.1; 13.7; 14.6; Anlage 45; Anlage 53; Anlage 54; Anlage 57; Anlage 67; Anlage 76
E-Mail-Account	2.2; 7.2; Anlage 67
E-Mailversand	5.29
Ende-zu-Ende-Verschlüsselung	2.4; 14.1; 14.5; 15.1; Anlage 9; Anlage 20; Anlage 23; Anlage 61; Anlage 75
Entschließung der DSK	2.7; 2.8; 4.2; 4.3; 14.1; 14.5; 14.6; Anlage 1; Anlage 2; Anlage 3; Anlage 4; Anlage 5; Anlage 6; Anlage 7; Anlage 8; Anlage 9; Anlage 10; Anlage 11; Anlage 12; Anlage 13; Anlage 14; Anla-

	ge 15; Anlage 16; Anlage 17; Anlage 18; Anlage 19; Anlage 20; Anlage 21; Anlage 22; Anlage 23; Anlage 34; Anlage 39; Anlage 56; Anlage 73; Anlage 75;
E-Privacy-Richtlinie	4.1
Ereignis	A.1; 7.7; 7.8; 7.14; 7.16; 10.4; 15.5; Anlage 9
Erfahrungsaustausch	5.1; 5.2
Erforderlichkeit	2.10; 6.6; 7.7; 7.9; 7.15; 10.1; 13.5; Anlage 2; Anlage 39; Anlage 41; Anlage 69; Anlage 76
Erfurter Lösung	5.27
Erhebung von Verkehrsdaten	4.5
Erkennungsdienstliche Behandlung	7.12
Erkennungsdienstliche Erfassung	7.12
Erkennungsdienstliche Maßnahmen	6.6; 7.12; 10.1; 10.3
Ermittlungsakten	7.15; 7.20; 10.5; Anlage 25; Anlage 53
Ermittlungsunterlagen	7.20; 7.21; Anlage 32; Anlage 58
Ermittlungsverfahren	5.33; 7.1; 7.3; 7.7; 7.8; 7.12; 7.15; 7.16; 7.20; Anlage 7; Anlage 24; Anlage 33; Anlage 42; Anlage 50; Anlage 58
Erstwähler	5.33
Erwerbsfähigkeit	12.2
Europa	2.1; 2.2; 2.8; 3; 3.1; 3.2; 4.1; 4.2; 5.27; 10.4; 12.3; 12.8; 14.4; Anlage 2; Anlage 3; Anlage 4; Anlage 8; Anlage 13; Anlage 14; Anlage 15; Anlage 16; Anlage 19; Anlage 22; Anlage 23; Anlage 30; Anlage 34; Anlage 37; Anlage 56; Anlage 67; Anlage 69; Anlage 73; Anlage 75
Europaausschuss des Thüringer Landtags	3.2
Europäische Datenschutzgrund-	

verordnung	3.1; Anlage 8
Europäische Ermittlungsanordnung	Anlage 32
Europäische Notrufnummer	3.2
Evaluierungsklausel	7.13
Facharzt	6.4; 12.2
Fachkunde	5.6
Fahreignung	12.2
Fahrerlaubnisbehörde	12.2
Fahrtauglichkeit	6.4
Fahrzeug	3.2; 4.4; 5.22; 6.4; 7.3; 7.4; 7.7; 7.10; 10.5; 12.2; 12.4; 16.1; Anlage 30; Anlage 31; Anlage 32; Anlage 53; Anlage 66
Fahrzeughalter	12.4
Fanpages	4.3; Anlage 14; Anlage 38
Fernwartung	5.4; 6.5; 10.4
Filialbüro	12.1
Finanzamt	9.2; 9.6; 12.1
FINDUS	7.14
Fingerabdruck	6.6; 7.12; 10.3; Anlage 64
Forderungen für die neue Legislaturperiode	Anlage 23; Anlage 75
Formblätter	6.5; 15.2
Forschungsprivileg	12.4
Forschungsprojekte	Anlage 4; Anlage 34
Fotos	2.2; 5.19; 5.22; 6.1; 7.3; 7.5; 7.21; 12.4; Anlage 32
Fraktionsvorsitzende	5.28
Freibäder	Anlage 27
Freihandelszone	Anlage 13
Fremdenverkehrsabgabe	5.20; Anlage 37
Friedrich, Hans-Peter	2.2
Funk-Chip	12.8
Funktion des unbemerkten Mithörens (Ambience Listening)	7.23
Gästeinformation	5.10
Gaststätte	5.32
Geburtsurkunde	5.7

Gefahr im Verzug	4.5
Gefahrenabwehr	3.3; 7.14; 7.17; 12.4; 15.1; Anlage 24
Gefangenenpost	10.1
Geheimdienste	2.2; 2.4; 5.19; 14.4; 14.5; Anlage 19; Anlage 20; Anlage 67; Anlage 69; Anlage 70; Anlage 73; Anlage 74; Anlage 75; Anlage 76
Geheimnisverrat	7.2
Gehörlose	15.3
Geldautomat	12.10; 12.11
Geldforderungen	5.11
Geldkarte	12.8; 12.9
Gemeinde	5.1; 5.2; 5.4; 5.9; 5.10; 5.13; 5.14; 5.20; 5.23; 5.24; 5.25; 5.27; 9.4; 9.5; 12.7; Anlage 26; Anlage 27
Gemeinde- und Städtebund Thüringen	5.2
Generalstaatsanwalt	7.11; Anlage 50
Geobasisdaten	5.21, 12.7
Gericht	2.1; 2.3; 2.6; 2.7; 2.9; 2.10; 3.1; 4.3; 5.10; 5.20; 5.27; 6.1; 6.5; 7.2; 7.3; 7.4; 7.6; 7.9; 7.11; 7.12; 7.13; 7.17; 7.18; 7.19; 7.20; 7.21; 9.1; 10.1; 10.2; 10.3; 10.4; 10.5; 12.4; 12.5; 13.4; Anlage 1; Anlage 2; Anlage 5; Anlage 8; Anlage 19; Anlage 22; Anlage 23; Anlage 24; Anlage 25; Anlage 26; Anlage 27; Anlage 28; Anlage 31; Anlage 37; Anlage 41; Anlage 48; Anlage 50; Anlage 56; Anlage 58; Anlage 66; Anlage 78
Gesamtgutachten	12.2
Geschäftsordnung	5.27; 5.28; 7.13; 16; 16.1
Geschwindigkeitsverstoß	12.4
Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung	2.7; Anlage 1

Gesetzentwurf zur Optimierung der Geldwäscheprävention	2.8
Gesprächsaufschaltung	5.1
Gesundheitsdaten	3.2; 5.17; 6.4; 6.5; 6.8; 10.1; Anlage 21; Anlage 36
Gewahrsamsräume	7.6
Gewerbebehörde	5.32
Gewerbedaten	5.30
Gewerbeordnung	5.30
Gewerkschaft der Polizei	2.9
GEZ	14.6; Anlage 10
Girogo	12.9
Giroverband	12.9
Gleitzeitvereinbarung	6.7
Glücksspielgesetz	9.3
Glücksspielstaatsvertrag	9.3
GPS-Funktion	7.23; Anlage 66;
Großveranstaltungen	7.17
Grundrecht auf informationelle Selbstbestimmung	2.6; 5.19; 5.27; 6.4; 7.2; 7.3; 7.4; 7.13; 7.17; 7.18; 7.20; 7.21; 10.1; 10.3; 10.5; 11.3; 12.4; 15.1; 15.5; Anlage 12; Anlage 19; Anlage 21; Anlage 22; Anlage 23; Anlage 28; Anlage 30; Anlage 31; Anlage 32; Anlage 39; Anlage 53; Anlage 64; Anlage 75;
Grundrechtsgefährdung	7.18
Grundsatz der Datensparsamkeit	9.3; Anlage 27; Anlage 32
Grundschule	13.3; 13.6; 13.7
Grundstückseigentümer	5.21; 5.22
Gruppenauskunft	5.14
Haftungsfragen	5.3
Hallenbäder	5.3
HAMASYS	15.4
Handwerkskammer	15.1
Handy	4.4; 7.20; 7.21; 12.8; 15.3; Anlage 58
Hauptpersonalrat	7.23
Hausrecht	2.1; 11.3

Hinweis	A.1; 4.2; 5.6; 5.10; 5.12; 5.13; 5.16; 5.17; 5.18; 6.1; 6.3; 6.6; 7.7; 7.13; 7.15; 7.19; 7.23; 10.1; 10.3; 11.2; 11.4; 12.1; 12.5; 12.9; 13.5; 13.7; 14.1; 15.1; 15.2; 15.3; Anlage 9; Anlage 15; Anlage 24; Anlage 32; Anlage 33; Anlage 36; Anlage 37; Anlage 38; Anlage 39; Anlage 45; Anlage 50; Anlage 57; Anlage 64; Anlage 65; Anlage 68
Höchstfrist	7.15
Hörgeschädigte	15.3
Hundehaltung	5.12
Identifizierung des Vertragspartners	2.8
Identität	2.2; 5.26; 7.17; 9.1; 9.2; 10.1; 10.3; 11.4; 14.5; 14.6; Anlage 10; Anlage 18; Anlage 19; Anlage 30; Anlage 67
IHK	12.5; 12.6
IHK-GfI mbH	12.6
Industrie- und Handelskammer	12.5; 12.6; 15.1
Informationsfreiheitsgesetz	A.Vorwort; Anlage 26; Anlage 31
Inkassounternehmen	5.11
Innenministerium von Baden-Württemberg	10.4
Innenrevision der Landesregierung	5.16
INPOL	7.7; 7.16
Integrationsverfahren Polizei (IGVP)	7.14
Intelligente Stromzähler	12.3
Internet	2.2; 2.4; 2.7; 2.8; 2.10; 4.3; 4.5; 5.1; 5.9; 5.27; 5.30; 6.1; 7.8; 7.13; 7.15; 7.19; 9.2; 12.3; 12.6; 13.4; 13.5; 14.1; 14.2; 14.3; 14.4; 14.5; 14.6; 15.4; Anlage 1; Anlage 7; Anlage 9; Anlage 19; Anla-

	ge 21; Anlage 26; Anlage 35; Anlage 39; Anlage 44; Anlage 45; Anlage 46; Anlage 49; Anlage 54; Anlage 56; Anlage 59; Anlage 60; Anlage 61; Anlage 63; Anlage 65; Anlage 67; Anlage 71; Anlage 72; Anlage 73
Internetknotenpunkt	2.2
Internetseite	2.10; 5.1; 5.27; 7.8; 7.15; 12.6; 14.2; Anlage 26; Anlage 35; Anlage 56; Anlage 65
IP-Adresse	7.13; 7.19; 14.1; Anlage 9; Anlage 15; Anlage 16; Anlage 24
IPv6	14.1; Anlage 9
Irismuster	6.6
IT-Grundschutz-Kataloge	14.3
IT-Planungsrat	14.5; Anlage 20; Anlage 56
IT-Sicherheitskonzept	5.1; 5.4; 6.2; 7.23; 14.5
Jobcenter	5.7; 5.8; 11.2; 11.4; Anlage 31
Journalist	7.21; Anlage 28
Jugendamt	5.7; 11.2
Jugendliche	7.12; 13.4; Anlage 49; Anlage 52
Justiz	2.2; 2.7; 2.9; 4.5; 7.11; 7.19; 10; 10.1; 10.2; 10.3; 10.5; Anlage 1; Anlage 2; Anlage 8; Anlage 24; Anlage 34; Anlage 50
Justizministerium	2.2; 7.11; 7.19; 10.2; 10.3
Justizvollzug	10.1; 10.3
Justizvollzugsanstalt (JVA)	10.1
Justizvollzugsgesetzbuch	10.3
Kamera	5.6; 5.18; 5.19; 5.22; 5.27; 7.10; 7.18; 10.1; 13.6; Anlage 4; Anlage 28; Anlage 32; Anlage 63
Kameraattrappen	13.6
Kamerawagen	5.22
Kartenleser	9.2; 12.8
Kassenbereich	5.6
Kaufvertrag	5.25
Kfz-Kennzeichen	7.5; 12.4
Kfz-Steuer	9.6

Kfz-Zulassungsstelle 6.4
Kinder 5.24; 10.4; 11.2; 13.4; 13.7; Anlage 49; Anlage 51; Anlage 52; Anlage 63
Kindergarten 5.24
Klausur 7.1; 7.2
Klopapier 7.18
Kommunalaufsicht 5.20
Kommunalkontrollen 5.1
Kommunalordnung 5.9; 5.27; 5.28; 5.29
Kommunalverwaltung 5.1; Anlage 54
Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2.2; 13.1; 14.1; 14.2; 14.5; 14.6; Anlage 1; Anlage 2; Anlage 3; Anlage 4; Anlage 5; Anlage 7; Anlage 8; Anlage 9; Anlage 10; Anlage 11; Anlage 12; Anlage 13; Anlage 14; Anlage 15; Anlage 16; Anlage 17; Anlage 19; Anlage 20; Anlage 21; Anlage 22; Anlage 23; Anlage 31; Anlage 34; Anlage 36; Anlage 39; Anlage 51; Anlage 52; Anlage 56; Anlage 69; Anlage 73; Anlage 75
Konkreter Gefahrenbegriff 7.13
Konkretisierungs- und Umgrenzungsfunktion 7.21
Kontaktliste 7.20
Kontoauszüge 11.4; 12.9
Kontrolle der Gerichte 10.2
Kontrollkompetenz 10.2; Anlage 77
Kooperation 11.2; 13.1; 13.3; 13.4; 14.2; 14.5; Anlage 27; Anlage 31; Anlage 37; Anlage 47; Anlage 49; Anlage 51; Anlage 52; Anlage 72; Anlage 73
Kooperationsvereinbarung 11.2; Anlage 47
Kooperative Betriebsmodelle 14.2
Kopierer 14.7; Anlage 62

Korruptionsbekämpfung	5.16; Anlage 32
Krankenversicherungskarte	11.4
Krankheitsbilder	13.7
Krankschreibung	6.8
Kreditkarte	2.7; 12.8; 12.10
Kriminalakte (KAN)	7.14; 7.15; Anlage 25
Kulturförderabgabe	5.10
Kundendaten	12.10; 7.19
Kündigung	2.1; 12.5
Kündigungsschutz	2.1
Kurbeitrag	5.13
Kurbeitragssatzung	5.13
Landesamt für Verfassungsschutz	A.1; 2.2; 2.9, 7.9; 7.14; 7.15; 8.1; 8.2; Anlage 48
Landesärztekammer	11.1
Landeskrankenhausgesellschaft	11.1; Anlage 36
Landeskriminalamt	A.1; 2.9; 7.3; 7.5; 7.7; 7.15; 7.16; 7.17; 7.18; 7.23; 16.1; Anlage 25; Anlage 32; Anlage 33; Anlage 52; Anlage 55
Landgemeinde	5.1
Landtag	A.Vorwort; 2.2; 2.3; 2.10; 3.2; 5.27; 7.1; 7.6; 7.9; 7.13; 7.19; 7.20; 15.1; 15.2; 16; 16.1; Anlage 24; Anlage 25; Anlage 26; Anlage 27; Anlage 28; Anlage 29; Anlage 30; Anlage 31; Anlage 32; Anlage 36; Anlage 37; Anlage 40; Anlage 50; Anlage 58; Anlage 78
Landtagsabgeordnete	7.13; 7.19; 7.20; Anlage 58
Längerfristige Observation	7.3; 7.4
Langzeitspeicherung	15.5
Lastschriftverfahren	9.6
Lehrer	4.3; 13.1; 13.2; 13.4; 13.5; 13.7; Anlage 47; Anlage 49; Anlage 51; Anlage 52; Anlage 71
Lehrerfortbildung	13.2; 13.4; Anlage 47; Anlage 49; Anlage 51; Anlage 52;
Lehrgang	12.5; 13.2

Leistungskontrolle	5.6; 5.18; 6.2
Leistungsmerkmale	5.1; 7.23; 15.1; Anlage 32; Anlage 76
Leistungsmissbrauch	11.2; Anlage 31
Leitfaden	A.1; 4.1; 7.8; 7.14; 7.15; Anlage 65
Like-Button	4.3
Livemitschnitt	5.27
Lobbyarbeit	3.1
Löschüberprüffrist	5.18; 6.1; 7.7; 7.8; 7.14; Anlage 6; Anlage 25
Lösch-Überprüfungs-Datum	7.15
Löschung personenbezogener Daten	4,2; 5.13; 5.17; 5.18; 5.31; 6.1; 6.5; 6.7; 7.1; 7.7; 7.8; 7.9; 7.12; 7.14; 7.15; 7.16; 7.17; 7.20; 7.23; 8.1; 13.3; Anlage 2; Anlage 5; Anlage 6; Anlage 14; Anlage 25; Anlage 31; Anlage 35; Anlage 48; Anlage 58; Anlage 62; Anlage 67
Mädchentoilette	13.6
Mandantenfähigkeit	14.2
MDR	Anlage 25; Anlage 28; Anlage 33; Anlage 53; Anlage 55
Medienbildung	13.4
Medienkompetenz	13.1; Anlage 47; Anlage 51; Anlage 71
Medienkompetenzentwicklung bei Schülern	13.4
Medienunternehmen	5.27
Meldeamt	5.9; 5.11; 5.33; 14.6; Anlage 10
Meldebehörde	2.10; 5.9; 5.11; 5.14; 5.23; 5.33; 14.6; Anlage 8; Anlage 10; Anlage 40; Anlage 41
Meldedaten	5.11; 5.14; 5.23; 5.33; 9.2; 14.6; Anlage 7; Anlage 10
Meldepflicht	5.23; 12.11; Anlage 7; Anlage 68
Melderecht	2.10; 5.11; 9.1; Anlage 7; Anlage 42

Melderegister	2.10; 5.9; 5.11; 5.14; 5.23; Anlage 7; Anlage 40; Anlage 41
Melderegisterauskunft	2.10; 5.11; 5.14; Anlage 7; Anlage 40; Anlage 41
Meldeschein	5.13
Meldewesen	2.10; 5.13; Anlage 40; Anlage 42
Mikrochip	5.12
Mikrozensusgesetz	2.6
MiStra	7.11
Mitarbeiter	7.2; Anlage 16; Anlage 26; Anlage 28; Anlage 35; Anlage 37; Anlage 51; Anlage 52; Anlage 63;
Mitarbeiterdatenschutz	siehe Beschäftigtendatenschutz
Mitbestimmung des Personalrats	7.18
Mitgliedsgemeinde	5.24; 9.4; 12.7
Mitteilungspflicht bei Daten-Pannen	12.10
Mitteldeutscher Rundfunk	7.22; Anlage 33
Modellprojekt "Grundschulen"	13.3
Modernes Datenschutzrecht	2.1; Anlage 2; Anlage 34
Monitoring	5.3; 5.6
Moratorium	7.9
Multifunktionsgerät	14.7; Anlage 62
Museum	5.6
Nationales Waffenregister	2.9
Nationalsozialistischer Untergrund (NSU)	2.2; 7.9; Anlage 25
Near Field Communikation (NFC)	12.8; 12.9
Neubürger	5.9
Nichteheliche und einzeladoptierte Kinder	10.4
Nicht-öffentliche Stadtratssitzung	5.27; 5.28; 5.29
Niederschriften	5.28; 5.29
Niederschriften aus nicht-öffentlichen Sitzungen	5.29
Notfallrettung	5.5
Notruf	3.2; 4.4; 5.5; 7.23; 15.1; 15.3
Notrufsystem	3.2

Novellierung	2.1; 2.5; 4.1; 7.6; 7.13; 7.15; 7.19; 15.2; Anlage 37; Anlage 39
Novellierungsbedarf	7.13; 7.15
NSA	2.2; 14.4; Anlage 69; Anlage 77
NSU	2.2; 7.9; Anlage 25
Nutzung von personenbezogenen Daten	5.12; 6.4
Obdachlosenheim	5.17
Oberbürgermeister	5.28
Observation	7.3; 7.4; 7.18; Anlage 33; Anlage 53; Anlage 55
Öffentlich zugängliche Bereiche	5.6; 5.18; 11.3; 13.7; Anlage 4
Öffentliche Bekanntmachung	10.2
Öffentliche Sicherheit	5.17; 6.4; 7.22; 8.2; Anlage 22; Anlage 23; Anlage 30; Anlage 75
Öffentliche Stadtratssitzung	5.29
Öffentliche Verwaltung	7.1; Anlage 15
Öffnungszeiten	5.18
Ordnungsbehörde	5.12; 7.6; 7.13; Anlage 28; Anlage 30
Ordnungswidrigkeitengesetz	5.26; 5.33
Ordnungswidrigkeitenverfahren	5.26; 11.2
Organisatorische Maßnahmen	9.3; 10.5; 14.5; Anlage 20; Anlage 39; Anlage 62
Organisatorische Trennung	5.4
Organleihe	10.4
Orientierungshilfe Cloud Computing	10.4; Anlage 7.6
Orientierungshilfe Krankenhausinformationssysteme (OH KIS)	11.1
Orientierungshilfe Mandantenfähigkeit	14.2
Orientierungshilfe Videoüberwachung	5.3
Orientierungshilfe zum datenschutzgerechten Smart Metering	Anlage 6; Anlage 39
OSCI-Transport	14.5; 14.6; Anlage 10; Anlage 20; Anlage 23; Anlage 75

PAG	7.5; 7.6; 7.8; 7.9; 7.13; 7.14; 7.15; 7.19; 7.22; Anlage 24; Anlage 25; Anlage 30
Papierabfall	7.1
Papstbesuch	A.1; 7.17; 7.20; 7.21; 7.22; Anlage 58
Parlamentarische Anfragen	2.1; 16; 16.1
Partnerschaftsgesellschaft	12.1
Passwörter	7.2; 14.3
Passwortsicherheit	14.3
Patientenrechte	Anlage 5
Pay-As-Yor-Drive-Versicherungsverträge	3.2
Personalausweiskopie	11.4
Personalrat	7.2; 7.18; 7.23; 15.1; Anlage 53
Personalunterlagen	7.1
Personenkennzeichen	9.1
Personenstandsgesetz	5.7; 5.8
Persönliche und sachliche Verhältnisse	7.5; 7.21; Anlage 16; Anlage 30
Persönlichkeitsprofil	9.1; Anlage 63
Polizei	A.1; 2.2; 2.9; 4.2; 7; 7.1; 7.2; 7.3; 7.4; 7.5; 7.6; 7.7; 7.8; 7.9; 7.10; 7.12; 7.13; 7.14; 7.15; 7.16; 7.17; 7.19; 7.20; 7.21; 7.22; 7.23; 12.4; 15.1; 16.1; Anlage 2; Anlage 8; Anlage 11; Anlage 22; Anlage 24; Anlage 25; Anlage 28; Anlage 30; Anlage 32; Anlage 35; Anlage 37; Anlage 50; Anlage 52; Anlage 53; Anlage 54; Anlage 58; Anlage 65; Anlage 78
Polizeiaufgabengesetz	7.6; 7.9; 7.13; 7.19; 7.22; Anlage 24; Anlage 25; Anlage 30
Polizeiliche Fahndung	4.2
Portal	2.7; 12.6; 13.4; Anlage 12
Post	2.2; 5.14; 5.15; 5.19; 7.1; 7.2; 7.13; 9.6; 10.1; Anlage 53; Anlage 54; Anlage 59
Postfächer	7.1; 7.2; Anlage 53

Postzustellung	9.6
PPS-Richtlinie	7.14
Prantl, Heribert	2.2
Prepaidkarten	2.8
Pressemitteilung	2.2; 2.4; 4.1; 5.16; 6.6; 8.1; 15.1; Anlage 32; Anlage 33; Anlage 34; Anlage 35; Anlage 36; Anlage 37; Anlage 38; Anlage 39; Anlage 40; Anlage 41; Anlage 42; Anlage 43; Anlage 44; Anlage 45; Anlage 46; Anlage 47; Anlage 48; Anlage 49; Anlage 50; Anlage 51; Anlage 52; Anlage 53; Anlage 54; Anlage 55; Anlage 56; Anlage 57; Anlage 58; Anlage 59; Anlage 60; Anlage 61; Anlage 62; Anlage 63; Anlage 64; Anlage 65; Anlage 66; Anlage 67; Anlage 68; Anlage 69; Anlage 70; Anlage 71; Anlage 72; Anlage 73; Anlage 74; Anlage 75; Anlage 76; Anlage 77; Anlage 78
PRISM	2.2; 13.4; Anlage 19; Anlage 67; Anlage 70; Anlage 74
Privacy Impact Assessment (PIA)	12.8
Private Dateien	7.2
Private Zwecke	7.3; 7.4; Anlage 32; Anlage 53
Private-Cloud	2.2; 14.4; Anlage 21; Anlage 38; Anlage 67; Anlage 69; Anlage 76
Privatgrundstück	5.22
Privatsphäre	2.2; 2.6; 4.1; 5.19; 10.1; 12.3; 13.4; Anlage 6; Anlage 14; Anlage 19; Anlage 23; Anlage 39; Anlage 56; Anlage 67; Anlage 69; Anlage 70; Anlage 74; Anlage 75
Projekt 6	2.2
Projektgruppe Digitalfunk	7.23

Protokollstandard 14.1
Prüffrist; Prüffristen A.1; 7.7; 7.8; 7.12; 7.14; 7.15; 7.16; Anlage 25; Anlage 65
Pseudonymisierung von Krebsregisterdaten Anlage 17; Anlage 56
Rangliste 13.7
Raumüberwachung 5.1; 15.1; Anlage 32
Recht auf informationelle Selbstbestimmung 2.6; 5.19; 5.27; 6.4; 7.3; 7.4; 7.17; 7.20; 7.21; 10.1; 10.3; 10.5; 11.3; 15.1; Anlage 21; Anlage 24; Anlage 30; Anlage 31; Anlage 32; Anlage 39; Anlage 64
Rechtsanwalt 3.2; 7.8; 7.13; 7.14; Anlage 5; Anlage 28; Anlage 68
Registrierung 2.7; 9.2; Anlage 17
Religionsgemeinschaft 14.6; Anlage 10
Rentner 2.6
Repräsentativstatistik 2.6
Rettungsleitstelle 4.4; 5.5
Rettungswagen 11.3
RFID 12.8
Rheinland-Pfalz 7.6; 13.1
Richterliche Anordnung 7.3; 7.14; Anlage 32
Richterlicher Beschluss 7.4
Richtervorbehalt 7.13; 7.19
Richtlinie zur Korruptionsbekämpfung 5.16
RLAktenThürPol 7.14; Anlage 25
Routing 14.4; Anlage 19; Anlage 69
Ruhestörung 5.32
Sachverständige 2.1; 12.2; 12.6
Safe-Harbour-Abkommen 2.2
Sanktionsmöglichkeiten 16.1; Anlage 16; Anlage 26
SARS 7.21
Satzung 5.6; 5.10; 5.13; 5.20; Anlage 26; Anlage 27
Scanner 5.22; 9.2; 10.4; 14.7; Anlage 62; Anlage 76
Schengener Informations-

system (SIS) 3.3
Schreddern 7.9
Schriftform 5.12; 5.15
Schriftwechsel 10.1
Schulamt; Schulämter 13.2; 13.3; 13.7
Schulaufsicht 13.2
Schuldnerverzeichnis 2.7; Anlage 1
Schuldnerverzeichnisführungs-verordnung 2.7
Schule 2.1; 4.3; 6.1; 7.1; 7.2; 13.1; 13.2 ; 13.3; 13.4; 13.5; 13.6; 13.7; Anlage 47; Anlage 49; Anlage 51; Anlage 52; Anlage 59; Anlage 60; Anlage 71
Schüler 4.3; 7.2; 13.1; 13.2; 13.3; 13.4; 13.6; 13.7; Anlage 47; Anlage 49; Anlage 51; Anlage 52; Anlage 71
Schulleitung 13.2; 13.4; 13.6
Schulnoten 13.7
Schulträger 13.2; 13.3
Schutz der Bevölkerung 5.12
Schutz vor unbefugtem Zugriff 6.5
Schutzbedarf 7.17; 10.4; 15.5; Anlage 6; Anlage 16
Schutzfristverkürzung 2.3
Schwärzung 5.12; 5.13; 7.3; 10.3; 11.4; 12.2
Schwimmbäder 5.3; 5.19; Anlage 37
Section Control 12.4
Selbstständig tätige Person 12.1
SEPA-Verfahren 9.6
SGB II 5.8; 11.2; 16.1; Anlage 31
Sicherheitsbehörden 7.19; Anlage 11; Anlage 22; Anlage 24; Anlage 63; Anlage 75; Anlage 76
Sicherheitskonzept 5.1; 5.4; 6.2; 13.2; Anlage 63
Sicherheitsstufe 4 10.4
Sicherheitstechnik 5.4; 9.2; 10.5
Signaturkarte 9.2
Sitzungsniederschrift 5.28

Skimming	12.10; 12.11
Smart Metering	12.3; Anlage 6; Anlage 39
Snowden, Edward	2.2
Sorgfaltspflicht	2.8
Sozial- und Gesundheitswesen	Anlage 21; Anlage 23; Anlage 75
Sozialdaten	2.4; 11; 11.2; 11.4; Anlage 31; Anlage 37; Anlage 61
Soziale Netzwerke	4.2; 4.3; Anlage 14; Anlage 49; Anlage 51; Anlage 52; Anlage 56
Sparkasse	11.4; 12.8; 12.9
SparkassenCard	12.9
Speicherdauer	7.15
Speicherung von Unterstützern	2.2
Spiegel	2.2; Anlage 38; Anlage 63
Spielersperre	9.3
Staatsanwaltschaft	A.1; 4.5; 5.33; 7.3; 7.11; 7.14; 7.15; 7.18; 10.5; Anlage 33; Anlage 50; Anlage 58; Anlage 65; Anlage 66
Staatsanwaltschaft Erfurt	4.5
Staatsanwaltschaft Gera	4.5; 10.5
Staatsanwaltschaft Meiningen	Anlage 58
Staatsanwaltschaft Mühlhausen	7.3
Staatsarchiv	2.3; 5.6; 8.1; 15.5; Anlage 25; Anlage 48
Stadtarchiv	5.15
Städtische Beschäftigte	5.27
Stadtrat	5.14; 5.27; 5.28; 5.29
Stadtratsmitglieder	5.27; 5.29
Stadtratssitzung	5.27; 5.28; 5.29
Stadtverwaltung	3.3; 5.1; 5.4; 5.10; 5.13; 5.14; 5.19; 5.22; 5.23; 5.27; 5.28; 5.31; Anlage 32
Stand der Technik	2.4; 5.4; 14.4; 14.5; 15.5; Anlage 6; Anlage 18; Anlage 21; Anlage 57; Anlage 61
Standesamt	5.7; 5.8; 10.4
Standortdaten	4.5; 7.23; 15.3; Anlage 16
Statistikregistergesetz	12.1

Statistikstelle	5.4
Steuerbehörde	5.10
Steuerberaterin	9.2; 12.1
Steuerdaten	2.4; 5.10; 9.4; 9.5; Anlage 61
Steuererklärung	9.2
Steuergeheimnis	9.1; 9.4; 9.5; 12.1; Anlage 61
Steuer-ID	9.1
StPO	4.5; 5.33; 7.3; 7.4; 7.10; 7.12; 7.14; 7.20; 7.21; Anlage 24
Strafanzeige	5.33
Strafbefehlsantrag	7.11
Strafprozessordnung	4.5; 5.33; 7.2; 7.3; 7.4; 7.10; 7.12; 7.18; 7.20; 7.21; 12.10; 15.1; Anlage 24; Anlage 50; Anlage 53
Straftat	3.3; 7.2; 7.3; 7.4; 7.8; 7.12; 7.14; 7.22; 9.4; Anlage 4; Anlage 7; Anlage 28
Strafverfahren	7.11; 7.12; 12.10
Strafverfolgung	7.12; 7.17; 7.18; 7.19; 7.20; 7.21; 12.10; 15.1; Anlage 3; Anlage 24; Anlage 34; Anlage 35; Anlage 66
Straßenzustand	5.22
Stromverbrauch	12.3
Strukturerhebung im Dienstleistungsbereich (SiD)	12.1
Subsidiaritäts-Frühwarnsystem	3.2
Süddeutsche Zeitung	2.2
Summer of Snowden	2.2
Supergrundrecht auf Sicherheit	2.2
Tag der deutschen Einheit	7.17
Telefonanlage	A.1; 5.1; 5.5; 15.1; Anlage 32; Anlage 35; Anlage 54; Anlage 76
Telekommunikationsgesetz (TKG)	4.1; 4.4; 7.13; 7.19; 7.21; 15.3; Anlage 24
Tempora	2.2; Anlage 19; Anlage 67; Anlage 74
Testamentsverzeichnisüberführungsgesetz (TVÜG)	10.4

The Government Communications Headquarters (GCHQ)	2.2
The Guardian	2.2
The Washington Post	2.2
Thüringer Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften	10.5
Thüringer Archivgesetz (ThürArchivG)	2.3; 7.15; 8.1; Anlage 25; Anlage 48
Thüringer Datenschutzgesetz (ThürDSG)	A.Vorwort; 2.1; 2.6; 2.9; 3.1; 4.3; 5.1; 5.3; 5.4; 5.6; 5.7; 5.8; 5.9; 5.10; 5.12; 5.14; 5.17; 5.18; 5.19; 5.20; 5.21; 5.23; 5.24; 5.25; 5.26; 5.27; 5.28; 5.29; 5.30; 5.31; 6.1; 6.2; 6.4; 6.5; 6.6; 6.7; 6.8; 7.1; 7.3; 7.6; 7.7; 7.9; 7.10; 7.15; 7.18; 7.20; 10.2; 10.3; 12.1; 12.4; 12.10; 12.11; 13.2; 13.5; 13.7; 15.2; 15.4; 16.1; Anlage 25; Anlage 26; Anlage 27; Anlage 28; Anlage 30; Anlage 32; Anlage 37; Anlage 69; Anlage 71
Thüringer Disziplinargesetz (ThürDG)	7.2
Thüringer Gesetz zum Schutz der Bevölkerung vor Tiergefahren (TierGefG)	5.12
Thüringer Innenministerium (TIM)	5.16; 5.20; 6.1; 7.2; 7.9; 7.13; 7.14; 7.19; 7.22; 7.23; 13.2; 15.1; 15.3; Anlage 24; Anlage 25; Anlage 26; Anlage 28; Anlage 32; Anlage 54; Anlage 78
Thüringer Justizministerium (TJM)	7.11; 7.19; 10.2; 10.3
Thüringer Kommunalabgabengesetz (ThürKAG)	5.10; 5.13; Anlage 27
Thüringer Kommunalordnung (ThürKO)	5.9; 5.27; 5.28; 5.29

Thüringer Landesamt für Verfassungsschutz (TLfV)	A.1; 2.2; 2.9, 7.9; 7.14; 7.15; 8.1; 8.2; Anlage 48
Thüringer Landesamt für Vermessung und Geoinformation (TLVermGeo)	5.21
Thüringer Landeskriminalamt (TLKA)	A.1; 2.9; 7.3; 7.5; 7.7; 7.15; 7.16; 7.17; 7.18; 7.23; 16.1; Anlage 25; Anlage 32; Anlage 33; Anlage 52; Anlage 55
Thüringer Landesrechenzentrum	15.1; 15.2
Thüringer Landesverwaltungsamt	5.19; Anlage 26; Anlage 32; Anlage 37
Thüringer Landkreistag	5.2
Thüringer Landtag	A.Vorwort; 2.2; 2.3; 2.10; 3.2; 5.27; 7.1; 7.6; 7.9; 7.13; 7.19; 7.20; 15.1; 15.2; 16; 16.1; Anlage 24; Anlage 25; Anlage 26; Anlage 27; Anlage 28; Anlage 29; Anlage 30; Anlage 31; Anlage 32; Anlage 36; Anlage 37; Anlage 40; Anlage 50; Anlage 58; Anlage 78
Thüringer Meldegesetz (ThürMeldeG)	2.10; 5.9; 5.11; 5.13; 5.14; 5.23; 5.33; Anlage 41
Thüringer Ministerium für Bildung, Wissenschaft und Kultur (TMBWK)	13.2; 13.3; 13.4; 13.5
Thüringer Polizeiaufgabengesetz (ThürPAG)	7.6; 7.9; 7.13; 7.19; 7.22; Anlage 24; Anlage 25; Anlage 30
Thüringer Rettungsdienstgesetz (ThürRettG)	5.5
Thüringer Staatskanzlei	2.4; 7.13; 7.17; 15.1; Anlage 32
Thüringer Verfassungsgerichtshof (ThürVerfGH)	7.13
Thüringer Verfassungsschutzgesetz	

(ThürVSG) 2.2; 7.9; 7.19; 8.1; 8.2; Anlage 24; Anlage 48
Thüringer Verordnung über die Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) 7.7; 7.8;7.14; 7.16
Thüringer Verwaltungsblätter (ThürVBl) 7.2
Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) 2.4; 5.26
Thüringisches Hauptstaatsarchiv 8.2; 15.5; Anlage 25; Anlage 48
ThürPAG-Novellierung 7.6; 7.13; 7.19
Tierarzt 5.12
Tiergefahren 5.12
TK-Anlage 15.1; Anlage 32
Toilettenpapier A.1; 7.18; 13.6; Anlage 55
Tonaufzeichnung 7.6
Tonkassetten 12.10
Tourismus- und Marketingkonzept 5.14
Tracking 7.23; Anlage 9; Anlage 67
Transponder 5.12
Transport von Akten 10.5
Transsexuelle 9.1
Twitter 15.3
Über- Unterordnungsverhältnis 6.6
Übermittlungssperre Anlage 10
Übernachtung 5.10; 16.1; Anlage 27

Überschreiben und Löschen von Videoaufzeichnungen 7.10
Überwachung A.1; 2.1; 2.2; 4.5; 5.1; 5.3; 5.6; 5.14; 5.18; 5.19; 5.30; 7.6; 7.10; 7.18; 7.19; 7.23; 9.3; 10.1; 11.3; 12.3; 12.4; 13.2; 13.4; 13.6; 14.4; 15.1; 16.1; Anlage 4; Anlage 9; Anlage 12; Anlage 19; Anlage 22; Anlage 26; Anlage 28; Anlage 32; Anlage 37; Anlage 38; Anlage 53; Anlage 66; Anlage

	69; Anlage 71; Anlage 73; Anlage 74; Anlage 75; Anlage 76
Überwachung der Telekommunikation	4.5; Anlage 53
Unabhängigkeit der Richter	10.2
Unbefugte Kenntnisnahme	10.5; 15.5
Unbefugter Zugriff	2.2; 2.9; 6.2; 6.5; 7.1; 9.2; 10.4; 12.3; 14.3; 14.4; 15.5; Anlage 6; Anlage 37; Anlage 69
Unterbringung	11.2
Unterkunftskosten	11.4
Unterrichtsmedien	13.4
Unterrichtungspflicht	15.2
Unterstützungspflicht	7.18; 13.7; Anlage 55; Anlage 58
Untersuchungsausschuss	2.2; 2.3; 7.9; Anlage 25
Untersuchungsausschussgesetz	7.9
Untreue	7.3; 7.4
US-amerikanischer Generalkonsul Powell, Mark J	2.2; Anlage 70
Vaterschaftsanerkennung	5.7
Verbundverfahren	15.4
Verfahrensverzeichnis	6.5; 13.2; 15.2
Verfassung des Freistaats Thüringen (ThürVerf)	7.2; 7.9; 7.13; 10.1; Anlage 30; Anlage 31
Verfassungskonforme Auslegung	7.9; 7.13; Anlage 24
Verfassungsschutz	A.1; 2.2; 2.9; 7.9; 7.14; 7.15; 7.19; 8; 8.1; 8.2; Anlage 11; Anlage 24; Anlage 48; Anlage 65
Verhaltens- und Leistungskontrolle	5.6; 6.2
Verhaltensprofile	2.2; 4.1; 7.23; 9.1; 12.3; 14.1; Anlage 2; Anlage 15; Anlage 39; Anlage 63; Anlage 66; Anlage 67
Verhältnismäßigkeit	2.6; 3.2; 7.4; 7.18; 10.1; 12.4; 13.6; Anlage 11; Anlage 23; Anlage 24; Anlage 30; Anlage 41; Anlage 53; Anlage 64; Anlage 70
Verkehrskontrolle	12.4
Vermieter	2.7; 11.4; 16.1; Anlage 1; Anlage 7; Anlage 30; Anlage 62

Vernehmung	7.12
Vernichtung	5.14; 7.7; 7.8; 7.9; 7.15; 8.1; 10.4; Anlage 25; Anlage 32; Anlage 33; Anlage 48
Veröffentlichung	2.1; 5.14; 5.22; 5.24; 5.27; 5.30; 6.1; 11.1; 12.6; 13.5; Anlage 26; Anlage 44;
Verschlüsseln	2.2; 2.4; 5.29; 9.2; 12.8; 13.4; 14.3; 14.4; 14.5; 14.6; 15.1; 15.5; Anlage 10; Anlage 20; Anlage 21; Anlage 23; Anlage 61; Anlage 62; Anlage 67; Anlage 74; Anlage 75; Anlage 76
Verschlüsselungsverfahren	2.4; 5.29; 14.4; 14.6; 15.5; Anlage 10; Anlage 21; Anlage 61
Verschollener	10.2
Verschollenheitsgesetz	10.2
Versicherungsschutz	12.11
Verstoß	A.1; 4.3; 5.5; 5.10; 5.24; 5.25; 5.27; 5.28; 5.29; 5.31; 6.6; 6.7; 7.1; 7.2; 7.3; 7.7; 7.14; 7.18; 7.20; 7.22; 8.1; 12.2; 13.7; Anlage 1; Anlage 4; Anlage 24; Anlage 25; Anlage 26; Anlage 31; Anlage 32; Anlage 43; Anlage 37; Anlage 48; Anlage 50; Anlage 53; Anlage 58; Anlage 61; Anlage 66; Anlage 71
Vertretungspläne	13.5
Verwaltungsvereinbarung	10.4
Verwaltungsgemeinschaft	5.1; 5.9; 5.12; 5.20; 5.24; 9.4; 12.7; Anlage 26
Verwaltungshelfer	9.5
Verwaltungsstruktur	5.31
Videoaufzeichnung	5.3; 5.18; 7.18; 7.22; Anlage 28
Videobeobachtung	5.3; 5.18; Anlage 28
Videomaterial	7.5; 7.18
Videoüberwachung	A.1; 2.1; 2.2; 5.3; 5.6; 5.18; 5.19; 5.27; 7.5; 7.6; 7.10; 7.18; 7.22; 10.1; 10.3; 12.4; 13.4; 13.6; 14.1;

	16.1; Anlage 4; Anlage 12; Anlage 26; Anlage 28; Anlage 37; Anlage 59; Anlage 63
VISkompakt	6.2
Voice over IP (VoIP)	15.1
Volkszählungsurteil	2.6; 9.1; 10.1
Vorabkontrolle	5.6; Anlage 2
Vorgärten	5.22
Vorläufiges Einfrieren	7.9
Waffenbehörden	2.9
Wahlberechtigter	5.33
Weiße Karteikarten	10.4
Weiterbildung	12.5
Werbezwecke	2.10; 5.11; Anlage 41
Wettbewerbsverzerrung	11.3
Widerruf der Bestellung des bDSB	7.1
Widerspruch	2.10; 4.1; 5.8; 5.14; 5.22; 5.27; 5.33; 6.3; 8.2; 9.3; 12.1; 12.9; 13.7; 15.3; 15.4; Anlage 6; Anlage 7; Anlage 11; Anlage 31; Anlage 32; Anlage 35; Anlage 40; Anlage 41; Anlage 42; Anlage 44
Wiedereinreisesperre	3.3
Wirksame Einwilligung	7.17; Anlage 16
Wirtschaftsförderung	5.30
Wohngebiet	5.19; 7.10
Zeiterfassung	6.6; 6.7; Anlage 64
Zeitkontingent	13.2
Zensus 2011	2.5; 5.4
Zensusgesetz 2011	5.4
Zentrales Testamentsregister	10.4
Zentralregister	7.8; 7.17; 9.3; Anlage 31
Zertifikat	2.2; 9.2
Zeuge	3.2; 5.26; 7.14; 7.20; 9.1
Zeugenschutz	9.1
Zeugnisse	13.7
Zeugnisverweigerungsrecht	7.20
Zugangskontrolle	6.6; 10.5
Zugriffsrechte	6.2; 7.1; 10.3
Zuhörer	5.27

Zwangsvollstreckung 2.7
Zweckänderung 5.30

1. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich

des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Berichtszeitraum: 5. Dezember 2011 bis 31. Dezember 2013
Zitiervorschlag: 1. TB LfDI Thüringen

Der 1. Tätigkeitsbericht steht im Internet unter der Adresse www.tlfdi.de zum Abruf bereit.

Erfurt, im Mai 2014

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

Inhaltsverzeichnis

B Nicht-öffentlicher Bereich

Vorwort 7

1 Schwerpunkte im Berichtszeitraum 10

2 Düsseldorfer Kreis 12

3 Wirtschaftsunternehmen in Thüringen 13
3.1 Gründung des Runden Tisches "Orientierungshilfe Aktenaufbewahrung (OHA)" 13
3.2 Dialog mit den Handwerkskammern (HWK) – Reanimation notwendig 14
3.3 Neue Besen …. 15
3.4 ERFA-Kreis 16
3.5 Der TLfDI rät: Widerspruch gegen Werbungsschreiben nach § 28 Abs. 4 BDSG nutzen – sonst ist Werbung einer Schuldnerberatung zulässig 17
3.6 Auch wenn Du nicht willst, …ich schreib´ Dir trotzdem – Wann ist die Nutzung personenbezogener Daten zu Werbezwecken unzulässig? 18
3.7 Akten außer Kontrolle 19
3.8 Wahrnehmung des Hausrechts darf nicht vorgeschoben werden: Videogaga 1 23
3.9 Ich weiß, was Du isst, also weiß ich, was Du bist: Videogaga 2 24
3.10 Busfahrer im Visier: Videogaga 3 25
3.11 Wertvoller Schrott im Blick: Videogaga 4 27
3.12 Schrott unter Beobachtung: Videogaga 5 29
3.13 Schrott-Video: Videogaga 6 31
3.14 Der nicht privilegierte Konzern 34
3.15 Teurer Schrott 36
3.16 Zwei Fliegen mit einer Klappe 38
3.17 Problemzonen im Autohaus: Videogaga 7 39
3.18 Die Pause ist für die Videoüberwachung tabu: Videogaga 8 41
3.19 Online-Präsenz? Datenschutz nicht vergessen! 41

3.20 Sagst Du es mir nicht, frag‘ ich jemand anderen.....43
3.21 Aus der Röhre geguckt: Videogaga 9 44
3.22 Videokameras fast im Wohnzimmer: Videogaga 10.....46
3.23 Der betriebliche Datenschutzbeauftragte – woher nehmen? 47
3.24 Der Anwalt, nicht immer Dein Freund und Helfer – von fragwürdigen Praktiken dubioser Verbraucherschützer und Rechtsanwaltskanzleien 49
3.25 Patientendaten – Ab in die blaue Tonne?.....51
3.26 Patientenarmbänder.....52
3.27 Dashcam – Trashcam: Videogaga 11.....53
3.28 Feuermelder mit Augen: Videogaga 12 55
3.29 Seniorenwohnheim – datenschutzrechtlich keine Idylle 57
3.30 Veröffentlichung personenbezogener Daten auf Gegnerliste durch Rechtsanwaltskanzlei.....57
3.31 Ein Autohaus in den Fängen des Autokonzerns: Videogaga 13.....59
3.32 Finger von der Wurst: Videogaga 14 60
3.33 … bis zur Bahre: Patientenakten am Ende.....61
3.34 Argusaugen wachen über Material…oder vielleicht doch über die Arbeitnehmer?: Videogaga 15.....62
3.35 Einkauf unter Beobachtung: Videogaga 16.....64
3.36 Weniger ist mehr: Reduzierung von Videokameras in einer Einkaufsgalerie: Videogaga 17 66
3.37 Hotel California: Videogaga 18 67
3.38 Video *vor* dem Kaufhaus – zulässig?: Videogaga 19.....69
3.39 Datenschutz gerade auch in Frauenschutzeinrichtungen 70
3.40 Vorsicht bei Gesundheitsdaten! 71
3.41 Datenverkauf im Apothekenrechenzentrum? 73
3.42 Taxi - alles im Blick: Videogaga 20.....75
3.43 Keine Beobachtung öffentlicher Straßen zur Zugangskontrolle: Videogaga 21 77
3.44 Das "elektronische Auge" des Nachbarn: Videogaga 22.....78
3.45 Prüfungspflicht der Banken nach dem Geldwäschegesetz.....79
3.46 Immer wieder der Geburtstag.....81
3.47 Meldepflicht nach Hackerangriff 82
3.48 Personalausweiskopie? Schrott!.....83
3.49 Video im Wind: Videogaga 23.....85

3.50 Pakete auf datenschutzrechtlichen Abwegen: Videogaga 24 86
3.51 „Livestream“ aus dem Friseursalon: Videogaga 25 88
3.52 Peepshow im Wald: Videogaga 26 90
3.53 Offene Tür 92

4 Ordnungswidrigkeitenverfahren 94

5 Veranstaltungen 100
5.1 TLfDI ist los! 100

Anlagen

Anlage 1 Fragenkatalog für Kontrollen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit 103

Beschluss der obersten Aufsichtsbehörde im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 17. Januar 2012)

Anlage 2 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft 110

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 18./19. September 2012)

Anlage 3 Near Field Communication (NFC) bei Geldkarten 127

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 26./27. Februar 2013)

Anlage 4 Videoüberwachung in und an Taxis 128

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 11./12. September 2013)

Anlage 5 Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen.....131

B Nichtöffentlicher Bereich

Vorwort

Dr. Lutz Hasse

Mit Inkrafttreten der Novellierung des Thüringer Datenschutzgesetzes, also seit dem 9. Dezember 2011, konnte der Thüringer Landesbeauftragte für den Datenschutz gemäß § 42 Abs. 1 Thüringer Datenschutzgesetz die Funktion der Aufsichtsbehörde nach § 38 Abs. 6 Bundesdatenschutzgesetz im nicht-öffentlichen Bereich wahrnehmen. Bereits am 9. März 2010 hatte der Europäische Gerichtshof (EuGH, Rechtssache C-518/07) Artikel 28 Abs. 1 der Europäischen Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. I. 281 S. 31 bis 50)) dahingehend ausgelegt, dass die Datenschutzaufsicht in völliger Unabhängigkeit wahrgenommen werden müsse. Eine solche Unabhängigkeit schließe jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, aus, durch die die Aufgabenerfüllung der Datenschutzaufsicht in Frage gestellt werden könnte. Der EuGH attestierte insoweit, dass die staatliche Aufsicht, der die für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Kontrollstellen in Deutschland unterworfen waren bzw. sind, *nicht* mit dem Unabhängigkeitserfordernis vereinbar sei. Damit gab der Europäische Gerichtshof vor, dass die datenschutzrechtliche Aufsicht vom Thüringer Landesverwaltungsamt auf den Thüringer Landesbeauftragten für den Datenschutz zu übertragen war. Der besondere Reiz dieser neuen Aufgabe liegt darin, „ein Feld zu beackern“, das in den zurückliegenden 20 Jahren vom Thüringer Landesverwaltungsamt nur mit 0,85 so

genannten Vollbeschäftigungseinheiten bestellt werden konnte. Um diese „Brache“ in eine „blühende Landschaft“ zu verwandeln, bedarf es besonderer Anstrengungen. Die Fallzahlen im nicht-öffentlichen Bereich haben sich von 2011 zu 2013 vervielfacht, insbesondere die Zahl der Ordnungswidrigkeitenverfahren ist derart stark angestiegen, dass trotz guten Arbeitsklimas und hoch motivierter Arbeitnehmer die Behörde des TLfDI deutlich an ihre Kapazitätsgrenzen stößt. Geplant ist daher die Einrichtung eines vierten Referates „Datenschutz im nicht-öffentlichen Bereich“. Denn gerade in diesem Bereich werden sowohl Verwaltungs- als auch Ordnungswidrigkeitenverfahren geführt, die rechtlich in aller Regel hohe Anforderungen stellen; bei ca. 80 % der Verfahren ist auf Seiten der datenschutzrechtlich verantwortlichen Stelle (Unternehmen) eine anwaltliche Beteiligung zu verzeichnen. Dies ist auch naheliegend, verfolgen doch die nicht-öffentlichen Stellen in der Regel wirtschaftliche Interessen und können bzw. wollen Bußgelder oder Zwangsgelder nicht widerstandslos hinnehmen. Verfahren im nicht-öffentlichen Bereich sind mithin sehr viel aufwendiger als Verfahren im öffentlichen Bereich. Der Prozentsatz der Bescheide des TLfDI, die mit einem Rechtsbehelf angegriffen werden, ist hoch. Gleichwohl wurden sämtliche Verfahren bisher erfolgreich geführt. Hinzu kommt, dass parallel zum vermehrten Arbeitsanfall in den Rechtsreferaten auch das Technik-Referat in verstärktem Maße gefordert ist – etwa bei Kontrollen oder Stellungnahmen gerade auch im nicht-öffentlichen Bereich. Waren beim Datenschutzbeauftragten im Jahr 2012 noch 449 Vorgänge zu bearbeiten, waren es im Jahr 2013 bereits 810. In den nächsten Jahren wird diese Zahl weiterhin ansteigen. Der TLfDI hofft mit Blick auf die Gewährung neuer Personalstellen auf die weitere konstruktive Unterstützung durch die Landtagsfraktionen, die Landtagspräsidentin und den Personalrat der Thüringer Landtagsverwaltung.

Auf der Grundlage des 2012 gefassten Beschlusses des Beirates beim TLfDI erfasst der Tätigkeitsbericht zum nicht-öffentlichen Bereich zusätzlich den Monat Dezember des Jahres 2011.

Der TLfDI hat in seiner Funktion als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich die Befugnis, verantwortliche Stellen in seinem Zuständigkeitsbereich anlasslos zu kontrollieren, § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG). Um diese Kontrolle wirksam durchführen zu können, hat der Gesetzgeber dem TLfDI und seinen Mitarbeitern eine Reihe an Werkzeugen an die

Hand gegeben. So darf der TLfDI von Unternehmen umfassende Auskunft verlangen und die einzelnen Betriebe vor Ort kontrollieren. Dabei hat er Zutritt zu allen Geschäftsräumen und das Recht, in alle Unterlagen Einsicht zu nehmen, § 38 Abs. 4 Satz 1 BDSG. Während den meisten vom TLfDI durchgeführten Kontrollen ein bestimmter Anlass, meist ein Hinweis durch einen Bürger, zu Grunde liegt, hat der TLfDI einige anlasslose Kontrollen in Wirtschaftsunternehmen durchgeführt. Dabei wurde sowohl auf die regionale Verteilung als auch darauf geachtet, dass sowohl große als auch kleine Unternehmen kontrolliert wurden. Ein Schwerpunkt wurde hierbei auf Unternehmen aus der Recycling-Branche gelegt. Alle Unternehmen wurden dabei nach dem im Anhang unter Anlage 1 beigefügten Fragenkatalog geprüft. Der Fragenkatalog wird fortlaufend durch den TLfDI unter Berücksichtigung der bei den Kontrollen gewonnenen praktischen Erfahrungen überarbeitet. In den folgenden Beiträgen werden die Ergebnisse der Kontrollen dargelegt. Auf der Internetseite des TLfDI werden fortlaufend weitere Hinweise eingestellt werden.

Als unabhängige Behörde darf der TLfDI die Funktion der Aufsichtsbehörde im nicht-öffentlichen Bereich wahrnehmen. Trotz bester Motivationslage der Arbeitnehmerinnen und Arbeitnehmer des TLfDI sollte die personelle Ausstattung dem Aufgabenzuwachs entsprechen (§ 36 Abs. 5 ThürDSG).
Der TLfDI hat in seiner Funktion als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich die Befugnis, verantwortliche Stellen in seinem Zuständigkeitsbereich aufgrund eines besonderen Anlasses oder auch anlasslos zu kontrollieren. Hierzu hat er Zutritt zu allen Geschäftsräumen und das Recht in alle Unterlagen Einsicht zu nehmen.

1 Schwerpunkte im Berichtszeitraum

Datenschutz
© Coloures Pic – Fotolia.com

Die aufsichtsbehördliche Tätigkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im nicht-öffentlichen Bereich war im Wesentlichen durch drei Schwerpunkte beansprucht:
Den größten Einschnitt stellte die Übernahme der aufsichtsbehördlichen Tätigkeit im nicht-öffentlichen Bereich mit dem Inkrafttreten des Gesetzes zur Änderungen des Thüringer Datenschutzgesetzes (ThürDSG) Ende des Jahres 2011 dar. Bis zu diesem Zeitpunkt war diese Tätigkeit dem Thüringer Landesverwaltungsamt zugeteilt, welches für die datenschutzrechtliche Aufsicht aller Unternehmen in Thüringen 0,8 Vollzeitstellen eingeplant hatte. Die sich aus dieser Unterbesetzung ergebende Vakanz in Sachen datenschutzrechtlicher Aufsichtstätigkeit und den sich daraus entwickelnden Folgen war eine der Herausforderungen, mit denen der TLfDI zu kämpfen hatte und hat. So war „der Datenschutz“ in vielen Thüringer Unternehmen, die der TLfDI seit seiner Aufgabenübernahme kontrollierte, ein unbekanntes Feld, von dem man bestenfalls ungenaue Vorstellungen hatte. Dass das Bundesdatenschutzgesetz für diese Unternehmen seit der Wende Anwendung fand, diese Tatsache aber unbekannt ist, war und ist leider sehr häufig festzustellen.
Aus diesem Grund hat sich der TLfDI nach seiner Amtsübernahme um einen steten und intensiven Austausch zu den in Thüringen vertretenen Industrie- und Handelskammern bemüht. Er legte großen Wert darauf, die Unternehmen in Thüringen in datenschutzrechtlicher Hinsicht auf den richtigen Weg zu bringen. Es wurden unter anderem Informationsveranstaltungen durch den TLfDI initiiert.
Einen weiteren Eckpunkt des Berichtszeitraumes stellt der Aufbau des Ordnungswidrigkeitenverfahrens dar. Auch hier lag bislang die Zuständigkeit beim Thüringer Landesverwaltungsamt. Das Ordnungswidrigkeitenverfahren als besonderes Verwaltungsverfahren

stellte den TLfDI und seine Behörde vor besondere Herausforderungen. Es sind wenige Parallelen zu den bisherigen Verfahrensweisen vorhanden. Vielmehr handelt es sich um ein streng formalisiertes Verfahren mit festem Aufbau. Um auch diese Verfahren von Anfang an erfolgreich zu betreuen, hat der TLfDI einen Juristen angestellt, der primär mit dem Aufbau und der Durchführung dieses Verfahrens betraut ist. Der Aufbau des Verfahrens konnte zwischenzeitlich hinsichtlich der gängigsten Verfahrensformen abgeschlossen werden; die bisherigen Ordnungswidrigkeitenverfahren verliefen erfolgreich.
Schließlich stellt die Videoüberwachung in all ihrer Vielfalt einen weiteren Schwerpunkt aus dem Berichtszeitraum dar. Ständig in Quantität steigend, ständig in technischer Sicht besser und damit auch in der Qualität zunehmend, stellt diese Art der Datenerhebung und in meisten Fällen auch -speicherung eines der größten datenschutzrechtlichen Probleme und damit eine Herausforderung für den TLfDI auch in Zukunft dar. Ein Großteil der Fälle im nicht-öffentlichen Bereich, der zu einer aufsichtsbehördlichen Reaktion führt, steht im Zusammenhang mit Videoüberwachung. In den seltensten Fällen ist die Überwachung zulässig. Ebenso selten ist die Einsicht der Unternehmen, die die Überwachung durchführen.

Die Schwerpunkte im Berichtszeitraum waren der erfolgreiche Start der aufsichtsbehördlichen Kontrolltätigkeit des TLfDI, die Durchführung des oftmals daraus resultierenden Ordnungswidrigkeitenverfahrens in neuer eigener Zuständigkeit sowie die immer stärker zunehmende Videoüberwachung in allen nicht-öffentlichen Bereichen.

2 Düsseldorfer Kreis

Runder Tisch Business
© fotomek – Fotolia.com

Ursprünglich war der Düsseldorfer Kreis das Gremium der obersten Datenschutzaufsichtsbehörden in Deutschland. Nachdem die Datenschutzaufsicht bis auf den Ausnahmefall des Bayrischen Landesamtes für Datenschutzaufsicht auf die Landesdatenschutzbeauftragten übergegangen ist, ist der Düsseldorfer Kreis nunmehr ein Arbeitskreis der Datenschutzkonferenz. Im Düsseldorfer Kreis treffen sich die Datenschutzaufsichtsbehörden, um ihre Aufsichtstätigkeit im nicht-öffentlichen Bereich zu koordinieren. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen hat den Vorsitz. Jede Datenschutzaufsichtsbehörde kann Themen in den Düsseldorfer Kreis einbringen, die nach ihrer Auffassung ein bundeseinheitliches Vorgehen erfordern. Sofern eine Einigkeit erzielt werden kann, fasst der Düsseldorfer Kreis einstimmige Beschlüsse, die veröffentlicht werden. Gegenstand der Beschlüsse ist eine datenschutzrechtliche Bewertung eines bestimmten Sachverhalts aus dem nicht-öffentlichen Bereich, die der Wirtschaft Rechtssicherheit geben sollen. Unternehmen können davon ausgehen, dass die angesprochenen Themen von den Datenschutzaufsichtsbehörden in Deutschland einheitlich behandelt werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) veröffentlicht die Beschlüsse des Düsseldorfer Kreises auf seiner Homepage unter http://www.tlfdi.de/tlfdi/berichte/duesseldorf/. Die im Berichtszeitraum gefassten Beschlüsse des Düsseldorfer Kreises sind im Anhang veröffentlicht.

Der Düsseldorfer Kreis fasst Beschlüsse, in denen eine einheitliche datenschutzrechtliche Bewertung eines bestimmten Sachverhalts aus dem nicht-öffentlichen Bereich bundeseinheitlich festgeschrieben wird.

3 Wirtschaftsunternehmen in Thüringen

Warnschild Videoüberwachung
© bilderzwerg – Fotolia.com

3.1 Gründung des Runden Tisches "Orientierungshilfe Aktenaufbewahrung (OHA)"

Nachdem sich der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Anschluss an das Immelborn-Aktenlagerungs-Desaster an einem Runden Tisch mit thüringischen Archivierungsdienstleistern einen Überblick über die branchenspezifischen Probleme verschafft hatte, gelang es ihm, „big player“ aus der Branche der Archivierungsdienstleister und von Seiten der betrieblichen Datenschutzbeauftragten an einen Runden Tisch zu bitten, um zu erörtern, wie konzeptionell ein zweiter Fall Immelborn verhindert werden kann. Als Ziel kristallisierte sich zügig heraus, dass es zur Konkretisierung unpräziser gesetzlicher Vorgaben dringend einer „Orientierungshilfe Aktenaufbewahrung (OHA)“ bedarf. Sie soll einerseits Archivierungsdienstleistern, andererseits aber auch Unternehmen, die diese Dienstleister beauftragen wollen, eine Richtschnur an die Hand geben, auf welche Weise die rechtlichen Vorgaben einzuhalten sind und wie sich Auftraggeber (vorab) von der Einhaltung dieser Vorgaben unterrichten können. Die gemeinsam erarbeitete Orientierungshilfe soll sodann mit dem zuständigen Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgestimmt werden, um so die bundesweite Anwendung der Orientierungshilfe zu gewährleisten.
Die Arbeiten an der Orientierungshilfe gestalten sich aufwendig, sodass bis zur „Marktreife“ der Orientierungshilfe noch einige Zeit vergehen wird.
Allen Beteiligten ist jedoch daran gelegen, ein weiteres Datenschutz-Desaster wie in Immelborn (siehe hierzu Punkt 3.7) zu verhindern – das ist aller Mühen wert!

Der Runde Tisch „Orientierungshilfe Aktenaufbewahrung (OHA)“ wird eine Orientierungshilfe entwickeln, die zum einen Archivierungsdienstleister in die Lage versetzen soll, datenschutzrechtlich korrekt zu arbeiten, und zum anderen Unternehmen, die diese Dienstleister beauftragen wollen, dazu befähigen soll, etwa anhand von Checklisten die Archivierungsdienstleister einer qualifizierten Bewertung unterziehen zu können.

3.2 Dialog mit den Handwerkskammern (HWK) – Reanimation notwendig

Während die Kooperation mit den Industrie- und Handelskammern (IHK) etwas an Fahrt aufnimmt, gestaltet sich der Dialog mit den Handwerkskammern (HWK) zäh, bzw. ein Desinteresse der HWKs an einem datenschutzrechtlichen Dialog mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wird deutlich signalisiert. Das ist bedauerlich, da die HWKs auf diese Weise ihren Mitgliedern die Chance nehmen, mit dem TLfDI z. B. an Runden Tischen über Datenschutzthemen aus Sicht der Handwerksbetriebe sowie aus Sicht des Datenschutzbeauftragten zu diskutieren. Es fand unter anderem ein Gesprächstermin in der Handwerkskammer Erfurt statt, bei dem der TLfDI sich vorstellte und anbot, einen Datenschutz-Flyer zu gestalten, der speziell für Handwerksbetriebe datenschutzrechtliche Fragen und Probleme aufgreift. Zur Vorbereitung sollten fünf repräsentative Handwerksbetriebe besucht werden, um sich einen Überblick über die datenschutzrechtliche Situation und die datenschutzrechtlichen Anforderungen in Handwerksbetrieben zu verschaffen. In der Folge wurden ein Autohaus und ein Café besucht. Trotz mehrmaliger Nachfrage des TLfDI fanden sich keine weiteren Handwerksbetriebe, bei denen eine repräsentative Kontrolle durchgeführt werden konnte.
Aufgrund der bisher gemachten Erfahrungen im Bereich der Handwerksbetriebe ist die Erstellung von Informationen für diese Zielgruppe noch nicht möglich gewesen. Gleichwohl wird der TLfDI weiterhin versuchen, die „leblose“ Kommunikation „zu reanimieren“, um datenschutzrechtliche Informationen an die Handwerksbetriebe heranzutragen. Dessen ungeachtet werden die Handwerksbetriebe künftig verstärkten Kontrollen ausgesetzt sein, um auch auf diese Weise den ausgeprägten Datenschutzdefiziten entgegen wirken zu können.

Im Gegensatz zur Kommunikation mit den IHKs gestaltet sich der Dialog zwischen den HWKs und dem TLfDI als noch verbesserungswürdig. Eine Ausblendung des Datenschutzes gehört jedoch der Vergangenheit an. Der TLfDI wird daher weiterhin den Dialog suchen, daneben aber auch andere Wege finden, den Datenschutzgedanken in die Handwerksbetriebe zu tragen.

3.3 Neue Besen ….

Dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) war nach der Amtsübernahme klar, dass bei den Unternehmen in Thüringen in Sachen Datenschutz einiges im Argen liegt, stand doch für diese Aufgabe im Thüringer Landesverwaltungsamt nicht einmal eine Person mit ihrer gesamten Arbeitskraft zur Verfügung (siehe Vorwort). In dem Bewusstsein, dass diese Situation nicht durch die Unternehmen verursacht worden ist, wollte der TLfDI nicht mit „harter Hand“ vorgehen, sondern suchte zunächst Kontakt zu den Wirtschaftsverbänden (siehe hierzu auch Punkt 3.2). Er nahm zu allen drei Industrie- und Handelskammern (IHK) in Thüringen Kontakt auf, und führte mit den Geschäftsführern ein persönliches Gespräch. Hierbei legte er dar, dass er großen Wert darauf legt, die Unternehmen in Thüringen datenschutzrechtlich auf den richtigen Weg zu bringen. Er bot an, über seine Behörde und sein Anliegen z. B. im Rahmen einer Mitgliederversammlung der IHK zu berichten. Zunächst wurde vereinbart, dass der TLfDI in der Mitgliederzeitung der IHK über den Datenschutz im Unternehmen berichtet. Dann war die Teilnahme an einigen Veranstaltungen der IHK zu Informationszwecken vorgesehen. Die Verwirklichung gestaltete sich jedoch sehr unterschiedlich. So war der TLfDI in beiden Berichtsjahren auf dem Ostthüringer Unternehmer- und Gründertag vertreten. Er hielt einen Vortrag zu Chancen und Risiken des Datenschutzes für Unternehmen auf dem Seminar der IHK Ostthüringen zum Thema „Sind Ihre Unternehmensdaten sicher?“ Ebenfalls besuchte der TLfDI eine Veranstaltung der IHK Südthüringen, in der er Unternehmern zunächst in einem Vortrag, dann in einer Gesprächs- und Fragerunde das Thema Datenschutz näherbrachte. Ansonsten erfolgten jedoch keine Einladungen an den TLfDI zu Informationsveranstaltungen. Dies ist etwas bedauerlich, da den Arbeitnehmern des TLfDI bei Vor-Ort-Kontrollen in Unter-

nehmen des Öfteren mitgeteilt wurde, dass es hilfreich gewesen wäre, wenn diese über datenschutzrechtliche Anforderungen vorab informiert gewesen wären.
Mit der IHK Erfurt erarbeitete der TLfDI einen Flyer zum „Datenschutz im Unternehmen“ der unter dem Link:
http://www.tlfdi.de/tlfdi/wir/info/datenschutz_im_unternehmen/
eingesehen werden kann. Ein aufwendiges Unterfangen stellte die Erarbeitung einer Broschüre zu § 28 Bundesdatenschutzgesetz (BDSG) dar. Diese wurde vom TLfDI erstellt, während die IHK Erfurt das Layout und den Druck übernahm. Diese Broschüre ist unter
http://www.tlfdi.de/imperia/md/content/datenschutz/themen/unternehmen/datenschutz_f__r_unternehmen_pdf_19.03.2014.pdf auf der Homepage des TLfDI veröffentlicht. Sie richtet sich an Unternehmerinnen und Unternehmer, um diesen einen verhältnismäßig schnellen Einblick in das Datenschutzrecht zu ermöglichen. Die für Unternehmen wichtige, aber sehr komplizierte Vorschrift des § 28 BDSG wird darin in einzelnen Fallbeispielen aus dem Unternehmeralltag hoffentlich verständlich dargestellt; Rückmeldungen dazu aus der Unternehmerschaft werden fortlaufend eingearbeitet.
Nach diesem ersten Aufschlag hat der TLfDI dann im zweiten Berichtsjahr damit begonnen, Unternehmen in Thüringen auch anlassunabhängig zu kontrollieren. Hierzu wurde die im Anhang unter Anlage 1 beigefügte Frageliste verwendet, mit der alle datenschutzrechtlich relevanten Bereiche im Unternehmen abgefragt werden sollten. Die Ergebnisse dieser Kontrollen sind in den nachfolgenden Tätigkeitsberichtsbeiträgen nachzulesen.

Nach seiner Amtsübernahme nahm der TLfDI zunächst Kontakt mit den IHKs auf, um sein Anliegen zum Datenschutz im Unternehmen bekannt zu machen. Er bot den IHKs Unterstützung in Form von Informationsveranstaltungen und der Veröffentlichung von Beiträgen an; ein wichtiger Schritt ist die Erstellung der Broschüre zu § 28 BDSG.

3.4 ERFA-Kreis

Im Berichtszeitraum nahm der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an vier Sitzungen des Erfahrungsaustausch-Kreises (ERFA-Kreises) teil. Dabei handelt

es sich um eine Zusammenkunft von vornehmlich betrieblichen Datenschutzbeauftragten, mit dem Zweck des gegenseitigen Austausches. Gebildet wurden diese regionalen Kreise durch die Gesellschaft für Datenschutz und Datensicherheit e. V.
Die ERFA-Kreise stehen grundsätzlich allen Interessierten offen, bedürfen jedoch der vorherigen Anmeldung. Eingeladen sind in erster Linie Datenschutzbeauftragte.
Der TLfDI hat bei seinen Besuchen dieser Tagungskreise jeweils unterschiedliche Schwerpunkte seiner Tätigkeit vorgestellt und aktuelle Fragen und Problemstellungen der Teilnehmer geklärt.

Der ERFA-Kreis ist ein gutes Instrument zur Klärung datenschutzrechtlicher Fragen aus dem nicht-öffentlichen Bereich.

3.5 Der TLfDI rät: Widerspruch gegen Werbungsschreiben nach § 28 Abs. 4 BDSG nutzen – sonst ist Werbung einer Schuldnerberatung zulässig

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit wurde darüber informiert, dass eine in Thüringen ansässige Schuldnerberatung Anschreiben versandt hatte, mit denen über das Privatinsolvenzverfahren informiert wurde. Im Raum stand die damit verbundene Frage, wie solche Schreiben datenschutzrechtlich zu bewerten sind und ob die Nutzung personenbezogener Daten für solche Schreiben zulässig ist.
Das von der Schuldnerberatung versandte Anschreiben diente dazu, über die Möglichkeit zu informieren, sich durch ein Privatinsolvenzverfahren zu entschulden. Insofern war das Anschreiben als Werbungsschreiben für die Schuldnerberatung anzusehen.
Die Nutzung personenbezogener Daten für Werbungszwecke ohne schriftliche Einwilligung richtet sich nach § 28 Abs. 3 Bundesdatenschutzgesetz (BDSG). Da sich die Nutzung der personenbezogenen Daten auf den Namen sowie die Anschrift beschränkte, bewegte sich auch das Werbungsschreiben der Schuldnerberatung innerhalb des rechtlich zulässigen Rahmens. Darüber hinaus konnte der betroffenen Person mitgeteilt werden, dass die Schuldnerberatung die für das Werbungsschreiben benötigten personenbezogenen Daten nicht gespeichert hatte.

Möchten Sie Ihren Briefkasten entlasten? Dann machen Sie von Ihrem Widerspruchsrecht Gebrauch:
Zur Abwehr unerwünschter Werbung räumt § 28 Abs. 4 BDSG dem Betroffenen ein uneingeschränktes Widerspruchsrecht gegenüber der verantwortlichen Stelle bezüglich der Verarbeitung und Nutzung seiner Daten zu Zwecken der Werbung oder Markt- und Meinungsforschung ein. Das Widerspruchsrecht besteht unabhängig davon, ob die Werbung ohne oder mit Einwilligung des Betroffenen erfolgt. Ein solcher Widerspruch ist an keine Form gebunden, wonach er telefonisch, konkludent oder auch durch einen Vermerk auf dem Werbungsschreiben „Annahme verweigert“ gegenüber der verantwortlichen Stelle geäußert werden kann.
Für weitere Informationen zum Widerspruch siehe: http://www.bfdi.bund.de/DE/Themen/GrundsaetzlichesZumDatenschutz/BDSGAuslegung/Artikel/Widerspruchsrecht.html?nn=409922.

3.6 Auch wenn Du nicht willst, …ich schreib´ Dir trotzdem – Wann ist die Nutzung personenbezogener Daten zu Werbezwecken unzulässig?

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) eine Beschwerde eines promovierten Universitätsmitarbeiters. Nach seinen Angaben erhielt er von einem Verein in Thüringen unaufgefordert Werbe-Mails, in denen ihm die Möglichkeit der Teilnahme an Veranstaltungen angeboten wurde. Trotz mehrfacher Aufforderung des Beschwerdeführers, dies zu unterlassen, erhielt er weiterhin unerwünschte Nachrichten per E-Mail an seine dienstliche E-Mail-Adresse.
Der TLfDI hat sich daraufhin an den Verein gewandt und um Auskunft zu den zum Beschwerdeführer gespeicherten Daten sowie zu der Herkunft dieser Daten gebeten. Ferner interessierten den TLfDI die Empfänger oder Kategorien von Empfängern, an die diese Daten weitergegeben werden bzw. worden sind, sowie der Zweck der Speicherung dieser Daten (§ 6 Abs. 1 i. v. m. § 34 Abs. 1 BDSG). Da eine Verarbeitung und Nutzung personenbezogener Daten des Betroffenen für Zwecke der Werbung bei Widerspruch des Betroffenen unzulässig ist (§ 28 Abs. 4 BDSG), forderte der TLfDI den Verein auf, mitzuteilen, warum der Löschaufforderung des Betroffenen bislang nicht nachgekommen wurde.

Zwar zeigte sich der Verein reumütig und sagte zu, die Beschwerde zum Anlass zu nehmen, die Daten des Betroffenen unverzüglich zu löschen und keine weiteren E- Mails an den Beschwerdeführer zu versenden, ging aber davon aus, dass das Bundesdatenschutzgesetz (BDSG) im vorliegenden Fall keine Anwendung finde. Weder die Datenerhebung noch die Datenverarbeitung erfolge beim Verein mittels automatisierter Datenverarbeitung, sondern durch manuelle Eingabe der selbständig gesammelten Daten. Zudem handele es sich bei den vom Betroffenen gespeicherten Daten allein um allgemein zugängliche Daten nach § 28 Abs. 1 Nr. 3 BDSG (die E-Mail-Adresse sei z. B. auch auf der Internetseite einer Universität zu finden). Weitere Daten seien nicht erhoben oder gespeichert worden.
Der TLfDI hat die Anwendbarkeit des BDSG als gegeben angesehen und ist davon ausgegangen, dass zumindest die Datenverarbeitung automatisiert erfolgte, sodass eine weitere Verarbeitung und Nutzung der personenbezogenen Daten des Beschwerdeführers für Zwecke der Werbung (für Veranstaltungen und ähnliches), bedingt durch das Vorliegen seines Widerspruchs, unzulässig war (§ 28 Abs. 4 BDSG). Auch eine Zulässigkeit der Datenspeicherung nach § 28 Abs. 1 Nr. 3 BDSG wurde seitens des TLfDI verneint, da das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse des Vereins überwiege.
In Anbetracht dessen, dass die personenbezogenen Daten des Betroffenen umgehend gelöscht wurden, hat der TLfDI die Angelegenheit als erledigt betrachtet und den Beschwerdeführer entsprechend informiert. Der Verein wurde aufgefordert, zukünftig bei Widersprüchen von Betroffenen die weitere Verarbeitung oder Nutzung dieser Daten gemäß § 28 Abs. 4 BDSG zu unterlassen.

Auch bei Einladungen zu einer – wenn auch kostenlosen – Veranstaltung müssen der Datenschutz und das Interesse des Betroffenen berücksichtigt werden.

3.7 Akten außer Kontrolle

Auf den Hinweis eines Arztes hin, dass er an seine Patientenakten nicht mehr heran käme, kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Sommer 2013 die Geschäftsräume des betreffenden Aktenarchivie-

rungsunternehmens in Immelborn und stellte dabei desaströse Zustände fest. Problematisch war hierbei, dass sich das Unternehmen seit einigen Jahren in Insolvenz befand und sich der ehemalige Geschäftsführer und jetzige Liquidator ins Ausland abgesetzt hat. Auf drei Etagen und insgesamt ca. 3000 qm Nutzfläche stehen hunderttausende Akten in Regalen und in Kartons verpackt. Teilweise sind die Aufbewahrungsfristen für die Akten (vermutlich) bereits abgelaufen, teilweise aber auch nicht. Das größte Problem ergibt sich jedoch aus der Tatsache, dass das Unternehmen nach dem sogenannten „chaotischen System“ eingelagert hat. Dies ist in dieser Branche durchaus üblich und aus deren Sicht vermutlich sinnvoll, da so der vorhandene Lagerplatz effektiver genutzt werden kann. Dabei werden Akten nicht nach einlagerndem Unternehmen geordnet, sondern kommen dorthin, wo grade Platz ist. Wo einzelne Akten stehen, ist im Computer abgelegt. Leider wurde jedoch, soweit der TLfDI durch Dritte informiert worden ist, durch den vom Gericht bestellten Insolvenzverwalter zunächst die EDV verwertet, möglicherweise aber auch von Dritten gestohlen. Jedenfalls ist die Computertechnik nicht mehr vorhanden. Damit ist aus dem chaotischen System das „System“ verschwunden und das „Chaos“ geblieben. Die Folge ist, dass die Aktenbestände mühsam von Hand gesichtet und registriert werden müssen, bevor sie – wie datenschutzrechtlich vorgesehen – an die Personen und Firmen, die die Akten dort eingelagert haben, zurückgeführt werden können. Hierfür muss jeder Aktenordner in die Hand genommen werden. Für einen kleineren Teil der Akten ist dies im Berichtszeitraum bereits erfolgt. Hintergrund ist, dass das rechtliche Konstrukt hinter einer solchen Aktenverwahrung ein Vertrag über die Auftragsdatenverarbeitung ist. Richtig angewendet erlaubt ein derartiger Vertrag es dem Auftraggeber (z. B. Arzt oder sonstiger Unternehmer), personenbezogene Daten an den Auftragnehmer (Archivierungsunternehmen) weiterzugeben, ohne dass die besonderen Voraussetzungen für eine Übermittlung im Sinne des Bundesdatenschutzgesetzes gegeben sein müssen. Allerdings bleibt der Auftraggeber weiterhin für die ordnungsgemäße Verarbeitung der personenbezogenen Daten verantwortlich, was weitestgehend unbekannt ist. So auch in diesem Fall. Ansprechpartner sind für den TLfDI daher die einlagernden Stellen oder Personen.

Doch bevor mit der eigentlichen Aufgabe, der Rückführung der Akten begonnen werden kann, musste sich der TLfDI nach dem Hinweis einen Überblick über die dort herrschenden Zustände ma-

chen. Da staatliches Handeln in einem Rechtsstaat wie Thüringen nur mit einer Rechtsgrundlage möglich ist, konnte der TLfDI nicht einfach „mit der Tür ins Haus fallen“. Da in diesem Fall davon auszugehen war, dass der Eigentümer der Immobilie und Geschäftsführer des insolventen Unternehmens nicht zur Kontrolle anwesend sein wird, musste zunächst das rechtskonforme Öffnen der Türen vorbereitet werden. Dies konnte mit einem öffentlich zugestellten Bescheid – eine Meldeadresse des Unternehmers war nicht ermittelbar – erreicht werden, indem das Unternehmen über die bevorstehende Kontrolle in Kenntnis gesetzt und verpflichtet wurde, den TLfDI das Gelände und die Geschäftsräume betreten zu lassen. Für den Fall der Nichtbefolgung wurde das Zwangsmittel der Ersatzvornahme, konkret das Öffnen der Türen, angedroht.

Auf den oben bereits erwähnten drei Etagen und 3000 qm Nutzfläche bot sich dem TLfDI und seinen Mitarbeitern dann ein unerwartetes Ausmaß an Chaos. Akten waren aus Regalen gestoßen und lagen auf dem feuchten Boden, teilweise waren Regale im Einsturz begriffen. Auf der obersten Etage erwartete den TLfDI dann noch eine Steigerung: Stellen Sie sich vor, Sie nehmen einen großen Raum (ca. 1000 qm), stellen diesen bis unter die Decke voll mit auf Palletten gestapelten und mit Akten gefüllten Kartons und schütteln diesen solange, bis kaum noch ein Karton auf dem anderen steht. Ein professioneller Aktenverwahrer, der im Auftrag einer vom TLfDI angeschriebenen verantwortlichen Stelle das Objekt besichtigt hat, um die Abholung bestimmter Akten vorzubereiten, teilte mit, dass er so etwas, trotz langjähriger Arbeit in diesem Metier, noch nicht erlebt hätte.

Selbstverständlich können die Akten nicht einfach vernichtet werden, schon gar nicht auf Kosten des Steuerzahlers. Vielmehr sind die einzelnen Akten der jeweils verantwortlichen Stelle, also der Person oder dem Unternehmen, welches die Einlagerung vorgenommen hat, zuzuordnen. Dazu hat der TLfDI zwei Herkulesaufgaben zu bewältigen: Er muss feststellen, wer Akten eingelagert hat und dokumentieren, wo diese im Gebäude liegen.

Um diese Aufgabe, der die immer noch viel zu kleine Behörde des TLfDI in personeller Hinsicht nicht gewachsen ist, bewältigen zu können, hat der TLfDI sich über das Thüringer Innenministerium an die Polizei gewandt, mit der Bitte Amtshilfe zu leisten. Vorgesehen war, dass einige Bereitschaftspolizisten für das Herstellen arbeitsfähiger Zustände und das Sichten bereitgestellt werden. Dieses Ersu-

chen wurde abgelehnt, denn leider sei die Polizei nicht in der Lage, auf ihre Beamten zu verzichten. Sie könne ihre sonstigen Aufgaben ansonsten nicht mehr wahrnehmen. Nur am Rande sei bemerkt, welch trauriges Bild das Innenministerium hier über den Zustand der Thüringer Polizei zeichnet, dem Exekutivorgan, das eigentlich die Aufgabe hat, die öffentliche Sicherheit und Ordnung zu gewährleisten und nötigenfalls bei Rechtsverstößen gegen das Datenschutzrecht, wie zum Beispiel im Immelborner Aktenlager, die Rechtsordnung wiederherzustellen.

Bisher versucht der TLfDI, so gut es geht, mit seiner kleinen Behörde auf eigene Faust in Immelborn wieder ordnungs- und datenschutzrechtlich ordnungsgemäße Zustände herbeizuführen. Bei einem geschätzten Aktenbestand von ca. 250.000 Akten ist dies jedoch eine langwierige Aufgabe. Für etwa 80.000 Akten ist diese Arbeit erledigt. Jedoch wartet auch das sonstige beträchtliche Tagesgeschäft des TLfDI nicht solange, bis die Akten in Immelborn aufbereitet sind.

Sobald alle Akten registriert sind, können die verantwortlichen Stellen bzw. Personen vom TLfDI aufgefordert werden, die jeweiligen Akten abzuholen. Es kann dann geplant werden, in welcher Reihenfolge und auf welche Art und Weise dies sinnvoll ist.

Auch hier drohen Verzögerungen. Nicht jede Stelle wird akzeptieren, dass sie für die teilweise vor langer Zeit eingelagerten Akten verantwortlich ist. Die Einlagerungsgebühren wurden in der Regel im Voraus für teilweise zehn Jahre gezahlt. Eine erneute Einlagerung oder Vernichtung ist mit erneuten Kosten verbunden, die von der verantwortlichen Stelle getragen werden müssen.

Zwar kann und wird der TLfDI die Verantwortlichen mittels Anordnung zum Handeln zwingen, jedoch steht den verantwortlichen Stellen selbstverständlich gegen solche Verwaltungsakte der Rechtsweg offen. Streitigkeiten vor dem Verwaltungsgericht binden wiederum Personal und sind vor allem eines: langwierig.

Wann „die Akte Immelborn“ geschlossen werden kann, steht derzeit noch in den Sternen. Ohne die Unterstützung anderer Behörden bleibt dem TLfDI nichts anderes übrig, als sich Hilfe im privaten Bereich zu holen. Dies wird den Steuerzahler aber einiges kosten. Vernünftiger wäre es daher, wenn sich das Thüringer Innenministerium (TIM) doch zum Helfen durchringen und Personal, Generatoren für Licht, große Leuchter, Hubwagen etc. zur Verfügung stellen könnte. So könnte wenigstens der erste Schritt, die eigentliche Sich-

tung des Aktenbestands, zügig und erfolgreich erledigt werden. Bei weiterer Verweigerung der Amtshilfe seitens des TIM wird der TLfDI diese Unterstützung gerichtlich einklagen.

Wenn Akten ausgelagert werden müssen, sollte der Preis nicht das einzige Kriterium für die Auswahl des zu beauftragenden Unternehmens sein. Auch wenn die Akten nicht mehr im Schrank des einlagernden Unternehmens stehen, bleibt dieses verantwortliche Stelle. Deswegen ist es notwendig und gesetzlich vorgeschrieben, sich vor und auch nach dem Auslagern darüber zu versichern, dass die Akten in einer Art und Weise gelagert werden, die auch dem Datenschutz genügt.
Auch muss ein Vertrag über eine Auftragsdatenverarbeitung (vgl. 5. TB Anlage 23 - Mustervertrag) geschlossen werden, der den gesetzlichen Anforderungen genügt. Ansonsten ist mit einem Ordnungswidrigkeitenverfahren wegen unerlaubter Verarbeitung von personenbezogenen Daten zu rechnen.

3.8 Wahrnehmung des Hausrechts darf nicht vorgeschoben werden: Videogaga 1

Ein anonymer Hinweis brachte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf die Spur eines Cafés, das seinen Gastraum durch Videokameras überwacht. In der daraufhin durchgeführten Vorortkontrolle bestätigte sich die vermutete unzulässige Videoüberwachung. Auch bei einem Café handelt es sich um einen öffentlich zugänglichen Bereich, auch hier gilt die abschließende Regelung des Gesetzgebers in § 6 b Bundesdatenschutzgesetz zur Zulässigkeit von Videoüberwachungen in diesen Bereichen. Der auf Nachfrage mitgeteilte Zweck der Videoüberwachung war die Überwachung des Eingangs zum Café, also die Ausübung des Hausrechts. Unglücklich war allerdings, dass die Kameras die Bilder auf einen Tablet-PC übertrugen. Dieser lag zumeist mit entladener Batterie und nicht eingeschaltet in der Wohnung des Betreibers. Mit anderen Worten, die Videokameras filmten zwar, konnten aber den mit Ihnen verfolgten Zweck gar nicht erfüllen. Die Videoüberwachung muss nach dem Gesetz auch für den Zweck der Ausübung des Hausrechts geeignet und erforderlich sein. Das ist nur dann der Fall, wenn durch die Videoüberwachung die Ausübung des Hausrechts zumindest unterstützt wird und kein ande-

res Mittel zur Verfügung steht, das in die Rechte der Gäste weniger stark eingreift. Ebenfalls darf kein Anhaltspunkt dafür erkennbar sein, dass schutzwürdige Interessen der Betroffenen überwiegen. Die hier festgestellte Videoüberwachung war schon deswegen unzulässig, da sie überhaupt nicht geeignet war, den angestrebten Zweck zu erreichen. Aber selbst wenn dies der Fall gewesen wäre, sind in Gaststätten immer Anhaltspunkte dafür erkennbar, dass die Interessen der gefilmten Gäste überwiegen. Dabei kommt es auch nicht darauf an, ob und wie gefilmt wird bzw. ob aufgezeichnet wird. Es handelt sich um einen Ort, der der Freizeitgestaltung dient. Hier muss eine Entfaltung der Persönlichkeit möglich sein, die nicht unter dem Eindruck der ständigen Beobachtung steht. Der TLfDI hat hier die Demontage der Kameras angeordnet.

Die Videoüberwachung muss für den von ihr verfolgten Zweck geeignet und erforderlich sein. Videokameras in Gaststätten, die im Gastraum aufgebaut sind bzw. in diesen hineinfilmen, sind grundsätzlich datenschutzrechtswidrig.

3.9 Ich weiß, was Du isst, also weiß ich, was Du bist: Videogaga 2

So oder so ähnlich scheinen es derzeit mehrere Gastronomen in Thüringen zu betrachten. Beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) laufen derzeit mehrere Verwaltungsverfahren hinsichtlich Videoüberwachung im Gastronomiebereich, die alle auf Hinweise aus der Bevölkerung zurückzuführen sind. Ganz besonders genau scheint es ein Erfurter Unternehmen zu nehmen, wenn es große Teile des Gastraums und den überwiegenden Teil des Arbeitsbereiches der Gaststätte überwacht. Dabei kann man fast pauschal sagen, dass diese Art der Videoüberwachung rechtswidrig ist.
Die Überwachung im Gastraum ist ohnehin rechtswidrig, da eine Videoüberwachung im öffentlich zugänglichen Bereich schon dann unzulässig ist, wenn Anhaltspunkte darüber vorhanden sind, dass schutzwürdige Interessen Betroffener das Interesse des Betreibers an der Beobachtung überwiegen, § 6 b Abs. 1 Bundesdatenschutzgesetz. Dies ist im Gastraum eines Cafés, einer Bar oder eines Restaurants immer der Fall, weil dies ein Ort ist, an dem eine ungestörte

Entfaltung der Persönlichkeit im Rahmen der Freizeitgestaltung möglich sein muss.
Die Videoüberwachung von Arbeitnehmern ist in aller Regel ebenfalls unzulässig. Ein Umgang mit Arbeitnehmerdaten ist nämlich immer nur dann erlaubt, wenn dies zur Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Eine Videoüberwachung im Rahmen eines Arbeitsverhältnisses kann zum Beispiel dann erforderlich sein, wenn extreme (Arbeits-)Umstände vorliegen, wie beispielsweise eine lebensbedrohliche Arbeitsumgebung, bei der der oder die Arbeitnehmer ständig beobachtet werden müssen, um im Fall eines Unfalls sofort eingreifen zu können. Umstände also, die im Arbeitsbereich von Gastronomiebetrieben eher selten gegeben sein dürften.
Der TLfDI hat dem – uneinsichtigen – Unternehmen gegenüber eine Anordnung erlassen, in der die Deinstallation der Kameras verlangt wird, um wieder rechtskonforme Zustände herzustellen.

Videoüberwachung im Gastronomiebereich ist in der Regel unzulässig. Sollten Sie eine solche Anlage bemerken, wenden Sie sich bitte an den TLfDI, damit dieser der Sache nachgehen kann.

3.10 Busfahrer im Visier: Videogaga 3

Auf einen anonymen „Wink“ hin wurde die Aufmerksamkeit des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf ein Thüringer Nahverkehrsunternehmen gelenkt. In dem Hinweis wurde von einer umfangreichen Videoüberwachung sämtlicher Busse gesprochen. Nicht nur das Betriebsgelände, sondern auch die Busfahrer selbst sollten überwacht werden. Insgesamt seien ca. 40 Videokameras in Betrieb.
Im Laufe der Kontrolle wurde durch die Arbeitnehmer des TLfDI in der Tat eine umfangreiche Videoüberwachungsanlage festgestellt. Hervorzuheben ist dabei insbesondere die festgestellte Kamera im Bus, die den Busfahrer bei seiner Arbeit filmt. Diese Kamera ist rechts oberhalb des Busfahrers angebracht und filmt nach links Richtung vordere Einstiegstür. Aufgenommen werden dabei auch Bereiche außerhalb des Busses und zwar sowohl in Fahrtrichtung sowie auf der Einstiegsseite. Allerdings ist auch das Lenkrad mit den Armen und Händen des Busfahrers zu erkennen. Teilweise – jeweils von Bus und Fahrer abhängig – auch der Kopf des Fahrers.

Rechtlich gesehen sind ein Bus und die Straße um diesen herum nicht anders zu beurteilen als sonstige Bereiche, die öffentlich zugänglich sind. Dabei kommt es nämlich nicht darauf an, ob es sich um Privatbesitz handelt oder nicht. Vielmehr ist maßgeblich, ob die jeweiligen Flächen vom äußeren Erscheinungsbild her den Eindruck erwecken, von jedermann betreten werden zu dürfen. Umso mehr unter den Begriff der öffentlich zugänglichen Bereiche fallen dann Bereiche, die dazu gedacht sind, von jedermann betreten zu werden: Busse zum Beispiel.

Videoüberwachung in diesen Bereichen ist problematisch, wie man auch daran erkennen kann, dass dieser Komplex immer wieder in diesem Tätigkeitsbericht zur Sprache kommt. Der Gesetzgeber hat nämlich erkannt, dass Videoüberwachungsanlagen in besonderem Maße in die Grundrechte der Bürger eingreifen und deren Gebrauch in öffentlich zugänglichen Bereichen daher abschließend reglementiert. Nur in den gesetzlich zulässigen Fällen ist eine Videoüberwachung zulässig, wenn diese erforderlich ist und keine Anhaltspunkte dafür bestehen, dass Interessen der jeweils Betroffenen dem entgegenstehen, so der Gesetzgeber in § 6 b Bundesdatenschutzgesetz (BDSG).

Nach dieser Regelung (§ 6 b BDSG) sind die Aufnahmen außerhalb des Busses nur dann zulässig, wenn dies zur Durchsetzung des Hausrechts bzw. wegen berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Beide Alternativen scheiden hier aus: das Hausrecht, weil ein Busunternehmen auf Straßen und Fußwegen kein Hausrecht ausübt; besondere Interessen, weil diese nicht für konkrete Zwecke festgelegt wurden.

Hinsichtlich der hier beleuchteten Kamera über dem Busfahrer kommen auch noch Arbeitnehmerdatenschutzaspekte hinzu. So ist eine Erhebung von Arbeitnehmerdaten immer nur dann erlaubt, wenn dies zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist.

Unter beiden Gesichtspunkten ist die über dem Fahrer installierte Kamera in der derzeitigen Installation unzulässig.

Die Zulässigkeit dieser Aufnahmen scheitert schon offensichtlich daran, dass diese nicht für die Durchführung des Arbeitsverhältnisses von Belang sind.

Aber auch die Aufnahmen der Bereiche außerhalb des Busses sind datenschutzrechtlich problematisch. So werden Fahrzeuge (und deren Kennzeichen) vor dem Bus genauso erfasst, wie auf den Fußwe-

gen laufende und an Haltestellen stehende Menschen. Diese Beobachtung des öffentlich zugänglichen Bereiches ist jedoch nur unter den oben beschriebenen Voraussetzungen möglich, wenn diese zur Durchsetzung des Hausrechts oder eines besonderen Interesses für festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für überwiegende schutzwürdige Interessen Betroffener bestehen.
Insoweit ist die juristische Prüfung noch nicht abgeschlossen, jedoch sind die Kameras, die den Busfahrer und die Außenbereiche aufnehmen, nach summarischer Prüfung mit dem BDSG nicht zu vereinbaren.
Der TLfDI wird nach Abschluss der Prüfung dem Unternehmen das Ergebnis mitteilen. Reagiert das Unternehmen hierauf nicht und belässt es bei den festgestellten rechtswidrigen Verfahrensweisen, wird der TLfDI gegenüber dem Unternehmen eine Anordnung erlassen, mit der er diesem die entsprechenden Verhaltensweisen untersagt. Sofern im Ergebnis nach Abschluss der juristischen Prüfung eine unzulässige Videoüberwachung festgestellt werden sollte, wird der TLfDI ebenfalls die Einleitung eines Ordnungswidrigkeitenverfahrens prüfen.

Wenn Arbeitnehmer bei ihrer Tätigkeit permanent videoüberwacht werden, ist dies in aller Regel unzulässig. Auch die Aufnahme des öffentlichen Verkehrsraums ist regelmäßig rechtswidrig.

3.11 Wertvoller Schrott im Blick: Videogaga 4

Im Rahmen seiner Tätigkeit führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) verschiedene anlassunabhängige Kontrollen durch. Mit Übernahme der Zuständigkeit im nicht-öffentlichen Bereich Ende 2011 durch den TLfDI führte dieser mehrere Informationskampagnen für Unternehmen durch. Im Anschluss an diese Informationsphase, die mit einer Art „Schonfrist“ für die Unternehmen verbunden war, begann der TLfDI mit anlasslosen Kontrollen bei Unternehmen. In diesem Zusammenhang wurden auch diverse Recyclingunternehmen kontrolliert, weil es aus dieser Branche bereits diverse Beschwerden beim TLfDI gab. Bei diesen Unternehmen ergaben sich vielfältige, auf den ersten Blick nicht ersichtliche datenschutzrechtliche Problemstellungen. Eine davon ist der umfangreiche Einsatz von Videoüberwachungstechnik.

So auch in diesem Fall. Zwar ist die juristische Bewertung bislang noch nicht abgeschlossen, allerdings wird auch in diesem Fall von einer Videotechnik in einem Umfang Gebrauch gemacht, der nach summarischer Prüfung nicht mit dem Bundesdatenschutzgesetz (BDSG) vereinbar ist.
So ist unter anderem eine umfangreiche Videoüberwachung im Außenbereich eingerichtet, die möglicherweise nicht den gesetzlichen Voraussetzungen entspricht und damit unzulässig ist. Durch eine solche Videoüberwachungsanlage werden personenbezogene Daten erhoben und gespeichert. Dies ist jedoch nur zulässig, wenn die betroffenen Personen in die Datenerhebung und -speicherung eingewilligt haben, was bei einer Videoüberwachung wirklichkeitsfremd wäre, oder das Gesetz eine entsprechende Erlaubnisnorm für den konkreten Fall des Einsatzes bereithält.
Im hiesigen Fall ist die einschlägige Erlaubnisnorm § 6 b Bundesdatenschutzgesetz (BDSG). Diese regelt den Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen. Zu solchen zählt auch der Betriebshof eines Recyclingunternehmens, soweit dieser so gestaltet ist, dass jedermann diesen betreten kann. In solchen Bereichen ist eine Videoüberwachung durch ein nicht-öffentliches Unternehmen nur dann zulässig, wenn diese zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke durchgeführt wird und hierfür auch erforderlich ist.
Während diese Voraussetzungen zumeist vorliegen mögen bzw. deren Hürde nicht sonderlich schwer zu nehmen ist, stellt § 6 b BDSG noch eine weitere Anforderung an eine zulässige Videoüberwachung. So dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener die Interessen des Videoüberwachenden überwiegen. Im Gegensatz zu den vorherigen Voraussetzungen stellt dies eine hohe Hürde für die Zulässigkeit einer Videoüberwachung im nicht-öffentlichen Bereich dar. Bereits Anhaltspunkte dafür, dass Interessen Betroffener überwiegen, führen zur Unzulässigkeit der Anlage. Daher ist eine Videoüberwachung in solchen Bereichen nur dann zulässig einsetzbar, wenn es dafür wirklich triftige und schwerwiegende Gründe gibt, die eventuelle schutzwürdige Interessen Betroffener in jedem Fall überwiegen.
Der TLfDI wird in diesem Fall nach Abschluss der Prüfung dem Unternehmen in einem Kontrollergebnis mitteilen, welche Mängel festgestellt wurden. Sollte das Unternehmen daraufhin die entspre-

chenden Mängel nicht abstellen, wird der TLfDI dem Unternehmen gegenüber eine Anordnung erlassen, mit der die Beseitigung der Mängel durchgesetzt werden. Darüber hinaus muss das Unternehmen wegen des hohen Eingriffspotentials von Videoaufnahmen in das Persönlichkeitsrecht der Betroffenen mit der Einleitung von Ordnungswidrigkeitenverfahren rechnen.

Bevor Investitionen zur Einrichtung einer Videoüberwachungsanlage getroffen werden, sollte genau geprüft werden, ob diese mit dem BDSG vereinbar ist. Hierbei sollte man nicht nur auf die Aussagen des installierenden Unternehmens vertrauen, da diese in erster Linie ihr Produkt und ihre Dienstleistung verkaufen möchte. Die Voraussetzungen für eine zulässige Videoüberwachung sind oftmals hoch und bedürfen der Prüfung durch Fachpersonal. Dabei sind unbedingt die Voraussetzungen, die das Gesetz an die jeweilige Art der Videoüberwachung richtet, einzuhalten. Unternehmen sollten erwägen, vor einer Videoinstallation den TLfDI zu Rate zu ziehen.

3.12 Schrott unter Beobachtung: Videogaga 5

Im Rahmen der anlasslosen durchgeführten Kontrolle suchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein größeres Recyclingunternehmen auf. Dieses Unternehmen besaß keinen betrieblichen Datenschutzbeauftragten. Es war bislang nicht üblich, die Arbeitnehmer, die mit der Verarbeitung von personenbezogenen Daten betraut sind, auf das Datengeheimnis zu verpflichten. Nach § 5 Bundesdatenschutzgesetz (BDSG) muss jedes Unternehmen seine mit der Verarbeitung von personenbezogenen Daten betrauten Arbeitnehmer auf das Datengeheimnis verpflichten. Auf der Homepage des TLfDI findet sich eine Mustervorlage zur Verpflichtung auf das Datenschutzgeheimnis. Das Unternehmen wird diese Verpflichtung der Arbeitnehmer nachholen.
Das Verfahrensverzeichnis befand sich im Aufbau. Es gab bereits Festlegungen des Qualitätsmanagements, die sich mit den Verfahren der Verarbeitung von personenbezogenen Daten befassen. Diese müssen jedoch noch strukturiert und zusammengefasst werden, um den gesetzlichen Anforderungen zu genügen. Nach § 9 BDSG muss das Unternehmen die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung datenschutzrechtlicher Bestimmungen zu gewährleisten. Im Nachgang zur Kontrolle

reichte das Unternehmen bereits umfangreiche Unterlagen ein, diese werden derzeit geprüft.
Auf dem Gelände des Unternehmens gab es eine umfangreiche Videoüberwachung mit 10 Dome-Kameras, die sich sowohl innerhalb des Firmengebäudes als auch außerhalb befanden. Die Zwecke für die Videoüberwachung waren bei den einzelnen Kameras unterschiedlich. Sie wurden bei der Begehung erläutert, waren jedoch nicht im Rahmen eines Sicherheitskonzeptes dokumentiert. Eine Videoaufzeichnung fand nicht statt, die Bilder waren in einem separaten Wachraum durch den Wachmann live zu sehen. Auch das reine Monitoring fällt unter den Begriff der Videoüberwachung nach § 6 b BDSG. Es handelt sich hierbei um die Beobachtung mit optisch-elektronischen Einrichtungen nach § 6 b Abs. 1 BDSG. Gegenüber der Videoaufzeichnung stellt das reine Monitoring einen geringeren Eingriff in die Rechte der Betroffenen dar, da die Aufnahme der Person nur in Echtzeit erfolgt und nachträglich nicht mehr wieder herstellbar ist. Gleichwohl muss die durchgeführte Videoüberwachung den Anforderungen des § 6 b BDSG genügen, soweit sie in öffentlich zugänglichen Räumen erfolgt, ansonsten müssen die Anforderungen des § 28 BDSG erfüllt oder, wenn die Beobachtung von Mitarbeitern im Fokus steht, die Voraussetzungen des § 32 BDSG gegeben sein. Der TLfDI hat die Prüfung der Zulässigkeit der Videoüberwachung in dem Unternehmen noch nicht abgeschlossen. Für jede einzelne Kamera muss festgestellt werden, ob diese den jeweils geltenden rechtlichen Anforderungen entspricht. Jedenfalls wird der TLfDI vom Unternehmen die Erstellung eines Verfahrensverzeichnisses nach § 4 g Abs. 2 bzw. 2 a BDSG verlangen. Außerdem müssen die konkreten Zwecke der Videoüberwachung nach § 6 b Abs. 1 bzw. 28 Abs. 1 Satz 2 BDSG schriftlich festgelegt werden.

Zwar stellt die reine Videobeobachtung einen geringeren Eingriff dar als die Videoaufzeichnung. Auch sie ist jedoch nur bei Vorliegen einer gesetzlichen Ermächtigung zulässig. Vor Beginn der Videoüberwachung ist der konkrete Zweck der Überwachungsmaßnahme schriftlich festzulegen und es sind die erforderlichen technischen und organisatorischen Maßnahmen zur Einhaltung datenschutzrechtlicher Anforderungen zu treffen.

3.13 Schrott-Video: Videogaga 6

Im Zuge der anlasslos durchgeführten Unternehmenskontrollen suchte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein Unternehmen auf, dessen Hauptgeschäft das Elektronikschrott-Recycling ist. In diesem Unternehmen gab es etliche datenschutzrechtliche Probleme:
Das rechtlich selbstständige Unternehmen ist Tochter eines größeren Konzerns, der die Personalverwaltung für das Unternehmen übernommen hat. Nach § 11 Bundesdatenschutzgesetz (BDSG) bleibt weiterhin das auftraggebende Unternehmen für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. In diesem Fall ist ein schriftlicher Auftrag zu erteilen, der den Anforderungen des § 11 Abs. 2 Satz 2 BDSG entsprechen muss. Es müssen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, der Umfang der Weisungsbefugnis, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält und vieles mehr geregelt werden. Ein solches Vertragsverhältnis existierte zwischen Konzerntochter und Konzernmutter jedoch nicht.
Zwar hatte das Unternehmen einen Datenschutzbeauftragten, dieser hatte jedoch noch keine speziellen Datenschutzkenntnisse erworben. Es gab im Betrieb auch keine Richtlinien bzw. Anweisungen zur Einbeziehung des Datenschutzbeauftragten. Es fehlten schriftliche Festlegungen zur Sperrung und Löschung von nicht mehr erforderlichen Daten. Ein schriftliches Konzept zu allgemeinen technischen und organisatorischen Maßnahmen existierte ebenso wenig wie ein Konzept über die Gesamtheit der Sicherheitsmaßnahmen (IT-Sicherheitskonzept).
Weiterhin wurde auf dem Gelände eine Videoüberwachung mit vier Kameras durchgeführt. Eine Kamera filmte dabei Arbeitnehmer auf einem dauerhaft eingerichteten Arbeitsplatz an einem Förderband. Zwar ist der von der Kamera überwachte Bereich öffentlich zugänglich, jedoch steht hier der Beschäftigte im Fokus der Überwachung. In diesen Fällen haben sich die Aufsichtsbehörden der Länder darauf geeinigt, die Zulässigkeit der Videoüberwachung an den Vorausset-

zungen des § 32 BDSG zu messen. Danach dürfen personenbezogene Daten eines Arbeitnehmers für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses zu dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Arbeitnehmers nur dann erhoben, verarbeitet oder genutzt werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Da beide Voraussetzungen nicht vorlagen, war die Kamera in dieser Ausrichtung nicht zulässig.

Eine weitere Kamera wurde auf Wunsch eines Kunden installiert. Dieser wollte dokumentiert haben, dass seine Produkte, die geheimhaltungsbedürftige Daten enthielten, ordnungsgemäß geschreddert bzw. vernichtet worden sind. Hier reicht es aus Sicht des TLfDI im Rahmen der Erforderlichkeit aus, die Kamera nur bei der Auftragstätigkeit für diesen Kunden zu aktivieren.

Die Zulässigkeit der übrigen Kameras war, da das Betriebsgelände während der Geschäftszeiten für den Publikumsverkehr geöffnet war, an § 6 b BDSG zu messen. Nach § 6 b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht mit einem anderen (wirtschaftlich oder organisatorisch) zumutbaren, in die Rechte der Betroffenen weniger einschneidenden Mittel, erreicht werden kann.

Eine weitere Kamera, die den Eingangsbereich absichern sollte, war teilweise auch auf den öffentlichen Verkehrsgrund gerichtet. Hier war nicht ersichtlich, wieso die Aufnahme dieses Bereiches für die verfolgten Zwecke erforderlich sein sollte. Die Kamera sollte dazu dienen, eine Annahmestelle für Elektroschrott, die sich vor dem Tor auf dem Betriebsgelände befand, zu überwachen. Wer außer seinem Grundstück auch öffentlichen Raum, wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt.

Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten oder sonstige Verkehrsteilnehmer, zurück.

Eine weitere Kamera wurde angebracht, um einen Bereich zu überwachen, der schlecht einsehbar war. Es sei in der Vergangenheit häufiger dazu gekommen, dass Personen nachts über den Zaun auf das Gelände gelangt sind. Hier hielt der TLfDI eine Überwachung während der Geschäftszeiten für nicht erforderlich.
Die aufgezeichneten Bilder wurden von dem Unternehmen 84 Stunden gespeichert. Nach § 6 b Abs. 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erfüllung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Das bedeutet, Videoaufzeichnungen sind grundsätzlich nach 48 Stunden zu löschen.
Das Unternehmen forderte von sämtlichen Kunden Kopien der Personalausweise. Dies ist grundsätzlich unzulässig und nicht erforderlich (hierzu wird auf den Beitrag unter Punkt 3.48 verwiesen).
Der TLfDI teilte dem Unternehmen das Ergebnis seiner Kontrolle mit und gab diesem Gelegenheit zur Stellungnahme. Es bleibt abzuwarten, ob das Unternehmen alle datenschutzrechtlichen Forderungen des TLfDI erfüllt oder eine verwaltungsrechtliche Anordnung erforderlich sein wird. Derzeit wird geprüft, ob ein Bußgeldverfahren eingeleitet wird.

Für Unternehmen in Thüringen bestehen zahlreiche datenschutzrechtliche Anforderungen. Es ist beispielsweise im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret anzugeben und die gesetzlichen Voraussetzungen sind für jede Kamera gesondert zu prüfen. Diese Festlegungen sind Teil der durch das Unternehmen zu treffenden technischen und organisatorischen Maßnahmen nach § 9 BDSG.

3.14 Der nicht privilegierte Konzern

Im Rahmen seiner Tätigkeit führte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) verschiedene anlassunabhängige Kontrollen durch. In diesem Zusammenhang wurden auch diverse Recyclingunternehmen kontrolliert. In dieser Branche ergeben sich vielfältige, auf den ersten Blick nicht ersichtliche datenschutzrechtliche Problemstellungen. Im Fall des nunmehr kontrollierten Unternehmens wurden mögliche Probleme hinsichtlich der Auftragsdatenverarbeitung festgestellt. Dies ist insbesondere bei solchen Unternehmen ein Problemschwerpunkt, die in eine umfangreiche Konzernstruktur eingebunden sind. Ein Konzern entsteht immer dann, wenn mehrere Unternehmen zusammenarbeiten und eines davon die anderen beherrscht. Typischerweise werden in solchen Strukturen beispielsweise Arbeitnehmerdaten an eine beherrschte Verwaltungsgesellschaft weitergeleitet, die dann alle damit verbundenen Aufgaben, wie Lohnsteuerberechnungen übernimmt.

Im Zusammenhang mit dem Datenschutz führt dies oftmals zu Problemen, je nachdem, wie die Aufgabenteilung im jeweiligen Konzern organisiert ist. Denn, woran man denken muss: Das Bundesdatenschutzgesetz (BDSG) kennt keine Sonderregelungen für Konzerne. Demensprechend gibt es auch kein „Konzernprivileg“ im BDSG.

Während es sich also auf den ersten Blick so „anfühlt“, als würden personenbezogene Daten innerhalb eines Unternehmens bleiben, weil man diese innerhalb der selben Unternehmensgruppe „verschiebt“, werden datenschutzrechtlich betrachtet personenbezogene Daten zwischen verschiedenen Unternehmen übermittelt. Hierfür gelten dieselben Einschränkungen, die auch für Unternehmen gelten, die nicht durch einen Beherrschungsvertrag verbunden sind.

Dieses falsche Gefühl führt oftmals dazu, dass zwischen den konzerneigenen Unternehmen keine oder nur mangelhafte Auftragsdatenverarbeitungsverträge geschlossen werden. Tatsächlich ist eine solche Verarbeitung von Daten aber nur dann zulässig, wenn entweder ein solcher Auftragsdatenverarbeitungsvertrag geschlossen wurde, der Betroffene einwilligt oder es eine entsprechende Erlaubnisnorm gibt. Hinsichtlich der Einwilligung bestehen aber wegen der sozialen und wirtschaftlichen Abhängigkeit des Arbeitnehmers vom Arbeitgeber hohe Anforderungen. Die Versuchung, sämtliche Maß-

nahmen des Arbeitgebers „abzunicken“, um diesem zu gefallen, wird als hoch eingeschätzt. Da die Einwilligung nach den gesetzlichen Vorgaben freiwillig erfolgen muss, aber solche autonomen Gründe, die vom Arbeitnehmer selbst stammen und zur Einwilligung geführt haben müssen, fehlen, scheidet eine Einwilligung als Zulässigkeitsgrund im Arbeitsverhältnis in der Regel aus. Der Wille, zu gefallen, oder sonstiger Anpassungsdruck von außen stellt nämlich keinen autonomen Grund dar.

Auch der Weg über die Erlaubnisnorm ist holprig. Zwar stellt das Gesetz mit § 28 BDSG bzw. bei Arbeitnehmerdaten mit § 32 BDSG Normen bereit, die für diesen Anwendungsbereich in Frage kommen, jedoch müssen die Unternehmen hierbei jedes Mal erneut umfangreich prüfen, ob eine Übermittlung oder sonstige Verarbeitung von personenbezogenen Daten noch von der jeweiligen Norm gedeckt ist.

Einfacher stellt sich hier die Auftragsdatenverarbeitung, geregelt in § 11 BDSG, dar. Für ein solches Rechtsverhältnis schreibt das BDSG Form und Inhalt vor. Dieser Auftrag zur Datenverarbeitung ist schriftlich zu erteilen, wobei nach § 11 Abs. 2 Satz 2 BDSG insbesondere im Einzelnen festzulegen sind:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Wesentlicher Vorteil für den Datenverkehr innerhalb des Konzerns ist der, dass bei einem Auftragsdatenverarbeitungsverhältnis kraft gesetzlicher Fiktion keine Datenübermittlung erfolgt und somit die Voraussetzungen der entsprechenden Erlaubnisnorm (für die Übermittlung) entfallen. Allerdings ist zu beachten, dass der Auftraggeber eines solchen Vertragsverhältnisses auch datenschutzrechtlich verantwortliche Stelle bleibt. Werden beim Auftragnehmer datenschutzrechtswidrige Zustände festgestellt, bleibt folglich dennoch der Auftraggeber Ansprechpartner der Aufsichtsbehörde.
Im hiesigen Fall konnten bis heute die entsprechenden Verträge nicht nachgereicht werden. Dies kann unter Umständen dazu führen, dass die jeweils vorgenommenen Übermittlungen in unbefugter Art und Weise erfolgten. Wenn sich diese Annahme bestätigt, muss das Unternehmen mit der Einleitung entsprechender Ordnungswidrigkeitenverfahren durch den TLfDI rechnen.

Auch innerhalb eines Konzerns gelten die Regelungen des BDSG zum Datenschutz im nicht-öffentlichen Bereich ohne Einschränkungen. Hier bietet es sich oftmals an, Verträge über eine Auftragsdatenverarbeitung zwischen Unternehmen zu schließen, die regelmäßig personenbezogene Daten übermitteln sollen. Allerdings sind dabei die gesetzlichen Mindeststandards für einen solchen Vertrag einzuhalten

3.15 Teurer Schrott

Die wenigsten Unternehmen können alle Bereiche, bei denen personenbezogene Daten verarbeitet werden müssen, selber abwickeln. Hierzu bedient man sich dann anderer Unternehmen, die sich auf den entsprechenden Bereich spezialisiert haben. Typisches Beispiel hierfür ist die Altpapiervernichtung. Ein vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) kontrolliertes Unternehmen setzte einen Dienstleister ein, um seine alten Datenträger zu vernichten, auf denen personenbezogene Daten

gespeichert waren. Hierbei handelt es sich um ein so genanntes Auftragsdatenverhältnis, an das das Bundesdatenschutzgesetz (BDSG) bestimmte Anforderungen stellt. Allerdings entsprach der diesem Auftragsverhältnis zu Grunde liegende Vertrag nicht den vom Gesetz vorausgesetzten formalen und inhaltlichen Ansprüchen. Zwar entsprach der Vertrag der vom Gesetz geforderten Schriftform, jedoch war weder der Gegenstand des Auftrags ausreichend bezeichnet, noch wurde auf den Umfang, die Art und den Zweck der vorgesehenen Verarbeitung der Daten, die Art der Daten und die Betroffenen eingegangen. Die zu regelnden notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG waren ebenso nicht enthalten, wie ein dem Auftraggeber einzuräumendes Kontrollrecht. Auch fehlte eine Regelung, die den Auftragnehmer dem Weisungsrecht des Auftraggebers unterwirft und ersteren verpflichtet, Verstöße gegen den Datenschutz seinem Auftraggeber zu melden. Letztlich fehlte auch eine Regelung über die Rückgabepflicht von personenbezogenen Daten nach Ende des Vertragsverhältnisses an den Auftraggeber. Die Folge ist, dass kein Auftragsdatenverarbeitungsverhältnis im Sinne des Datenschutzrechts besteht und es sich bei der Weitergabe der Festplatten zum Zweck der Vernichtung damit um eine Übermittlung personenbezogener Daten im Sinne des BDSG handelt. Allerdings um eine Übermittlung, für die keine Rechtsgrundlage besteht und die damit unbefugt erfolgte. Eine unbefugte Übermittlung von personenbezogenen Daten ist allerdings mit einem Bußgeld von bis zu 300.000 Euro bedroht. Der TLfDI hat das Unternehmen aufgefordert, ein dem BDSG entsprechendes Vertragswerk aufzusetzen, um so den Anforderungen des BDSG zu genügen. Ob ein Ordnungswidrigkeitenverfahren eingeleitet werden soll, wird derzeit geprüft.

Wenn personenbezogene Daten im Auftrag verarbeitet werden sollen, müssen Unternehmen unbedingt darauf achten, dass ein wirksamer und inhaltlich richtiger Vertrag über die Auftragsdatenverarbeitung geschlossen wird. Liegt kein Auftragsdatenverarbeitungsvertrag im Sinne des Datenschutzrechts vor, handelt es sich um eine Datenübermittlung, die einer eigenen Rechtsgrundlage bedarf. Fehlt diese, kann es ganz schnell teuer werden.

3.16 Zwei Fliegen mit einer Klappe

Eines der vielen vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen einer anlasslosen Kontrollreihe kontrollierten Unternehmen war ein Hersteller großer industrieller Fertigungsanlagen.
Bereits zu Beginn der Kontrolle war offensichtlich, dass der Geschäftsführer des Unternehmens vom Datenschutz, wie ihn das Gesetz versteht, noch nichts gehört hatte. Der Unternehmer verstand unter dem Begriff vielmehr den Schutz der Unternehmensdaten vor Zugriffen von außen und von innerhalb des Unternehmens und dabei vor allem Daten, die für das Unternehmen von Wert sind, wie z. B. Konstruktionspläne. Sicherlich sind solche Datensätze für Unternehmen schützenswerte Daten, handelt es sich doch im Kern um das Kapital des Unternehmens. Leider ist diese fehlerhafte, zumindest aber unvollständige Auffassung hinsichtlich des Begriffes Datenschutz weit verbreitet und zumindest zu kurz gegriffen.
Mit dem Bundesdatenschutzgesetz (BDSG) hat der Gesetzgeber Unternehmern und anderen privaten Stellen aufgegeben, mit personenbezogenen Daten Dritter nur insoweit umzugehen, wie es das Gesetz vorsieht oder der Einzelne es zulässt. Sonstige schützenswerte Daten, wie z. B. Geschäftsgeheimnisse, hatte der Gesetzgeber nicht im Sinn. Dennoch sind beide Bereiche nicht völlig voneinander zu trennen. Wer, so wie es das Gesetz vorschreibt, für den Schutz von personenbezogenen Daten ein Sicherheitskonzept erstellt und den Zugang zu unterschiedlichen Bereichen sowie Programmen regelt, um den Zugriff Unbefugter auf personenbezogene Daten zu verhindern und eine ausschließliche Verarbeitung im Rahmen der gesetzlichen Vorschriften zu gewährleisten (Zugriffs- und Zutrittsregelungen), wird seine Überlegungen ohne größere Umstände auch auf die nicht personenbezogenen Daten des Unternehmens ausweiten können.
Im hiesigen Fall stellte es sich genau anders herum dar. Das Unternehmen hatte einiges an Mitteln in den Schutz der unternehmenseigenen Konstruktionspläne investiert. Zwar wurden vom TLfDI und seinen Mitarbeitern der eine oder andere Mangel festgestellt, jedoch war das Unternehmen dann auch hinsichtlich der personenbezogenen Daten weit besser aufgestellt als die meisten anderen kontrollierten Unternehmen. So waren alle Maßnahmen zum technischen und organisatorischen Datenschutz bereits getroffen und mussten nur noch

auf die eigentlich zu schützenden personenbezogenen Daten ausgeweitet werden. Insbesondere existierte ein detailliertes IT-Sicherheitskonzept, was zwar notwendig, aber nach den bisherigen Erfahrungen in Thüringen leider noch nicht selbstverständlich ist.
Die detaillierten Unterlagen liegen dem TLfDI zur Prüfung vor und werden noch ausgewertet. Sodann wird dem Unternehmen in einem Schreiben mitgeteilt werden, welche Veränderungen und Maßnahmen noch notwendig sind, um die Einhaltung des BDSG zu gewährleisten. Sofern bei der Detailprüfung keine schwerwiegenden Verstöße mehr festgestellt werden und den Forderungen des TLfDI Folge geleistet wird, ist das Verfahren damit abgeschlossen.

Ein datenschutzrechtlich ordnungsgemäß arbeitendes Unternehmen hat auch aus unternehmerischer Sicht einen Marktvorteil. Zunächst danken es einem die Arbeitnehmer, Lieferanten und Kunden, wenn mit ihren Daten ordnungsgemäß umgegangen wird, gleichzeitig können aber auch sonstige Daten des Unternehmens in das technisch-organisatorische Schutzkonzept des Unternehmens mit eingebunden werden. So schlägt man zwei Fliegen mit einer Klappe.

3.17 Problemzonen im Autohaus: Videogaga 7

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte im Rahmen seiner Tätigkeit ein Autohaus. Die juristische Bewertung ist bislang noch nicht abgeschlossen. Es ist allerdings ersichtlich, dass sich die datenschutzrechtlichen „Problemzonen“ dieses Autohauses nicht von den sonstigen Problemen im Einzelhandel unterscheiden. So ist unter anderem eine umfangreiche Videoüberwachung im Außenbereich eingerichtet, die möglicherweise nicht den gesetzlichen Voraussetzungen entspricht und damit unzulässig ist. Durch eine solche Videoüberwachungsanlage werden personenbezogene Daten erhoben und gespeichert. Dies ist jedoch nur zulässig, wenn die betroffenen Personen in die Datenerhebung und -speicherung eingewilligt haben, was fallbezogen bei der Videoüberwachung wirklichkeitsfremd wäre, oder das Gesetz eine entsprechende Erlaubnisnorm für den konkreten Fall des Einsatzes bereithält. Im hiesigen Fall ist die einschlägige Erlaubnisnorm § 6 b Bundesdatenschutzgesetz (BDSG). Diese regelt den Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Räumen. Zu solchen zählt auch das Areal eines Autohauses, da es

einem nicht näher bestimmbaren Personenkreis zugänglich ist und der Betreiber sogar möchte, dass Kundschaft das Gelände bzw. die Räumlichkeiten betritt. In solchen Bereichen ist eine Videoüberwachung durch ein nicht-öffentliches Unternehmen nur dann zulässig, wenn diese zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke durchgeführt wird und hierfür auch erforderlich ist. § 6 b BDSG stellt daneben noch eine weitere Anforderung an eine zulässige Videoüberwachung: So dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener die Interessen des Videoüberwachenden überwiegen. Hierbei muss der Unternehmer im Vorfeld die beeinträchtigten Interessen der Personen, die zukünftig und gegen seine Interessen an der Videoüberwachung abwägen. Stellt er hierbei fest, dass seine Interessen die der Betroffenen nicht überwiegen könnten, so ist die angedachte Videoüberwachung unzulässig. Mit dieser Anforderung an eine Videoüberwachung in öffentlich zugänglichen Bereichen wirkt der Gesetzgeber flächendeckenden Videoüberwachungen entgegen. Es soll also nur dann eine Videoüberwachung in solchen Bereichen durchgeführt werden, wenn ein wirklich triftiger Grund vorliegt.

Der TLfDI wird nach Abschluss der Prüfung dem Unternehmen mitteilen, welche Mängel festgestellt wurden. Sollte das Unternehmen daraufhin die entsprechenden Mängel nicht beheben, wird der TLfDI dem Unternehmen gegenüber eine Anordnung erlassen, mit der die Beseitigung der Mängel durchgesetzt wird. Darüber hinaus wird, sofern im Ergebnis feststeht, dass die Videoüberwachung in unzulässiger Art und Weise durchgeführt wurde, die Einleitung eines Ordnungswidrigkeitenverfahrens geprüft.

Bevor Investitionen zur Einrichtung einer Videoüberwachungsanlage getroffen werden, sollte genau geprüft werden, ob diese mit dem BDSG vereinbar ist. Hierbei sollte man nicht nur auf die Aussagen des installierenden Unternehmens vertrauen, da diese in erster Linie ihr Produkt und ihre Dienstleistung verkaufen möchte. Stellt der TLfDI später fest, dass die Videoüberwachung nicht mit dem BDSG vereinbar ist, kann dies ein Ordnungswidrigkeitenverfahren nach sich ziehen.
Daher sollte zuvor vom Unternehmen erwogen werden, den TLfDI um eine Stellungnahme zur geplanten Videoinstallation zu bitten.

3.18 Die Pause ist für die Videoüberwachung tabu: Videogaga 8

Die Videoüberwachung war auch Thema bei der Kontrolle eines in der Lebensmittelbranche tätigen Produktionsunternehmens. Neben einer umfangreichen Videoüberwachung innerhalb der Produktionsgebäude waren auch außerhalb des Gebäudes Videokameras angebracht. Dabei muss zunächst darauf hingewiesen werden, dass es sich um ein Unternehmen handelte, welches den Datenschutz ernst nimmt. Dies war bereits daran erkennbar, dass die Videoüberwachung innerhalb des Gebäudes vorbildlich eingerichtet ist. Eine Arbeitnehmerüberwachung findet nicht statt. Alle Bereiche in denen sich Arbeitnehmer aufhalten und aufhalten könnten, sind geschwärzt und damit bereits vom Aufzeichnungsvorgang ausgeschlossen. Die Überwachung richtet sich allein auf die Produktion und ist damit zulässig. Für die Kontrollierenden, die eher weitgehende datenschutzrechtliche Verstöße gewöhnt sind, sehr ungewohnte Umstände. Allerdings sind auch in diesem Betrieb Mängel festgestellt worden: Im Zuge der Einführung eines betriebsweiten Rauchverbots war ein Unterstand für Raucher eingerichtet worden. Allerdings wurde dabei nicht bedacht, dass sich dieser im Aufnahmebereich der Außenkameras befindet. Pausenräume für Arbeitnehmer dürfen selbstverständlich nicht überwacht werden. Ebenfalls war die Aufzeichnungsdauer der gesamten Videoüberwachung zu lang gestaltet. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit steht mit dem Unternehmen in Kontakt, um datenschutzrechtlich konforme Zustände zu erreichen. Sollte dies nicht gelingen, werden entsprechende Maßnahmen per Anordnung auf verwaltungsrechtlichem Wege durchgesetzt werden.

Im Regelfall ist die dauerhafte Videobeobachtung von Arbeitnehmern unzulässig. Dies gilt insbesondere für Rückzugsräume. Dabei kommt es auch nicht darauf an, ob die Videokamera zu diesem Zweck eingerichtet worden ist. Die theoretische Möglichkeit der Beobachtung reicht für einen Verstoß aus.

3.19 Online-Präsenz? Datenschutz nicht vergessen!

In einem kontrollierten Unternehmen, das im Einzelhandel tätig ist, wurde neben dem eigentlichen Ladengeschäft auch ein Online-Handel mit eigener Internetpräsenz betrieben. Die dafür benötigte

Hardware wurde bei einem der vielen Hoster auf dem Markt zusammen mit der Domain angemietet. Datenschutzrechtlich problematisch daran ist, dass jeder Kunde, der über diesen Shop etwas kauft, seine hierfür notwendigen Daten angeben muss. Diese darf zwar der Betreiber des Onlineshops erheben und speichern, allerdings werden in diesem Fall die Daten nicht durch den Betreiber des Shops gespeichert, sondern liegen, zumindest physisch, auf den Festplatten des Hosters. Damit speichert der Hoster personenbezogene Daten für den Betreiber des Onlineshops. Diese Art der Datenverarbeitung ist nur zulässig, soweit zwischen dem Hoster als Auftragnehmer und dem Onlineshopbetreiber als Auftraggeber ein Auftragsdatenverarbeitungsverhältnis nach § 11 Bundesdatenschutzgesetz (BDSG) vereinbart wurde. Sobald also durch die Internetpräsenz personenbezogene Daten verarbeitet werden, muss ein solcher Vertrag geschlossen werden. Der Vertrag hat dem Schriftformerfordernis zu genügen. Dies setzt also voraus, dass der Vertrag in Papierform existiert und von beiden Parteien unterzeichnet wird. Eine E-Mail oder ein Fax genügt dieser Form nicht. Darüber hinaus muss der Gegenstand des Auftrags ausreichend bezeichnet, der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung der Daten, die Art der Daten und die Betroffenen angegeben sein. Die zu regelnden notwendigen technischen und organisatorischen Maßnahmen nach § 9 BDSG müssen ebenso enthalten sein, wie ein dem Auftraggeber einzuräumendes Kontrollrecht. Auch eine Regelung, die den Auftragnehmer dem Weisungsrecht des Auftraggebers unterwirft und ersteren verpflichtet, Verstöße gegen den Datenschutz seinem Auftraggeber zu melden, muss enthalten sein.

Einen solchen Vertrag hat das Unternehmen mit seinem Hoster nicht geschlossen. Der Thüringer Landesbeauftragte hat das Unternehmen aufgefordert, diesen rechtswidrigen Zustand zu beenden. Dies kann entweder durch Abschalten des Internetshops, den Umzug der Präsenz auf eigene Hardware oder am einfachsten durch Abschluss eines entsprechenden Vertrages über eine Auftragsdatenverarbeitung geschehen.

Jedes Mal, wenn Datenverarbeitungsvorgänge ausgelagert werden und das übernehmende Unternehmen dabei weisungsgebunden bleiben soll, ist ein Vertrag über eine Auftragsdatenverarbeitung zu schließen. Es ist unerheblich, ob die Auslagerung nur vorüberge-

hend, einmal oder regelmäßig erfolgt. Sobald Datenverarbeitungsvorgänge an Dritte gegeben werden, muss ein solcher Vertrag nach § 11 BDGS geschlossen werden.

3.20 Sagst Du es mir nicht, frag‘ ich jemand anderen

Die Mutter eines Betroffenen hat den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) auf ein Gebaren der Arbeitgeberin ihres Sohnes aufmerksam gemacht, welches nicht mit dem Bundesdatenschutzgesetz (BDSG) zu vereinbaren war.
Der Arbeitgeber hatte dem Arbeitnehmer gekündigt. Dieser stellte im Rahmen eines Kündigungsschutzprozesses den Antrag auf Feststellung der Unwirksamkeit eben jener Kündigung. Um sich nunmehr seiner Beweisnot (der Arbeitgeber ist für die Darlegung der Kündigungsgründe beweisbelastet) zu entziehen, nutzte der Arbeitgeber personenbezogene Daten des Arbeitnehmers, die er bei einem weiteren Arbeitnehmer erhoben oder von diesem erlangt hat.
Der TLfDI nahm sodann dahingehend Stellung, dass, soweit die personenbezogenen Daten bei einem Dritten erhoben wurden, dies gegen den Grundsatz der Direkterhebung (beim unmittelbar Betroffenen, dem Sohn) verstoße. Der Gesetzgeber hat die Erhebung von personenbezogenen Daten eines Betroffenen bei Dritten nur in abschließend geregelten Fällen zugelassen, die hier nicht greifen, § 4 Abs. 2 BDSG. Folge sei eine rechtswidrige Erhebung, weswegen auch die darüber hinausgehende Nutzung der Daten unzulässig sei.
Das Gericht nahm die Stellungnahme des TLfDI, die durch den Kläger in den Prozess eingeführt wurde, zur Kenntnis. Allerdings gelangte das Gericht zur Überzeugung, dass die personenbezogenen Daten der beklagten Arbeitgeberin ohne eigenes Zutun durch einen Dritten zugespielt wurden. Mit anderen Worten, nach Feststellung des Gerichts hat die Beklagte die Herausgabe der Daten an sie weder verlangt noch sonst wie gefördert. Damit handelt es sich nicht um eine Erhebung, weswegen auch nicht gegen den Direkterhebungsgrundsatz verstoßen werden kann. Gleichwohl hat sich das Gericht auf Grund der Stellungnahme des TLfDI entschieden, den entsprechenden personenbezogenen Daten eine untergeordnete Rolle zuzuordnen. Dies ist umso mehr begrüßenswert, als dass das Gericht an Aussagen des TLfDI gegenüber einer Prozesspartei ohnehin nicht

gebunden ist und einfache Rechtsverstöße im Zivilrecht kein Beweisverwertungsverbot nach sich ziehen.
Ebenso wie das Gericht nicht an die rechtliche Bewertung des TLfDI gebunden ist, ist dieser auch nicht an die Verlautbarungen des Gerichts gebunden. In einem Ordnungswidrigkeitenverfahren wird derzeit der für den TLfDI maßgebliche Sachverhalt erforscht.

Personenbezogene Daten dürfen grundsätzlich nur beim Betroffenen direkt erhoben werden. Die hiervon zu machenden Ausnahmen sind vom Gesetzgeber in § 4 Abs. 2 BDSG geregelt. So darf man hiervon abweichen, wenn der Gesetzgeber dies in einem anderen Gesetz ausdrücklich geregelt hat oder wenn die Erhebung beim Betroffenen mit einem unverhältnismäßigen Aufwand verbunden ist. Letztere Variante ist aber nur sehr eingeschränkt anwendbar und mit einer strengen Verhältnismäßigkeitsabwägung verbunden.
Wird gegen diesen Direkterhebungsgrundsatz verstoßen, führt dies zur Rechtswidrigkeit der Datenerhebung und deren Nutzung bzw. Speicherung. Ein Ordnungswidrigkeitenverfahren kann die Folge sein.

3.21 Aus der Röhre geguckt: Videogaga 9

Aufgrund eines Hinweises erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon, dass in einem Unternehmen im Raucherraum eine Kamera versteckt angebracht sein sollte. Eine Kontrolle vor Ort ergab, dass es sich um eine Videokamera handelte, die in einer in den Pausenraum ragenden Rohrhülse verborgen war. Dem Unternehmen wurde mitgeteilt, dass der Einsatz dieser Kamera mit dem geltenden Datenschutzrecht nicht vereinbar ist. Eine Videoüberwachung ist nur dann möglich, wenn das Gesetz eine entsprechende Erlaubnisnorm bereithält. Dies deshalb, weil das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich unzulässig ist, es sei denn, es gibt eine Erlaubnisnorm in oder außerhalb des BDSG oder der Betroffene hat eingewilligt (sogenanntes Verbot mit Erlaubnisvorbehalt).
Eine Einwilligung der Arbeitnehmer lag selbstverständlich nicht vor, sie wäre auch unwirksam gewesen, da es im Beschäftigungsverhältnis in der Regel an der Freiwilligkeitsvoraussetzung des § 4 a Absatz 1 Satz 1 BDSG fehlt. Da es sich bei dem Raucherraum

in einem Unternehmen nicht um öffentlich-zugänglichen Raum handelt, kommt als Erlaubnisnorm nicht § 6 b BDSG, sondern nur § 32 BDSG in Betracht. Nach dieser Vorschrift können personenbezogene Daten eines Arbeitnehmers für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Diese Voraussetzungen sind in den allermeisten Fällen der Arbeitnehmerüberwachung nicht gegeben. So auch im vorliegenden Fall. Eine heimliche Videoüberwachung ist nur in absoluten Ausnahmefällen zulässig. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Arbeitnehmers nach § 32 Abs. 1 Satz 2 BDSG nur dann erhoben, verarbeitet oder genutzt werden, wenn vorab zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Arbeitnehmers an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. In der Abwägung wird auch gewichtet, ob den Arbeitnehmern überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich verbleibt. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind ebenfalls von der Überwachung auszunehmen.
Die Kamera wurde laut Aussage des Unternehmens nicht mehr genutzt. Auch wenn eine ungenutzte Kamera keine Daten erhebt, ist sie dennoch unzulässig (siehe hierzu näher Punkt 3.22).
Bei der Vorort-Kontrolle teilte das Unternehmen mit, die Kamera abbauen zu wollen. Dies ist mittlerweile geschehen.

Eine heimliche Videoüberwachung von Arbeitnehmern ist nur in absoluten Ausnahmefällen zur Aufdeckung von Straftaten zulässig. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind von der Überwachung stets auszunehmen.

3.22 Videokameras fast im Wohnzimmer: Videogaga 10

Ganz soweit ist es noch nicht, dass Eigentümer versuchen, Videokameras in den Wohnungen ihrer Mieter unterzubringen. Allerdings hat die digitale Revolution auch nicht vor Wohnblöcken halt gemacht. Vielerorts werden Videokameras in Wohnanlagen installiert, oftmals, ohne dass sich die verantwortliche Stelle Gedanken über die datenschutzrechtliche Zulässigkeit solcher Einrichtungen macht.
Etwas harmloser stellte sich ein Fall dar, der dem TLfDI 2012 zur Bearbeitung vorlag. Auf einen Hinweis hin wurde ein Wohnhaus kontrolliert, welches umfangreich videoüberwacht sein sollte. Tatsächlich wurde im Rahmen der Kontrolle allerdings lediglich eine Kamera festgestellt. Noch dazu war diese nicht einmal in Betrieb. Vielmehr sollte sie als Attrappe eingesetzt werden. Positioniert war die Kamera im Eingangsbereich, wo sich ebenfalls die Klingeltafel sowie die Concierge befanden.
Datenschutzrechtlich sind Videoaufnahmen in Wohnhäusern alles andere als einfach und von Einzelfall zu Einzelfall differenziert zu betrachten. Je nach den festgestellten Umständen finden unterschiedliche, im Bundesdatenschutzgesetz (BDSG) befindliche Normen Anwendung, die die (Un-)Zulässigkeit der jeweiligen Videoüberwachung regeln.
Um das Ergebnis vorweg zu nehmen: Im hiesigen Fall erachtete der TLfDI die eingesetzte Kameraatrappe für zulässig. In ihrer datenschutzrechtlichen Prüfung unterscheiden sich solche Attrappen aber kaum von richtigen Kameras. Dies liegt daran, dass es subjektiv für den Betroffenen keinerlei Unterschied macht, ob eine Kamera in Betrieb oder ausgeschaltet ist. Denn dieser Zustand ist von Außen nicht erkennbar, womit der Überwachungsdruck für den Betroffenen gleichbleibt. Dieser Überwachungsdruck hat in der Regel eine Verhaltensänderung zur Folge, was wiederum einen Eingriff ins allgemeine Persönlichkeitsrecht darstellt. Nach § 1 Abs. 1 BDSG ist Zweck dieses Gesetzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Da durch die täuschend echte Simulation (Attrappe) des Umgangs mit personenbezogenen Daten auch eine Beeinträchtigung des Persönlichkeitsrechts gegeben ist, sind die Grundsätze des BDSG entsprechend heranzuziehen.
Allerdings konnte in diesem Fall nachgewiesen werden, dass im Vorfeld in Form von wiederholtem Vandalismus und ähnlichen

Vorkommnissen zu Lasten des Eigentümers große Schäden entstanden sind, die auch eine echte Kamera zur Ausübung des Hausrechts rechtfertigen würden. Die Videoüberwachung ist zulässig, wenn der Vermieter schwerwiegende Beeinträchtigungen seiner Rechte auf diese Weise verhindern kann und das Recht des Mieters, sich in sämtlichen allen Bewohnern zugänglichen Bereichen unbeobachtet zu bewegen, nicht überwiegt. Die im Einsatz befindliche Videoattrappe im Haupteingangs- und Conciergebereich erschien unter Berücksichtigung der dargelegten bisherigen Schäden und Vorkommnisse in dem Gebäude als zulässig.

Kameras in Wohnbereichen sind wegen des besonders privaten Aufstellungsorts aus datenschutzrechtlicher Sicht besonders heikel. Die Beurteilung der datenschutzrechtlichen Zulässigkeit ist kompliziert, da die rechtliche Einordnung von unterschiedlichen Umständen des Einzelfalls abhängig ist. Zulässig kann eine Kamera im Eingangsbereich sein, wenn es zuvor zu wiederholtem Vandalismus und ähnlichen Vorkommnissen gekommen ist.

3.23 Der betriebliche Datenschutzbeauftragte – woher nehmen?

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) kontrollierte ein IT-Unternehmen, dessen primäres Aufgabenfeld in der Auftragsdatenverarbeitung für andere Unternehmen liegt. Die Kontrolle verlief erfreulich, die juristische Prüfung ist noch nicht abgeschlossen, aber soweit ersichtlich, ergaben sich mit einer Ausnahme aus datenschutzrechtlicher Sicht keine tiefgreifenden Bedenken. Das Angebot des Unternehmens beinhaltet auch Dienstleistungen für Auftraggeber, die als automatisierte Datenverarbeitung unter Umständen einer Vorabkontrolle unterfallen. Dabei handelt es sich in der Regel um automatisierte Verfahren, die in besonderem Maße in Grundrechte Betroffener eingreifen. In solchen Fällen verlangt das Bundesdatenschutzgesetz auch vom Auftragnehmer eines solchen Vertragsverhältnisses, dass dieser einen betrieblichen Datenschutzbeauftragten beschäftigt und zwar, ohne dass es irgendwelcher Mindestanzahlen von Arbeitnehmern bedarf, § 4 f Abs. 1 Satz 6 Bundesdatenschutzgesetz (BDSG).
Zwar hat das kontrollierte Unternehmen einen betrieblichen Datenschutzbeauftragten bestellt, jedoch handelt es sich hierbei um einen der Geschäftsführer, die gleichzeitig auch die einzigen Arbeitnehmer

des Unternehmens darstellen. Genau hierin liegt die Krux. An einen betrieblichen Datenschutzbeauftragten werden zwar keine besonderen Voraussetzungen im Sinne einer besonderen Ausbildung gesetzt, jedoch verlangt das Gesetz in § 4 f Abs. 2 BDSG, dass dieser die erforderliche fachliche Eignung und Zuverlässigkeit besitzt. An der fachlichen Eignung des Geschäftsführers war nichts auszusetzen, doch gehört zur Zuverlässigkeit eines betrieblichen Datenschutzbeauftragten, dass dieser eine gewisse Unabhängigkeit besitzt. Nicht ohne Grund kann einem solchem Datenschutzbeauftragten auch nur unter sehr strengen Voraussetzungen gekündigt werden. Stellt nun ein Mitglied der Geschäftsführung den betrieblichen Datenschutzbeauftragten, ist zumindest ein Interessenkonflikt zwischen den Interessen der Geschäftsführung und denjenigen des Datenschutzes nicht auszuschließen. Daher geht die herrschende Meinung und mit dieser der TLfDI davon aus, dass es in einer solchen Konstellation an der notwendigen Zuverlässigkeit des betrieblichen Datenschutzbeauftragten mangelt. Rechtsfolge ist, dass die Abberufung des betrieblichen Datenschutzbeauftragten verlangt werden kann. Außerdem folgt aus den hier dargestellten Umständen, dass Unternehmen, die nur aus geschäftsführenden Gesellschaftern bestehen, aber gleichzeitig der Bestellung eines Datenschutzbeauftragten bedürfen, entweder für diese Aufgabe einen Arbeitnehmer einstellen oder diese Aufgabe extern vergeben müssen. Sollte die derzeitige Annahme des TLfDI auch nach Abschluss der juristischen Prüfung weiter bestehen, so wird dieser dem Unternehmen gegenüber anordnen, einen Datenschutzbeauftragten wirksam zu bestellen. Darüber hinaus muss das Unternehmen in diesem Fall mit der Einleitung eines Ordnungswidrigkeitenverfahrens rechnen.

Es ist von unbedingter Wichtigkeit, dass Unternehmen selbstständig prüfen, ob sie einen betrieblichen Datenschutzbeauftragten benötigen. Zwar wird auch der TLfDI eine Notwendigkeit der Bestellung feststellen, jedoch ist eine solche mit erheblichen Verwaltungskosten verbunden und kann ein empfindliches Bußgeld nach sich ziehen. Die gesetzlichen Vorschriften zur Bestellungspflicht sind jedoch umfangreich und auch nicht nur von einer Norm abhängig. In nicht eindeutigen Fällen sollte folglich fachkundiger Rat eingeholt werden, gerne auch beim TLfDI. Um ein Bußgeld zu vermeiden, müssen Unternehmen spätestens einen Monat nach Aufnahme Ihrer Tätigkeit

einen Datenschutzbeauftragten bestellt haben, sofern das Gesetz ihnen dies vorschreibt.

3.24 Der Anwalt, nicht immer dein Freund und Helfer – von fragwürdigen Praktiken dubioser Verbraucherschützer und Rechtsanwaltskanzleien

Kommt Ihnen der nachfolgende Sachverhalt vielleicht bekannt vor? Sie waren bis vor kurzem Kunde einer Bank, die nun insolvent ist. Allein das ist meistens schon ein Umstand, der mit nicht wenig Bürokratie und vielen Terminen für Sie verbunden ist. Zu allem Überfluss bekommen Sie dann aber noch ein wenig später Post von einem eingetragenen Verein, der sich, wie sein Name suggeriert, den Verbraucherschutz auf die Fahnen geschrieben hat. Dieser Verein teilt Ihnen mit, dass Sie Kunde der insolventen Bank gewesen sind und er, der Verein, gern bereit ist, nicht nur Ihre Interessen, sondern die Belange vieler weiterer Kunden zu vertreten. Nur gemeinsam sei man stark, um viel versprechende Schadensersatzklagen gemeinsam zu meistern. Ihr gesunder Menschenverstand schaltet sich ein und Sie stellen sich die nahe liegende Frage: Woher haben die meine personenbezogenen Daten? Ihr darauf folgender Anruf bei dem freundlichen Verein bringt immerhin insoweit Klarheit, als dass eine Datenspeicherung lediglich bei dem Auftraggeber des Vereins, einer Rechtsanwaltskanzlei erfolgte. Auf Ihre darauf folgende E-Mail und Anfrage an die Rechtsanwaltskanzlei, woher diese denn bitteschön Ihre personenbezogenen Daten habe, erklärt man Ihnen von dort lapidar: Als Mandant würden Sie in der Rechtsanwaltskanzlei nicht geführt. Soweit im Rahmen der Mandatsbearbeitung zusätzliche Daten Dritter – also auch von Ihnen – gespeichert würden, entstammten diesen öffentlichen Registern bzw. den einsehbaren Unterlagen der Insolvenzgerichte. Eine Nutzung dieser Daten erfolge ausschließlich im Rahmen der Interessenwahrnehmung für Mandanten als geschädigte Kapitalanleger.
An dieser Stelle wird der Sachverhalt auch für den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) interessant. Denn auch in Thüringen haben sich im Berichtszeitraum mehrere Kunden von Banken oder Beteiligungsfonds, die genau denselben Sachverhalt erlebt hatten, an den TLfDI gewandt und ihn gebeten, zu klären, woher die Rechtsanwaltskanzlei

bzw. der „dazwischengeschaltete“ Verein, die personenbezogenen Daten erhalten haben.

Der TLfDI hat mit den ihm zur Verfügung stehenden Mitteln versucht aufzuklären, auf welchem Wege die Rechtsanwaltskanzlei die personenbezogenen Daten erhalten hat. Oftmals waren ihm im Ergebnis aber die Hände aus folgenden Gründen gebunden: Dem TLfDI steht im Ergebnis kein Auskunftsanspruch aus § 38 Abs. 3 Satz 1 Bundesdatenschutzgesetz (BDSG) gegenüber einer Rechtsanwaltskanzlei zu. Dies ergibt sich aus § 1 Abs. 3 Satz 2 BDSG, der bestimmt, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vom BDSG unberührt bleiben. Genau eine solche Verschwiegenheitspflicht hat das Kammergericht Berlin (Entscheidung vom 20. August 2010 – Aktenzeichen 1 Ws (B) 51/07 – 2 Ss 23/07) aus § 43 a Abs. 2 Satz 1 und 2 der Bundesrechtsanwaltsordnung (BRAO) jedoch abgeleitet. Diese Regelungen lauten: „Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist.“

Diese Regelung, die grundsätzlich ihre Berechtigung hat, weil der Rechtsanwalt ein Organ der Rechtspflege ist (§ 1 BRAO), hatte in den konkreten Fällen aber zur Folge, dass dem TLfDI nach Abschluss seiner Recherchen nur die Möglichkeit blieb, die betreffenden Bürgerinnen und Bürger an die Rechtsanwaltskammer Thüringen zu verweisen, um dort noch einmal ihren Sachverhalt vorzutragen. Denn die Rechtsanwaltskammern sind für die Einhaltung des Standesrechts der Rechtsanwälte und die Kontrolle der anwaltlichen Schweigepflicht zuständig.

Abschließend sei noch einmal festgehalten: Es ist nicht die Absicht des TLfDI, an dieser Stelle „einen Stab“ über die redlichen Thüringer Rechtsanwälte zu brechen. Allerdings sind die wenigen „schwarzen Schafe“ unter den Rechtsanwälten in akuter Erklärungsnot, wenn Sie im Rahmen von Akteneinsichten bei Gerichten und Staatsanwaltschaften die kompletten Listen von Bankkunden oder Investoren finden, diese dann zur Akquise neuer Mandanten verwenden und zwecks Ablenkung darüber einen Verein „zwischenschalten“.

Dem TLfDI bleibt es natürlich unbenommen, Rechtsanwaltskanzleien einer datenschutzrechtlichen Kontrolle zu unterziehen.

Wenn Sie auch Post von einem Verbraucherschutzverein erhalten, der Sie als geprellten Bankkunden oder Gesellschafter eines Fonds bei der Wahrnehmung Ihrer rechtlichen Interessen unterstützen will, dann seien Sie auf der Hut. Fragen Sie schriftlich bei dem Verein an, woher dieser Ihre personenbezogenen Daten generiert hat. Verweist der Verein Sie darauf hin an eine Rechtsanwaltskanzlei, so wenden Sie sich in Thüringen an die Rechtsanwaltskammer Thüringen, Bahnhofstraße 46, 99084 Erfurt, damit diese Ihren Fall standesrechtlich überprüfen kann.

3.25 Patientendaten – ab in die blaue Tonne?

Aufgrund einer Beschwerde wurde eine Arztpraxis in Hinblick auf die Einhaltung datenschutzrechtlicher Vorschriften gerade in Bezug auf die ordnungsgemäße Entsorgung und Vernichtung von Dokumenten mit Patientendaten kontrolliert. Angeblich hätten sich in der im Hof frei zugänglichen Papiertonne Patientendaten befunden. Dieser Vorwurf hat sich bei der Kontrolle nicht bestätigt.
Trotzdem soll an dieser Stelle darauf hingewiesen werden, dass bei hochsensiblen Patientendaten, die aufgrund ihrer Schutzbedürftigkeit einem sehr hohen Vertraulichkeitsgrad unterfallen, strenge Anforderungen an die Entsorgung zu stellen sind. Daten auf Papier, welche Rückschlüsse auf bestimmte oder zumindest bestimmbare Personen zulassen, dürfen keinesfalls nach dem Motto: "zerreißen und ab in den Papierkorb" entsorgt werden. Bei Arztpraxen gilt dies insbesondere für Altakten, vertippte Briefe mit bereits ausgefülltem Adresskopf, nicht brauchbare Kopien, fehlerhaft ausgefüllte Rezepte und Überweisungsträger. Es ist notwendig, dass diese Dokumente stets so geschreddert werden, dass eine Wiederherstellung des Inhaltes dauerhaft unmöglich gemacht wird und die einzelnen Papierstücke in keinen Zusammenhang mehr gebracht werden können. Bei der Auswahl des Gerätes ist der erhöhte Vertraulichkeitsgrad der Dokumente ausschlaggebend. Es ist daher notwendig, dass in Arztpraxen Aktenvernichtungsgeräte verwendet werden, die nach der alten DIN-Norm 32757 mindestens die Sicherheitsstufe 4 oder nach der neuen DIN 66399-1 mindestens die Sicherheitsstufe P-5 aufweisen. Erst nach einer solchen Vernichtung ist eine Entsorgung der verbleibenden Papierstücke in der blauen Tonne möglich. Zu beachten ist auch, dass das Sammeln von zu vernichtendem Datenmaterial immer in Behältern erfolgen soll, die vor unbefugtem Zugriff geschützt sind.

Zudem sollte eine schriftliche Dienstanweisung an alle Arbeitnehmer erfolgen, in welcher alle Maßnahmen für eine ordnungsgemäße Entsorgung festgelegt werden. Weitergehend sollte auch deren Einhaltung in regelmäßigen Abständen durch die Ärzte kontrolliert werden. Sollten sowohl größere Datenmengen oder auch nur einzelne Dokumente mit personenbezogenen Daten nicht ordnungsgemäß vernichtet worden sein, so können Ärzten neben Sanktionen nach dem Bundesdatenschutzgesetz, auch die strafrechtliche Verfolgung nach § 203 Strafgesetzbuch (StGB) i. V. m. § 9 der Berufsordnung der Landesärztekammer Thüringen auch ein Berufsverbot gemäß § 70 StGB drohen. Sollte seitens des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit ein solcher Verstoß bei einem Arzt oder Krankenhaus festgestellt werden, wird dieser grundsätzlich der zuständigen Staatsanwaltschaft weitergeleitet.

An eine ordnungsgemäße Vernichtung und Entsorgung von Patientendaten sind besonders strenge Anforderungen zu stellen. Es ist notwendig, dass Dokumente stets so geschreddert werden, dass eine Wiederherstellung dauerhaft unmöglich gemacht wird. In Arztpraxen müssen Aktenvernichtungsgeräte mit mindestens der Sicherheitsstufe 4 der alten DIN-Norm 32757 oder nach der neuen DIN 66399-1 mindestens die Sicherheitsstufe 5 verwendet werden.

3.26 Patientenarmbänder

Nachdem in der örtlichen Presse darüber berichtet wurde, dass in einem Krankenhaus ab sofort alle Patienten mit einem Patientenarmband versehen werden sollen, ging der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) der Sache nach. Zwar ist ein solches Patientenarmband für das Krankenhaus durchaus praktisch. So kann beispielsweise jederzeit festgestellt werden, um welchen Patienten von welcher Station es sich handelt. Dies kann in Fällen, in denen der Patient nicht selbst kommunizieren kann, äußerst wichtig sein. Allerdings ist der Einsatz von Patientenarmbändern aus datenschutzrechtlicher Sicht kritisch zu prüfen, denn die Angaben, die auf dem Patientenarmband gemacht werden, sind grundsätzlich für alle Personen im Krankenhaus, also auch die Mitpatienten und die Besucher, sichtbar. Es ist daher unzulässig, medizinische Informationen, beispielsweise die Zugehörigkeit zu einer bestimmten Station, offen sichtbar auf dem Patientenarmband fest-

zuhalten. Nach § 27 Abs. 3 Satz 1 Thüringer Krankenhausgesetz dürfen Patientendaten nur genutzt werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses erforderlich ist. Die Mitteilung medizinischer Informationen mittels eines Patientenarmbands ist hierzu nicht erforderlich. Auch zur Identifikation ist ein solches Patientenarmband in aller Regel nicht erforderlich, denn die Patienten können im Normalfall selbst die nötigen Angaben machen. Auf Nachfrage teilte das Krankenhaus mit, dass das Tragen des Armbandes freiwillig sei. Der Patient müsse vorab einwilligen. Diese Einwilligung könne auch jederzeit widerrufen werden. Auf dem Armband selbst befinden sich lediglich der Name des Patienten sowie sein Geburtsdatum und ein Strichcode, der der eindeutigen Identifizierung des Patienten dient. Aufgrund der Freiwilligkeit des Angebots und der Tatsache, dass keine medizinischen Informationen aus den auf dem Armband befindlichen Angaben ersichtlich sind, war das Vorhaben aus datenschutzrechtlicher Sicht nicht zu bemängeln.

Patientenarmbänder dienen der Sicherheit der Patienten und dem reibungslosen Ablauf im Krankenhaus. Der Einsatz ist aber nur zulässig, wenn er datenschutzgerecht gestaltet ist und insbesondere keine Gesundheitsdaten auf dem Patientenarmband preisgegeben werden.

3.27 Dashcam – Trashcam: Videogaga 11

Auto, Fahrrad, LKW;
die Dashcam ist dabei – oje.
davor, dahinter, nebendran,
Personen, Unfall, Autobahn,
Dashcam zeichnet’s auf – ein Wahn.

Tatsächlich, und da herrscht Einigkeit,
verfehlt sie die Datenschutz-Zulässigkeit.
Zwar sind schon von Gesetzes wegen
Ausnahmetatbestände vorgegeben,
das Filmen in Familienkreisen
sowie auch von privaten Reisen,
dem Bundesdatenschutz entreißen.

Dashcams muss man,
das sollte man wissen,
nach dem BDSG besser doch missen.
Das Filmen von Unfällen, eigenen - fremden,
um das dann vor Gericht zu verwenden,
ist keine persönliche Tätigkeit,
die vom Anwendungsbereich befreit.

Vom Filmen von öffentlichen Räumen,
darf der Einzelne nur träumen,
es sei denn, man hat das Hausrecht inne
und dieses dabei auch im Sinne.
Ebenfalls, so die Gesetze,
kann aus berechtigtem Interesse
dann aber nur zu bestimmtem Zwecke
die Kamera an des Hauses Ecke.

Darüber hinaus, man glaubt es kaum,
sind schutzwürdige Interessen im Raum.
Erst wenn keine Punkte vorliegen,
dass diese Interessen nicht überwiegen,
wird es mit der Filmerei
mehr als nur `ne Träumerei.

Beim Autofahren, so sei bedacht,
ist die Kamera damit nicht angedacht,
so liegt es nach Natur der Dinge,
auf der Straße wird’s mit dem Hausrecht dünne.
Zwar sind fürs Filmen die eig‘nen Interessen
des Autofahrers nicht sogleich vermessen,
doch beim Aufnehmen anderer im Verkehr,
ist für jeden erkennbar gar nicht schwer,
dass Anhaltspunkte sind vorhanden
für‘s Überwiegen der Interessen der and‘ren,
nämlich gerade auch der Passanten.

Wegen des hier Erreimten sei dem Bürger gesacht,
dass der Datenschützer über den Datenschutz wacht.
Der Verstoß, wie grade berichtet,

wird gern mit Bußgeldern gerichtet.
Daher hier noch ein letzter Satz:
Lieber Besitzer einer Dashcam,
diese gehört ganz schnell in die Trashcan!

Jetzt mal ohne Flachs: Das Betreiben von Autokameras, auch bekannt als Dashcams, insbesondere zum Zwecke der Beweissicherung im Falle eines Unfalls, fällt nicht in den Ausnahmetatbestand der persönlichen oder familiären Tätigkeit, § 1 Abs. 2, Nr. 3 Bundesdatenschutzgesetz (BDSG). Damit ist das BDSG anwendbar und solche Kameras sind nur nach Maßgabe des § 6 b BDSG zulässig. Dessen Voraussetzungen sind jedoch unter keinem Gesichtspunkt erfüllt, da zumindest immer Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen, was absolutes Ausschlusskriterium für die Beobachtung öffentlich zugänglicher Räume ist.
Damit handelt es sich bei solchen Aufnahmen um ein unerlaubtes Erheben und Speichern von personenbezogenen Daten, was als Ordnungswidrigkeit mit einem Bußgeld von bis zu 300.000 € geahndet werden kann.

3.28 Feuermelder mit Augen: Videogaga 12

Über einen anonymen Hinweisgeber wurde dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) der Tipp gegeben, dass ein Arbeitgeber in der Umkleidekabine mit angeschlossenem Duschraum seines Unternehmens eine verdeckte Videoüberwachung – getarnt als Rauchmelder – durchführen würde.
Am Folgetag hat der TLfDI eine vor Ort Kontrolle durchgeführt. Nachdem man die Arbeitnehmer des TLfDI widerwillig auf das Betriebsgelände ließ, musste allerdings festgestellt werden, dass der entsprechende Umkleideraum über Nacht umfassend renoviert wurde. Es roch sogar noch nach Farbe.
Im darauf folgenden Verwaltungsverfahren konnte festgestellt werden, dass der Arbeitgeber mit der Videokamera Einbrüche in die Spinde seiner Arbeitnehmer aufklären wollte. Die Kamera wurde nach einem dokumentierten Einbruch installiert. Es handelte sich dabei um ein sogenanntes Blackbox-System. Die Kamera zeichnete auf eine angeschlossene Festplatte auf, nach 48 Stunden wurde der Speicherinhalt überschrieben, an einen anderen Ort wurden die auf-

genommenen Bilder nicht übermittelt. Insgesamt wurde die Kamera etwa zwei Wochen betrieben. In diesem Zeitraum kam es erneut zu einem Einbruch, die Festplatte wurde ausgebaut, durch ein Fachunternehmen ausgewertet, der Täter ermittelt und ihm gekündigt. Nach dem Vorfall wurde die Festplatte bis jetzt nicht wieder eingebaut. Was vorbildlich klingen mag, ist es leider manchmal nicht, so auch in diesem Fall. Auch wenn aus Sicht des Arbeitgebers alles wunderbar geklappt hat, sind auch im Bereich des Arbeitsverhältnisses datenschutzrechtliche Vorschriften zu beachten. Nicht alles, was zweckmäßig erscheint, ist auch zulässig.
Zwar sieht § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz explizit die Datenerhebung zu Zwecken der Aufklärung von Straftaten im Beschäftigungsverhältnis vor, jedoch sind diese auch nur unter besonderen Voraussetzungen zulässig. Dabei fließt auch mit ein, dass eine Videoüberwachung in einem Umkleideraum anders zu bewerten ist, als eine Videoüberwachung in einem Kassenbereich.
So darf eine heimliche Videoüberwachung nur dann durchgeführt werden, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Bereits der letzte Punkt ist in dieser Konstellation nicht gegeben. Eine verdeckte Videoüberwachung in einem Umkleideraum, der für eine Komplettentkleidung vorgesehen ist, ist fast immer unverhältnismäßig, da hier in einem Maße in die Intim- und damit Persönlichkeitssphäre der Betroffenen eingegriffen wird, die eine Abwägung zu Gunsten der Interessen des Überwachenden fast unmöglich macht. Darüber hinaus wurden in diesem Fall jedenfalls nicht alle anderen Mittel zur Aufklärung ausgeschöpft. Ein Ordnungswidrigkeitenverfahren wurde eingeleitet.

Die (verdeckte) Überwachung von Arbeitnehmern ist nur unter bestimmten Aspekten zulässig und Arbeitgeber müssen beachten, dass die Anforderungen hierfür hoch sind und weiter steigen, je mehr sie in den Intimbereich Ihrer Arbeitnehmer eingreifen. Empfohlen wird, vor der Installation von Videoanlagen den TLfDI um eine Stellungnahme zu bitten.

3.29 Seniorenwohnheim – datenschutzrechtlich keine Idylle

Anlässlich eines Fundes von in einer Plastiktüte verstauten Gesundheitsdaten über Bewohner eines Seniorenheimes unterzog der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) das in Frage kommende Heim einer datenschutzrechtlichen Kontrolle. Hierbei offenbarten sich mehrere datenschutzrechtliche Verstöße: Zum einen mangelte es an einem Datenschutzbeauftragten (§ 4 f Bundesdatenschutzgesetz [BDSG]); zum anderen wurden sämtliche (!) Daten des Seniorenwohnheims an den Mutterkonzern übermittelt, obwohl ein Vertrag zur Auftragsdatenverarbeitung (§ 11 BDSG) nicht existierte. Ein solcher Vertrag existierte ebenfalls nicht hinsichtlich der Inanspruchnahme einer Firma zur Abwicklung von Zahlungsvorgängen. Schließlich mangelte es in erheblichem Umfang an der Festlegung technisch-organisatorischer Maßnahmen (§ 9 BDSG) zur Gewährleistung der Ausführung der Vorschriften des BDSG. Die Leitung des Seniorenwohnheims wurde gebeten, die datenschutzrechtlichen Mängel abzustellen. Der Träger des Seniorenwohnheims hat sich Beistand bei einem Rechtsanwalt gesucht.

Auch Seniorenwohnheime – sofern als nicht-öffentliche Stelle betrieben – unterliegen den Anforderungen des BDSG. Regelungen des BDSG unter anderem zu technisch-organisatorischen Maßnahmen (§ 9 BDSG), zur Auftragsdatenverarbeitung (§ 11 BDSG) und zur Bestellung eines Datenschutzbeauftragten (§ 4 f BDSG) sind einzuhalten.
Datenschutzrechtliche Ordnungswidrigkeits- oder Strafverfahren sind auch hier nicht ausgeschlossen.

3.30 Veröffentlichung personenbezogener Daten auf Gegnerliste durch Kanzlei

Im Berichtszeitraum erreichte den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) die Frage, inwieweit eine Rechtsanwaltskanzlei berechtigt sei, Firmennamen auf einer Gegnerliste zu veröffentlichen.
Eine Gesellschaft bürgerlichen Rechts (GbR) begehrte bei einer Rechtsanwaltskanzlei die Löschung des GbR-Namens von der Inter-

netpräsenz der Kanzlei. Die GbR war zuvor in die Liste der Gegner der Rechtsanwaltskanzlei auf deren Internetseite mit ihrem Firmennamen namentlich aufgenommen worden. Die Mitglieder der GbR befürchteten berufliche und private Nachteile durch die Nennung auf der Internetseite.
Insoweit wurde der TLfDI um datenschutzrechtliche Prüfung sowie Auskunft zur Rechtslage ersucht.
Das Bundesverfassungsgericht (BVerfG) hat in der Entscheidung vom 12. Dezember 2007 (1 BvR 1625/06) die Frage der Werbung mit Gegnerlisten behandelt und die sachliche und unkommentierte Benennung von Unternehmen in Gegnerlisten zu Werbezwecken erlaubt.
Darüber hinaus wurde klargestellt, das allgemeine Persönlichkeitsrecht etwaiger betroffener Firmen werde durch eine solche Nennung nicht verletzt. Das BVerfG hat in seiner Entscheidung anerkannt, dass ein berechtigtes Informationsinteresse potentieller Mandanten zu der Frage, über welche Erfahrung eine Kanzlei bzw. ein Rechtsanwalt verfügt, besteht. Schließlich begründet das BVerfG seine Entscheidung mit dem Grundrecht der Berufsfreiheit, das auch die freie Entscheidung über die Art und Weise der beruflichen Außendarstellung schütze.
Die Gegnerliste auf der Homepage der Rechtsanwaltskanzlei enthielt keine Wertungen dahingehend, dass eventuell ausgesprochene Abmahnungen oder Forderungen an die Fima sowie an die anderen in der Liste genannten Gegner berechtigt oder unberechtigt waren. Dies wurde auch ausdrücklich in der Kopfzeile der Gegnerliste klargestellt. Unter dem Link war lediglich eine – nicht abschließende – Liste von Gegnern veröffentlicht. Dabei ging es um urheber- und medienrechtliche Angelegenheiten. Nach außen sollte diese Liste darstellen, gegen welche Gegner eine Beratung, eine außergerichtliche oder auch gerichtliche Vertretung der Mandantschaft erfolgt war und damit die Erfahrungen der Rechtsanwälte auf diesem Rechtsgebiet widerspiegeln.
Eine solche Nutzung wurde durch das BVerfG als zulässig erachtet.
Aus datenschutzrechtlicher Sicht konnte daher keine Löschung des Firmennamens von der Gegnerliste der Rechtsanwaltskanzlei erwirkt werden.

Das Bundesverfassungsgericht hält (Aktenzeichen 1 BvR 1625/06) die wertungsfreie Nutzung von Firmennamen auf sogenannten Gegnerlisten von Rechtsanwälten für zulässig.
Das Namensrecht als Teil des allgemeinen Persönlichkeitsrechts ist hier im Rahmen der konkreten Bewertung von untergeordneter Bedeutung, da gerade juristische Personen und Personengesellschaften (beispielsweise auch die GbR) sich über einen öffentlichen Auftritt im Geschäftsleben (beispielsweise über Internetseiten) definieren. Insoweit gilt der Grundsatz über die Selbstbestimmung einer Nutzung des Namens (Zeit, Ort und Medium) nur eingeschränkt.

3.31 Ein Autohaus in den Fängen des Autokonzerns: Videogaga 13

Bei der Kontrolle des Autohauses kamen vielschichtige Datenschutzprobleme zum Vorschein. Es wurde festgestellt, dass eine Videokamera existiert, die allerdings nicht in Betrieb war. Die Firma wurde darauf hingewiesen, dass beim Einsatz von Attrappen zwar keine Verarbeitung personenbezogener Daten und damit auch keine Beobachtung im Sinne von § 6 b Bundesdatenschutzgesetz stattfindet. Eine für echt gehaltene Attrappe wird jedoch von den betroffenen Bürgern ebenso als Grundrechtseingriff empfunden wie eine tatsächlich funktionierende Kamera. Da die Videobeobachtung an der Stelle, an der sich die Kamera befand, nicht zulässig gewesen wäre, wurde der Inhaber gebeten, die Kamera zu entfernen.
Die Verwaltung der Kundendaten im Autohaus war datenschutzgerecht. Ein Problem bestand allerdings darin, dass in dem Autohaus vornehmlich Kraftfahrzeuge eines bestimmten Herstellers veräußert wurden. Dieser Hersteller, der seinen Sitz nicht in Thüringen hat, verlangte von dem Autohaus, dass die Daten der Arbeitnehmer bei dem Autokonzern gespeichert werden. Auch die Werbeansprache der Kunden des Autohauses erfolgte durch den Autokonzern, bei dem alle Kundendaten gespeichert waren. Entsprechende Verträge des Autohauses mit dem Konzern zur Auftragsdatenverarbeitung konnten allerdings nicht vorgelegt werden. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat den am Sitz des Autokonzerns zuständigen Landesdatenschutzbeauftragten mit der Angelegenheit befasst.
Weiterhin betreibt das Autohaus einen Autoverleih in Form eines Franchisings. Der Kunde muss vor der Ausleihe eines Fahrzeugs den Personalausweis und den Führerschein vorlegen. Die Dokumente

werden kopiert und die Kopien zu den Akten genommen. Nach § 14 Nr. 2 des Personalausweisgesetzes (PAuswG) darf die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises durch nichtöffentliche Stellen nur nach §§ 18 bis 20 PAuswG erfolgen. Danach ist das Anfertigen von Kopien datenschutzrechtlich nicht zulässig, es sei denn, sie ist durch eine spezielle gesetzliche Ermächtigung erlaubt (siehe hierzu genauer Punkt 3.48). Zum Nachweis der Identität eines Kunden ist es ausreichend, sich den Personalausweis vorlegen zu lassen und hierüber einen Vermerk zu machen, der allein die notwendigen Identitätsdaten enthält. Da der Franchisegeber aber die Anfertigung der Kopien verlangt, steht der TLfDI weiterhin im Dialog mit den Beteiligten. Bereits mehrfach fanden zur datenschutzrechtlichen Bewertung der Einzelprobleme Termine statt, an der auch Vertreter der Handwerkskammer teilnahmen. Hier ist noch einige Überzeugungsarbeit zu leisten.

Ein rechtlich selbständiger Betrieb ist die für die Datenverarbeitung verantwortliche Stelle. Auch wenn er Beziehungen zu einem größeren Konzern hat, darf er seine Daten nicht ohne einen den gesetzlichen Anforderungen entsprechenden Auftragsdatenverarbeitungsvertrag übermitteln.
Das Erstellen von Personalausweiskopien ist zum Nachweis der Identität einer Person nicht erforderlich, wenn der Personalausweis eingesehen werden kann. Kopien sind damit unzulässig.

3.32 Finger von der Wurst: Videogaga 14

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte sich mit einem Bauern auseinanderzusetzen, der in seinen Verkaufsstellen für landwirtschaftliche Produkte eine umfangreiche und nahezu flächendeckende Videoüberwachung durchführte. In einer Filiale war gar der einzige unbeobachtete Ort die Arbeitnehmertoilette. Auf Nachfrage meinte der Betreiber, die Videoüberwachung sei notwendig, weil er vermutet, dass immer mal eine Scheibe Wurst fehle. Mit dem Bundesdatenschutzgesetz (BDSG) ist eine solche Videoüberwachung von Arbeitnehmern und Kunden selbstverständlich nicht zu vereinbaren. Zwar sieht das BDSG die Möglichkeit der Datenerhebung zu Aufklärung von Straftaten im Arbeitsverhältnis vor, jedoch nur in sehr engen Grenzen und

vor allem in verhältnismäßigem Rahmen. Jedenfalls muss eine solche Videoüberwachung das allerletzte Mittel sein. Vorher muss z. B. bei Diebstahlverdacht eine Taschenkontrolle unter Heranziehung der örtlichen Polizei erfolgen. Die Kameras waren jedenfalls zu entfernen.
In diesem Fall musste der TLfDI die Einhaltung des BDSG nicht mit Hilfe einer Anordnung durchsetzen. Der Betreiber der Läden hat einen Rechtsanwalt hinzugezogen, der seinen Mandanten davon überzeugen konnte, der Aufforderung des TLfDI Folge zu leisten.

Eine Arbeitnehmerüberwachung zur Aufdeckung von Straftaten ist nur dann zulässig, wenn diese Überwachung das letzte zur Verfügung stehende Mittel ist und alle anderen Möglichkeiten erfolglos durchgeführt worden sind. Außerdem muss die Überwachung in Hinblick auf die vermeintliche Straftat verhältnismäßig sein. Wegen des Diebstahls einer Wurstscheibe ist eine Videoüberwachung in jedem Fall unzulässig.

3.33 … bis zur Bahre: Patientenakten am Ende

Nach der Insolvenz eines Arztes oder einer Einrichtung zur ambulanten medizinischen Versorgung stellt sich immer die Frage, was mit den Patientenakten passiert. Bei Patientenakten handelt es sich nach § 3 Abs. 9 des Bundesdatenschutzgesetzes (BDSG) um besondere Arten von personenbezogenen Daten, da sie Angaben über die Gesundheit enthalten. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 und Abs. 7 BDSG nur unter den dort genannten Voraussetzungen zulässig. In einem vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) zu untersuchenden Fall hatte sich ein Nachfolger für die Arztpraxis gefunden. Aufgrund einer Eingabe war zu untersuchen, wie bei der Übernahme durch den neuen Praxisinhaber mit den Patientendaten des bisherigen Arztes verfahren wurde. Im Rahmen einer Vor-Ort-Kontrolle wurde geprüft, wie Patientendaten aufbewahrt werden. Dort konnte festgestellt werden, dass es im Hinblick auf die elektronischen Patientendaten eine Trennung gab. Die Patientendaten der übernehmenden Praxis waren auf dem dortigen Server gespeichert. Die elektronischen Patientendaten der übernommenen Praxis waren separat auf einer USB-Platte gesichert. Die Papierakten der übernommenen

Praxis wurden in einem von der übrigen Praxis getrennten abgeschlossenen Raum aufbewahrt. Grundsätzlich unterliegen diese Patientendaten (der übernommenen Praxis) nicht dem Zugriff des neuen Inhabers. Diese werden nur im Falle der Einwilligung des Patienten für die neue Praxis aktiviert. Eine Übernahme der elektronischen Akten ist nicht möglich. Sofern Befunde benötigt werden, werden diese ausgedruckt und zu den Akten der übernehmenden Praxis genommen. Zugriff auf die Patientendaten des übernommenen Arztes, die sich in Akten befinden, wird nur genommen, wenn der Patient hiermit einverstanden ist. Dieses Verfahren war datenschutzrechtlich nicht zu beanstanden.
Beim Praxisverkauf oder bei der Praxisübernahme ist zu beachten, dass der übernehmende Arzt nicht automatisch ein Zugriffsrecht auf die Patientendaten der übernommenen Praxis hat. Gemäß § 203 Abs. 1 Satz 1 Strafgesetzbuch wird derjenige mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, der unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis offenbart, welches ihm als Arzt anvertraut wurde. Der Verkauf einer Praxis oder die Insolvenz stellt dabei keine Befugnis dar, die anvertrauten Geheimnisse einem anderen Arzt zu offenbaren. Für die Übernahme der Patientenakten muss es daher eine Einwilligungserklärung aller Patienten geben. Diese kann im Rahmen der laufenden Behandlung mündlich erfolgen, alle anderen Patienten müssen schriftlich befragt werden. Bei der Praxisübernahme wird daher oft auf das so genannte Zwei-Schrank-Modell zurückgegriffen. Dabei werden die übernommenen Patientenakten zunächst separat im ersten Schrank aufbewahrt. Sobald das Einverständnis erteilt worden ist, werden die Akten dann im laufenden System der übernehmenden Praxis eingefügt (zweiter Schrank).

Die Verpflichtung zur ärztlichen Schweigepflicht besteht auch bei der Übernahme einer Praxis an einen anderen Arzt. Sämtliche Patienten müssen um ihr Einverständnis zur Weitergabe ihrer Gesundheitsdaten gebeten werden.

3.34 Argusaugen wachen über Material…oder vielleicht doch über die Arbeitnehmer?: Videogaga 15

Aufgrund der Vorgaben des europäischen Rechts zur Schaffung unabhängiger Aufsichtsbehörden für den Datenschutz auch im nicht-

öffentlichen Bereich, was der Europäische Gerichtshof in seinem Urteil vom 9. März 2010 Az. C-518/07 Kommission ./. Bundesrepublik Deutschland unterstrichen hat, ging der Zuständigkeitsbereich für den nicht-öffentlichen Bereich vom Thüringer Landesverwaltungsamt (TLVwA) auf den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) über. Mit Übernahme der Zuständigkeit des nicht-öffentlichen Bereiches hat der TLfDI verschiedene Verfahren vom TLVwA übernommen. So auch einen besonders krassen Fall von Arbeitnehmerüberwachung. Unter dem Deckmantel des Verarbeitens besonders wertvoller Materialien betreibt das Unternehmen sechzehn Kameras, von denen eine Vielzahl direkt auf die Arbeitsplätze der Arbeitnehmer ausgerichtet sind, sodass auf den betroffenen Arbeitnehmer ein massiver Überwachungsdruck ausgeübt wird. Besonders intensiv ist die Videoüberwachung in einem Büro gestaltet. Dort werden zwei Computerarbeitsplätze aus nächster Nähe videoüberwacht. Begründet wird dies damit, dass es sich um die Entwicklungsabteilung handele und die Daten höchster Geheimhaltung unterlägen. Darauf kommt es allerdings nicht an. Das informationelle Selbstbestimmungsrecht der Arbeitnehmer überwiegt das Interesse des Arbeitgebers in einem solchen Fall nahezu immer. In jedem Fall war die Speicherdauer aller Kameras mit mehreren Wochen unabhängig von deren Zulässigkeit zu lang gewählt. Auch rechtmäßig erhobene Daten dürfen nur so lange vorgehalten werden, wie dies nach deren Zweck notwendig ist. Zur Aufklärung eventueller Verstößen sind hierfür in der Regel 48 Stunden und über das Wochenende (Freitag - Montag) 72 Stunden ausreichend.

Mit Übernahme des Verfahrens hat der TLfDI eine Kontrolle durchgeführt, durch die oben genannte Umstände erst festgestellt werden konnten. Dem Unternehmen wurde mitgeteilt, dass die Art und Weise der durchgeführten Videoüberwachung unzulässig ist, was das Unternehmen dazu veranlasste, einen Rechtsanwalt einzuschalten. Der Geschäftsführer möchte gern an der Videoüberwachung seiner Arbeitnehmer festhalten.

Nach langwieriger und aufwendiger Korrespondenz mit der Interessenvertretung des Unternehmens ist der TLfDI nunmehr zur Erkenntnis gelangt, dass hier auf ein Einsehen und Einhalten der datenschutzrechtlichen Regelungen nicht zu hoffen ist. Es ist eine Anordnung in Vorbereitung, die die Deinstallation der meisten Kameras verlangen wird. Mit einem langjährigen und aufwendigen verwal-

tungsgerichtlichen Verfahren ist zu rechnen. Wie in allen Fällen der unzulässigen Videoüberwachung ist hier die Einleitung eines Ordnungswidrigkeitenverfahrens naheliegend.

§ 32 Bundesdatenschutzgesetz regelt, dass das Erheben und Verarbeiten von Arbeitnehmerdaten nur dann zulässig ist, wenn dies für die Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Bei einer Videoüberwachung ist dies in aller Regel nicht der Fall. Daher gilt: Jede Videokamera, die auf Arbeitsplätze oder sonstige Orte gerichtet ist, an denen sich Arbeitnehmer regelmäßig aufhalten, ist unzulässig. Lediglich zur Aufklärung von Straftaten hat der Gesetzgeber unter engen Voraussetzungen das Erheben und Verarbeiten von Arbeitnehmerdaten zugelassen. Dabei darf es sich allerdings nur um das allerletzte Mittel handeln und es müssen vorher dokumentierte Vorfälle vorgelegen haben. Außerdem bedarf es einer umfangreichen Verhältnismäßigkeitsprüfung.

3.35 Einkauf unter Beobachtung: Videogaga 16

Aufgrund einer Beschwerde erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) davon Kenntnis, dass in einem Lebensmittelladen großflächig eine Videoüberwachung betrieben wird. Eine Kontrolle vor Ort bestätigte dies. In dem Geschäft wurden insgesamt zahlreiche Domekameras eingesetzt, die sämtlich an der Decke des Marktes installiert waren. Die Aufnahmen der im angegliederten Getränkemarkt befindlichen Kameras wurden nicht aufgezeichnet. Die übrigen Kameras waren vorzugsweise in den Gängen zu den Regalen angebracht. Eine direkte Überwachung fest eingerichteter Arbeitsplätze konnte nicht festgestellt werden. Diese Aufnahmen wurden über 24 Stunden gespeichert und dann überschrieben. Der Festplattenrecorder und die Bildschirme zu den Kameras befanden sich in einem separaten Büro der Geschäftsleitung, zu dem nur der Geschäftsleiter und sein Stellvertreter Zutritt hatte. Der Anzeige- und Beobachtungsbildschirm sind beide abschaltbar sowie durch ein Passwort und einen besonderen Schalter mit einem Sicherheitsschlüssel, über den nur die Geschäftsleitung und eine Sicherheitsfirma verfügt, gesichert. Die Anlage wird rund um die Uhr betrieben, allerdings sind die Bildschirme nur in

Betrieb, wenn sich entweder die Geschäftsstellenleitung oder ein Sicherheitsmann im Büro aufhalten.
Der TLfDI stellte fest, dass der Markt zunächst seiner Hinweispflicht nach § 6 b Abs. 2 Bundesdatenschutzgesetz (BDSG) nicht hinreichend nachgekommen war. Zwar existierten Schilder. Diese waren jedoch so angebracht, dass die von der Videoüberwachung Betroffenen den Umstand der Videoüberwachung nicht ohne weiteres erkennen konnten. Auf Aufforderung des TLfDI hin wurde dies geändert.
Zum Zweck der Videoüberwachung gab der Geschäftsstellenleiter glaubhaft an, dass es in der Vergangenheit im verstärkten Maße zu Diebstählen gekommen war. Die Kameras sollen dazu dienen, Diebstähle verfolgen zu können und sollen auch eine abschreckende Wirkung erzielen.
Bei dem Lebensmittelladen handelt es sich um einen öffentlich zugänglichen Raum. Daher ist nach § 6 b Abs. 1 BDSG die Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Geschäftsstellenleitung konnte glaubhaft machen, dass die Videoüberwachung zur Wahrnehmung des Hausrechts bzw. zur Wahrnehmung berechtigter Interessen erforderlich ist. In den ersten Monaten nach der Kamerainstallation wurden zahlreiche Diebstähle registriert, diese hatten sich nachweislich bis zum Kontrollzeitpunkt signifikant reduziert. Allerding bestanden aufgrund der Vielzahl der angebrachten Kameras Anhaltspunkte dafür, dass schutzwürdige Interessen der Betroffenen überwogen. Bis auf den Kassenbereich wurde der Markt nahezu komplett videoüberwacht. Hier musste eine Abwägung erfolgen zwischen den durch die Zwecke der Videoüberwachung grundrechtlich geschützten Positionen des Geschäftsinhabers und dem Grundrecht auf informationelle Selbstbestimmung derjenigen, die Objekt der Videoüberwachung sind. Die permanente lückenlose Überwachung mit Aufzeichnung eines bestimmten Raumes, der sich der Betroffene nicht entziehen kann, stellt einen sehr weitreichenden Grundrechtseingriff dar. Der im Markt einkaufende Kunde sowie auch der dort beschäftigte Arbeitnehmer hat keine Möglichkeit, sich der Videoüberwachung zu entziehen. Der Kunde ist nahezu während des gesamten Einkaufs und der Arbeitnehmer während der gesamten Arbeitszeit unter Beobachtung. Der TLfDI unterzog daher sämtliche Kameras einer eigenen datenschutzrechtlichen Bewertung und kam

mit dem Inhaber des Lebensmittelmarkes überein, dass ein Drittel der Kameras abzuschalten ist. Es wurde außerdem im Datenschutzkonzept schriftlich festgelegt, unter welchen konkreten Voraussetzungen die Auswertung der Bilddaten möglich ist.

Videoüberwachung kann im Einzelhandel zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen zulässig sein. Allerdings darf keine permanente und lückenlose Überwachung stattfinden, der sich Kunden oder Arbeitnehmer nicht entziehen können. Zur Auswertung von Videomaterial müssen konkrete schriftliche Festlegungen getroffen werden.

3.36 Weniger ist mehr: Reduzierung von Videokameras in einer Einkaufsgalerie: Videogaga 17

Im Düsseldorfer Kreis – einem Arbeitskreis derjenigen Landesdatenschutzbeauftragten und des Bayerischen Landesamtes für Datenschutzaufsicht, die auch für den nicht-öffentlichen Bereich zuständig sind[a] – wurde die Zulässigkeit des Einsatzes von Videoüberwachung in den Einkaufszentren eines europaweit agierenden Unternehmens, das auch in Deutschland Einkaufszentren betreibt, diskutiert. Zu diesem Zweck wurden die datenschutzrechtlichen Aufsichtsbehörden um Vorort-Besichtigungen in den Einkaufszentren im jeweiligen Zuständigkeitsbereich gebeten. Ziel der Kontrollen war nicht die Videoüberwachung in den einzelnen Geschäftslokalen, sondern in der Einkaufspassage selbst. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) hatte diese Aufgabe vom vormals zuständigen Thüringer Landesverwaltungsamt übernommen. Dieses hatte festgestellt, dass in der Einkaufspassage 16 Kameras installiert waren. Die Kontrollen der Aufsichtsbehörden zeigten offensichtlich Wirkung, sodass sich das Unternehmen zu einem bundesweiten Abbau von Kameras in seinen Einrichtungen entschloss. Zum Zeitpunkt der Vorort-Kontrolle durch den TLfDI gab es im Einkaufszentrum noch lediglich drei Kameras, deren Betrieb einer datenschutzrechtlichen Beurteilung unterzogen wurde. Das Management konnte schlüssig darlegen, dass die von den verbliebenen Kameras überwachten Bereiche zur Verhinderung und Verfolgung von Straftaten (Aufbrüche, Warendiebstähle, Drogende-

[a] Siehe Punkt 2

likte) und hohen Sachschäden (durch unachtsames Rangieren von LKWs) zur Wahrnehmung des Hausrechts erforderlich sind. Kritik übte der TLfDI an den nicht ausreichend angebrachten Hinweisen auf die Videoüberwachung sowie die Beobachtung einer benachbarten, nicht zum Einkaufzentrum gehörenden Einfahrt. Die festgestellten Mängel wurden durch das Einkaufszentrum kurzfristig beseitigt.

Oftmals wird durch die Reduzierung der Anzahl von Videokameras der gesetzlich zugelassene Zweck ebenfalls erreicht und gleichzeitig schutzwürdige Interessen der Betroffenen werden nicht überwiegend beeinträchtigt.

3.37 Hotel California: Videogaga 18

In diesem bekannten Lied wird ein Hotel besungen, das, einmal betreten, zwar wieder verlassen werden kann, es richtig hinter sich zu lassen, ist jedoch unmöglich. So ähnlich ist das auch mit einem Thüringer Hotel, wobei es hier weniger um Sehnsüchte als mehr um Videokameras geht. Wollten Sie schon immer mal wissen, mit wem Ihr Partner in diesem Hotel am Frühstücktisch saß? In diesem Hotel bislang kein Problem, sofern der Geschäftsführer Sie an die Videodaten lässt.
Sämtliche Gemeinschaftsbereiche des Hotels sind videoüberwacht. Dies beginnt beim Frühstücksraum und endet beim Billardraum. „Selbstverständlich“ zeichnen alle Kameras auf, das ist ja auch Stand der Technik. Aufgefallen ist das Hotel aber seltsamerweise nicht, weil sich Gäste beschwert haben, sondern weil auch der Außenbereich des Hotels überwacht wird und sich Dritte zu Recht gestört fühlen.
Tatsächlich ist es nicht so, dass Videoüberwachung in einem Hotel per se unzulässig ist. Allerdings sind die Hürden hierfür sehr hoch anzusetzen. Was jedoch vollkommen unzulässig ist, ist die Überwachung von Räumen, die der Erholung und Freizeitgestaltung dienen.
Videoaufnahmen von Personen stellen personenbezogene Daten dar. Der Umgang mit diesen, also das Erheben, Verarbeiten und Nutzen, ist nur dann zulässig, wenn das Bundesdatenschutzgesetz (BDSG) oder ein anderes Gesetz hierfür eine Erlaubnisvorschrift bereithält oder der einzelne Betroffene in den Umgang mit diesen Daten eingewilligt hat, § 4 Abs. 1 BDSG. Es handelt sich um ein so genanntes Verbot mit Erlaubnisvorbehalt.

Für öffentlich zugängliche Räume, und um solche handelt es sich bei Hotelräumen, die für alle Hotelgäste zugänglich sind, hat der Gesetzgeber die Zulässigkeit von Videobeobachtung und Speicherung dieser Daten abschließend geregelt. Diese in § 6 b BDSG getroffene Regelung verfügt über einen abgestuften Voraussetzungskatalog, der zur Unzulässigkeit der Beobachtung und/oder Speicherung führt, wenn einer der Punkte nicht erfüllt wird.
So ist eine Videobeobachtung öffentlich zugänglicher Räume nur dann zulässig, wenn diese zur Durchsetzung des Hausrechts oder für berechtigte Interessen zu konkret festgelegten Zwecken erforderlich ist. Darüber hinaus dürfen keine Anhaltspunkte dafür vorhanden sein, dass schutzwürdige Interessen der Betroffenen überwiegen.
Ähnlich wie bei der Überwachung von Gasträumen in Gaststätten ist die Videoüberwachung von Aufenthalts- und Essensräumen in Hotels immer unzulässig, da hier immer Anhaltspunkte dafür vorhanden sind, dass die schutzwürdigen Interessen Betroffener die des Überwachenden überwiegen. Diese Räume stehen den Gästen zur Verfügung, um einer ungestörten Entfaltung der Persönlichkeit im Rahmen der Freizeitgestaltung nachzugehen. In dieser Entfaltung der Persönlichkeit könnten sich einzelne Personen durch die Videoüberwachung gehemmt fühlen. Zum Beispiel in der Frage, mit wem man sich an einen Frühstückstisch setzt.
Die bei der Kontrolle auch geprüfte Videoüberwachung im Außenbereich war in Teilen ebenfalls unzulässig. Insbesondere eine Kamera, die Teile des Nachbargrundstücks erfasste, ist von Erlaubnistatbeständen des BDSG nicht mehr gedeckt bzw. überhaupt nicht vorgesehen. So ist in § 6 b BDSG die Beobachtung öffentlich zugänglicher Bereiche geregelt. Um solche handelt es sich bei einem privaten Nachbargrundstück aber in der Regel und auch hier nicht. Daneben käme noch § 28 BDSG in Betracht, welcher den Datenumgang zu eigenen Geschäftszwecken regelt. Allerdings handelt es sich bei der Beobachtung des Nachbargrundstücks nicht um die Erfüllung eigener Geschäftszwecke, weswegen auch diese Norm als Erlaubnistatbestand ausscheidet.
Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) wird gegen das betroffene Hotel in Kürze eine Anordnung erlassen, die darauf abzielt, datenschutzrechtlich konforme Zustände durchzusetzen. Darunter fällt auch die Demontage einiger Kameras. Ein Bußgeldverfahren ist wahrscheinlich.

Videoüberwachung in Bereichen, die der Freizeitgestaltung dienen, ist unzulässig. Hierzu zählen auch die entsprechenden Räume in Hotels, die allen Gästen zugänglich sind. Sollten Sie eine solche Videoanlage bemerken, wenden Sie sich bitte an den TLfDI, damit dieser der Sache nachgehen kann.

3.38 Video *vor* dem Kaufhaus – zulässig?: Videogaga 19

Erfreulicherweise meldete sich wieder einmal ein Bürger beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und gab an, im Eingangsbereich eines Kaufhauses würden Videoaufnahmen gefertigt, die auch den öffentlichen Verkehrsraum erfassten; zudem fehle ein Hinweisschild zu den Videokameras.
§ 6 b Bundesdatenschutzgesetz (BDSG) erlaubt nicht-öffentlichen Stellen die Videoüberwachung zur Wahrnehmung des Hausrechts und berechtigter Interessen für konkret festgelegte Zwecke, soweit dies *erforderlich* ist *und schutzwürdige Interessen der Betroffenen nicht überwiegen.*
Selbst wenn – etwa aufgrund vorhergegangener Straftaten (z. B. Diebstahl, Sachbeschädigung, Graffiti) – eine Videoüberwachung eines Kaufhaus*eingangs*bereichs erforderlich erscheint, weil für die Betroffenen (Passanten) weniger belastende Maßnahmen nicht (mehr) in Betracht kommen, so scheitert eine Videoüberwachung gleichwohl an den überwiegenden Interessen der Passanten, wenn (auch) der öffentliche Verkehrsraum videografiert wird. Die Schutzbedürftigkeit dieser öffentlichen Räume ist hoch, da sich hier Menschen typischerweise länger aufhalten und untereinander kommunizieren. Der Videoüberwachung auszuweichen, etwa durch einen Wechsel der Straßenseite, wird infolge der zunehmenden Überwachungsdichte immer schwieriger nicht mehr in Betracht. Diese auch von der Rechtsprechung vertretenen Positionen kamen in dem von der Bürgerin beanstandeten Fall jedoch nicht zum Tragen, denn einerseits wurde der öffentliche Verkehrsraum nur in unerheblichem Maße videografiert – die Rechtsprechung lässt je nach der Ausgestaltung des Einzelfalls zu, dass der öffentliche Raum in einer Breite von bis zu 1 Meter aufgenommen wird. Diese richterrechtlichen Vorgaben waren in concreto eingehalten. Zum anderen existierte tatsächlich ein entsprechendes Hinweisschild (§ 6 b Abs. 2 BDSG). Bei dieser Gelegenheit: Ein Schild, das auf eine Videoüberwachung

hinweist, macht diese nicht rechtmäßig. Vielmehr ist auf eine rechtmäßige (!) Videoüberwachung mittels Schildes hinzuweisen! Dabei ist auch die für die Videoüberwachung zuständige Stelle zu benennen.

Die Videoüberwachung öffentlich zugänglicher Räumen durch nichtöffentliche Stellen richtet sich nach § 6 b BDSG.
Selbst wenn danach eine Videoüberwachung als erforderlich zu qualifizieren sein mag, überwiegt das nach dieser Norm zu berücksichtigende schutzwürdige Interesse der Betroffenen (Passanten) grundsätzlich, wenn der öffentliche Verkehrsraum videoüberwacht wird.
Die Videoüberwachung ist dann datenschutzrechtswidrig. Auch ein Schildchen, das auf die Videoüberwachung hinweist, hilft dann nicht mehr. Denn nicht das Schildchen macht die Videoüberwachung rechtmäßig, sondern auf eine rechtmäßige(!) Videoüberwachung muss das Schildchen hinweisen!

3.39 Datenschutz gerade auch in Frauenschutzeinrichtungen

Aufgrund einer Beschwerde brachte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in Erfahrung, dass in einem neu entworfenen Verfahren der Leistungsgewährung und Abrechnung von Frauenschutzeinrichtungen durch das Landratsamt des Unstrut-Hainich-Kreises eine datenschutzrechtlich unzulässige Forderung vorgesehen war. Nach dem Vertrag zwischen Landkreis und dem privaten Träger des Frauenhauses sollten personenbezogene Daten (Name, Wohnanschrift) der von Gewalt betroffenen Frauen und Kinder unverzüglich per Fax an das Landratsamt weitergeleitet werden.
Indem sich das Landratsamt diese Daten von betroffenen Frauen und Kindern zuleiten lässt, erhebt es Daten im Sinne des Thüringer Datenschutzgesetzes (ThürDSG). Dies ist nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist, § 19 Abs. 1 ThürDSG. Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben, § 19 Abs. 2 Satz 1 ThürDSG. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn entweder eine Rechtsvorschrift dies vorsieht oder die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen erforderlich macht oder die Erhebung

beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Allerdings ist die Erhebung bei Dritten in den beiden zuletzt genannten Fällen nur zulässig, wenn keine Anhaltspunkte dafür vorliegen, dass überwiegend schutzwürdige Interessen des Betroffenen beeinträchtigt werden, § 19 Abs. 2 Satz 2 ThürDSG.
Nach Auffassung des TLfDI war eine Erforderlichkeit für die Übermittlung des Namens und der Wohnanschrift der von der Gewalt betroffenen Frau bzw. des Kindes in nicht anonymisierter Form nicht gegeben. Dem Landratsamt muss es zwar möglich sein, die zweckentsprechende Verwendung öffentlicher Gelder im Einzelfall nachprüfen zu können. Dazu reicht es jedoch aus, dass die jeweilige Einrichtung dem Landratsamt die Zahl der sich in dieser Einrichtung aufhaltenden Frauen und Kinder regelmäßig übermittelt. Die erforderliche Kontrolle durch das Landratsamt kann durch stichprobenartige Einsicht in die Belegungslisten gewährleistet werden. Im Hinblick darauf, dass die Arbeitnehmer des Landratsamtes der Amtsverschwiegenheit unterliegen, ist im Regelfall nicht davon auszugehen, dass gegen die Einsichtnahme bei Stichproben schutzwürdige Interessen des Betroffenen überwiegen. Treten jedoch besondere Konstellationen auf, wie z. B. die Unterbringung der Frau eines Bediensteten der entsprechenden Behörde des Landratsamtes, so können im Einzelfall durchaus schutzwürdige Interessen der Frauen am Ausschluss der Datenerhebung vorliegen.
Das Landratsamt nahm die Stellungnahme des TLfDI zum Anlass, den Vertrag zu überarbeiten. In der neu abzuschließenden Vereinbarung wurde ein Ablauf festgelegt, nach dem die Einrichtung Namen und Wohnanschrift der Betroffenen nicht standardmäßig erheben und übermitteln wird.

Es ist nicht zulässig, dass das Landratsamt personenbezogene Daten der von Gewalt betroffenen Frauen und Kinder von einer Frauenschutzeinrichtung erhebt. Stichprobenartige Kontrollen können zum Zweck der Leistungsprüfung im Einzelfall zulässig sein.

3.40 Vorsicht bei Gesundheitsdaten!

Aufgrund einer Nachfrage der Landesapothekerkammer erlangte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) von einem geplanten sozialen Projekt Kenntnis. Von den Initiatoren des Projekts war geplant, Bedürftigen mithilfe

eines Sponsorenkontos bei verschreibungsfreien Medikamenten einen Sonderpreis in Höhe 50 % des Apothekenverkaufspreises einzuräumen. Zu diesem Zweck sollen die Bedürftigen zunächst eine Berechtigungskarte erhalten und sich dann von ihrem Arzt ein sogenanntes "Grünes Rezept" ausstellen lassen, welches dann zusammen mit dem Ausweis in der Apotheke vorgelegt werden sollte. Mit dem Grünen Rezept werden Medikamente verschrieben, die in der Regel nicht auf Kosten der gesetzlichen Krankenkassen verordnet werden können. Bei der Einlösung des Rezepts soll der Patient 50 % des Arzneimittelpreises bezahlen, während die anderen 50 % von einem Sponsorenkonto bezahlt werden sollen.

Gegen dieses Verfahren meldete der TLfDI datenschutzrechtliche Bedenken gegen die Übermittlung von Patientendaten durch Apotheken an eine private Verrechnungsstelle an. Bei Gesundheitsdaten handelt es sich um besondere Arten personenbezogener Daten, § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG). Für derartige Daten gelten nach BDSG besonders strenge Anforderungen. Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten für eigene Geschäftszwecke ist nach § 28 Abs. 6 BDSG zulässig, soweit nicht der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat, wenn eine der in § 28 Abs. 6 Nummer 1 bis 4 BDSG genannten Voraussetzungen vorliegen. Da keine dieser Voraussetzungen vorlag, ist die Datenübermittlung nur mit der Einwilligung des Betroffenen möglich. Eine wirksame Einwilligung setzt nach § 4 a Abs. 1 BDSG voraus, dass 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, 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. Zudem ist, da besondere Arten personenbezogener Daten betroffen sind, die Einwilligung ausdrücklich auf diese Daten, das heißt auf die Übermittlung der Rezepte, zu beziehen.

Daher ist eine ausdrückliche schriftliche Einwilligungserklärung des Patienten in die Übermittlung der Rezepte an die private Abrechnungsstelle gegenüber der jeweils übermittelnden Apotheke erforderlich. Das sollte machbar sein. Hingewiesen wurde auch darauf, dass sich nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch strafbar macht, wer

unbefugt – in diesem Fall also ohne Einwilligung des Betroffenen – ein fremdes Geheimnis offenbart, das ihm als Apotheker anvertraut worden ist.
Da sich im Laufe des Verfahrens herausstellte, dass der Träger des Projektes eine kirchliche Einrichtung ist, wurde das Verfahren insoweit an den zuständigen kirchlichen Datenschutzbeauftragten abgegeben. Mit Blick auf das verfassungsrechtlich garantierte Selbstbestimmungsrecht von Religionsgemeinschaften gilt das Bundesdatenschutzgesetz im Bereich der Kirchen nicht.

Auch wenn ein guter Zweck verfolgt wird, sind die Anforderungen des Datenschutzrechts zu beachten. Eine Übermittlung von Gesundheitsdaten ist nur bei einer vorliegenden schriftlichen Einwilligung, die sich ausdrücklich auf diese Daten bezieht oder bei Vorliegen der Voraussetzungen des § 28 Abs. 6 BDSG zulässig. Für kirchliche Einrichtungen besteht keine Zuständigkeit des TLfDI.

3.41 Datenverkauf im Apothekenrechenzentrum?

Aus der Presse war zu entnehmen, dass die Verrechnungsstelle der süddeutschen Apotheken (VSA) Millionen von Patientendaten nur unzureichend verschlüsselt an den Gesundheitsdienstleister und Marktforscher IMS Health verkauft haben soll. Die Apothekenrechenzentren bieten für die Apotheken in Deutschland die Dienstleistung der Abrechnung mit den Kassen an. Dies ist nach § 300 Abs. 2 Satz 1 des Fünften Buches Sozialgesetzbuch (SGB V) zulässig. Danach dürfen die Apotheken zur Erfüllung ihrer Verpflichtungen Rechenzentren in Anspruch nehmen. § 300 Abs. 2 Satz 2 SGB V legt fest, dass die Rechenzentren diese Daten nur für diese Zwecke verarbeiten und nutzen dürfen, anonymisierte Daten allerdings dürfen auch für andere Zwecke verarbeitet und genutzt werden. Das bedeutet, dass die Daten, wenn sie anonymisiert sind, von den Rechenzentren auch an andere Dienstleister oder Pharmaunternehmen verkauft werden dürfen. Nach § 3 Abs. 6 Bundesdatenschutzgesetz (BDSG) ist Anonymisieren 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. Entscheidend für die datenschutzrechtli-

che Zulässigkeit der Tätigkeit der Apothekenrechenzentren ist beim Verkauf von Daten an Dritte, ob diese entsprechend den gesetzlichen Vorgaben anonymisiert sind. Laut den damaligen Pressemitteilungen war die Identität der Patienten lediglich durch einen 64-stelligen Code verschleiert, der sich leicht auf die tatsächliche Versichertennummer zurückrechnen ließ.

Es besteht ein großes wirtschaftliches Interesse an der Auswertung von Verordnungsdaten. Die Apothekenrechenzentren sind daher grundsätzlich bestrebt, eine Auswertung der Daten weitestgehend zu ermöglichen. Um die Tätigkeit der Apothekenrechenzentren bundesweit einheitlich zu bewerten, wurde die Unterarbeitsgruppe „Apothekenrechenzentren“ des Arbeitskreises „Gesundheit und Soziales“ der Datenschutzkonferenz eingerichtet. Diese Unterarbeitsgruppe kam unter Vorsitz des Bayerischen Landesamtes für Datenschutzaufsicht zweimal im Berichtszeitraum in Ansbach zusammen.

Von einer Anonymisierung kann dann nicht mehr gesprochen werden, wenn die Verordnungsdaten in einer Art und Weise an Dritte weitergegeben werden, dass diese zu einem Rezept die Versicherungsnummer des Patienten und die Arztnummer des verschreibenden Arztes, wenn auch mit einigem Aufwand, bestimmen können. Bei den Sitzungen der Unterarbeitsgruppe ging es vor allem darum festzulegen, wann von einer Anonymisierung der Daten gesprochen werden kann. Nach Auffassung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist eine absolute Anonymisierung die sicherste Methode, um die gesetzlichen Anforderungen zu erfüllen. Eine Anonymisierung kann jedenfalls dann nicht erreicht werden, wenn dasselbe Anonym für einzelne Ärzte, Versicherte und Apotheken über einen unbestimmten Zeitraum dauerhaft verwendet wird. Mit fortschreitender Zeit vergrößert sich die Gefahr, dass durch gezielte Abfragen, die immer wieder in anderer Weise miteinander verknüpft werden, die Anonyme personifiziert werden können. Daher ist zu fordern, dass die bei der Übermittlung verwendeten Schlüssel eine kurze Gültigkeit haben, dass Daten einzelner Ärzte nicht gezielt abgefragt werden, sondern Ärzte-Cluster größeren Umfangs zu bilden sind. Gleiches gilt für Patientendaten. Im Nachgang zu den Sitzungen der Unterarbeitsgruppe „Apothekenrechenzentren“, hat der TLfDI auch ein Apothekenrechenzentrum in Thüringen geprüft. Offensichtliche Anhaltspunkte für ein gesetzwidriges Verhalten gab es dabei nicht. Da die Verfah-

ren allerdings äußerst komplex sind, ist die Prüfung noch nicht abgeschlossen. Der TLfDI wird das Ergebnis der Prüfung im nächsten Tätigkeitsbericht darlegen.

Apothekenrechenzentren dürfen Rezeptdaten auch für andere Zwecke als die Abrechnung verwenden, wenn diese anonymisiert sind. An die Anonymisierung sind wegen der enthaltenen Sensibilität der Gesundheitsdaten hohe Anforderungen zu stellen.

3.42 Taxi - alles im Blick: Videogaga 20

Es ist bekannt, dass Taxifahrer Opfer einer Straftat werden können, entweder indem ein Fahrgast „das Bezahlen vergisst“ oder der Fahrer sogar überfallen und ausgeraubt wird. Da liegt es nahe, auch in diesem Bereich auf die Wirkung der Videoüberwachung zu setzen. Im Düsseldorfer Kreis (siehe oben Punkt 2) wurde darüber beraten, unter welchen Voraussetzungen aus datenschutzrechtlicher Sicht die Videoüberwachung des Taxiinnenraums zulässig ist. Dabei wurde festgestellt, dass grundsätzlich der Einsatz von Videokameras, z. B. im Armaturenbrett, im Dachhimmel usw. nicht ausgeschlossen ist. Hierbei müssen aber die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer Beachtung finden. Es sind daher die berechtigten Sicherheitsinteressen und die schutzwürdigen Interessen der Betroffenen gegeneinander abzuwägen und die Videoüberwachung auf das unbedingt erforderliche Maß zu beschränken. Die Zulässigkeit einer Videoüberwachung durch ein Taxi-Unternehmen bestimmt sich nach § 6 b Abs. 1 Nr. 3 Bundesdatenschutzgesetz (BDSG), wonach die Beobachtung und vorliegend auch die Aufzeichnung mittels Videokameras nur zulässig ist, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Düsseldorfer Kreis verweist dabei darauf, vorrangig alternative und weniger einschneidende Schutzmaßnahmen (z. B. anlassbezogene Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals) zu ergreifen. Eine Videoüberwachung kann außerdem nur in Orten als erforderlich angesehen werden, die eine hohe Kriminalitätsrate aufweisen. Falls eine Videoüberwachung danach als erforderlich anzusehen ist – wovon in Thüringen in aller Regel nicht auszugehen ist – dann sollte sich diese auf

das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen beschränken. Soweit eine Aufzeichnung erfolgt, ist diese ohne ein Vorkommnis unverzüglich zu löschen. Dem Transparenzgebot nach § 6 b Abs. 2 BDSG ist Rechnung zu tragen, indem an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung hingewiesen werden.
Da Taxis rund um die Uhr am Straßenverkehrsgeschehen teilnehmen, ist hier die Gefahr hoch, in einen Unfall verwickelt zu werden. Sowohl vermeintlich findige Versicherungsunternehmen als auch Taxibetriebe verfolgen deshalb die Idee, durch die Installation von Außenkameras, häufig in Form von so genannter „Dashboardkameras“, die auf dem Armaturenbrett (Dashboard) angebracht werden und das Verkehrsgeschehen durch die Windschutzscheibe aufzeichnen, im Falle eines Schadensereignisses vorsorglich Beweise zu sichern. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit geht davon aus, dass diese Form der Videoüberwachung nicht die gesetzlichen Anforderungen an eine zulässige Videoüberwachung erfüllt. Jeder Verkehrsteilnehmer kann sich im Verkehrsraum grundsätzlich darauf verlassen, nicht ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Ausdruck des Rechts auf informationelle Selbstbestimmung ist es, sich in der Öffentlichkeit, auch im Verkehrsraum, frei und ungezwungen bewegen zu können. Der Düsseldorfer Kreis hat deshalb den Beschluss gefasst, dass es eine Rechtsgrundlage für diese Form der Datenerhebung nicht gibt und die Ausstattung von Taxis mit Außenkameras, wie dies von Versicherungsunternehmen vorgeschlagen wird, unzulässig ist (Beschluss des Düsseldorfer Kreises am 26./27. Februar 2013, siehe Anlage 4).

Eine anlasslose Videoüberwachung in Taxis ist weder erforderlich noch angemessen. Zum einen hat der Taxifahrer ein Recht darauf, nicht durchgängig während seiner Arbeitsschicht beobachtet zu werden, zum anderen müssen auch unbescholtene Fahrgäste nicht damit rechnen, permanent während der Fahrt unter Videobeobachtung zu stehen.
Die Beobachtung des Verkehrsgeschehens durch Außenkameras bei Taxis ist grundsätzlich unzulässig.

3.43 Keine Beobachtung öffentlicher Straßen zur Zugangskontrolle: Videogaga 21

Auf polizeilichen Hinweis kontrollierte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) ein Recyclingunternehmen in Thüringen, das über eine umfangreiche Videoüberwachung verfügte. Dabei wurde festgestellt, dass eine der Kameras auf die öffentliche Straße in Richtung des anliegenden Dorfes ausgerichtet war. Jeder im Dorf und jeder der die betroffene öffentliche Straße nutze, musste davon ausgehen, Gegenstand einer Videoüberwachung zu werden. Nach dem Bundesdatenschutzgesetz (BDSG) bedarf jedoch die Videoüberwachung öffentlich zugänglicher Bereichen wie Straßen grundsätzlich einer Rechtsgrundlage. Gemäß § 6 b BDSG ist die Videobeobachtung zum einen zulässig, sofern sie zu Zwecken der Ausübung des Hausrechts erforderlich ist. Außerdem darf sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke durchgeführt werden. In beiden Fällen darf kein Anhaltspunkt ersichtlich sein, dass schutzwürdige Interessen Betroffener überwiegen. Diese Voraussetzungen waren hier nicht gegeben. Darüber überwiegen in aller Regel die Interessen Dritter, wenn eine ganze Straße in den Bereich der Videoaufnahmen fällt. Bei der Beobachtung öffentlicher Straßen werden immer auch Personen „Opfer“ der Beobachtung, die die Straße benutzen müssen, von der Beobachtung nichts wissen und keinen Anlass für eine Beobachtung gegeben haben. Da das Unternehmen uneinsichtig war und immer neue Ausflüchte suchte, untersagte der TLfDI dem Unternehmen die in dieser Weise durchgeführte Videoüberwachung mit Hinweis auf den dadurch auf Passanten ausgeübten Überwachungsdruck. Dem Unternehmen wurde im Wege einer Anordnung unter Zwangsgeldandrohung aufgegeben, die Kamera wahlweise zu verhüllen oder in eine zulässige Position zu verdrehen.

Es ist unerlässlich, dass sich Unternehmen mit den Grenzen der Videoüberwachung vertraut machen. Dies gilt nicht nur, aber insbesondere für die Videoüberwachung in öffentlich zugänglichen Bereichen. In der Regel verstößt das Ausrichten einer Videokamera auf eine öffentliche Straße oder einen öffentlichen Fußweg gegen Datenschutzrecht.

3.44 Das "elektronische Auge" des Nachbarn: Videogaga 22

Gegenstand einer Beschwerde waren Videoaufnahmen von Bewohnern und Besuchern eines Grundstücks, die ein Nachbar mit seiner Videokamera aufgenommen und ohne Erlaubnis der Abgebildeten seinen Gästen zur Schau gestellt haben soll. Nach § 1 Abs. 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) sind Videoaufnahmen mit personenbezogenen Daten nur dann am BDSG zu messen, wenn ihre Erhebung, Verarbeitung und Nutzung nicht ausschließlich für persönliche oder familiäre Zwecke erfolgt.
Obwohl der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) im Rahmen seiner Aufsichtstätigkeit kontrollieren kann, ob die Videoaufnahmen ausschließlich für persönliche oder familiäre Zwecke gefertigt werden, befriedigt ihn die oben dargelegte Rechtslage nicht, da sie ihn von Maßnahmen trotz etwaiger Datenerhebungen im unter Umständen sehr privaten Bereich (z. B. Video) abhält, wenn diese Datenerhebungen lediglich privaten oder familiären Zwecken dienen.
Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben eine gemeinsame Orientierungshilfe zur Videoüberwachung erarbeitet. In diesem Zusammenhang hat sich der TLfDI dafür eingesetzt, dass die Datenschutzaufsichtsbehörden im Falle einer durch Privatpersonen durchgeführten Videoüberwachung, die zugleich auch öffentliche Bereiche, wie z. B. öffentliche Parkplätzen, Gehwege und Straßen erfassen, zuständig sein sollen. Zum Thema private Videoüberwachung ist gegenwärtig eine Klage vor dem Europäischen Gerichtshof (EUGH, C-212/13) anhängig. Dieses Vorabentscheidungsersuchen betrifft die Frage, ob der Betrieb eines Kamerasystems, das an einem Einfamilienhaus zum Zwecke des Schutzes des Eigentums, der Gesundheit und des Lebens der Besitzer des Hauses angebracht ist, unter die Verarbeitung personenbezogener Daten, „die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird“ im Sinne des Art. 3 Abs. 2 der Richtlinie 95/46/EG gefasst werden kann, obschon dieses System auch öffentlichen Raum überwacht. Der Ausgang dieses Gerichtsverfahrens und sein Einfluss auf die künftige Rechtlage sind derzeit jedoch noch nicht abzusehen.
Im konkreten Fall wurde festgestellt, dass die Videoaufnahmen durch den Nachbarn einen privaten Bereich betrafen und zu aus-

schließlich privaten Zwecken erfolgten, weswegen eine Zuständigkeit des TLfDI nicht gegeben war.
Insofern wurde der Beschwerdeführer auf die Möglichkeit, über die ordentliche Gerichtsbarkeit auf zivilrechtlichem Wege (§ 823 BGB i. V. m. § 1004 BGB) gegen eine solche Videoüberwachung vorzugehen, hingewiesen. Nach § 22 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturheberrechtsgesetz [KunstUrhG]) dürfen Bildnisse nur mit Einwilligung der Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Nach § 33 KunstUrhG wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer entgegen §§ 22, 23 KunstUrhG ein Bildnis verbreitet oder öffentlich zur Schau stellt.

Gegen Videoaufnahmen mit personenbezogenen Daten, die einen privaten Bereich betreffen und zu ausschließlich privaten oder familiären Zwecken gefertigt werden, kann sich der Betroffene auf dem Zivilrechtsweg zur Wehr setzen.
Wer Bildnisse ohne Einwilligung der Abgebildeten verbreitet oder öffentlich zur Schau stellt, verstößt gegen das KunstUrhG. Dies kann eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe zur Folge haben.

3.45 Prüfungspflicht der Banken nach dem Geldwäschegesetz

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) erhielt die Anfrage eines Vorsitzenden eines nicht in das Vereinsregister eingetragen Vereins. Dieser Verein hatte bei einer Bank ein Konto eröffnet: Die Bank verlangte nun die Übermittlung von Namens-, Vornamens-, Geburts-, Geburtsorts-, Wohnanschrifts-, Wohnorts-, Staatsangehörigkeits- sowie Personalausweisnummerdaten nebst ausstellender Behörde zu jedem Vereinsmitglied. Begründet wurde diese Anforderung der Daten mit dem § 4 Abs. 5 Geldwäschegesetz (GWG).
Um die Zulässigkeit der Datenerhebung beurteilen zu können, wurde die Bank um Stellungnahme gebeten. Die Bank teilte mit, dass sie vor Eröffnung einer Geschäftsbeziehung den Geschäftspartner (wirtschaftlicher Berechtigter) nach § 4 GWG identifizieren müsse. Wirtschaftlich Berechtigter im Sinne von § 1 Abs. 6 Satz 1 GWG sei die natürliche Person, in deren Eigentum oder unter deren Kontrolle der Vertragspartner letztlich stehe oder die natürliche Person, auf deren

Veranlassung die Transaktion letztlich durchgeführt oder eine Geschäftsbeziehung begründet werde. Darunter sei nach § 1 Abs. 6 Nr. 2 d GWG insbesondere auch jede natürliche Person zu zählen, die auf sonstige Weise unmittelbar oder mittelbar beherrschenden Einfluss auf die Vermögensverwaltung oder Ertragsverteilung ausübe.
Da der Verein nicht im Vereinsregister eingetragen war, konnte die Bank den wirtschaftlich Berechtigten nicht mittels Auskunft aus dem Vereinsregister feststellen. Bei einem nicht rechtsfähigen Verein sind alle Vereinsmitglieder (im Außenverhältnis) als wirtschaftliche Berechtigte mit potenzieller Verfügungsmacht über das Vereinsvermögen anzusehen. Eine etwaige satzungsmäßige Übertragung von Verfügungsrechten auf einzelne Mitglieder wie Vorstandsmitglieder und Schatzmeister würde sich mangels einer entsprechenden Registereintragung nur in dessen Innenverhältnis auswirken. Die Bank ist verpflichtet, aufgrund der Vorschriften des GWG die Identifizierung des Kontoinhabers, Erfassung der Kontrollrechte und Abklärung des wirtschaftlichen Berechtigten zu erfragen. Bei Zweifelsfragen hat der Kontoinhaber nach § 4 Abs. 6 GWG mitzuwirken. Da der Verein seiner Mitwirkungspflicht nicht nachkam, hat die Bank letztendlich die Geschäftsverbindung gekündigt und das Konto gelöscht.
Da sich der Verein in dieser Angelegenheit auch an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) gewandt hatte, hat der TLfDI die BaFin mit Einverständnis des Vereins gebeten, das Prüfergebnis zu übersenden. Die BaFin sieht die Verfahrensweise der Bank in diesem Fall als vertretbar an.
Im Ergebnis ist daher die von der Bank geforderte Übermittlung personenbezogener Daten der Vereinsmitglieder zur Ermittlung wirtschaftlich Berechtigter im Sinne der spezialgesetzlichen Normen des GWG nicht als Verstoß gegen datenschutzrechtliche Bestimmungen anzusehen. Es wird jedoch angeraten, in ähnlichen Fällen künftig die erforderlichen Prüfungen bereits vor Aufnahme der Geschäftsbeziehung vorzunehmen.

Nach § 4 GWG muss die Bank vor Eröffnung einer Geschäftsbeziehung den Geschäftspartner (wirtschaftlicher Berechtigter) identifizieren. Bei einem Verein, der nicht im Vereinsregister eingetragen ist, oder bei einer Gesellschaft bürgerlichen Rechts kann die Bank den wirtschaftlich Berechtigten nicht mittels Auskunft aus einem öffentlichen Register feststellen. Bei Zweifelsfragen hat der Kontoinhaber

(Verein) daher mitzuwirken und die Daten der Vereinsmitglieder zu übersenden.

3.46 Immer wieder der Geburtstag

Manche Menschen werden gerne an ihrem Geburtstag gefeiert und empfinden es als Affront, wenn ihr Geburtstag vergessen wird. Andere werden am liebsten gar nicht daran erinnert, dass schon wieder ein Jahr vergangen ist. Vor diesem Konflikt stehen auch Kollegen, die in einem Betrieb zusammen arbeiten. Regelmäßig erreichen den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Anfragen, ob es in Unternehmen zulässig ist, einen Geburtstagskalender mit den Angaben zu den Arbeitnehmern (Name und Datum) zu führen. Da es sich bei den Geburtstagsdaten um Arbeitnehmerdaten handelt, ist § 32 Bundesdatenschutzgesetz (BDSG) anzuwenden. Danach dürfen personenbezogene Daten eines Arbeitnehmers für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Eine konkrete Erforderlichkeit für diese Zwecke besteht bei dem Führen eines Geburtstagskalenders jedoch nicht.
Ohne zu verkennen, dass es sich bei der Gratulation zum Geburtstag um einen Teil im Rahmen des sozialen Miteinanders auch im Beschäftigungsbereich handelt, wäre eine Nutzung des Geburtsdatums der Arbeitnehmer nur mit der Einwilligung der Betroffenen möglich, da nach § 4 Abs. 1 BDSG die Verarbeitung und Nutzung personenbezogener Daten alternativ auch auf Einwilligungsbasis zulässig ist, wenn eine konkrete Rechtsvorschrift diesbezüglich nicht vorhanden ist. Die Anforderungen an eine Einwilligung sind in § 4 a BDSG aufgelistet. Sie könnte bestenfalls bereits bei der Einstellung eines Betroffenen eingeholt werden, wobei konkret auf den vorgesehenen Zweck (Gratulation zum Geburtstag) hingewiesen wird. Dabei muss eine Einwilligung auf der freien Entscheidung des Betroffenen beruhen. Aus einer Verweigerung dürfen keine Folgen entstehen. Damit liegt es in der freien Entscheidung eines jeden Arbeitnehmers, ob er in einer Geburtstagsliste aufgenommen werden möchte. Die Angabe des Geburtsjahres ohne Einwilligung des Betroffenen ist jedenfalls

nicht zulässig, da sie zum Zweck der Gratulation zum Geburtstag nicht erforderlich ist.

Das Führen einer Geburtstagsliste ist nur zulässig für die Arbeitnehmer, die in die Nennung Ihres Geburtsdatums eingewilligt haben. Das Geburtsjahr darf nicht genannt werden.

3.47 Meldepflicht nach Hackerangriff

Wie auch immer wieder in verschiedenen Printmedien zu lesen ist, häufen sich in letzter Zeit Angriffe auf IT-Anlagen von Unternehmern. Ziel dieser Angriffe sind meist solche Daten, die für den Angreifer unmittelbaren finanziellen Vorteil bieten. Bankdaten zum Beispiel. Aus diesem Grund hat der Gesetzgeber den Unternehmen in solchen Fällen umfangreiche Pflichten aufgegeben. § 42 a Bundesdatenschutzgesetz (BDSG) sieht vor, dass Unternehmen, denen besondere personenbezogene Daten abhanden gekommen oder von diesen solche Daten unrechtmäßig an Dritte übermittelt worden sind, weitreichenden Informations- und Meldepflichten unterliegen. Unter besonderen personenbezogenen Daten versteht man nach § 3 Abs. 9 BDSG „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben“. Denselben Pflichten unterliegen diese Unternehmen, wenn statt der besonderen personenbezogenen Daten, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, oder eben auch personenbezogene Daten zu Bank- oder Kreditkartenkonten betroffen sind.
Zunächst muss das Unternehmen prüfen, ob für die Betroffenen schwerwiegende Beeinträchtigungen ihrer Rechte drohen. Dabei handelt es sich um eine Einzelfallentscheidung. Zumindest aber bei Bank- oder Kreditkartendaten dürfte dies immer der Fall sein. Drohen solche Beeinträchtigungen, sind durch das Unternehmen der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) sowie die einzelnen Betroffenen zu informieren. Diese Information hat unverzüglich zu erfolgen, das heißt ohne schuldhaftes Zögern, nachdem Maßnahmen zur Sicherung der entsprechenden Daten eingeleitet wurden. Einzige Ausnahme hierzu ist eine eventuelle Gefährdung strafrechtlicher Ermittlungen. Die Aufsichtsbehörde und die Betroffenen sind darüber zu unterrichten, in

welcher Art und Weise Dritte unrechtmäßig Kenntnis der personenbezogenen Daten nehmen konnten. Auch müssen Hinweise und Empfehlungen zu Maßnahmen enthalten sein, mit denen mögliche nachteilige Folgen gemindert werden können.
Aus Unternehmenssicht bietet es sich an, einen Notfallplan zu erarbeiten, der alle notwendigen Maßnahmen im Falle eines Abhandenkommens von Daten beschreibt, so eben auch die notwendigen Meldungen an die Betroffenen und den TLfDI. Diese „Checkliste“ ist zwar nicht gesetzlich vorgeschrieben, erleichtert jedoch das Vorgehen im Falle des Falles. Dies ist auch deswegen wichtig, weil eine vergessene, verspätete oder unzureichende Meldung nach § 42 a BDSG vom TLfDI mit einer Geldbuße von bis zu 300.000 Euro geahndet werden kann.
In Thüringen gab es für den Berichtszeitraum vier Meldungen, die beim TLfDI eingegangen sind und geprüft wurden.

Sobald ein Unternehmen feststellt, dass personenbezogene Daten, die in den Anwendungsbereich von § 42 a BDSG fallen, abhanden gekommen sind, ist der Aufsichtsbehörde und den Betroffenen unverzüglich eine dem § 42 a BDSG entsprechende Mitteilung zu machen. Andernfalls drohen empfindliche Geldbußen. Daher ist es sinnvoll, zumindest in Unternehmen, in denen ein meldepflichtiger Fall nicht unwahrscheinlich ist, für alle Fälle einen Notfallplan zu entwerfen.

3.48 Personalausweiskopie? Schrott!

Den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) liegen mehrere Eingaben vor, in denen sich Bürger darüber beschweren, dass Metall-Recycling-Firmen den angebotenen Metallschrott nur dann annehmen, wenn die Lieferanten der Erstellung einer Kopie ihres Personalausweises zustimmen. Eine solche Praxis hält der TLfDI für unzulässig.
Das betroffene Unternehmen gab an, dass die Bundesvereinigung Deutscher Stahl-Recycling- und Entsorgungsunternehmen e. V. in einem Rundschreiben das Kopieren von Personalausweisen empfiehlt. Im Schrotthandel gebe es einige „schwarze Schafe“. Die Finanzbehörden hätten deshalb die gesetzlichen Nachweis- und Dokumentationserfordernisse deutlich verschärft. Es sei in der Vergangenheit regelmäßig zur Nichtanerkennung von Betriebsausgaben

durch die Finanzbehörden gekommen, wenn der Ankäufer nicht den Empfänger der Zahlungen zweifelsfrei benennen konnte. Im Rahmen eines solchen Empfängerbenennungsverfahrens des Finanzamtes nach § 160 der Abgabenordnung sei es inzwischen häufiger vorgekommen, dass die Finanzbehörden die Benennung vordringlich mittels Vorlage einer Personalausweiskopie einforderten.
Der TLfDI wandte sich daraufhin an die Thüringer Landesfinanzdirektion. Diese teilte mit, dass seitens der Thüringer Finanzbehörden von den Schrott- bzw. Recyclingfirmen keine Kopien der Personalausweise der Lieferanten für steuerliche Zwecke verlangt würden. Damit besteht keine Erforderlichkeit des Kopierens des Personalausweises und auch keine Rechtsgrundlage für diese Datenerhebung. Die Anfertigung von Personalausweiskopien ist nicht nach § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich.
Die Unzulässigkeit der Anfertigung einer Kopie des gesamten Personalausweises ergibt sich insbesondere aus den §§ 14 ff des Personalausweisgesetzes (PAuswG). Nach § 14 Nr. 2 PAuswG darf die Erhebung und Verwendung personenbezogener Daten auf dem Ausweis oder mit Hilfe des Ausweises ausschließlich durch öffentliche und nicht-öffentliche Stellen nach Maßgabe der §§ 18 bis 20 PAuswG erfolgen. Die Vorlage eines Personalausweises dient primär der Erfüllung der gesetzlich vorgeschriebenen Ausweispflichten im öffentlichen Bereich. §§ 18 und 19 PAuswG regeln den elektronischen Identitätsnachweis. Darüber hinaus ist es nach § 20 Abs. 1 PAuswG auch zulässig, den Personalausweis als Ausweis- und Legitimationspapier zu verwenden. Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nicht-öffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden, § 20 Abs. 2 PAuswG. In der Gesetzesbegründung zu § 14 PAuswG heißt es: „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mit Hilfe des Ausweises künftig nur über die vorgesehenen Wege erfolgen darf. […] Weitere Verfahren z. B. über die optoelektronische Erfassung („Scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden.“ (BR-DRs 550/2008 Seite 69 f).
Der TLfDI beabsichtigt daher das Unternehmen unter Zwangsgeldandrohung aufzufordern, für die Zukunft keine Personalausweisko-

pien mehr anzufertigen. Zulässig ist allenfalls die Kopie des Personalausweises mittels einer Schablone, auf der die nicht-erforderlichen Daten, wie das Lichtbild und die Personalausweisnummer verdeckt sind. Ansonsten reicht es aus, wenn das Unternehmen vermerkt, dass sich eine betreffende Person mittels Personalausweis ausgewiesen hat. Das entsprechende Verwaltungsverfahren läuft derzeit noch.

Die Anfertigung von Personalausweiskopien durch nicht-öffentliche Stellen ist grundsätzlich unzulässig. In aller Regel ist die Anfertigung einer Kopie des Personalausweises zur Erfüllung eigener Geschäftszwecke oder zur Wahrnehmung berechtigter Interessen nicht erforderlich, weil die Identität des Betroffenen vor Ort selbst durch Vorlage des Personalausweises geklärt werden kann.

3.49 Video im Wind: Videogaga 23

Ein Betroffener wandte sich an den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) und teilte mit, dass – wahrscheinlich durch den Betreiber eines Windparks – in einer bestimmten Region öffentliche Wege in Thüringen videoüberwacht würden. Der TLfDI musste zunächst die verantwortliche datenverarbeitende Stelle ermitteln und schrieb das Unternehmen an, das in der betreffenden Region Windräder betreibt. Nach umfangreichen Aufklärungsarbeiten stellte sich heraus, dass das in Thüringen ansässige Unternehmen nicht der Betreiber der vorhandenen Videoüberwachung war. Das Thüringer Unternehmen liefert lediglich die Windenergieanlagen. Eine Firma, die in einem anderen Bundesland ansässig ist, war jedoch der Betreiber und hatte auch die Videoüberwachung vor Ort zu verantworten. Diese Firma hat zwischenzeitlich mitgeteilt, dass die Videoüberwachung eingestellt worden sei; damit war über die Frage der Zuständigkeit des TLfDI für den vorliegenden Sachverhalt nicht mehr zu entscheiden.
Grundsätzlich kommt es für die Zuständigkeit der Aufsichtsbehörde darauf an, in welchem Bundesland die datenverarbeitende Stelle ihren Sitz hat. Da weder das Bundesdatenschutzgesetz noch das Thüringer Datenschutzgesetz zur örtlichen Zuständigkeit der Aufsichtsbehörde Regelungen treffen, ist das Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) ergänzend heranzuziehen. Nach § 3 Abs. 1 Nr. 2 ThürVwVfG ist in Angelegenheiten, die sich auf

den Betrieb eines Unternehmens oder einer seiner Betriebsstätten beziehen, die Behörde örtlich zuständig, in deren Zuständigkeitsgebiet das Unternehmen oder die Betriebsstätte betrieben wird oder werden soll.

Für die örtliche Zuständigkeit der Aufsichtsbehörde ist grundsätzlich der Sitz der datenverarbeitenden Stelle entscheidend. Grundsätzlich ist die Aufsichtsbehörde zuständig, in deren Gebiet (Bundesland) sich der Sitz des Unternehmens befindet. Bei Betriebsstätten in anderen Bundesländern kann es zu abweichenden Zuständigkeiten kommen.

3.50 Pakete auf datenschutzrechtlichen Abwegen: Videogaga 24

Aufgrund einer Beschwere wurde der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auf einen Missstand in einem Paketshop aufmerksam. Über zweierlei beschwerte sich der Bürger: Zum einen würden die zur Abholung bereitliegenden Pakete teilweise für jedermann sichtbar im Laden herumliegen, weswegen jeder, der wollte, Absender und Adressat erkennen könne, zum anderen könne man die Pakete nur gegen Vorzeigen des Personalausweises und Speicherung bestimmter darauf enthaltender Daten, wie zum Beispiel der Ausweisnummer, abholen. Bei der in der Folge durch den TLfDI durchgeführten Kontrolle wurden diese Umstände bestätigt und ein weiteres Problemfeld aufgetan.
Beide vom Bürger gerügten Aspekte sind datenschutzrechtlich relevant. Gemäß § 39 des Postgesetzes unterliegen alle näheren Umstände des Postverkehrs natürlicher wie auch juristischer Personen sowie der Inhalt der Postsendung dem Postgeheimnis. Zu den näheren Umständen des Postverkehrs gehören insbesondere alle Verbindungsdaten, die nicht den Inhalt der konkreten Sendung selbst betreffen, wie z. B. Name und Anschrift des Absenders und Empfängers, Ort und Zeit der Aufgabe der Postsendung, Art und Weise der Inanspruchnahme der Dienstleistung. Daher ist es erforderlich, dass Pakete und Briefsendungen so aufbewahrt werden müssen, dass Dritte nicht die Möglichkeit haben, auf diese Daten zuzugreifen. Damit ist es aus datenschutzrechtlicher Sicht unzulässig, Pakete auf eine Art zu lagern, die es unbeteiligten Dritten ermöglicht, Adressat und Absender zur Kenntnis zu nehmen.

Hinsichtlich der Abholung der Pakete stellt sich die Rechtslage ein wenig komplizierter dar. Gemäß § 8 Abs. 1 der Postdienste-Datenschutz-Verordnung (PDSV) können die Postdienstleister verlangen, dass sich die am Postverkehr beteiligte Person durch Vorlage eines gültigen Personalausweises oder Passes oder durch Vorlage sonstiger amtlicher Ausweispapiere ausweist, wenn dies erforderlich ist, um die ordnungsgemäße Ausführung des Postdienstes sicherzustellen. Gemäß § 8 Abs. 2 PDSV kann der Postdienstleister die Art des Ausweises, die ausstellende Behörde sowie die Nummer des Ausweises und das Ausstellungsdatum speichern, sofern ein besonderes Beweissicherungsinteresse dahingehend besteht, dass der jeweilige Postdienst ordnungsgemäß ausgeführt wurde. Dieses Beweissicherungsinteresse besteht bereits hinsichtlich des Zugangs von Paketen. Insoweit stellt das Speichern dieser Informationen kein datenschutzrechtliches Problem dar. Allerdings verlangte der Paketshop zwingend einen Pass oder Personalausweis. Unter den Begriff des amtlichen Dokuments fallen jedoch alle Dokumente, die von einer Behörde zum Zwecke des Ausweisens ausgegeben wurden, beispielsweise der Führerschein. Dies ist insoweit ein Problem, als dass das informationelle Selbstbestimmungsrecht, soweit der gesetzliche Rahmen dies zulässt, dem Einzelnen auch die Entscheidung überlässt, welche personenbezogenen Daten erhoben und gespeichert werden. Hierzu gehört auch die Entscheidung darüber, ob der Einzelne sich bei Abholung eines Pakets lieber per Ausweis oder zum Beispiel per Führerschein ausweisen möchte.

Im Rahmen der Kontrolle konnte die verantwortliche Stelle jedoch glaubhaft machen, dass ihr durch das entsprechende Paketunternehmen keine Wahl bei den Ausweisdokumenten eingeräumt wird. Das vom versendenden Unternehmen bereitgestellte Programm akzeptiert ausschließlich Pass- oder Personalausweisnummern, ansonsten ist das Austragen von Sendungen und deren Übergabe an den Kunden nicht möglich. Hinsichtlich dieser Problematik wird sich der TLfDI mit der für das Paketunternehmen zuständigen Aufsichtsbehörde in Verbindung setzen.

Ebenfalls wurde bei der durchgeführten Kontrolle festgestellt, dass in dem Unternehmen eine umfangreiche Videoüberwachung durchgeführt wurde. Nach rechtlicher Prüfung musste der TLfDI feststellen, dass diese nach § 6 b BDSG nicht erforderlich und damit unzulässig war. Auf einer Ladenfläche von ca. 7 qm wurden drei Videokameras aus verschiedenen Blickwinkeln betrieben. Zweck der

Überwachung sollte die Verfolgung von Diebstählen sein. Hierzu ist bei einer solch kleinen Ladenfläche jedoch keine Videoüberwachung erforderlich. Vielmehr kann die Verkaufsfläche hier ohne weiteres durch den Verkäufer überwacht werden.
Noch dazu übertrug das Unternehmen die Videoaufnahmen „live“ ins Internet und publizierte diese auf der Homepage des Unternehmens. Ein solches Vorgehen stellt selbstverständlich einen massiven Datenschutzverstoß dar, der unabhängig von der grundsätzlichen Zulässigkeit einer Videoüberwachungsanlage unzulässig ist, da diese Datenübermittlung nicht durch § 28 Abs. 1 BDSG gedeckt ist. Diese Norm regelt die Zulässigkeit des Umgangs mit personenbezogenen Daten zu eigenen Geschäftszwecken. Auf den Hinweis des TLFDI hin stellte das Unternehmen die Übertragung über das Internet unverzüglich ein.
Der TLfDI hat dem Unternehmen mitgeteilt, dass die Lagerung der Pakete so zu erfolgen hat, dass eine Einsichtnahme Dritter in Absender- oder Adressdaten nicht möglich ist. Sofern das Unternehmen dieser Aufforderung nicht nachkommt, wird der TLfDI eine entsprechende Anordnung erlassen, mit der das Unternehmen zu einer datenschutzgerechten Handhabung angehalten wird.
Wegen der durchgeführten unzulässigen Videoüberwachung und der Übertragung der Bilddaten auf die Unternehmenshomepage wird der TLfDI ein Ordnungswidrigkeitenverfahren gegen das Unternehmen oder dessen Geschäftsführer einleiten.

Pakete sind in Läden, die neben ihrem eigentlichen Kerngeschäft auch als Paketshop dienen, so aufzubewahren, dass Kunden die entsprechenden Adressaufkleber nicht einsehen können, da diese dem Postgeheimnis unterfallen.

3.51 „Livestream“ aus dem Friseursalon: Videogaga 25

Auf einen Hinweis hin erfuhr der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), dass die Inhaberin eines Friseursalons auf der Homepage eine „Live-Ansicht“ ihres Geschäftes veröffentlicht habe, wodurch Arbeitnehmer und Kunden für jedermann jederzeit im Internet sichtbar wären.
Nach Recherchen des TLfDI war auf der Homepage des Friseursalons über einen Link tatsächlich eine „Live-Ansicht“ möglich, indem durch ein Anklicken auf den Spruch „Klicken Sie hier und schauen

Sie uns bei der Arbeit zu“ ein „Livestream“ aus dem Friseursalon einsehbar war. Die Aufnahmekamera war unmittelbar auf die Friseurstühle gerichtet, sodass Kunden und Arbeitnehmer vollständig gesehen werden konnten. Zum Zwecke der Beweiserhebung wurden mehrere Screenshots aufgenommen und der Akte beigefügt. Darauf zu sehen waren die Inhaberin des Friseursalons und ein männlicher Kunde, dem gerade die Haare geschnitten wurden sowie eine weitere Kundin, die für ein kurzes Gespräch das Geschäft betreten hatte.
Nachdem die Saloninhaberin vom TLfDI aufgefordert wurde, einen Fragenkatalog unter anderem zum Zweck der Videoüberwachung zu beantworteten und die angeforderten Nachweise, wie zum Beispiel den Grundriss des Salons, den Standort der Kamera und Screenshots beim TLfDI einzureichen, erläuterte der TLfDI den Sachverhalt wie folgt: Eine Videokamera ist eine Überwachungsanlage. Ihr bleibt nichts verborgen. Gerade am Arbeitsplatz kann eine Überwachung dazu führen, dass man sich ständig beobachtet und kontrolliert fühlt. Bei der Überwachung am Arbeitsplatz stoßen zudem die Interessen von Arbeitnehmer und Arbeitgeber aufeinander.
Die Aufzeichnung von Bildern stellt eine Datenerhebung dar, die nach § 4 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nur zulässig ist, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift sie erlaubt. Weder die Kunden noch die Arbeitnehmer hatten in die Videoüberwachung wirksam eingewilligt. Die Kunden waren sich zum einen der Überwachung oftmals nicht bewusst, zum anderen kann aufgrund des bloßen Verweilens in dem Geschäft nicht von einer wirksamen Einwilligung ausgegangen werden. Nach § 4 a Abs. 1 Satz 3 BDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Hiervon kann angesichts der Schwere des Eingriffs nicht ausgegangen werden. Eine wirksame Einwilligung setzt jedenfalls voraus, dass der Betroffene sich der Art und des Umfangs des Eingriffes bewusst ist. Dies war nicht der Fall. Bei Arbeitnehmern kann aufgrund des bestehenden Abhängigkeitsverhältnisses zum Arbeitgeber generell nicht von einer nach § 4 a Abs. 1 Satz 1 BDSG erforderlichen, „freien Entscheidung des Betroffenen“ ausgegangen werden.
Als mögliche gesetzliche Grundlage für eine Videoüberwachung kommt § 6 b BDSG in Betracht. Bei öffentlich zugänglichen Flächen und Arbeitsplätzen, wie in diesem Fall dem Friseursalon, ist die Videokontrolle gemäß § 6 b BDSG nur erlaubt, wenn sie zur Wahr-

nehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Die Inhaberin des Salons benannte als Zweck der Videoüberwachung und Übertragung ins Internet die Werbung für ihr Geschäft. Hierbei handelt es sich sicherlich um ein berechtigtes Interesse, für das die Videoüberwachung auch noch erforderlich sein mag. Jedenfalls aber überwiegen die schutzwürdigen Interessen der Kunden und Arbeitnehmer daran, bei dem Friseurbesuch oder bei der Arbeit nicht gefilmt zu werden sowie daran, dass diese Aufnahmen nicht der Weltöffentlichkeit zur Verfügung gestellt werden.
Die Saloninhaberin wurde vom TLfDI aufgefordert, die Videoüberwachung nach Erhalt des Schreibens unverzüglich zu beenden. Die Kamera war sofort zu entfernen. Des Weiteren war der Link „Klicken Sie hier und schauen Sie uns bei der Arbeit zu“ sowie der dazugehörige Hinweis: „Live Ansicht“ von der Homepage zu entfernen. Den entsprechen Nachweis hat die Saloninhaberin beim TLfDI erbracht.

Ein Livestream (aus dem Friseursalon) stellt immer einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Kundinnen und Kunden und der Arbeitnehmerinnen und Arbeitnehmer dar. Hier überwiegen in aller Regel die schutzwürdigen Interessen dieser Betroffenen das Interesse derjenigen Person, die die Aufnahmen ins Internet einstellt.

3.52 Peepshow im Wald: Videogaga 26

Die Presse berichtete wiederholt über die datenschutzrechtliche Problematik bei Tierbeobachtungskameras im Wald. Rechtlich stellt sich die Lage wie folgt dar:
Die Zulässigkeit von Tierbeobachtungskameras ist nach dem Bundesdatenschutzgesetz (BDSG) zu beurteilen. Nach § 6 b BDSG ist die Beobachtung öffentlich zugänglicher Bereiche zur Wahrnehmung berechtigter Interessen zulässig, wenn die damit verfolgten Zwecke vorher konkret festgelegt worden, die Beobachtung auch zur Erfüllung dieser Zwecke erforderlich ist und keine Anhaltspunkte für ein Überwiegen schutzwürdiger Interessen der Betroffenen erkennbar sind. Es ist daher im Einzelfall eine Abwägung zwischen den

Interessen des Kamerabetreibers, in aller Regel des Jägers, und den Interessen der Personen abzuwägen, die potenziell Gegenstand der Videobeobachtung im Wald werden können. Aufgrund des Grundrechts auf informationelle Selbstbestimmung nach Artikel (Art.) 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz bzw. Art. 6 Abs. 2 Thüringer Verfassung hat jeder Einzelne das Recht, sich in der Öffentlichkeit frei und ungezwungen aufhalten zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Jedermann darf sich im Wald generell frei bewegen und auch abseits der Wald- bzw. Wanderwege durch das Gelände streifen. Hierbei rechnet er keinesfalls damit, in den Aufnahmebereich einer Videokamera zu gelangen. Bei dem Aufenthalt im Wald stehen die Entspannung und der Rückzug der Persönlichkeit im Vordergrund. Daher besteht hier ein besonders hoher Schutzbedarf des Persönlichkeitsrechts des Betroffenen. Es ist daher davon auszugehen, dass in aller Regel die schutzwürdigen Interessen derjenigen überwiegen, die potenziell von der Videoüberwachung erfasst werden können. Jedenfalls sind aber Anhaltspunkte für ein solches Überwiegen vorhanden, weswegen die Kameras zur Wildbeobachtung in der Regel unzulässig sind.

Aus diesem Grund trat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) an das Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz (TMLFUN) heran, und bat um Mitteilung, ob und gegebenenfalls an welchen Stellen es in Thüringen derartige Videoüberwachung durch Jäger im Wald gibt. Dieses teilte mit, dass es unter anderem zur Überwachung von Schwarzwildkirrungen oder zum Nachweis von Luchs oder Wildkatze über sogenannte Risse Fotofallen gäbe, die Jäger aus privaten Gründen betrieben. Angaben zu konkreten Standorten oder zu Videoüberwachung konnten nicht gemacht werden.

Der TLfDI kann nur tätig werden, wenn konkrete Hinweise auf eine bestimmte Videoüberwachung vorliegen. Es gab eine Beschwerde, bei der ein Beschwerdeführer lediglich Fotos von der Kamera einreichte, den genauen Standort der Videoüberwachung im Wald aber – auch auf Nachfrage hin – nicht näher bezeichnete. Daher konnte der Eingabe nicht nachgegangen werden. Der TLfDI steht allerdings mit dem Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt hinsichtlich der allgemeinen datenschutzrechtlichen Problematik mit Wildkameras in Kontakt.

In aller Regel überwiegen bei Tierbeobachtungskameras im Wald die schutzwürdigen Interessen der von der Videoüberwachung Betroffenen und die Videoüberwachung ist unzulässig. Der TLfDI kann allerdings nur bei konkreten Hinweisen tätig werden.

3.53 Offene Tür

Fast zufällig entdeckte der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in den Betriebsräumen eines alten volkseigenen Betriebes eine Vielzahl an Arbeitnehmerakten, die mehr oder weniger zugänglich in den alten Betriebsräumen gelagert wurden. Die Akten befanden sich in einem Raum, der durch einen „leeren“ Türrahmen, das heißt ohne Tür, zugänglich war. Einzigen Schutz vor Zugriffen Dritter bot der nicht ganz einfach zu findende Weg durch das Gebäude selbst. Noch dazu war dieses teilweise an andere Unternehmen vermietet, die theoretisch dadurch einfach Zugang zu den Akten hatten.
Dies stellt selbstverständlich einen datenschutzrechtlich nicht hinnehmbaren Zustand dar. Datenschutzrechtliche Normen greifen nicht nur dann, wenn die verantwortliche Stelle personenbezogene Daten erheben, verarbeiten oder nutzen möchte. Vielmehr hat die verantwortliche Stelle auch so genannte technische und organisatorische Maßnahmen zu treffen, durch die sichergestellt ist, dass die Anforderungen des Bundesdatenschutzgesetzes (BDSG) gewährleistet werden, § 9 BDSG. Eine solche technische Maßnahme stellt in diesem Fall beispielsweise eine Tür mit Schloss und Schlüssel, eine organisatorische Maßnahme die dazugehörige Schlüsselregelung dar.
Da die nach BDSG verantwortliche Stelle nicht ohne weiteres feststellbar war, wurden die Akten unter zu Hilfenahme des örtlich zuständigen Ordnungsamtes zunächst gegen einen Zugriff Unbefugter gesichert. Inzwischen konnte der TLfDI aber die verantwortliche Stelle ermitteln. Auf Wirken des TLfDI hin wird eine ausreichend sichere Tür installiert, damit die Arbeitnehmerakten bis ans Ende ihrer Aufbewahrungsfrist sicher verwahrt werden können.

Arbeitnehmerakten müssen nach den Vorschriften des BDSG gelagert werden. Entweder gibt man diese dazu in die Hände eines seriösen Aktenverwahrunternehmens und schließt den hierzu notwendigen Auftragsdatenverarbeitungsvertrag ab oder man lagert die Akten selbst. In letzterem Fall ist allerdings ebenfalls mit derselben Sorgfalt

das Mindestmaß an Datenschutz, so wie es das BDSG beschreibt, einzuhalten.

4 Ordnungswidrigkeitenverfahren

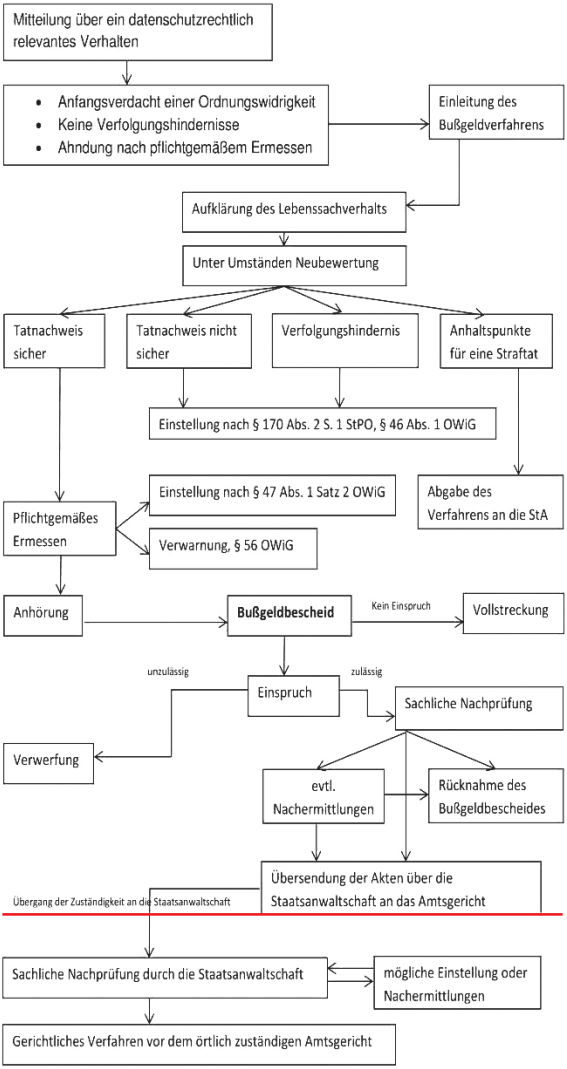
Mit Übertragung der Zuständigkeit für den Datenschutz im nicht-öffentlichen Bereich auf den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist dieser auch zuständige Behörde für Ordnungswidrigkeiten nach § 43 Bundesdatenschutzgesetz (BDSG) geworden. Das Verfahren musste auch behördenintern neu aufgebaut werden, da es sich um ein vom bisherigen Zuständigkeitsbereich völlig unterschiedliches Verfahren handelt. Das Ordnungswidrigkeitenverfahren bietet mit seinen großzügigen Verweisen in das Strafprozessrecht eine Vielzahl an neuen Ermittlungsansätzen, mit denen sich die Behörde zunächst vertraut machen musste. Es ist davon auszugehen, dass die Fallzahlen weiter stark ansteigen werden. Das Ordnungswidrigkeitenverfahren ist eine besondere Unterart des Verwaltungsverfahrens. Es ist streng von anderen Verfahren zu trennen. Im Unterschied zum grundsätzlich formfreien Verwaltungsverfahren handelt es sich um ein streng formalisiertes Verfahren mit vielen Parallelen zum strafrechtlichen Ermittlungsverfahren. Ziel des Verfahrens ist es, Verstöße gegen das Bundesdatenschutzgesetz zu ahnden und auf diesem Wege eine Änderung im Verhalten des Verstoßenden zu erreichen.
Im Wesentlichen teilt sich die Befugnis des TLfDI bei Ordnungswidrigkeiten wegen eines Verstoßes gegen Formalien des BDSG sowie gegen inhaltliche Vorgaben des BDSG auf. Erstere können mit einem Bußgeld bis zu 50.000 Euro, letztere mit bis zu 300.000 Euro geahndet werden. Dabei wird die Höhe der Geldbuße durch die Bedeutung der Ordnungswidrigkeit und den Vorwurf, der den Täter trifft, bestimmt. Es wird also die vorsätzliche Übermittlung von Gesundheitsdaten mit einem höheren Bußgeld geahndet als die versehentliche Herausgabe von Kundendaten eines Tabakgeschäftes, wobei die Herausgabe eines Datensatzes weniger schwer wiegt, als die Herausgabe vieler Datensätze. Letztlich ist die Höhe des Bußgeldes immer anhand des Einzelfalls und der damit einhergehenden Besonderheiten festzumachen. An die eben genannten Obergrenzen ist der TLfDI bei der Bemessung der Geldbuße allerdings dann nicht gebunden, wenn durch den zu ahndenden Verstoß ein wirtschaftlicher Vorteil über diesen Betrag hinaus entstanden ist. Diesen Vorteil soll die Geldbuße auf jeden Fall übersteigen. Verstöße gegen das BDSG können auch als Straftaten verfolgt werden. Stellt der TLfDI

im Rahmen seiner Ermittlungen oder seiner sonstigen Verwaltungstätigkeit fest, dass der Tatbestand einer Ordnungswidrigkeit gegen Entgelt, mit Bereicherungs- oder Schädigungsabsicht verwirklicht worden ist, gibt er das Verfahren zur Straftatverfolgung an die zuständige Staatsanwaltschaft ab. Der TLfDI verfügt über ein eigenes Strafantragsrecht.

Wegen der Sensibilität von Berichten über Datenschutzverstöße im nicht-öffentlichen Bereich im Allgemeinen und im Bereich der Ordnungswidrigkeiten im Speziellen kann über die Tätigkeit des TLfDI in diesem Bereich nur sehr allgemein berichtet werden. Seit der Übernahme dieses Bereiches durch den TLfDI sind die Fallzahlen von 2011 auf 2012 um 100 % angestiegen, von 2012 zu 2013 gar um 250 %. Die Tendenz ist weiterhin steigend.

Zur besseren Verständlichkeit und Übersicht ist das Bußgeldverfahren hier als Grafik dargestellt, in der man die jeweils möglichen Verfahrenswege und -möglichkeiten erkennen kann. Ab der roten Linie sieht das Ordnungswidrigkeitenrecht vor, dass das Verfahren aus der Zuständigkeit der Verwaltungsbehörde (TLfDI) als Ermittlungsbehörde in die Zuständigkeit der Staatsanwaltschaft übergeht.

Übersicht über den Ablauf eines Bußgeldverfahrens



Bei den bisher anhängigen Verfahren wird in den meisten Fällen wegen Verstößen gegen das unbefugte Erheben oder Übermitteln von personenbezogenen Daten ermittelt. Berichtet wird hier nur über Fälle, die bereits abgeschlossen sind.

Interessant war ein Verfahren gegen einen Auszubildenden einer Bank, der einem besonderen Berufsgeheimnis unterlag. Der Auszubildende gab Informationen über einen Kunden seiner Arbeitgeberin an Dritte weiter. Dies erfüllt den Bußgeldtatbestand nach § 43 Abs. 2 Nr. 1 BDSG. Hier wird mit Bußgeld bedroht, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Die Weitergabe der Informationen stellt eine Übermittlung dar, die in den Überbegriff der Verarbeitung fällt. Damit war der Tatbestand erfüllt und der TLfDI erließ einen Bußgeldbescheid gegen den Auszubildenden. Eingeräumt wurde, dass er den Bußgeldbetrag in zwei Raten begleicht.

In einem weiteren Fall wandte sich ein Arbeitnehmer an den TLfDI mit folgendem Hinweis: Er habe bei zwei verschiedenen Arbeitgebern gearbeitet. Sein „Hauptarbeitgeber“ verlangte im Rahmen einer arbeitsrechtlichen Streitigkeit wegen nicht genehmigter Nebentätigkeit vom anderen Arbeitgeber den Arbeitsvertrag heraus, den dieser dann auch an den Hauptarbeitgeber faxte. Eine Übermittlung personenbezogener Daten ist jedoch nur dann möglich, wenn das BDSG oder eine andere datenschutzrechtliche Vorschrift hierzu einen Erlaubnistatbestand bereithält oder der Betroffene in die Übermittlung eingewilligt hat. Eine Einwilligung lag hier nicht vor. Ebenfalls war ein Erlaubnistatbestand nicht gegeben. Im Rahmen des Arbeitsverhältnisses kommt allenfalls § 32 BDSG als Erlaubnistatbestand in Frage. Dieser genehmigt das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses, soweit diese für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich sind. Hier mangelte es schon an der Zweckbindung der Handlung. Die Übersendung eines Arbeitsvertrages an Dritte ging hier über den Zweck des Beschäftigungsverhältnisses hinaus. Damit stellte das Versenden des Arbeitsvertrages eine unerlaubte Übermittlung dar, § 43 Abs. 2 Nr. 1 BDSG. Der TLfDI erließ dementsprechend einen Bußgeldbescheid gegen den (Neben-)Arbeitgeber.

Ähnlich gelagert war ein Fall um einen Hotelier, der einem Ehemann auf dessen Anfrage hin Angaben machte, mit welchem anderen

Mann dessen Ehefrau im Hotel übernachtet hätte. Da das BDSG keinen Übermittlungstatbestand für die Bekanntgabe eventueller Seitensprüngen bereithält, handelte es sich auch hierbei um eine vorsätzliche unerlaubte Übermittlung nach § 43 Abs. 2 Nr. 1 BDSG. Der Hotelier ging gegen den vom TLfDI erlassenen Bußgeldbescheid mit dem Rechtsmittel des Einspruchs vor, unterlag damit allerdings vor Gericht.

Nicht alle Anzeigen von angeblichen Ordnungswidrigkeiten nach dem BDSG führen zu einem Bußgeldbescheid. Oftmals ist eine Ordnungswidrigkeit nach dem laienhaften Empfinden zu einem Vorgang oder Sachverhalt zwar gegeben, stellt nach rechtlicher Betrachtung aber keine solche dar. Die Einstellung des Verfahrens ist dann zwingende Folge. Es kommt auch vor, dass sich dem „Täter“ nicht mehr alle notwendigen Elemente der Tat nachweisen lassen. Denn, daran muss man immer denken: Der TLfDI muss dem, gegenüber dem er einen Bußgeldbescheid erlässt, die Ordnungswidrigkeit in allen Punkten nachweisen. Dies ist nicht immer möglich. In solchen Fällen gilt die Unschuldsvermutung, mit der Folge, dass das Verfahren eingestellt werden muss.

Einen weiteren, weit verbreiteten Bußgeldtatbestand stellt das nicht oder nicht vollständige Beantworten von Auskunftsersuchen des TLfDI seitens der verantwortlichen Stellen, in der Regel Unternehmen, dar. Dies ist überraschend, denn die Tatsache, dass die Angeschriebenen zur Antwort verpflichtet sind und ein Unterlassen mit einem Bußgeld geahndet werden kann, wird bereits im ersten Anschreiben mitgeteilt. Die Antwort bekommt der TLfDI immer, es wird irgendwann für die Betroffenen nur sehr teuer. Denn jedes erneute Auskunftsersuchen, das nicht beantwortet wird, stellt einen neuen Bußgeldtatbestand dar, der wiederum mit einem neuen Bußgeld geahndet werden kann.

So war der folgende Fall gelagert: Der TLfDI wandte sich mit einem Auskunftsersuchen unter Fristsetzung an einen Bürger. Es wurden Informationen über eine von dieser Person durchgeführte Videoüberwachung verlangt. Nachdem die Frist fruchtlos auslief, wurde eine Nachfrist gesetzt. Als innerhalb dieser Frist ebenfalls keine Antwort einging, erließ der TLfDI nach erfolgter Anhörung einen Bußgeldbescheid wegen vorsätzlichen Nichtantwortens auf ein Auskunftsersuchen des TLfDI nach § 38 Abs. 3 BDSG. Diese Ordnungswidrigkeit ist in § 43 Abs. 1 Nr. 10 BDSG geregelt.

Der größte Teil der Fälle, die der TLfDI im Berichtszeitraum bearbeitete, ist allerdings noch nicht abgeschlossen. Entweder dauern die Ermittlungen noch an oder die Bußgeldbescheide sind noch nicht rechtskräftig. Von den im Berichtszeitraum erlassenen Ordnungswidrigkeitsbescheiden ist bisher kein einziger durch ein Gericht aufgehoben worden.
In besonders schweren Fällen des Verstoßes gegen Vorschriften aus dem BDSG kann der TLfDI auch einen Strafantrag bei der zuständigen Staatsanwaltschaft stellen. Diese prüft dann in eigener Zuständigkeit das Vorliegen einer Straftat. Eine solche kommt dann in Betracht, wenn eine der in § 43 Abs. 2 BDSG bezeichneten Handlung vorsätzlich gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, vorgenommen wird.
Im Berichtszeitraum hat der TLfDI einen Strafantrag gestellt. Dieser richtete sich gegen den ehemaligen Geschäftsführer und der-zeitigen Liquidator eines insolventen Aktenverwahrungsunternehmens.

Das Bußgeldverfahren wurde im Berichtszeitraum beim TLfDI erfolgreich aufgebaut. Es wird zunehmend an Bedeutung gewinnen, wie auch die steigenden Fallzahlen zeigen.

5 Veranstaltungen

Old man using a laptop with his grand son reading a newspaper
© Yuri Arcurs – Fotolia.com

5.1 TLfDI ist los!

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) war im Berichtszeitraum auf zahlreichen Veranstaltungen vertreten bzw. führte selbst Veranstaltungen rund um das Thema Datenschutz durch:
So fand eine mehrtätige Fortbildungsveranstaltung zum Datenschutz im Sozialrecht im Jobcenter Jena statt. Die Arbeitnehmer hatten dem TLfDI zuvor Fragen zugesandt, die dann im Rahmen der Veranstaltung beantwortet wurden.
Für die Studierenden der Verwaltungsfachhochschule Gotha wurde eine Vorlesung zu den Grundlagen des in Thüringen geltenden Datenschutzrechts entwickelt. Die Studierenden wurden dann an zwei Tagen in das Datenschutzrecht eingeführt.
Zweimal fand ein Runder Tisch mit der Landeskrankenhausgesellschaft Thüringen und Vertretern der Landesärztekammer sowie Vertretern von Krankenhäusern zur Weiterentwicklung der Orientierungshilfe Krankenhausinformationssysteme statt (siehe 10. Tätigkeitsbericht für den öffentlichen Bereich Punkt 11.1).
Der TLfDI war in dem Jahr beim Tag der offenen Tür des Thüringer Landtags vertreten, sowie im Folgejahr beim Bürgerfest „Rund um die Verfassung“.
Gemeinsam mit der Verbraucherzentrale Thüringen e. V. und dem Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien (ThILLM) führte der TLfDI eine Tagung „Soziale“ Netzwerke? Meine Daten! Mein Leben! – Dein Geschäft!“ durch. Bei dieser Veranstaltung sollten vor allem Schülern und Lehrern die Hintergründe Sozialer Netzwerke verdeutlicht und die damit verbundenen Probleme näher beleuchtet werden. Aufgrund der positiven

Resonanz, die der TLfDI wegen dieser Veranstaltung erhielt, führte er im Folgejahr wiederum gemeinsam mit der Verbraucherzentrale Erfurt e. V. eine Kooperationsveranstaltung zum Thema „Persönlichkeitsrechte – auch im Internet – keine Frage des Alters!“ durch, die sich speziell an Seniorinnen und Senioren richtete. Die Veranstaltung sollte den Teilnehmern in Vorträgen und Workshops ihre Rechte in der digitalen Welt aufzeigen. Der TLfDI war auch auf der Seniorenakademie der Stadt Gotha zum Thema „Der gläserne Bürger“ vertreten. Ebenfalls an Seniorinnen und Senioren richtete sich die Informationsveranstaltung der Eisenbahn- und Verkehrsgewerkschaft der Ortsverwaltung Erfurt, auf der der TLfDI zu Fragen des Datenschutzes zur Verfügung stand.

Mit der Evangelischen Akademie Thüringen und der Landesarbeitsgemeinschaft Kinder- und Jugendschutz e. V. veranstaltete der TLfDI eine Tagung zum Thema „Das Ende der Privatsphäre?“. Die Tagung befasste sich mit der Frage, wo heute die Grenzen zwischen Privatheit und Öffentlichkeit verlaufen und wie es gelingen kann, sinnvolle Regularien des digitalen Persönlichkeitsschutzes zu entwickeln.

Der TLfDI hat im Jahr 2013 in seiner Funktion als Landesbeauftragter für die Informationsfreiheit für ein Jahr den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland übernommen. In dieser Funktion richtete er zwei Sitzungen des Arbeitskreises der Informationsfreiheitsbeauftragten aus. Dieser Arbeitskreis bereitet die Sitzungen und Entschließungen der Konferenz der Informationsfreiheitsbeauftragten vor. Außerdem fanden am 27. Juni 2013 in Erfurt und am 28. November 2013 in Erfurt die 26. und 27. Konferenz der Informationsfreiheitsbeauftragten in Deutschland statt. Hierüber wird der TLfDI in seinem Tätigkeitsbericht als Informationsfreiheitsbeauftragter, der nächstes Jahr erscheinen wird, berichten.

Im Schulamt Nordthüringen führte der TLfDI eine Veranstaltung zum Thema Datenschutz und Internet als Fortbildungsveranstaltung für Lehrer durch. Ähnlich gelagerte Informationsveranstaltungen fanden am Friedrich-Schiller-Gymnasium Weimar, am Gustav-Freytag-Gymnasium Gotha und am Albert-Schweitzer-Gymnasium Ruhla für Lehrer statt.

Im Thüringer Landtag hielt der TLfDI für Bachelor-/Masterstudenten einen Vortrag über Maßnahmen zur Einhaltung bzw. Verbesserung des Datenschutzes in Thüringen speziell für

den Bereich Transport und Verkehr. Er nahm außerdem an der Podiumsdiskussion zum Thema „Die totale Überwachung - Gefahr im Netz für die Gesellschaft, für die Demokratie und für Medien?“ des Vereins zur Förderung der angewandten Informatik der Fachhochschule Erfurt teil.
Gegenüber dem Verband der Verwaltungsbeamten des höheren Dienstes in Thüringen e. V. stellte der TLfDI seine Behörde und ihr Aufgabengebiet vor. Dem gleichen Zweck diente die Teilnahme an der Konferenz der Datenschutzbeauftragten im Bereich der Katholischen Kirche Deutschlands am 19./20. Oktober 2013.
Der TLfDI war auch auf einigen Veranstaltungen der Industrie- und Handelskammern in Thüringen vertreten, hierzu wird auf den Beitrag unter Punkt 3.2 verwiesen. Im Berichtszeitraum nahm der TLfDI daneben an vier Sitzungen des ERFA-Kreises teil. Die Gesellschaft für Datenschutz und Datensicherheit e. V. hat zur Durchführung ihrer Aufgaben regionale Erfahrungsaustauschkreise (ERFA-Kreise) gebildet, die zum Ziel haben, die Arbeit der Teilnehmer in Fragen des Datenschutzes und der Datensicherheit zu unterstützen. Die ERFA-Kreise stehen grundsätzlich allen Interessierten offen, bedürfen jedoch der vorherigen Anmeldung. Eingeladen sind in erster Linie Datenschutzbeauftragte.
Die Fraktion „DIE LINKE“ initiierte eine Kryptoparty im Thüringer Landtag“, die der Information über Verschlüsselungstechniken diente. Der TLfDI nahm an der Podiumsdiskussion „Notwendigkeit (?) staatlicher Überwachung im Internet vs. Schutz der Privatsphäre“ teil. Zusammen mit der Friedrich-Ebert-Stiftung und der SPD-Fraktion führte er die Veranstaltung „Nach NSA: Kann die Verfassung uns noch vor den Geheimdiensten schützen?“ durch, die sich mit den Gefahren der ausufernden Überwachung auseinandersetzte. Anschließend gab es auch hier eine Kryptoparty.

Der TLfDI ist bestrebt, interessierten Stellen den Datenschutz auch im Wege des Dialogs nahezubringen. Zu diesem Zweck nahm er im Berichtszeitraum an zahlreichen Veranstaltungen teil und führte auch selbst Informations- und Fortbildungsveranstaltungen durch.

Anlagen

Anlage 1

Fragenkatalog für Kontrollen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Datum: .....
Uhrzeit: .....
Betrieb: .....
AP: .....

Fragenkatalog für Kontrollen TLfDI
- nichtöffentlicher Bereich -

Allgemeine Fragen

1. Welche Arten von personenbezogenen Daten werden in Ihrem Unternehmen verarbeitet?

2. Personaldaten (Lohnabrechnung, Zeiterfassung)

3. Kunden- und/oder Lieferantendaten (Detailfragen ab Pkt. 29.)

4. Werden personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet?

5. Werden Daten in nicht automatisierten Dateien, die aus einer automatisierten Verarbeitung stammen verarbeitet?

Datenschutzbeauftragter

6. Wie viele Personen sind in Ihrem Unternehmen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt (incl. Geschäftsleitung)?

7. Haben Sie einen betrieblichen Datenschutzbeauftragten (bDSB) gemäß § 4f BDSG?
   Gibt es für den bDSB eine schriftliche Bestellung?

8. Über welche fachlichen Kenntnisse verfügt der bDSB?

9. Welche (schriftlichen) Richtlinien / Anweisungen gibt es im Unternehmen zur Einbeziehung des bDSB?

10. Welcher Zeitanteil steht dem bDSB für seine Aufgaben zur Verfügung?

11. Welche sonstigen Aufgaben hat der Datenschutzbeauftragte neben dieser Funktion im Unternehmen noch wahrzunehmen?

12. Gibt es ein eigenes Budget für den Datenschutzbeauftragten?

13. Wie ist der Datenschutzbeauftragte in das Unternehmen eingegliedert und wem ist er unterstellt?

14. Wer ist Ansprechpartner für betroffene Personen, die ihre Datenschutzrechte wahrnehmen wollen?

15. Wie werden Ihre Mitarbeiter, die mit personenbezogenen Daten arbeiten, auf das Datengeheimnis (§ 5 BDGS) verpflichtet?
    Wer verpflichtet die Mitarbeiter?
    Wann erfolgt die Verpflichtung?

Auftragsdatenverarbeitung § 11 BDSG

16. Welche Dienstleister werden mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt?
    (Anmerkung: betrifft z.B. Verfahren der Lohn-/Gehaltsabrechnung, Kundenbindungsprogramme, Banküberweisungen, die das Unternehmen als Auftraggeber vertraglich durchführen lässt)

17. Welche Verträge wurden mit diesen Dienstleistern abgeschlossen?

In welcher Form sind die Verträge dokumentiert?

18. Nach welchen Kriterien werden die Dienstleistungsunternehmen ausgewählt und wie wird die ordnungsgemäße Auftragsabwicklung überwacht?

Technisch-organisatorischer Datenschutz

19. Welche allgemeinen technischen und organisatorischen Maßnahmen wurden in Ihren Unternehmen getroffen, um die Ausführung der Vorschriften des BDSG zu gewährleisen?

20. Wie sind diese Maßnahmen dokumentiert?

21. Gibt es ein Konzept über die Gesamtheit der Sicherheitsmaßnahmen (IT-Sicherheitskonzept)?

22. Wie sind der/die Server, die Rechner und das Netzwerk vor unbefugten Zugriffen von außen und innen geschützt?

23. Gibt es bzgl. der IT-Räume und der Datenverarbeitungsanlagen sowie der innerbetrieblichen Organisation Konzepte zur
    a. Zutrittskontrolle
    b. Zugangskontrolle
    c. Zugriffskontrolle

24. Wie erfolgt die Datensicherung? (Arbeitsanweisung, Workflow)

25. Werden mobile und andere Datenträger für personenbezogene Daten verwendet (USB-Sticks, CD-ROM; Laptop)?
    Sind diese sicher verschlüsselt?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

26. Was ist zur Sperrung bzw. Löschung von nicht mehr erforderlichen Daten in Ihrem Unternehmen festgelegt?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

27. Wie werden gesperrte Daten gekennzeichnet?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

28. Wie wird bei der Abgabe von Altgeräten oder Altdatenträgern an Dritte in Bezug auf die auf ihnen befindlichen personenbezogenen Daten vorgegangen?
    Auf welche Weise werden die Daten gelöscht?
    Welches Verfahren wird für den Löschvorgang eingesetzt? (z. B. Entmagnetisierung bzw. Neuausrichtung, Überschreiben, wie oft?)
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

29. Auf welche Art und Weise wird Altpapier entsorgt?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

30. Werden E-Mails mit personenbezogenen Daten versendet? (ja/nein)
    Wenn ja, auf welche Art und Weise werden diese E-Mails versendet?
    Gibt es in diesem Zusammenhang Konzepte zur Weitergabekontrolle, zur Eingabekontrolle, zur Auftragskontrolle und zur Verfügbarkeitskontrolle? (Arbeitsanweisungen, Workflow)

31. Gibt es einen Notfallplan für die Aufarbeitung einer eventuellen Datenpanne nach § 42 a BDSG?
    Welche (schriftlichen) Verfahrensanweisungen gibt es?

Kundendaten/ Geschäftspartner

32. Wo sind Kunden- und/oder Lieferantendaten gespeichert?

33. Wer hat Zugriff auf die Kunden- und/oder Lieferantendaten?

34. Fordern Sie Einwilligungen von Ihren Kunden ein? Wenn ja: zu welchen Sachverhalten und in welcher Form?

35. Führen Sie adressierte Werbung durch? Wenn ja nach welchen Kriterien?

36. Wann und wie werden Kunden- und/oder Lieferantendaten gelöscht?

Arbeitnehmerdaten

37. Wo sind die Arbeitnehmerdaten gespeichert?

38. Wer hat Zugriff auf diese Daten?

39. Wie ist die Zeiterfassung in Ihrem Unternehmen geregelt?

40. Welche Festlegungen bestehen zur dienstlichen und privaten Nutzung von E-Mail, Internet und TK-Anlagen am Arbeitsplatz? Wann werden E-Mails gelöscht?

41. Was wird bei der Nutzung von E-Mail und Internet warum protokolliert?

42. Wann und durch wen werden die Protokolldateien ausgewertet und gelöscht?

43. Wie erfolgt eine evtl. Telefonabrechnung (Einzelverbindungsnachweis)?

44. Gibt es Bestimmungen zur Verwendung privater Geräte, wie bspw. Smartphones und Tablets, für dienstliche Zwecke (Bring Your Own Device – BYOD)?

45. Besteht in Ihrem Unternehmen ein Betriebsrat? Wenn ja, gibt es Betriebsvereinbarungen, die die oben genannten Bereiche oder anderen Umgang mit personenbezogenen Daten regeln?

46. Veröffentlichen Sie Arbeitnehmerdaten im Internet?

Internetseite

47. Betreiben Sie eine Internetseite? Wenn ja:

    - auf welchem Webserver?

    - Erfassen Sie Daten von Besuchern (bspw. mittels Tracking – Google-Analytics, Piwik…usw.)?

    - Betreiben Sie Foren und Blogs im Internet?

    - veröffentlichen Sie personenbezogene Daten?

48. Erfassen Sie auch Kundendaten über das Internet? Wenn ja über SSL/TLS?

Videoüberwachung

49. Findet Videoüberwachung innerhalb oder außerhalb des Firmengebäudes statt?

50. Wie viele Kameras sind an welchen Stellen im Unternehmen im Einsatz?

51. Für welche Zwecke erfolgt die Videoüberwachung und welche schriftlichen Festlegungen gibt es dazu?

52. Sind die Bilder bzw. Videosequenzen live zu beobachten?
    Wenn ja, wo und mit welchem Wiedergabemedium erfolgt die Beobachtung (PC-Bildschirm, mobiles Gerät)?

53. Erfolgt die Beobachtung permanent oder lediglich bei Bedarf (z. B. bei Vorkommnissen)?

54. Gibt es Zoommöglichkeiten und/oder ist/sind die Kamera/s schwenkbar?
    Wenn ja, bei welchen Kameras ist dies der Fall und zu welchem Zweck sind diese Funktionalitäten vorgesehen?

55. Gibt es in diesen Bildern bzw. Videosequenzen Schwärzungen?

56. Werden Bilder bzw. Videosequenzen aufgezeichnet?
Wenn ja, wie lange erfolgt die Speicherung?

57. Auf welchen Datenträgern werden Bilder/Videosequenzen aufgezeichnet?

58. Wird auf die Videoüberwachung hingewiesen? Wenn ja, auf welche Weise?

Anlage 2

Beschluss der obersten Aufsichtsbehörden im Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 17. Januar 2012)

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung[b]

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY1 daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z. B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (Krankenversicherung)2 benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache,

[b] Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5]
Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY *[Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird]* selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[7]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesund-

heitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

☐ Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[8] erhebt und für diese Zwecke verwendet. Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren[9] vor Antragstellung an die Versicherung XY übermittelt werden. Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang – soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von

ihrer Schweigepflicht. Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.[10]

Möglichkeit II:

☐ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

- in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder
der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[11] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte[12] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige

Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[13]

Möglichkeit I:

- ☐ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

Möglichkeit II:

- ☐ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.[14]

3.1. Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.[15]

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten
entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XYGruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter (Internetadresse) eingesehen oder bei (Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die

Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt. Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt. Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.
Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.[25] Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.
Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.
Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet[26]

Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheits-

daten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, http://www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.[28] Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen
ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Infor-

mationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragenweiterer

Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres
Ort, Datum	Unterschrift des gesetzlichen Vertreters

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel - BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt

keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z. B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung ***dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.***

---

[1] Hier und im Folgenden kann anstelle von „die Versicherung XY“ der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY“) jeweils „wir“ eingefügt werden.
[2] Hier kann die konkrete Sparte genannt werden.
[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier

einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

[4] Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

[5] Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4 a Abs. 1 Satz 2 BDSG

[6] Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

[7] Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

[8] Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

[9] Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

[10] Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i. V. m. Abs. 4 VVG

[11] Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

[12] Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

[13] Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z. B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

[14] Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

[15] Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.
[16] Der Satzteil "für sich und" ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.
[17] Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.
[18] In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragsdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.
[19] Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.
[20] Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z. B. Krankentransporte.

[21] Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.
[22] Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.
[23] „und sonstige Stellen“ – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.
[24] Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.
[25] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.
[26] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.
[27] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht.
Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

[28] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.
[29] Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.
[30] Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt.
Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.
[31] Es zählt das Datum der Unterschrift im Antrag.
[32] Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/ Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

Anlage 3

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 18./19. September 2012)

Near Field Communication (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6 c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

Anlage 4

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 26./27. Februar 2013)

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6 b Bundesdatenschutzgesetz (BDSG). Gemäß § 6 b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6 b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6 b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6 b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kame-

ras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

Anlage 5

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 11./12. September 2013)

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z. B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4 c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

Abkürzungsverzeichnis

Abkürzung	Bedeutung
Abs.	Absatz
Art.	Artikel
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BRAO	Bundesrechtsanwaltsordnung
BVerfG	Bundesverfassungsgericht
ERFA-Kreis	regionaler Erfahrungsaustauschkreis der Gesellschaft für Datenschutz und Datensicherheit e.V.
EuGH	Europäischer Gerichtshof
GbR	Gesellschaft bürgerlichen Rechts
GWG	Geldwäschegesetz
HWK	Handwerkskammer
i. V. m.	in Verbindung mit
IHK	Industrie- und Handelskammer
KunstUrhG	Kunsturheberrechtsgesetz
OHA	Orientierungshilfe Aktenaufbewahrung
OWiG	Ordnungswidrigkeitengesetz
PAuswG	Personalausweisgesetz
PDSV	Postdienste-Datenschutz-Verordnung
SGB	Sozialgesetzbuch
StPO	Strafprozessordnung
ThILLM	Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien
ThürMeldeG	Thüringer Meldegesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TLfDI	Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
TLvWA	Thüringer Landesverwaltungsamt
TMBWK	Thüringer Ministerium für Bildung, Wissenschaft und Kultur
TMLFUN	Thüringer Ministerium für Landwirtschaft, Forsten, Umwelt und Naturschutz
VSA	Verrechnungsstelle der Süddeutschen Apotheken

Sachregister

§ 28 BDSG	3.3; 3.12; 3.14; 3.37; Anlage 4.2
Absender	3.50
Adressdaten	3.50
Aktenaufbewahrung	3.1
Aktenvernichtung	3.25
Aktenverwahrer	3.7
Amtshilfe	3.7
Anlasslose Kontrolle	B. Vorwort
Anonymisierung	3.3; 3.39; 3.41;
Anwaltsgegnerliste	3.30
Apotheke	3.40; 3.41
Apothekenrechenzentrum	3.41
Arbeitgeber	3.14; 3.20; 3.28; 3.34; 3.51; 4;
Arbeitnehmer	B. Vorwort; 3.3; 3.9; 3.10; 3.12; 3.13; 3.14; 3.16; 3.18; 3.20; 3.12; 3.23; 3.25; 3.28; 3.31; 3.32; 3.34; 3.35; 3.39; 3.46; 3.51; 3.53; 4; 5.1; Anlage 1
Arbeitnehmerakten	3.53
Arbeitnehmerüberwachung	3.32; 3.34
Archivierungsunternehmen	3.1
Arztpraxis	3.25; 3.33;
Arzt	3.7; 3.25; 3.33; 3.40; 3.41; 5.1; Anlage 2;
Attrappe	3.22; 3.31
Aufbewahrungsfrist	3.7; 3.53;

Aufenthalts- und Essensräume	3.21; 3.37
Aufklärung von Straftaten	3.28
Aufsichtsbehörde	B. Vorwort; B.1; B.2; 3.13; 3.14; 3.34; 3.36; 3.44; 3.47; 3.49; 3.50; Anlage 2; Anlage 3; Anlage 4; Anlage 5;
Auftragsdatenverarbeitung	3.1; 3.7; 3.13; 3.14; 3.15; 3.19; 3.23; 3.24; 3.29; 3.31; 3.53; Anlage 1; Anlage 2;
Aufzeichnung von Bildern	3.51
Auskunft	B. Vorwort; 3.24; 3.30; 3.45; 4; Anlage 2
Außenbereich	3.10; 3.17
Ausweisnummer	3.45; 3.50
Auto	3.2; 3.17; 3.27; 3.31
Autohaus	3.2; 3.17; 3.31
BaFin	3.45
Bank	3.24; 3.45; 3.47; 4; Anlage 1;
Berechtigte Interessen	3.13; 3.37
Berufsgeheimnis	3.47; 4
Berufsverbot	3.25
Beschlüsse	B. Vorwort; B.2
Besondere Arten von personenbezogenen Daten	3.40; 3.47; Anlage 2
Betretungsrecht	3.7
Betrieblicher Datenschutzbeauftragter	3.1; 3.4; 3.12; 3.23; Anlage 1
Beweisverwertungsverbot	3.20
Bilder	3.8; 3.12; 3.13; 3.28; 3.42; 3.44; 3.51; Anlage 1; Anlage 4;
Blackbox-System	3.28

Blühende Landschaft	B. Vorwort
Broschüre	3.3
Bus	3.10
Bußgeld	3.13; 3.15; 3.23; 3.27; 3.37;
Bußgeldverfahren	3.13; 3.37; 4
Café	3.2; 3.8; 3.9
Chaotisches System	3.7
Dashboardkamera	3.27; 3.42
Datenschutzbeauftragter	B. Vorwort; B.2; 3.1; 3.2; 3.4; 3.12; 3.13; 3.23; 3.29; 3.31; 3.40; 5; Anlage 1
Datenspeicherung	3.24; 3.6
Datenträger	3.14; 3.15; Anlage 1
Datenübermittlung	3.14; 3.40; 3.50; Anlage 2; Anlage 5
DIN 32757	3.25
DIN 66399-1	3.25
Direkterhebungsgrundsatz	3.20
Duschraum	3.28
Düsseldorfer Kreis	B.2; 3.36; 3.42; Anlage 2; Anlage 3; Anlage 4; Anlage 5
Eheleute	4
Einkaufszentrum	3.36
Einwilligung	3.5; 3.14; 3.21; 3.33; 3.40; 3.44; 3.46; 3.51; 4; Anlage 1; Anlage 2; Anlage 5;
Einzelhandel	3.17; 3.19; 3.35
ERFA-Kreis	3.4; 5
Erforderlichkeit	3.8; 3.9; 3.10; 3.12; 3.13; 3.17; 3.21; 3.23; 3.26; 3.31; 3.34; 3.35; 3.36; 3.38; 3.39; 3.40; 3.42;

	3.43; 3.45; 3.46; 3.48; 3.50; 3.51; 3.52; 4; Anlage 2; Anlage 4; Anlage 5
Europäische Datenschutzrichtlinie	B. Vorwort
Europäischer Gerichtshof	B. Vorwort; 3.34
Evangelische Akademie	5.1
Fachhochschule Erfurt	5.1
Fahrgast	3.42; Anlage 4
Finanzamt	3.48
Firmenname	3.30
Flyer	3.2; 3.3
Frauenschutzeinrichtung	3.39
Freiheitsstrafe	3.33; 3.44
Freizeitgestaltung	3.8; 3.9; 3.37
Friseursalon	3.51
Frühstücksraum	3.37
Fußweg	3.10; 3.43
Gastronomie	3.9
GbR	3.30
Geburtstagsliste	3.46
Geeignetheit	3.8; Anlage 2
Gegnerliste	3.30
Geheimnis	3.12; 3.24; 3.33; 3.40; 3.47; 3.50; 4; Anlage 1
Geldbuße	3.47; 4
Geldstrafe	3.44
Geldwäschegesetz	3.45
Gericht	3.20; 3.24; 3.27; 3.30; 3.34; 3.44; 4
Gesellschaft für Datenschutz und Datensicherheit e. V.	3.4
Gesundheitsdaten	3.26; 3.40; 3.41; 4; Anla-

	ge 2
Grünes Rezept	3.40
Hackerangriff	3.47
Handwerksbetriebe	3.2
Handwerkskammern	3.2
Hausrecht	3.8; 3.10; 3.11; 3.13; 3.17; 3.22; 3.27; 3.35; 3.36; 3.37; 3.38; 3.43; 3.51
Hinweispflicht	3.35; 3.38;
Hoster	3.19
Hotelier	3.37; 4
Identitätsnachweis	3.48
Immelborn	3.1; 3.7
Industrie- und Handelskammer (IHK)	B. 1; 3.2; 3.3; 5.1
Informationsfreiheitsbeauftragter	5.1
Informationsveranstaltung	3.3; 5.1
Innenministerium	3.7
Insolvenz	3.24; 3.33; 3.5; 3.7; 3.24
Insolvenzverwalter	3.7
Internet	3.19; 3.30; 3.50; 3.51; 5.1; Anlage 1; Anlage 2
Internetshop	3.19
IT-Sicherheitskonzept	3.13; 3.16; Anlage 1
Jäger	3.52
Jobcenter	5.1
Kamera	3.8; 3.9; 3.10; 3.12; 3.13; 3.17; 3.18; 3.21; 3.22; 3.27; 3.28; 3.31; 3.32; 3.34; 3.35; 3.36; 3.37; 3.38; 3.42; 3.43; 3.44; 3.51; 3.52; Anlage 1; Anlage 4;

Kaufhaus	3.38
Kirche	3.40; 5.1
Kirchlicher Datenschutzbeauftragter	3.40
Konzern	3.13; 3.14; 3.29; 3.31
Konzernprivileg	3.14
Kooperationsveranstaltung	5.1
Kopie	3.13; 3.25; 3.31; 3.48
Krankenhaus	3.25; 3.26; 5.1; Anlage 2
Kreditkarten	3.47
Kryptoparty	5.1
Kundendaten	3.13; 3.16; 3.24; 3.31; 3.32; 3.35; 3.50; 3.51; 4; Anlage 1; Anlage 2
Kündigungsschutzprozess	3.20
Kunsturhebergesetz	3.44
Landesärztekammer	3.25; 5.1
Landeskrankenhausgesellschaft	5.1
Landesverwaltungsamt	B. Vorwort; B.1
Lichtbild	3.48
Link	3.3; 3.10; 3.30; 3.51; 5.1
Livestream	3.51
Löschung	3.13; 3.14; 3.30; Anlage 1
Meldepflicht	3.47
Monitoring	3.12
Nahverkehr	3.10
Nebentätigkeit	4
Notfallplan	3.47; Anlage 1
Öffentlich zugängliche Räume	3.8; 3.9; 3.10; 3.11; 3.12; 3.13; 3.14; 3.17; 3.21; 3.27; 3.35; 3.37; 3.38; 3.43; 3.44; 3.48; 3.49;

	3.51; 3.52
Öffentliche Wege	3.10; 3.13; 3.27; 3.38; 3.42; 3.43; 3.44; 3.49
Ordnungsamt	3.53
Ordnungswidrigkeit	B. Vorwort; B.1; 3.10; 3.14; 3.15; 3.17; 3.20; 3.23; 3.29; 3.50; 4
Orientierungshilfe	3.1; 3.44
Örtliche Zuständigkeit	3.49
Ostthüringer Unternehmer- und Gründertag	3.3
Paketshop	3.50
Papierkorb	3.25
Passanten	3.13; 3.27; 3.38; 3.43
Pass	3.50
Patientenarmband	3.26
Patientendaten	3.7; 3.25; 3.26; 3.33; 3.40; 3.41
Pausenraum	3.18; 3.21
Personalausweiskopie	3.31; 3.48; 3.50
Persönlichkeitsrecht	3.11; 3.22; 3.28; 3.30; 3.42; 3.52; 5.1; Anlage 4
Podiumsdiskussion	5.1
Postdienstleister	3.50
Postverkehr	3.50
Praxisübernahme	3.33
Privatinsolvenz	3.5
Raucherecke	3.18; 3.21
Rechtsanwalt	3.24; 3.29; 3.30; 3.32; 3.34
Rechtsanwaltskammer	3.24
Recyclingunternehmen	B. Vorwort; 3.11; 3.12;

	3.13; 3.14; 3.15; 3.43; 3.48
Regelmäßige Datenübermittlung	3.14; 3.40; 3.50; Anlage 2; Anlage 5
Restaurant	3.9
Rezept	3.25; 3.40; 3.41
Runder Tisch	5.1
Schriftgutentsorgung	3.25
Schuldnerberatung	3.5
Schule	5.1
Schutzwürdige Interessen Betroffener	3.6; 3.8; 3.9; 3.10; 3.11; 3.13; 3.17; 3.21; 3.27; 3.35; 3.36; 3.37; 3.38; 3.39; 3.42; 3.43; 3.51; 3.52; Anlage 4
Schwärzung	3.18; Anlage 1
Schwarzwildkirrungen	3.52
Schwerpunkte im Berichtszeitraum	B. Vorwort; B.1
Senioren	3.29; 5.1
Seniorenwohnheim	3.29
Sicherheitskonzept	3.12; 3.13; 3.16; Anlage 1
Sicherungsmaßnahmen	3.13; 3.47; Anlage 1
Sitz des Unternehmens	3.31; 3.49
Sozialdatenschutz	3.40; 3.41; 5.1
Speicherdauer	3.34
Staatsanwaltschaft	3.25; 4
Steuerzahler	3.7
Stichprobe	3.39
Strafantragsrecht	4
Strafprozessrecht	4
Straftat	3.13; 3.21; 3.28; 3.32; 3.33; 3.34; 3.36; 3.38;

	3.42; 4
Strafverfahren	3.29
Taxi	3.42; Anlage 4
Technische und organisatorische Maßnahmen	3.12; 3.13; 3.14; 3.15; 3.16; 3.19; 3.29; 3.53; Anlage 1; Anlage 3; Anlage 4
Tierbeobachtungskamera	3.52
Überwachungsdruck	3.22; 3.34; 3.38
Umkleidekabine	3.21; 3.28
Unbefugte Übermittlung	3.15
Unschuldsvermutung	4
Unternehmen	B. Vorwort; B.1; B.2; 3; 3.1; 3.3; 3.7; 3.9; 3.10; 3.11; 3.12; 3.13; 3.14; 3.15; 3.16; 3.17; 3.18; 3.19; 3.21; 3.23; 3.28; 3.30; 3.34; 3.36; 3.41; 3.42; 3.43; 3.46; 3.47; 3.48; 3.49; 3.50; 3.53; 4; Anlage 1; Anlage 2; Anlage 4
Vandalismus	3.22
Verantwortliche Stelle	3.7; 3.22; 3.31; 3.50; 3.53; Anlage 4
Verbraucherschutzverein	3.24
Verbraucherzentrale	5.1; Anlage 2
Verdeckte Videoüberwachung	3.28
Verein	3.6; 3.24; 3.45
Vereinsregister	3.45
Verfahrensverzeichnis	3.12
Verkehrsraum	3.10; 3.38; 3.42; Anlage 4
Verpflichtung auf das Datengeheimnis	Anlage 1

Verschwiegenheitspflicht des Rechtsanwalts	3.24
Verwaltungsfachhochschule Gotha	5.1
Video	3.27; 3.28; 3.31; 3.32; 3.32; 3.34; 3.35; 3.36; 3.37; 3.38; 3.42; 3.43; 3.44; 3.49; 3.50; 3.51; 3.52; 4; Anlage 1; Anlage 4
Videoattrappe	3.22; 3.31
Videoaufzeichnung	3.11; 3.12; 3.13; 3.22; 3.37; 3.38; 3.43; 3.44; 3.50; Anlage 4
Videobeobachtung	3.12; 3.18; 3.27; 3.31; 3.35; 3.37; 3.42; 3.43; 3.52; Anlage 1; Anlage 4
Videoüberwachung Nahverkehrsunternehmen	3.10
Vorabkontrolle	3.23
Vorträge	3.3; 5.1
Wald	3.52
Internetseite	3.6; 3.30; Anlage 1
Werbe-Mail	3.6
Werbezwecke	3.5; 3.30
Werbung	3.5; 3.6; 3.30; 3.51; Anlage 1
Widerspruch	3.5; 3.6; Anlage 2
Widerspruchsrecht	3.5
Windpark	3.49
Wirtschaftlich Berechtigter	3.45
Wohnanlagen	3.22
Workshop	5.1
Zivilrechtsweg	3.44
Zugriffsregelung	3.16; 3.33; Anlage 1

Zutrittsregelung	3.16; Anlage 1
Zwangsgelder	B. Vorwort; 3.43; 3.48;
Zwei-Schrank-Modell	3.33