

Mitteilung

des Landesbeauftragten für den Datenschutz

32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg für die Jahre 2014/2015

Schreiben des Landesbeauftragten für den Datenschutz Baden-Württemberg vom
21. Januar 2016:

Anbei übersende ich Ihnen meinen 32. Tätigkeitsbericht, der mit Zustimmung des
Ständigen Ausschusses vom 24. September 2015 abweichend von § 31 Absatz 2
des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg erst jetzt
vorgelegt wird, um die Entwicklung des Datenschutzes im gesamten Berichtszeit-
raum darstellen zu können.

Klingbeil

32. Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz
Baden-Württemberg
2014/2015



Inhaltsverzeichnis

Vorwort	7
1. Zur Situation	11
1.1 Schöne neue Welt – steht der Datenschutz im Wege?	11
1.2 Die Europäische Datenschutzreform – zum Stand der Datenschutz-Grundverordnung	17
1.3 Die EU-Datenschutzrichtlinie für Polizei und Justiz – Flickenteppich statt Regenschirm?	19
1.4 Die Rechtsprechung des Europäischen Gerichtshofs in Datenschutzfragen	22
1.4.1 Urteil des EuGH vom 8. April 2014, C 293 und 594/12 (Vorratsdatenspeicherung)	22
1.4.2 Urteil des EuGH vom 13. Mai 2014, C 131/12 (Google Spain)	23
1.4.3 Urteil des EuGH vom 6. Oktober 2015, C-362/14 (Safe Harbor)	24
1.5 Internationaler Datenverkehr	26
1.6 Aus der Dienststelle	27
2. Innere Sicherheit	31
2.1 Rechtsprechung	31
2.1.1 Wer filmt, darf gefilmt werden – gleiches Recht für alle?	31
2.1.2 Automatische Kennzeichenlesesysteme der Polizei	32
2.1.3 Strategische Fernmeldeüberwachung	35
2.1.4 Quod non legitur, non creditur	37
2.1.5 Wie man sich irren kann!	39
2.2 Datenverarbeitung durch Sicherheits- und Ordnungsbehörden	41
2.2.1 Die Antiterrordatei – Neue Strategien zur Effektivierung der Kontrollpraxis	41
2.2.2 Precogs oder Precobs – die Zukunft der Verbrechensverhinderung?	43
2.2.3 Gut gemeint ist nicht immer gut	44
2.2.4 Der Kriminalaktennachweis – gehören Daten aus Ermittlungsverfahren wegen des Verdachts der exhibitionistischen Handlung in diese bundesweite Datei?	47
2.2.5 Steht der Datenschutz sich selbst im Wege?	53
2.2.6 Ende gut, alles gut?	54
2.2.7 Warum darf die Polizei die Daten von Fußballfans in verschiedenen Sportdateien speichern?	55
2.2.8 Stadionverbote – Was passiert, wenn die Polizei sich geirrt hat?	57
2.2.9 Das Nationale Waffenregister – Kontrollbesuche bei den Waffenbehörden	59
2.2.10 Glückssache!	63
2.3 Die Verfassungsschutzreform	66

32. Tätigkeitsbericht 2014/2015

3. Justiz		69
3.1	Vorratsdatenspeicherung	69
3.2	Einführung der Elektronischen Akte im Strafverfahren	70
3.3	Öffentlichkeitsfahndung in sozialen Netzwerken	71
3.4	Auskunftsanspruch für Grundstückseigentümer	72
3.5	Neuordnung des Notariatswesens	72
3.6	Kontrollen bei Notariaten	74
3.7	Kaputte Schlösser am Aktenschrank	75
3.8	Unberechtigte Informationsweitergabe zwischen Gerichtsvollziehern	75
3.9	Aufbewahrungsfrist für die Handakten des Rechtsanwalts	76
4. Steuern und Statistik		79
	Zensus 2011 – und kein Ende!	79
5. Kommunales und andere Verwaltungsbereiche		83
5.1	Haushaltsbefragung in einer Kommune	83
5.2	Wenn einer eine Reise tut – die Übernachtungssteuer	84
5.3	Inkrafttreten des Bundesmeldegesetzes – Chance auf Stärkung des Grundrechts auf informationelle Selbstbestimmung vertan	86
5.4	Die Karawane zieht weiter – Datenschutz im kommunalen Bereich	87
5.4.1	Datenübermittlungen an externe Energieberater	87
5.4.2	Notwendigkeit der Vermittlung datenschutzrechtlicher Grundlagen	88
5.4.3	Behördliche Datenschutzbeauftragte	88
5.4.4	Datenschutzrechtliches Verbot mit Erlaubnisvorbehalt	89
5.5	Bebauungspläne – Öffentliche Auslegung von Einwendungen	89
5.6	Fundsachen mit elektronischem Speicher	90
6. Verkehr		93
6.1	Datenschutz rund um das Kraftfahrzeug: Automatisiertes und vernetztes Fahren, Elektromobilität und Pkw-Maut	93
6.2	Projekt TwoGo	98
6.3	PolyGo: Eine für alles, alles auf einer?	101
6.4	Saisonkarten der Bodenseeschifffahrt	105
6.5	Reisezeitermittlung	107

32. Tätigkeitsbericht 2014/2015

7. Gesundheit und Soziales	111
7.1 Das Gesetz über den öffentlichen Gesundheitsdienst (Gesundheitsdienstgesetz)	111
7.2 Das Landesgesundheitsgesetz	112
7.3 Datenschutz in Krankenhäusern	113
7.3.1 Dauerpatient Krankenhaus	113
7.3.2 Umsetzung der Orientierungshilfe Krankenhausinformationssysteme	115
7.3.3 Auskünfte gegenüber Strafverfolgungsbehörden	116
7.4 Der neue Leitfaden zum Datenschutz in medizinischen Forschungsprojekten	118
7.5 Gesundheitsatlas Baden-Württemberg	119
7.6 Datenschutz bei Sozialleistungsträgern	120
7.6.1 Hausbesuche bei fehlgeleiteten Arbeitsunfähigkeitsbescheinigungen	120
7.6.2 Krankengeldfallmanagement der Krankenkassen	120
7.6.3 Bekanntgabe von Reha-Entlassungsberichten an die Deutsche Rentenversicherung	122
7.7 Datenschutz beim Medizinischen Dienst der Krankenversicherung	123
7.7.1 Kontrollbesuch beim Medizinischen Dienst der Krankenversicherung	123
7.7.2 Ende des Umschlagverfahrens	124
7.8 Datenschutz in Pflegeeinrichtungen	125
7.8.1 Datenerhebung durch Hilfsmittelerbringer in Pflegeeinrichtungen	125
7.8.2 Fotoaufnahmen von Pflegeheimbewohnern für Notfall- und Evakuierungspläne	127
7.9 Datenschutz bei Ärzten	128
7.9.1 Einsatz von Verrechnungsstellen durch Ärzte	128
7.9.2 Laborauftrag durch behandelnden Arzt	128
7.10 Informationspflicht bei Datenschutzverstößen	129
7.10.1 Datenlecks in Krankenhäusern	130
7.10.2 Diebstahl eines Praxiscomputers	131
7.10.3 Medizinischer Dienst der Krankenversicherung (MDK)	132
7.11 Datenschutz im Jobcenter	133
7.11.1 Bei Jobcentern vor Ort	133
7.11.2 Formulare	133
7.11.3 Auskunft an das Hauptzollamt?	134
7.12 Wohn-, Teilhabe- und Pflegegesetz	135
7.12.1 Das neue Gesetz	135
7.12.2 Prüfberichte der Heimaufsicht	135
7.12.3 Zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen	136
7.13 Wohngeld: Das Formular	137
7.14 Datenverarbeitung im Auftrag	138
8. Datenschutz an Schulen und Hochschulen	141
8.1 Verwaltungsvorschrift Datenschutz an öffentlichen Schulen	141
8.2 Medienbildung im Bildungsplan 2016	142

32. Tätigkeitsbericht 2014/2015

8.3	Toiletten-Schließanlagen an Schulen	143
8.4	Das neue Internetportal youngdata.de	143
8.5	Erst Verfahrensverzeichnis, dann Betrieb	144
9. Datenschutz in der Arbeitswelt		145
9.1	Mindestlohngesetz und Datenschutz	145
9.2	Abgleich von Beschäftigendaten mit Sanktionslisten der EU sowie sonstiger Drittstaaten	146
9.3	Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern: Die Ausnahme muss wieder zur Regel werden	147
9.3.1	Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern aus Sicht des Kunden	148
9.3.2	Aufzeichnung von Telefongesprächen in Call-Centern aus Sicht der Mitarbeiter	149
10. Datenschutz in der Wirtschaft		151
10.1	Datenschutzrechtliche Anforderungen an E-Mail-Werbung: Eine konkrete Anleitung mit Formulierungsvorschlägen für die Praxis	151
10.1.1	Grundsatz für E-Mail-Marketing: Nur mit vorheriger, informierter und ausdrücklicher Einwilligung der betroffenen Person zulässig	151
10.1.2	Formale Anforderungen an die Einwilligung: Abbestellbarkeit, Protokollierung und Abrufbarkeit	152
10.1.3	Inhaltliche Anforderungen an die Einwilligung	153
10.1.4	Eine Einwilligung in E-Mail-Werbung durch das pauschale Akzeptieren von „Kleingedrucktem“ ist unwirksam	154
10.1.5	Eine Einwilligung in Werbung per E-Mail durch erzwungenes Opt-in (Einwilligung als separates Pflichtfeld) ist unwirksam	155
10.1.6	Eine formal korrekte, aber zu wenig konkrete Einwilligung in E-Mail-Werbung ist unwirksam	156
10.1.7	Ausnahme vom Einwilligungserfordernis: Privileg des § 7 Absatz 3 UWG – aber nicht ohne Opt-out-Möglichkeit	156
10.2	Übermittlung der E-Mail-Adresse eines Kunden durch einen Online-Versandhändler an ein Logistik- oder Postunternehmen nur mit vorheriger Einwilligung zulässig	157
10.3	Kein finanzielles Risiko? Dann keine Bonitätsabfrage – auch nicht mit Einwilligung!	158
10.4	Die Suche nach dem Schuldner	160
10.5	Neues von der Rechtsprechung zum Scoring	161
10.6	Datenverarbeitung aufgrund einer Einwilligung	162
10.7	Auswirkung von Datenschutzverstößen auf gerichtliche Entscheidungen	164
10.8	Externe Datenschutzbeauftragte bei Stadtwerken	165
10.9	Die rechtlichen Grenzen bei der Beendigung der Bestellung eines betrieblichen Datenschutzbeauftragten	166
10.10	Datenschutz im Hotel	167
10.10.1	Dauerbrenner Personalausweiskopien – mehr Sicherheit bei „Stundengästen“?	168

32. Tätigkeitsbericht 2014/2015

10.10.2	Geschwätzige Reservierungsbestätigungen: Mit einer E-Mail reißen manche Hotels ein ...	169
10.10.3	Zweckänderung bei Meldedaten – dein Hotelier weiß, wo du wohnst	170
10.11	Landesweite schriftliche Datenschutzkontrolle bei Adresshandelsunternehmen sowie Markt- und Meinungsforschungsinstituten zeigt deutlich mehr Licht als Schatten	170
10.11.1	Landes- und branchenweite schriftliche Datenschutzkontrollen – ein Instrument mit mehrfacher Wirkung	171
10.11.2	Wie sind die Unternehmen mit dem Fragenkatalog umgegangen?	172
10.11.3	Kontrollergebnisse bei den Adresshandelsunternehmen	172
10.11.4	Kontrollergebnisse bei den Markt- und Meinungsforschungsinstituten	173
10.12	Datensparsame Fototaschen	175
10.13	Mehr Rechte für Verbraucherschutzorganisationen: Erweiterung des Unterlassungsklagegesetzes um datenschutzrechtliche Vorschriften	177
10.14	Orientierungshilfe zur Mieterselbstauskunft	179
10.15	Geldwäschebekämpfung mit Personalausweiskopien	179
10.16	In der Post verschollen: Meldepflicht bei Datenverlust	180
10.17	Hinweisinformationssystem der Versicherungswirtschaft (HIS)	181
10.18	Was man als Mieter über sich und alle anderen erfahren kann	182
10.19	Intelligente Stromzähler – Energiewende zu Lasten des Datenschutzes?	183
11. Technik und Medien		185
11.1	Videoüberwachung in allen Varianten	185
11.1.1	Einleitung	185
11.1.2	Videoüberwachung in Schwimmbädern	185
11.1.3	Videoüberwachung in öffentlichen Verkehrsmitteln	186
11.1.4	Videoüberwachung durch Privatpersonen: Was sagt der EuGH?	187
11.1.5	Dashcams	188
11.1.6	Drohnen: Harmloses Spielzeug oder eine Gefahr für das Persönlichkeitsrecht?	189
11.2	Novellierung des Telemediengesetzes – Störerhaftung bei offenen WLANs	191
11.3	Orientierungshilfe Smart-TV	192
11.4	GPEN Privacy Sweep 2014	194
11.5	Heartbleed Bug – der GAU	194
11.6	Fachkongress des IT-Planungsrats am 7. und 8. April 2014 in Stuttgart	195
11.7	Vorsicht Internet! – oder worauf man achten sollte, wenn man im Internet unterwegs ist	196
11.8	E-Government-Gesetz Baden-Württemberg	197
11.9	Die Evaluierung des Rundfunkbeitragsstaatsvertrags	199
Inhaltsverzeichnis des Anhangs		201
Stichwortverzeichnis		251

32. Tätigkeitsbericht 2014/2015

32. Tätigkeitsbericht 2014/2015 - Vorwort

Vorwort

Am 13. März 2016 wird ein neuer Landtag gewählt. Dieser Bericht ist daher der letzte in der 15. Legislaturperiode des baden-württembergischen Parlaments. Anlass genug für einen Rückblick auf das, was seit der Landtagswahl im März 2011 erreicht wurde. Für mich reicht dieser Blick sogar noch etwas weiter zurück, denn meine Amtszeit, die am 1. April 2009 begann, wird mit der Legislaturperiode am 30. April 2016 enden. Insofern werde ich leider keine Gelegenheit mehr haben, anlässlich der Aussprache im Plenum über diesen Bericht und die Stellungnahme der Landesregierung das Wort zu ergreifen. Ich möchte mich daher auf diesem Wege zunächst bei allen Parlamentariern bedanken, die die Anliegen des Datenschutzes und die Arbeit meiner Dienststelle in den letzten Jahren unterstützt und wohlwollend begleitet haben. Dies gilt in besonderer Weise für die Mitglieder des Ständigen Ausschusses des Landtags, dem ich regelmäßig über aktuelle Datenschutzthemen berichten durfte. Vor allem aber möchte ich mich für eine gute und vertrauensvolle Zusammenarbeit bei Herrn Landtagspräsidenten Wilfried Klenk MdL und seinen Amtsvorgängern bedanken, die seit dem 1. April 2011, als meine Dienststelle dem Landtag zugeordnet wurde, meine Hauptansprechpartner waren. Viele Probleme des täglichen Dienstbetriebs hätten ohne die stets sachkundige und verlässliche Unterstützung durch die Landtagsverwaltung nicht bewältigt werden können. Nicht zuletzt ist aber auch dieser Bericht – wie überhaupt die Aufgabenerledigung in den zurückliegenden fast sieben Jahren – wieder das Ergebnis einer Teamarbeit gewesen, für die mein herzlicher Dank daher meinen Mitarbeiterinnen und Mitarbeitern gilt.

Seit meinem Amtsantritt im Jahr 2009 hat sich einiges geändert. Damals war meine Dienststelle – wie schon seit ihrer Gründung im Jahr 1980 – nur für den Datenschutz im öffentlichen Bereich zuständig und wies 16 Stellen auf. Am 1. April 2011 erfolgte die Zusammenlegung mit der im Innenministerium angesiedelten Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich und die Zuordnung zum Landtag (vgl. 30. Tätigkeitsbericht 2010/2011, Landtagsdrucksache [LT-Drs.] 15/955, 1. Teil, Kapitel 1 und 5). Mit der Zusammenlegung wurden 6,5 Stellen des Innenministeriums übertragen. In

der Folgezeit kamen neue Aufgaben und neue Stellen hinzu – zuletzt zum Jahresende 2015 mit der neuen Funktion als Landesbeauftragter für die Informationsfreiheit –, so dass die Dienststelle nunmehr über 34,5 Stellen und mehrere Referate verfügt. Für die von allen Fraktionen stets einvernehmlich gebilligten Personalaufstockungen gilt mein besonderer Dank dem Landtag und dessen Finanzausschuss; sie waren in Anbetracht der allgemeinen Sparzwänge für die Landesbehörden nicht selbstverständlich.

Eine weitere strukturelle Aufwertung erfolgte in der 15. Legislaturperiode leider nicht, obwohl bereits die Koalitionsvereinbarung von 2011 vorsah, meiner Dienststelle „den Status einer obersten Landesbehörde mit eigenen Sanktionsbefugnissen für die Verfolgung und Ahndung von Ordnungswidrigkeiten“ zu verleihen. Insbesondere die Zuständigkeitsübertragung für datenschutzrechtliche Ordnungswidrigkeiten hätte gesetzestechnisch unproblematisch und für den Gesamthaushalt stellenneutral erfolgen können. Das Vorhaben sollte schon im Hinblick auf die 2018 in Kraft tretende europäische Datenschutzreform (siehe hierzu Kapitel 1.2 und 1.3) aber nun zeitnah angegangen werden.

War die Zeit seit 2011 in gesetzgeberischer Hinsicht für das allgemeine Datenschutzrecht eher geruhlos, so werden die nächsten Jahre unweigerlich erhebliche Umstellungen mit sich bringen: Am 15. Dezember 2015 haben sich die EU-Institutionen auf die EU-Datenschutz-Grundverordnung (EU-DSGVO) verständigt, die im Frühjahr 2016 endgültig verabschiedet und zwei Jahre später in Kraft treten wird. Da sie unmittelbar geltendes Recht wird, erfordert sie bis dahin zwingend eine Überprüfung des gesamten nationalen Datenschutzrechts, auch in Bezug auf die ausdifferenzierten bereichsspezifischen Regelungen in unzähligen Fachgesetzen auf Landes- und Bundesebene. Hier werden in erster Linie die Ministerien gefordert sein, die alsbald mit einer Bestandsaufnahme und der Klärung des Regelungsbedarfs beginnen müssen. Aber bereits vor Inkrafttreten der EU-DSGVO ist auch für meine Dienststelle mit einem erhöhten Beratungsbedarf der Wirtschaft zu rechnen, da die Verordnung zahlreiche, durchaus beschwerdeträchtige Themenfelder ausklammert bzw. allgemeinen Abwägungsklauseln überlässt (z. B. Beschäftigtenda-

32. Tätigkeitsbericht 2014/2015 - Vorwort

tenschutz, Videoüberwachung, Scoring usw.). Andererseits wird sie nicht nur von den hier ansässigen Unternehmen, sondern aufgrund des Markortprinzips auch von Konzernen, die außerhalb der EU ihren Sitz haben, aber hier geschäftlich tätig sind, zu beachten sein. Vieles, was hierzulande differenziert geregelt oder von einer langjährigen Rechtsprechung gestaltet worden ist, muss nun neu justiert werden. Zudem wird die EU-DSGVO für die Aufsichtsbehörden fristgebundene nationale und internationale Abstimmungsverfahren untereinander und auch strukturell neuartige Aufgaben mit sich bringen, so beispielsweise Folgenabschätzungen hinsichtlich bestimmter Datenverarbeitungen, in die die Aufsichtsbehörden einzubinden sind und auf die sich die Wirtschaft frühzeitig einstellen muss. Hinzu kommen umfassende Sanktionsbefugnisse. Für all diese neuen gesetzlichen Aufgaben müssen die unabhängigen Datenschutzbehörden der Länder rechtzeitig adäquat ausgestattet werden und sich partiell neu aufstellen, einschließlich Fortbildung, Sprachkompetenz und Organisation der Zusammenarbeit. Wir werden demnächst gemeinsam eine Abschätzung des für die Vorphase der Reform erforderlichen Personalbedarfs vornehmen und ich hoffe, dass der neue Landtag die notwendige Unterstützung nicht versagen wird. Die in den letzten Wochen von dem Landesvorsitzenden einer großen Partei geäußerte Kritik an der föderalen deutschen „Kleinstaaterei“ und einer angeblich nicht mehr zeitgemäßen Struktur mit 16 Landesbeauftragten und der Bundesbeauftragten für den Datenschutz mag seiner bundespolitischen Rolle geschuldet sein. Der Idee einer zentralen Bundesbehörde für Datenschutz mit „Zweigstellen“ in den Ländern trete ich jedenfalls entschieden entgegen. Es wird im Zuge der europäischen Datenschutzreform ohnehin zu einer gewissen Vereinheitlichung und Harmonisierung der Rechtsauslegung und -anwendung kommen; eine wichtige Rolle wird hierbei der Europäische Datenschutzausschuss spielen, in dem die Länder angemessen vertreten sein müssen. Und es macht hoffentlich auch aus Sicht des Landtags wenig Sinn, Landes- und kommunale Behörden von einer Bundesbehörde kontrollieren zu lassen; dies gilt ebenso für die baden-württembergischen Unternehmen, die auf eine unkomplizierte Zusammenarbeit der kurzen Wege Wert legen. Mit gravierenden Änderungen der Behördenstruktur rechne ich insofern nicht.

Mit größerer Sorge erfüllt mich indessen der von politischer Seite in den letzten Monaten zu beobachtende Frontalangriff auf zentrale Strukturprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung. Aus der nicht ganz neuen Behauptung, dass Daten der „Rohstoff der Zukunft in der digitalen Welt“ seien und sich die deutsche Wirtschaft in einem Wettlauf um die Wertschöpfung aus Kundendaten befinde, wird kurzerhand gefolgert, nun habe sich der Schutz der Privatsphäre den Interessen der nationalen Wirtschaft unterzuordnen; andernfalls fände die Wertschöpfung „irgendwo in Amerika oder Asien“ statt. Dementsprechend wird der Datenschutz teilweise als Hindernis für neue Geschäftsmodelle einer massenhaften Datenausbeutung („Big Data“) oder gar als „wirtschaftliches Problem“ bezeichnet. Dabei scheint mir die Grundrechtsorientierung des deutschen und des europäischen Datenschutzrechts aus dem Blick zu geraten, wie sie in langjähriger Tradition durch das Bundesverfassungsgericht und in den letzten Jahren zunehmend auch durch den Europäischen Gerichtshof geprägt wurde. Personenbezogene Daten sind eben nicht irgendwelche Rohstoffe wie Kohle oder Öl, sondern (auch) Teil der Persönlichkeit, die nicht dem ökonomischen Primat unterworfen werden sollten. Und weder einem Unternehmen noch dem Staat ist es gestattet, alle Daten über jeden Menschen auszuwerten, sondern nur die für den jeweiligen Zweck erforderlichen, wenn hierfür eine Rechtsgrundlage oder eine wirksame Einwilligung vorliegen, und auch dies nur unter Beachtung des Grundsatzes der Verhältnismäßigkeit. Wenn nun in den auf dem IT-Gipfel der Bundesregierung 2015 vorgestellten „Leitplanken Digitaler Souveränität“ davon die Rede ist, dass „datenbasierte digitale Geschäftsmodelle“ nicht durch ein „unzeitgemäßes Datensparsamkeitsdiktat“ verhindert werden dürften und bisherige „Grundprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung überprüft und durch Prinzipien der Datenvielfalt und des Datenreichtums ergänzt und ersetzt“ werden müssten, dann scheint das eher der Diktion der einschlägigen Branchenverbände zu entsprechen und geeignet zu sein, das Grundrecht auf informationelle Selbstbestimmung in Frage zu stellen.

Einzuräumen ist, dass es auf eine Reihe von Fragen, die mit der wirtschaftlichen Verwertung von personenbezogenen Daten einhergehen, noch kei-

32. Tätigkeitsbericht 2014/2015 - Vorwort

ne befriedigenden Antworten gibt, auch weil es noch kein adäquates Datenrecht gibt, das das „Eigentum“ oder die „Verwertung“ dieser Daten hinreichend regelt. Daten dienen im Internet mittlerweile zwar vielfach als „Währung“ für scheinbar kostenlose Dienste und werden von deren Anbietern anschließend kommerziell verwertet, häufig für Werbezwecke. Aber gibt derjenige, der seine Daten zur Verfügung stellt, damit alle Rechte auf? Wem „gehören“ beispielsweise die Daten über die Sehgewohnheiten eines Smart-TV-Nutzers? Dem Zuschauer, der sie erzeugt? Dem Gerätehersteller, der sie erhebt und an seine Werbepartner verkauft? Dem Sender, der wissen will, was seine Zuschauer mögen? Wem „gehört“ die Kaufhistorie eines Kunden in einem Onlineshop? Dem Händler oder dem Kunden? Wer darf über die Informationen über das Fahrverhalten in einem intelligent vernetzten Auto verfügen, wer erhält darauf Zugriff und wie? Der Halter, der über den Fahrzeugeinsatz entscheidet? Der jeweilige Fahrer, der tatsächlich fährt? Der Hersteller, um evtl. unberechtigte Haftungsansprüche bei Unfällen abzuwehren? Die freie Werkstatt, die einen Schaden reparieren, aber nicht vom Wissen des Herstellers profitieren soll? Viele Fragen, an die sich die rechtspolitische Diskussion erst allmählich annähert. Für die Datenschützer stehen traditionell die Persönlichkeitsrechte der Betroffenen im Vordergrund. Deshalb muss auch jeder die Chance haben, seiner eigenen kommerziellen Verwertung zuzustimmen oder diese abzulehnen. Aber in einer Zeit, in der die meisten Internetnutzer ihre informationelle Selbstbestimmung durch das „Häkchen setzen“ unter ungelesene ellenlange Nutzungsbedingungen ausüben, braucht es neue faire Ansätze, die den Einzelnen vor den Risiken der Digitalisierung in persönlichkeitsrechtlicher *und* in vermögensbezogener Hinsicht schützen, dabei aber auch den gesellschaftspolitischen Mehrwert einer Datenauswertung berücksichtigen. Koppelungsverbote, Pseudonymisierung und Anonymisierung, Transparenz der Verarbeitung und verbesserte Kontrollbefugnisse der Datenschutzbehörden können Erfolgsfaktoren auf diesem Weg sein, der in der EU-DSGVO teilweise bereits vorgezeichnet ist, aber nun mit Leben erfüllt werden muss. Der Datenschutz steht in den nächsten Jahren vor großen

Herausforderungen, für deren Bewältigung ich allen Akteuren im Lande viel Erfolg wünsche.

Jörg Klingbeil

32. Tätigkeitsbericht 2014/2015 - Vorwort

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

1. Zur Situation

1.1 Schöne neue Welt – steht der Datenschutz im Wege?

Die allgegenwärtige Datenerfassung und -verarbeitung hat mittlerweile ein Ausmaß angenommen, das noch vor wenigen Jahren unvorstellbar schien. Aussagen, wonach die verarbeitete Datenmenge sich alle zwei Jahre verdoppelt oder in den letzten Jahren mehr Informationen erzeugt wurden als in 40.000 Jahren zuvor, übersteigen ohnehin jedes menschliche Vorstellungsvermögen. Die **digitale Durchdringung unserer Lebenswirklichkeit** lässt sich auch im Alltag nicht mehr übersehen. So kann man immer mehr – vor allem jüngere – Leute beobachten, die überall, wo sie gehen, stehen oder sitzen, nach unten auf ihr Smartphone, also ein internetfähiges Mobiltelefon, starren, um dort die neuesten Mitteilungen ihrer Freunde zu lesen oder selbst Nachrichten an diese zu verfassen (überwiegend mit Instant-Messaging-Diensten wie WhatsApp), im Internet zu surfen, auf dem Gerät Filme anzuschauen, Musik zu hören oder schlicht zu spielen. Dabei kam das erste iPhone der Firma Apple erst 2007 auf den Markt. Es ist bereits von einer „Generation head-down“ und von drohenden körperlichen Gesundheitsschäden die Rede. Die Ausstattung der Haushalte mit Smartphones und Handys, aber auch der Gerätebesitz Jugendlicher hat 2015 in Deutschland praktisch die Sättigungsgrenze erreicht¹. Über 30 Mio. nutzen das Internet regelmäßig unterwegs². Auch die Nutzungsintensität ist beachtlich. Teilweise wird bereits Suchtverhalten konstatiert: Nach einer aktuellen Studie der Universität Bonn³ beschäftigten sich die Testpersonen der Altersgruppe 17–25 Jahre im Durchschnitt täglich knapp drei Stunden und sechsmal pro Stunde mit dem Smartphone, wobei das Telefonieren mit weniger als zehn Minuten pro Tag nur noch eine untergeordnete Rolle spielte. Nach Meinung der Forscher könnten Smartphones zum „digitalen Burnout“ führen und „abhängig, unproduktiv und unglücklich“

machen. Der permanenten Smartphone-Nutzung sollte – so ihr Ratschlag – mit einer „digitalen Diät“ und einer neuen Kommunikationsetikette begegnet werden.

Die allgegenwärtige Datenerfassung und -verarbeitung ist aber mittlerweile nicht mehr auf das Smartphone oder andere Mobilgeräte wie Tablets beschränkt; unter dem Vorzeichen „**Internet der Dinge**“ soll nahezu alles mit dem Internet vernetzt und dadurch schlau („smart“) werden: Das Haus (smart home), der Stromzähler (smart meter), das Stromnetz (smart grid), das vernetzte Auto, der Fernseher (smart-TV) sowie Uhren (smart watches) und andere Gegenstände, die am Körper getragen werden (wearables), um nur einige Beispiele zu nennen. Dabei dient das Smartphone oder Tablet häufig als Steuer- und Anzeigegerät, wobei als Alternative bzw. Ergänzung Sprach- und Gestensteuerung auf dem Vormarsch sind. Auf datenschutzrechtliche Aspekte einzelner Themen wird in den Kapiteln 6.1 (Datenschutz im Kraftfahrzeug), 10.19 (Intelligente Stromzähler) und 11.3 (Smart-TV) dieses Berichts eingegangen.

Die digitale Vernetzung liefert nebenbei Informationen für **normgerechtes Verhalten** und macht Normabweichungen transparent. Daraus können Anreize bzw. Sanktionen für Verhaltensänderungen entstehen: Seit einiger Zeit bietet zum Beispiel eine **Kfz-Versicherung** einen Rabatt an, wenn sich die Kunden durch eine im Fahrzeug montierte Telematikbox, die die Fahrweise (schnelles Beschleunigen, starkes Abbremsen, überhöhte Geschwindigkeit usw.), aber auch das Fahrgebiet oder Fahrten bei Nacht erfasst, kontinuierlich überwachen lassen. Bei der Auswertung hilft ein spanischer Mobilfunkanbieter, der aus den ausgelesenen Daten einen Scorewert für das Fahrzeug generiert, der – so der Anbieter – keine Rückschlüsse auf den einzelnen Fahrer bzw. Halter zulasse. Trotzdem: Wer mit Bleifuß durch die Gegend heizt, zahlt im Ergebnis mehr. Aber es sind nicht nur Autos, die zum Objekt der Neugier werden: Mittlerweile will eine der größten europäischen **Krankenversicherungen** ihre Versicherungsnehmer mit einem ermäßigten Tarif locken, wenn diese per Smartphone-App ihren Lebensstil, d. h. Fitness und Ernährung, kontrollieren lassen; die Versicherten sollen sich mit Hilfe des Computerprogramms also freiwillig selbst über-

¹ vgl. JIM-Studie 2015 des Medienpädagogischen Forschungsverbands Südwest, <http://www.mpfs.de/index.php?id=687>

² vgl. ARD/ZDF-Onlinestudie 2015, <http://www.ard-zdf-onlinestudie.de/index.php?id=540>

³ vgl. <https://www.uni-bonn.de/Pressemitteilungen/195-2015>

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

wachen, z. B. Schritte zählen, Gewicht messen, Sport und Kalorienmenge dokumentieren (Telemonitoring). Vorreiter derartiger Entwicklungen sind zumeist die USA; dort gibt es bei einer Krankenversicherung schon seit einigen Jahren einen Preisnachlass, wenn der Versicherte täglich eine bestimmte Anzahl von Schritten absolviert und dies auch nachweisen kann. Viele gesunde und fitte Versicherungsnehmer empfinden es vermutlich auch als gerecht, wenn sie nicht für die ungesunde Lebensweise ihrer Mitmenschen aufkommen müssen. Auch die hiesige Versicherung sieht sich als Interessenvertreterin vieler gesundheitsbewusster Kunden, die eine „risikogerechte Einordnung ihrer Lebensweise für ihre Versicherung berücksichtigt wissen wollen“, und vermutet, dass jeder fünfte Deutsche zu dieser Zielgruppe gehört. Und es sind keineswegs nur private Versicherungen, die über neue Angebote nachdenken; auch gesetzliche Versicherungen experimentieren mit Tracking-Technik: So ruft die AOK Nordost ihre Kunden in ihrem „Mobil Vital“-Programm auf, allerlei Daten (Ernährung, Rauchen, Alkoholkonsum, Sport usw.) in eine App einzutragen; außerdem wird der Kauf von Fitness-Trackern oder Apps mit max. 50 Euro bezuschusst, übrigens unabhängig von der jeweiligen Marke. Die Versicherung beteuert, keine Daten von den Versicherten zu erhalten, weder von den „wearables“ noch von den Apps. Dabei wird allerdings verschwiegen, dass die bezuschussten Fitness-Armbänder oder -Uhren – wie Tests gezeigt haben – in der Regel die erhobenen Daten in einer „Datenwolke“ (Cloud) irgendwo auf der Welt zu nicht immer transparenten Zwecken sammeln. Im Grunde greifen die neuen Geschäftsmodelle der Versicherungen nur bereits bestehende Trends auf: Zum einen den weit verbreiteten „Verkauf“ der eigenen Daten gegen „Vergünstigungen“ unterschiedlicher Art, etwa bei der Verwendung von Kundenkarten oder bei der scheinbar kostenlosen Nutzung sozialer Netzwerke, die die Daten ihrer Nutzer meistbietend an ihre Werbepartner verkaufen. Zum anderen ist seit einigen Jahren ein Hang zur Selbstbespiegelung und **Selbstvermessung** zu beobachten (sog. Quantified-Self-Bewegung). Analysten rechnen mit einer Vervielfachung des Absatzes von intelligenter Kleidung oder anderen „wearables“ in den nächsten Jahren.

Über rechtliche Bedenken hinaus berührt die geschilderte Entwicklung vor allem eine gesellschaftliche Dimension, denn sie verstärkt eine **Ökonomisierung unserer Lebensdaten**, wobei wesentliche Entscheidungen mit Hilfe von Algorithmen automatisiert zustande kommen. Drastisch ausgedrückt: „Die digitalen Supermächte sind dabei, jedem Menschen ein Preisschild anzuheften“⁴. Bereits 2011 sicherte sich z. B. Google ein Patent auf das sog. Dynamic Pricing; dabei wird in Online-Shops kein gleichbleibender Preis für eine Ware angezeigt, sondern ein individuell berechneter, der u. a. von dem jeweiligen Zugang oder dem verwendeten Endgerät abhängen kann. Teilweise wird ein gesuchtes Produkt auch gar nicht angezeigt, wenn der Kunde nicht in das gewünschte Profil passt⁵. Im Ergebnis wird der Betroffene jedenfalls in seinen Handlungsmöglichkeiten beschnitten und erfährt nicht einmal, welche Profile und Berechnungen sein Leben bestimmen. Auch bezogen auf Versicherungen kann eine Einteilung der Kunden nur nach dem Risikoäquivalenzprinzip zu Solidaritätsbrüchen und schließlich zu einer gnadenlosen Individualisierung führen. Zwar muss man sicher unterscheiden, ob Vitaldaten nur für die eigene Auswertung gedacht sind oder ob sie anderen zur Verfügung gestellt oder gar zum Maßstab für ein individuelles Versicherungsprofil gemacht werden. Die Selbstvermessung „für den Hausgebrauch“ gehört – auch wenn man das persönlich für sich ablehnen mag – schließlich zu der grundrechtlich geschützten informationellen Selbstbestimmung. Bedenklich wäre es aber, falls eines Tages Geschäftsmodelle die Oberhand gewinnen sollten, bei denen nur die Offenbarung von Gesundheitsdaten belohnt und die Verweigerung, sich für die Versicherung „gläsern“ zu machen, bestraft wird. Letzteres mag jene nicht schrecken, die heute fit und gesund sind; aber auch diese Personen werden das nicht immer und nicht auf Dauer sein. Wenn Menschen, egal ob als Arbeitnehmer, Kunden oder Versicherte, Leistungen (z. B. Vergünstigungen) nur dann erhalten, wenn sie sich norm- und marktkonform verhalten, also einem durchschnittlichen Risikotyp entsprechen, dann kommt dies einer schleichenden **Abkehr vom Solidaritätsprinzip** gleich. Solange es nur wenige

⁴ Sascha Lobo, FAZ vom 2. April 2014, S. 11

⁵ <http://www.welt.de/wirtschaft/webwelt/article146872671/Shoppen-per-iPhone-ist-guenstiger-als-mit-dem-PC.html>

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

Versicherungen (für Privatversicherte) sind, die auch nur geringe Vergünstigungen für die Selbstüberwachung ihrer Versicherten bieten, mag die Entwicklung beherrschbar bleiben; kritisch wird es aber dann, wenn diejenigen, die sich nicht selbst überwachen bzw. überwachen lassen wollen, durchgängig benachteiligt werden und mehrheitlich höhere Prämien zu bezahlen haben. Das ist – wenn man die Entwicklung im Versandhandel, bei Bankgeschäften oder bei Bahnfahrten bedenkt – keine fernliegende Sorge; hier zahlen mittlerweile gerade jene Kunden mehr, die ihre Geschäfte nicht online tätigen und ihre Daten nicht zur Verfügung stellen wollen. Zumindest bei der gesetzlichen Krankenversicherung sollte der Weg in die totale Individualisierung der Versicherten tabu sein und das bewährte Solidarprinzip erhalten bleiben, wonach die zu versichernden Krankheitsrisiken von der Gemeinschaft der Versicherten getragen werden und sich die Prämien nach dem Einkommen und nicht nach dem Risiko des Einzelnen richten.

Gesellschaftliche Auswirkungen dürfte auch die Wandlung **sozialer Netzwerke** zu **Medienunternehmen** haben; laut aktuellen Studien nimmt in den USA schon jeder dritte Nutzer Nachrichten über Facebook wahr. Dessen Gründer Mark Zuckerberg erklärte bereits, er wolle Facebook zur „besten personalisierten Zeitung der Welt“ machen. Dabei scheinen die dort platzierten Meldungen nicht immer den gleichen Stellenwert wie die Nachrichten zu haben, die in den etablierten Medien im Vordergrund stehen. Nach welchen Kriterien die zugrundeliegenden Algorithmen ihr Nachrichtenangebot auswählen, erfährt man allerdings grundsätzlich nicht. Medienwissenschaftler vertreten die Auffassung, dass soziale Netzwerke ein verzerrtes Bild der Realität zeichnen, was Folgen für die politische Kultur und den Diskurs habe. Die angewandten Kriterien seien letztlich Werkzeuge, um den Feed zu manipulieren, zumeist mit der Absicht, die „Zufriedenheit“ der Nutzer zu erhöhen, im Zweifelsfall eher durch banale als durch besonders gehaltvolle Nachrichten. Im Juni 2014 hatte Facebook übrigens die Newsfeeds von rd. 700 000 Nutzern manipuliert, um zu sehen, wie verschiedene Arten von Nachrichten die Stimmungslage der Nutzer beeinflussen. Kritiker sahen dies als „gigantisches soziales Experiment“ an, das zeige, wie politische Kommunikation in eine immer stärker personalisierte, private Transaktion

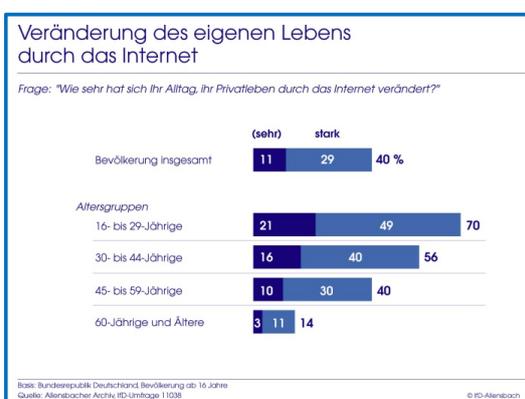
verwandelt werden könne. Dabei werde auch die öffentliche Sphäre grundlegend verändert, schon dadurch, dass sie weniger öffentlich werde. Da es den sozialen Netzwerken vorrangig darum gehe, dass sich Nutzer möglichst lange auf ihren Seiten aufhalten, um Werbeeinnahmen zu generieren, habe das für die Nutzer zur Folge, dass ihre Nachrichten nicht nach Relevanz, sondern nach ökonomischer Verwertbarkeit gefiltert würden. Demzufolge könne ein soziales Netzwerk wie Facebook redaktionelle Entscheidungen von großer Tragweite für die Öffentlichkeit treffen, weshalb eine öffentliche Debatte über die politische Dimension sozialer Medien erforderlich sei, ähnlich wie in der Anfangszeit des Rundfunks.

Außerhalb des privaten Umfelds dringt das „Internet der Dinge“ inzwischen unter dem Begriff **„Industrie 4.0“** – der wiederum verschiedene Einzelbausteine beinhaltet – in Produktionsbereiche vor (smart factory), setzt etablierte Geschäftsmodelle der Unternehmen unter Druck und schafft neue Wettbewerbssituationen. Strategisches Ziel ist dabei letztlich eine hochindividualisierte Herstellung von Produkten zu den Bedingungen der Massenproduktion. Dies bedingt zwangsläufig einen nahtlosen Durchgriff auf – teilweise personenbezogene – Daten von der Bestellung über die kaufmännischen (ERP-) Systeme bis hin zur Fertigung und Auslieferung, ggf. ergänzt um Wartung und Reparatur. Damit die gegenseitige Kommunikation und Steuerung zwischen Maschine und Werkstück funktioniert, müssen die Produkte ein „Gedächtnis“ (z. B. in Form von RFID-Chips) erhalten. Idealerweise wird dann das gewünschte Produkt erst nach Eingang der Bestellung fast in Echtzeit produziert, was die Lagerhaltung deutlich reduziert. Wegen der Individualisierung der Produkte und der Einbindung der Arbeitnehmer in den Produktionsprozess kann das nicht ohne Auswirkungen auf die Daten der Kunden und Beschäftigten bleiben. Über die eigenen Produktionsstätten hinaus eröffnet die digitale Vernetzung weitere lukrative Geschäftsfelder für die anschließende Überwachung der Produkte, etwa in Form neuer Betreiber- und Servicemodelle durch Zugriff auf Betriebs-, Verbrauchs- und Verschleißdaten, um notwendigen Reparaturen zuvorzukommen oder Erkenntnisse für die künftige Produktion zu gewinnen. Der Verkauf des einzelnen Produkts wird dabei an Bedeutung verlieren, wichtiger wer-

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

den dessen Nutzung und die dafür gebotene Dienstleistung. Kein Wunder, dass im Hintergrund schon massive industriepolitische Kämpfe um die Standardisierung bzw. die hard- und softwareseitige Vorherrschaft an der Schnittstelle zum Kunden geführt werden.

Wie eine Umfrage des Instituts für Demoskopie (IfD) Allensbach vom April 2015⁶ zeigt, spüren auch die Bürgerinnen und Bürger deutlich, dass sich ihr Alltag in den letzten Jahren durch das Internet stark verändert hat:



Quelle: IfD Allensbach

Über die Hälfte der Befragten gibt an, dass sich auch ihre Arbeitswelt durch das Internet z. T. schon deutlich verändert habe. Nach Meinung von 58 % überwiegen die Vorteile von Internet und Digitalisierung, 16 % sehen eher Nachteile, der Rest ist noch unentschieden. Knapp 90 % der Befragten erwarten überdies, dass Computer und Internet ihr Leben – sowohl privat wie am Arbeitsplatz – in den nächsten Jahren weiter einschneidend verändern werden, wobei eine auffällige **Diskrepanz zwischen der erwarteten und der erwünschten Entwicklung** zu Tage tritt: Mehr als 80 % rechnen mit einer zunehmenden Technisierung des Alltags, aber lediglich 4 % halten das für wünschenswert. Knapp 70 % rechnen damit, dass die Menschen sich in Zukunft noch mehr über E-Mails, SMS und Chat-Nachrichten austauschen werden, aber nur 5 % begrüßen diese Entwicklung. Die Studie kommt insgesamt zu dem Fazit, dass inmitten einer Entwicklung, die in ihrem bisherigen Verlauf von vielen durchaus

⁶ http://www.ifd-allensbach.de/uploads/tx_reportsdocs/FAZ_April_Digitalisierung.pdf

als Bereicherung erlebt werde, die Stimmungslage eher von Skepsis denn von Euphorie geprägt sei. Die meisten würden von den neuen Möglichkeiten Gebrauch machen und seien doch gleichzeitig besorgt, wie sich Wirtschaft und Gesellschaft durch die Vernetzung und den gesamten technologischen Fortschritt entwickeln.

Die damit verbundenen Risiken werden dabei durchaus realistisch eingeschätzt, wobei mangelnde Datensicherheit und die Sorge vor Datenmissbrauch dominieren:



Quelle: IfD Allensbach

Trotz dieser Bedenken gegen eine immer stärkere Vernetzung, zu der die Nutzer mit Hilfe mobiler internetfähiger Endgeräte selbst aktiv beitragen, halten sich die bei meiner Dienststelle eintreffenden Beschwerden der Bürgerinnen und Bürger über die datenschutzrechtlichen „Folgen und Nebenwirkungen“ ihres Handelns in überschaubaren Grenzen. Weder die Furcht vor einer potenziell permanenten Überwachung ihrer Kommunikation durch (ausländische) Geheimdienste noch die Sorge vor einer kommerziellen Verwertung ihres eigenen „Datenschattens“ scheint zu nennenswerten Verhaltensänderungen zu führen. Dies dürfte wohl an dem inzwischen weitläufig bekannten **„Privacy Paradox“** liegen, das Susan Barnes in Bezug auf die Nutzer von sozialen Netzwerken erstmals 2006 vorgestellt hatte⁷; diese verhielten sich in mehrfacher Hinsicht widersprüchlich: Sie würden online im Vergleich zu offline ungleich mehr private Informationen preisgeben und nicht erkennen, dass die Kommuni-

⁷ Susan Barnes, A privacy paradox: Social Networking in the United States, <http://firstmonday.org/article/view/1394/1312>

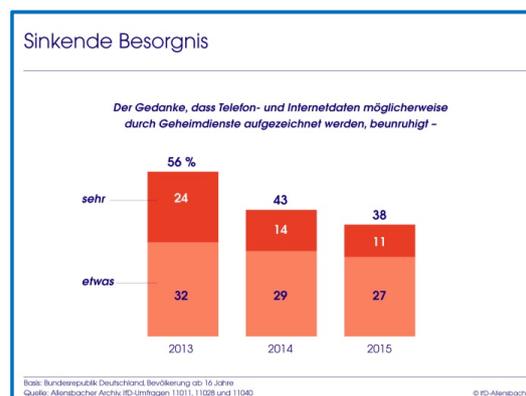
32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

kation im Internet öffentlich und nicht privat ist. Und auch, wenn sie erkennen, dass das Internet praktisch ein öffentlicher Raum ist, verbreiten sie dennoch viele private Informationen, auch weil das Wissen, was mit den Daten passiert, nur unzureichend ausgeprägt ist. Paradox sei, dass viele Nutzer trotz aller Offenherzigkeit starke Bedenken hinsichtlich der Wahrung der Privatsphäre haben.

Auch die o. g. Allensbach-Umfrage vom April 2015 kommt zum Ergebnis, dass selbst die von knapp drei Vierteln geäußerte Sorge vor Überwachung offenbar keine verhaltensändernde Wirkung entfaltet. Diejenigen, die sich um den Datenschutz im Netz sorgen, würden im selben Umfang Online-Banking praktizieren oder im selben Umfang Onlinekäufe tätigen wie diejenigen, die sich darüber nur wenig Gedanken machen. Die Vorteile der Nutzung des Internet würden eben direkt erlebt und von den meisten als wertvoll empfunden, während die möglichen Nachteile zwar reflektiert, aber im Alltag nur sporadisch erlebt würden. Offenbar zögern die Nutzer nicht, in problematische Datenerhebungen einzuwilligen, wenn sie sich davon einen Vorteil an Bequemlichkeit oder Kostenersparnis versprechen, obwohl sie auf der anderen Seite den Schutz ihrer persönlichen Daten durchaus für wichtig halten.

In meinem 31. Tätigkeitsbericht 2012/2013 (LT-Drs. 15/4600, S. 12) hatte ich über die erhebliche Unruhe berichtet, die die Enthüllungen über die Aktivitäten vor allem US-amerikanischer Geheimdienste bei Internetnutzern und Unternehmen im Jahre 2013 ausgelöst hatten. Wie eine weitere Umfrage des Instituts für Demoskopie (IfD) Allensbach vom Juni 2015 zeigt⁸, hat die Sorge, dass Telefon- und Internetdaten möglicherweise durch Geheimdienste aufgezeichnet werden, seit 2013 kontinuierlich abgenommen. Im Gegenzug wird nun die Funktion der Geheimdienste, um ein Land gegen Risiken zu schützen, von 78 % der Befragten als „wichtig“ oder sogar „sehr wichtig“ angesehen. 70 % halten eine enge Zusammenarbeit zwischen deutschen und amerikanischen Geheimdiensten wegen der Risiken durch den internationalen Terrorismus für erforderlich. Nur 13 % wollen verhindern, dass teilweise andere Länder bestimmen, was und wer überwacht

wird. Ich gehe davon aus, dass sich diese Sichtweise durch die terroristischen Anschläge 2015 in Paris und auf deutsche Touristen Anfang 2016 in Istanbul inzwischen eher verstärkt hat.



Quelle: IfD Allensbach

Die politischen Bemühungen, die **Spähaktivitäten ausländischer Geheimdienste** – einschließlich deren Zusammenarbeit mit deutschen Sicherheitsbehörden – weiter aufzuklären, verlaufen derweil eher zäh und werden von der Öffentlichkeit nur noch gelegentlich mit Aufmerksamkeit bedacht, weil sich gewichtigere Themen in den Vordergrund geschoben haben. Der Deutsche Bundestag hat auf Antrag aller Fraktionen (BT-Drs. 18/843) am 20. März 2014 einen **Untersuchungsausschuss zur NSA-Affäre** eingesetzt, der Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland aufklären soll. Die vom Ausschuss gefassten Beweisbeschlüsse, die schriftlichen Stellungnahmen der Sachverständigen sowie die Protokolle der Ausschusssitzungen sind auf der entsprechenden Internetseite des Bundestags⁹ zu finden. Für Aufregung sorgten im Sommer 2014 Meldungen, wonach der Ausschuss selbst durch BND-Mitarbeiter, offenbar im Auftrag des US-Geheimdienstes CIA, ausspioniert worden sei; als Gegenreaktion wurde der höchste Repräsentant des CIA in Deutschland zur Ausreise aufgefordert. Im Januar 2016 berichtete der Rechercheverbund von NDR, WDR und Süddeutscher Zeitung, dass der US-Geheimdienst NSA und der Bundesnachrichtendienst (BND) bei der Internetüberwachung wieder kooperierten. Die Zusammenarbeit war erst

⁸ vgl. http://www.ifd-allensbach.de/uploads/tx_reportsdocs/FAZ_Juni_Datenschutz.pdf

⁹ vgl. <http://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss>

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

im Frühjahr 2015 nach Kritik an der sog. Selektorenliste eingestellt worden; der BND hatte offenbar den mitgeschnittenen Internetverkehr ohne genaue Überprüfung der von den US-Behörden gelieferten Suchbegriffe weitergeleitet. Dabei waren auch „befreundete Staaten“, deutsche Staatsbürger, Firmen und Politiker ins Blickfeld geraten. Zwischen 2002 und 2013 sollen ca. 690.000 Telefonnummern und 7,8 Mio. IP-Adressen dem BND von US-Seite zugewiesen worden sein. Anfang Dezember 2015 kündigte die G-10-Kommission des Deutschen Bundestags an, vor dem Bundesverfassungsgericht zu klagen, um die bis dahin verweigerte Einsicht in die Selektorenliste zu erhalten; das wäre ein in der Geschichte des Deutschen Bundestags einmaliger Schritt.

Auch das **Europäische Parlament** ist zu diesem Thema nicht untätig geblieben: Am 12. März 2014 verabschiedete es einen vom Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) vorgelegten Abschlussbericht mit zahlreichen Forderungen an Mitgliedsstaaten und EU-Kommission¹⁰. Grundlage war u. a. eine umfangreiche Studie zu den Überwachungsprogrammen der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger¹¹. Spürbare Reaktionen sind nach meinem Eindruck bisher allerdings ausgeblieben, wohl auch wegen der verschärften Sicherheitslage aufgrund terroristischer Bedrohungen. Das Europäische Parlament verabschiedete am 29. Oktober 2015 eine Resolution gegen die Massenüberwachung von EU-Bürgerinnen und -Bürger durch Geheimdienste in EU und USA¹². Darin wurde u. a. darauf hingewiesen, dass der Europäische Gerichtshof kurz zuvor, am 6. Oktober 2015, den Transfer personenbezogener Daten in die USA auf der Grundlage der sog. Safe-Harbor-Entscheidung der Europäischen Kommission gerade wegen der Zugriffsrechte von US-Sicherheitsbehörden für unzulässig erklärt hatte (siehe hierzu Kapitel 1.4.3). Ungeachtet dessen werden in Deutschland mittler-

weile sogar Stimmen laut, die eine Nutzbarmachung der Vorratsdatenspeicherung für Nachrichtendienste fordern.

Auf den ersten Blick scheinen die kommerzielle Nutzbarmachung unserer digitalen Lebensdaten durch global agierende Internetkonzerne und die Massenüberwachung durch in- und ausländische Geheimdienste nicht viel miteinander zu tun zu haben. Auf den zweiten Blick jedoch ergeben sich beachtliche **Gemeinsamkeiten und Schnittmengen**: Nicht nur, dass Geheimdienste der USA und anderer Staaten vermutlich offiziell oder indirekt Zugriff auf Kundendaten privater Unternehmen erlangt haben dürften, um sie für ihre Zwecke zu nutzen. Vor allem die Methoden der massenhaften Datensammlung, der maschinellen Suche nach bestimmten Mustern und der daraus generierten Bildung von Risiko- und Verhaltensprofilen für Menschen folgen bei Unternehmen wie Sicherheitsbehörden derselben Logik. Das „Internet der Dinge“ wird die Menge der anfallenden Daten in den nächsten Jahren weiter drastisch erhöhen; im Jahr 2020 sollen im Bereich von „Industrie 4.0“ nach Prognosen von Fachleuten 50 Mrd. Geräte miteinander kommunizieren. Forderungen nach mehr Sicherheit der Daten und nach Schutz der Privatsphäre scheinen gegenüber der allgemeinen digitalen Euphorie in den Hintergrund zu treten. Bei wachsenden Datenmengen und immer schnelleren Rechnerkapazitäten ist mit immer genaueren Verhaltensanalysen zu rechnen. Die Mensch-Maschine-Beziehung wird sich vermutlich wesentlich ändern und die Abhängigkeit der Menschen von automatisierten Entscheidungsprozessen erhöhen, ohne dass im Gegenzug Transparenz und informationelle Selbstbestimmung wachsen. Nicht von ungefähr beruht das in den o. g. Umfragen zum Ausdruck kommende Unbehagen der Menschen angesichts der digitalen Vernetzung auf der Sorge vor einem schleichenden Kontrollverlust.

Der Datenschutz erweist sich mit einigen seiner Strukturprinzipien wie Datensparsamkeit, Personenbeziehbarkeit von Daten, Privacy by Design, Zweckbindung und Verbot mit Erlaubnisvorbehalt (d. h. gesetzliche Grundlage oder Einwilligung des Betroffenen erforderlich) als durchaus sperrig für die „schöne neue Welt“ der massenhaften Datenerfassung und -auswertung. Auch wenn manche schon

¹⁰ vgl.

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//DE>

¹¹ vgl.

[http://www.europarl.europa.eu/ReqData/etudes/note/join/2013/474405/IPOL-LIBE_NT\(2013\)474405_DE.pdf](http://www.europarl.europa.eu/ReqData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_DE.pdf)

¹² vgl.

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//DE>

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

einen Paradigmenwechsel und neue regulatorische Ansätze für den Datenschutz fordern¹³, so wird es angesichts des gerade erst beschlossenen neuen Rechtsrahmens für die Europäische Union (siehe hierzu Kapitel 1.2) in den nächsten Jahren darum gehen, die innovativen Chancen der verantwortungsbewussten Nutzung von Massendaten (z. B. im Gesundheitswesen) zu nutzen, ohne die Wahrung der Grundrechte zu vernachlässigen¹⁴. Es ist jedenfalls verfrüht, für den Datenschutz die „smarte Kapitulation“¹⁵ zu erklären.

1.2 Die Europäische Datenschutzreform – zum Stand der Datenschutz-Grundverordnung

In den vorangegangenen Tätigkeitsberichten habe ich bereits ausführlich über den damaligen Stand der Novellierung des europäischen Rechtsrahmens für den Datenschutz und insbesondere das europäische Gesetzgebungsverfahren zur Datenschutz-Grundverordnung, die die in die Jahre gekommene Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 ablösen und das Datenschutzrecht insgesamt fit für die Herausforderungen des digitalen Zeitalters machen soll, berichtet (30. Tätigkeitsbericht 2010/2011, LT-Drs. 15/955, S. 30; 31. Tätigkeitsbericht 2012/13, LT-Drs. 15/4600, S. 18 f.). Das Gesetzgebungsverfahren zur Datenschutz-Grundverordnung wurde im Berichtszeitraum fortgesetzt und steht nunmehr kurz vor dem Abschluss.

Noch vor seiner Neuwahl im Mai 2014 hat das Europäische Parlament am 12. März 2014 auf der Grundlage des vom federführenden LIBE-Ausschuss im Oktober 2013 erarbeiteten und in meinem 31. Tätigkeitsbericht näher dargestellten Kompromissvorschlags in erster Lesung dem Entwurf der EU-Datenschutz-Grundverordnung (EU-DSGVO) mit großer Mehrheit zugestimmt. Anders als für den

Deutschen Bundestag gilt für das EU-Parlament nicht der Grundsatz der Diskontinuität, wonach Gesetzesvorhaben, die innerhalb einer Legislaturperiode nicht verabschiedet werden, nach Ablauf dieser Periode verfallen. Die im Mai 2014 neu gewählten Abgeordneten des Europäischen Parlaments konnten deshalb entscheiden, dass sie auf dem am 12. März 2014 beschlossenen Entwurf aufbauen und das Gesetzgebungsvorhaben weiter verfolgen wollen.

Der Europäische Rat hat im Berichtszeitraum seine Befassung mit der Datenschutz-Grundverordnung fortgesetzt, im Jahr 2014 zunächst unter griechischer und in der zweiten Jahreshälfte unter italienischer Präsidentschaft. Am 15. Juni 2015 hat der Rat unter lettischer Präsidentschaft seine Beratungen mit der Verabschiedung eines Standpunkts zu einem vorläufigen Abschluss gebracht und damit die Aufnahme des sog. informellen Trilogverfahrens, d. h. der Verhandlungen zwischen Rat, Parlament und Kommission, ermöglicht. Sowohl die (seit 1. Juli 2015) Luxemburger Ratspräsidentschaft als auch die Europäische Kommission und das Europäische Parlament haben sich klar dazu bekannt, die Trilogverhandlungen noch im Verlauf des Jahres 2015 abzuschließen. Das ist tatsächlich gelungen. Am 15. Dezember 2015 hat die Europäische Kommission mitgeteilt¹⁶, dass eine Einigung im Trilogverfahren erzielt wurde. Inzwischen hat das Bayerische Landesamt für Datenschutzaufsicht (LDA) dankenswerter Weise eine Synopse mit den drei Ausgangsfassungen der EU-Kommission, des EU-Parlaments und des EU-Ministerrates für die Trilogverhandlungen (in deutscher Sprache) und mit der Schlussfassung vom 15. Dezember 2015 (in englischer Sprache) veröffentlicht.¹⁷ Der Text wird derzeit von der Kommission noch redaktionell überarbeitet; auch die Gliederung ist noch anzupassen. Danach wird der englischsprachige Text, der Grundlage der Verhandlungen war, in die 22 Amtssprachen der EU übersetzt. Voraussichtlich im März oder April 2016 soll dann die Verordnung vom Europäischen Parlament und durch den EU-Ministerrat verabschiedet und anschließend im Amtsblatt der

¹³ vgl. etwa Härting/Schneider: „Das Ende des Datenschutzes – es lebe die Privatsphäre“, Computer und Recht (CR-Report), 2015, S. 891 f.

¹⁴ vgl. auch die Stellungnahme 7/2015 des Europäischen Datenschutzbeauftragten (EDPS) „Bewältigung der Herausforderungen in Verbindung mit Big Data“ vom 19. November 2015,

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_DE.pdf

¹⁵ so die Überschrift eines Artikels in der FAZ am 5. Januar 2016, in dem der mögliche Kontrollverlust im Smart Home der Zukunft beschrieben wird.

¹⁶ vgl. Pressemitteilung: http://europa.eu/rapid/press-release_IP-15-6321_de.htm

¹⁷ vgl. https://www.lida.bayern.de/media/baylda_synopse.pdf

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

EU veröffentlicht werden. Zwei Jahre darauf wird die EU-DSGVO in Kraft treten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Berichtszeitraum in zwei Entschlüsseungen und in einem umfangreicheren Kernpunktepapier zum Stand des Gesetzgebungsverfahrens Stellung genommen (Entschlüsseungen vom 28. März 2014 und 19. März 2015, vgl. Anhänge 5 und 18, sowie „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung“ vom 29. Juli 2015¹⁸).

Der jetzt gefundene Kompromiss trägt den Forderungen der unabhängigen deutschen Datenschutzbehörden in vielen Punkten Rechnung, begegnet an mancher Stelle aber auch Kritik.

Positiv zu bewerten sind die folgenden Kernelemente der Neuregelung:

- **Marktortprinzip:**
Danach soll das Europäische Datenschutzrecht künftig auch für außereuropäische Unternehmen gelten, wenn diese Waren oder Dienstleistungen für den europäischen Markt anbieten.
- **Recht auf Vergessen:**
Betroffene solle künftig bei der Durchsetzung ihres Löschanforderungs gegenüber Dritten von der verantwortlichen Stelle stärkere Unterstützung erhalten als bisher.
- **Recht auf Datenübertragbarkeit:**
Die Nutzer sozialer Netzwerke sollen vom jeweiligen Anbieter des Netzwerkes ihre Daten in einem Format herausverlangen dürfen, das es ihnen ermöglicht, diese Daten bei einem anderen Anbieter weiter zu nutzen.
- **Privacy-by-Design/Privacy-by-Default:**
Wenn bereits Hersteller zu datenschutzfreundlichen Produkten und Voreinstellungen verpflichtet werden, stärkt dies die Datenschutzrechte der Betroffenen.

¹⁸ vgl. <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Datenschutzrechtliche-Kernpunkte-DSGVO.pdf>

- **Gesetzliche Verpflichtung zur Bestellung betrieblicher und behördlicher Datenschutzbeauftragter:**

Betriebliche und behördliche Datenschutzbeauftragte, deren Bestellung in Deutschland bislang in weitem Umfang gesetzlich vorgeschrieben war, haben sich als wichtiges Element einer effektiven Datenschutzaufsicht bewährt. Deshalb ist zu begrüßen, dass die Datenschutz-Grundverordnung die Bestellung von Datenschutzbeauftragten europaweit zumindest bei allen öffentlichen Stellen und solchen nicht-öffentlichen Stellen, die besonders risikoreiche Datenverarbeitungen vornehmen, verbindlich vorschreibt und dem EU-Gesetzgeber und den Mitgliedstaaten die Möglichkeit eröffnet, eine weitergehende Bestellopflicht einzuführen. Damit wird eine Harmonisierung auf einem gewissen Mindeststandard erreicht.

- **Datenschutz-Folgenabschätzungen:**
Für Datenverarbeitungen mit bestimmten Risiken ist künftig die Durchführung einer Datenschutz-Folgenabschätzung verbindlich vorgeschrieben.
- **Selbstregulierung und Zertifizierung:**
Die Datenschutz-Grundverordnung sieht einen Rahmen für die Schaffung von Verhaltensregeln und Zertifizierungsverfahren vor.
- **Effektive Durchsetzung des Datenschutzrechts:**
Im Vergleich zum bisherigen deutschen Datenschutzrecht sieht die Datenschutz-Grundverordnung die Verhängung weit höherer Bußgelder vor als bislang möglich. Zudem können die Datenschutzaufsichtsbehörden künftig durchsetzbare Anordnungen und Bußgelder nicht nur gegen nicht-öffentliche Stellen, sondern auch gegenüber Behörden erlassen.
- **Bessere Kontrolle über Datenübermittlungen aus der EU an Behörden und Gerichte in Drittstaaten:**
Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden, insbesondere Sicherheitsdiensten, eines Drittstaates, die einer Stelle in der EU die Übermittlung personenbezogener Daten in den Drittstaat auferlegen, stellen nach europäischem Recht keine hinreichende Rechtsgrundlage für diese Übermittlung dar; vielmehr müssen die allgemeinen Vorgaben für einen Drittstaatentransfer beachtet werden oder es bedarf internationaler Übereinkommen zur

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

Rechts- und Amtshilfe als Grundlage für solche Übermittlungen.

- Bessere Kooperation der Datenschutzaufsichtsbehörden in Europa:

Für grenzüberschreitende Fälle sieht die Datenschutz-Grundverordnung eine stärkere Kooperation der Datenschutzaufsichtsbehörden als bisher vor. Den Unternehmen soll im Wesentlichen die Aufsichtsbehörde an ihrem Hauptsitz als Ansprechpartner zur Verfügung stehen. Bürger können sich bei der Aufsichtsbehörde in ihrem Heimatland beschweren, die den Sachverhalt – sofern er grenzüberschreitend ist – mit den übrigen betroffenen Aufsichtsbehörden unter Federführung der Aufsichtsbehörde am Hauptsitz des Unternehmens klären soll.

- Beibehaltung der Zweckbindung im bisher gültigen Umfang:

Der Grundsatz der Zweckbindung ist eine tragende Säule des gültigen Datenschutzrechts und gilt weiterhin.

In einigen Punkten hätte man sich mutigere und datenschutzfreundlichere Lösungen vorstellen können. Das betrifft insbesondere folgende Punkte:

- Datenschutzfreundliche Regelung zur Einwilligung des Betroffenen:

Die Chance, stillschweigende bzw. konkludente Einwilligungen generell auszuschließen, wurde nicht genutzt. Eine ausdrückliche Einwilligung ist (auch) künftig nur für die Verarbeitung besonders sensibler personenbezogener Daten erforderlich.

- Ausdrückliche Regelung des Grundsatzes der Datensparsamkeit:

Die Datenschutzgrundverordnung enthält keine ausdrückliche Regelung des Grundsatzes der Datensparsamkeit. Dies wäre jedoch sinnvoll gewesen, um den Herausforderungen des Einsatzes von Big-Data-Technologien wirksam begegnen zu können.

- Wirksame Begrenzung der Profilbildung:

Die Datenschutzgrundverordnung enthält keine hinreichend detaillierten Regelungen zur Profilbildung. Ein wichtiger Bereich des materiellen Datenschutzrechts wurde damit im Gesetzge-

bungsverfahren nicht klar und abschließend geregelt.

Die deutschen Datenschutzbehörden haben bereits mit einer Bestandsaufnahme begonnen, welche Aufgaben und Befugnisse durch die EU-Datenschutz-Grundverordnung neu auf sie zukommen werden und wie sie ihre internen Abläufe und die Zusammenarbeit mit anderen Aufsichtsbehörden auf die neuen gesetzlichen Vorgaben ausrichten können. Wichtig dürfte dabei auch die Frage werden, wer in Zukunft in welchen Fällen für Deutschland in Europa sprechen darf. Dies könnte durch ein Bundesgesetz, einen Staatsvertrag oder eine Selbstregulierung der Datenschutzbehörden in Form einer Geschäftsordnung geregelt werden. Die größte Herausforderung für die deutschen Datenschutzaufsichtsbehörden, aber auch für die Rechtsanwender, d. h. die Betroffenen und die verantwortlichen Stellen (Unternehmen und Behörden) in Deutschland, wird jedoch sicherlich sein, dass sie sich mit den anderen Akteuren, insbesondere den Aufsichtsbehörden der übrigen europäischen Mitgliedstaaten auf ein einheitliches Verständnis und einen einheitlichen Vollzug des neuen Rechts werden einigen müssen.

1.3 Die EU-Datenschutzrichtlinie für Polizei und Justiz – Flickenteppich statt Regenschirm?

Pünktlich mit Ablauf des Jahres 2015 wurde der europäische Datenschutz auch im Bereich der polizeilichen und justiziellen Zusammenarbeit auf neue Füße gestellt. Nachdem die Europäische Datenschutzrichtlinie für Polizei und Justiz (sog. JI-Richtlinie) seit Veröffentlichung des Kommissionsvorschlages im Jahre 2012¹⁹ lange Zeit ins Stocken geraten war, wurden 2015 im Laufe weniger Monate Entwurfsfassungen des Parlaments und des Rates veröffentlicht, welche teils erheblich von der Ausgangsfassung der Kommission abwichen. Auch die anschließenden Trilogverhandlungen wurden unerwartet rasch noch 2015 abgeschlossen. Wurde die

¹⁹ Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM (2012) 10 endg, BR-Drs. Nr. 51/12.

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

JI-Richtlinie mit heißer Nadel gestrickt? Ein erster Blick auf die neuen Regelungen der Richtlinie offenbart ernstliche Mängel und ungenutzte Chancen.

Auf Basis der neu geschaffenen Gesetzgebungskompetenz des Artikels 16 Absatz 2 Satz 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) legte die Kommission am 27. Januar 2012 einen ersten Entwurf eines Reformpaketes für den Datenschutz vor. Der noch in der Kommissionsmitteilung zu einem „Gesamtkonzept für den Datenschutz in der Europäischen Union“²⁰ enthaltene Leitgedanke, ein einziges datenschutzrechtliches Rechtsinstrument zu schaffen, welches einheitlich sämtliches unionale Handeln unter seinem „Schirm“ vereint (sog. „umbrella legislation“), hatte nur kurz Bestand. Trotz formaler Auflösung der Säulenstruktur der Union wurde daran festgehalten, den polizeilichen und justiziellen Bereich gesondert zu regeln, um sektorspezifischen Besonderheiten Rechnung tragen zu können. Die Kommission legte daher zwei separate Legislativvorschläge vor, um ein höheres unionales Datenschutzniveau zu schaffen. Während die Datenschutz-Grundverordnung (EU-DSGVO) im Fokus der Aufmerksamkeit stand (siehe hierzu Kap. 1.2), blieb die Entwicklung der parallel veröffentlichten JI-Richtlinie lange Zeit unbeachtet. Überraschend und nahezu unbemerkt kam 2015 doch noch Bewegung ins Spiel: Innerhalb weniger Monate stellten Europäisches Parlament und Rat ihre Entwurfsfassungen vor. Die Trilog-Verhandlungen wurden zügig aufgenommen und – pünktlich vor Jahresablauf – am 15. Dezember 2015 abgeschlossen. Genau rechtzeitig, damit die JI-Richtlinie zeitgleich mit der EU-DSGVO angenommen werden konnte.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder positionierte sich seit Veröffentlichung des Kommissionsvorschlages mehrfach zu dem Gesamtkonzept der europäischen Datenschutzreform im Allgemeinen und der EU-DSGVO im Speziellen²¹. Am 29. Oktober 2015 erhob die Konferenz im Rahmen einer eingehenden Stellungnahme aber auch zur

JI-Richtlinie zahlreiche Forderungen.²² Die Konferenz wies u. a. darauf hin, dass

- die Anwendungsbereiche der JI-Richtlinie und der EU-DSGVO klar voneinander abgrenzbar bleiben müssen;
- eine strengere Zweckbindung der Daten gewährleistet werden muss; die Richtlinie selbst solle Regelungen zur Datenweiterverarbeitung durch die Mitgliedsstaaten enthalten;
- zwingend gesonderte Schutzniveaus für Unverdächtige, Zeugen und Opfer vorgesehen werden sollten;
- jede Datenspeicherung auf ihre Erforderlichkeit und Verhältnismäßigkeit überprüft werden muss; insbesondere sollte der Verhältnismäßigkeitsgrundsatz durch die verpflichtende Festlegung von Speicher- und Aussonderungsprüffristen konkretisiert werden;
- umfassende Benachrichtigungspflichten als Kernrechte des Betroffenen zu garantieren sind, beispielsweise durch Informationspflichten gegenüber dem Betroffenen;
- die Durchführung einer Datenschutz-Folgenabschätzung auch im Bereich der JI-Richtlinie verpflichtend sein muss;
- die Bestellung behördlicher Datenschutzbeauftragter nicht länger in das mitgliedstaatliche Ermessen gestellt werden dürfe.

Positive Hervorhebung verdient die in Artikel 5 der JI-Richtlinie vorgesehene Unterscheidung nach Personengruppen. Entsprechende Vorschriften gelten sowohl bereits für Europol²³ als auch Eurojust²⁴ und sind an die Empfehlung des Europarats Nr. R (87) 15 angelehnt. Eine fehlende Differenzierung war über Jahre hinweg ein Kritikpunkt gegenüber dem bislang geltenden Rahmenbeschluss zum Schutz personenbezogener Daten. Durch die Richtlinie kann diese Lücke nunmehr geschlossen werden. Hierdurch wird sichergestellt, dass Daten bestimmter Personengruppen (Zeugen, Opfer, Kontaktpersonen etc.) unter strengeren Voraussetzungen und mit kürzeren Fristen gespeichert werden

²⁰ KOM (2010) 609 endg.

²¹ vgl. 31. Tätigkeitsbericht, LT-Drs. Nr. 15/4600, S. 21 f. sowie Kap. 1.2 in diesem Bericht

²² vgl. <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Datenschutzrechtliche-Kernpunkte-für-die-Trilogverhandlungen.pdf>

²³ Artikel 14 des Europol-Beschlusses 2009/371/JI.

²⁴ Artikel 15 des Eurojust-Beschlusses 2009/426/JI.

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

und dass darüber hinaus Daten anderer Personen, die nicht einer Straftat verdächtig sind, entweder gar nicht oder nur in sehr begrenzten Fällen gespeichert werden dürfen.

Leider blieb dennoch ein Großteil der Vorschläge der Konferenz unberücksichtigt. Die konsolidierte Fassung der JI-Richtlinie erschöpft sich an vielen Stellen in allgemeinen Ausführungen und überlässt wesentliche Entscheidungen den nationalen Gesetzgebern und deren innerstaatlichem Recht. Dies mag damit begründet werden, dass es gerade dem Wesen einer Richtlinie entspricht, gesonderte nationale Umsetzungsakte zu verlangen und den umsetzenden Mitgliedstaaten einen Freiraum in Bezug auf die Form und die Wahl der Mittel zu überlassen. Im Gegensatz zu dem Handlungsinstrument der Verordnung sollen Richtlinien eben nicht direkte Geltung beanspruchen können. Der europäische Gesetzgeber ist gleichwohl auf Basis der Verträge (Artikel 16 AEUV) verpflichtet, einen einheitlich hohen Datenschutzstandard innerhalb des Unionsgebietes sicherzustellen. Dementsprechend hätten durch die Richtlinie selbst klar umrissene Mindestgrundsätze festgesetzt werden müssen, welche den Ermessensspielraum der einzelnen Mitgliedstaaten möglichst begrenzen. Je größer der Unterschied mitgliedstaatlicher Schutzstandards ist, desto erschwerter ist der Austausch vorhandener Informationen zwischen den zuständigen Behörden. Effektive polizeiliche und justizielle Zusammenarbeit setzt daher zwingend ein hohes Maß an Harmonisierung voraus. Wesentliche Grundsätze des EU-Datenschutzrechtes hätten direkt in die JI-Richtlinie aufgenommen werden müssen. Stattdessen werden wesentliche Entscheidungen dem Ermessen der Mitgliedstaaten überlassen.

Der Zweckbindungsgrundsatz bildet einen Eckpfeiler des Datenschutzes. Er bestimmt, dass ausgetauschte Daten nicht ohne weiteres für andere Zwecke weiterverarbeitet werden können, als zu welchen sie erhoben wurden. Begrüßenswert ist, dass die in der Entwurfsfassung des Rates noch enthaltene Möglichkeit zur zweckfremden Weiterverarbeitung ersatzlos gestrichen wurde. Nach Artikel 4 Absatz 2 der Ratsfassung sollte eine Weiterverarbeitung für einen anderen Zweck innerhalb der JI-Richtlinie zulässig sein, wenn es dafür nach (national) anwendbarem Recht eine Rechtsgrundlage gibt und die Weiterverarbeitung erforderlich und verhält-

nismäßig ist. Diese direkte Möglichkeit zur Zweckentfremdung hätte die Betroffeneninteressen in höchstem Maße gefährdet. Stattdessen wurde Artikel 4 lit. c neu aufgenommen, welcher die Mitgliedsstaaten dazu verpflichtet Sorge zu tragen, dass personenbezogene Daten im Verhältnis zu den Zwecken der Datenverarbeitung nicht exzessiv sind. Offen bleibt, wann eine solche exzessive Verarbeitung anzunehmen ist. Statt den unbestimmten Begriff der Exzessivität zu verwenden, wäre es sinnvoller und normenklarer gewesen, die Datenverarbeitung auf das für die Zwecke notwendige Mindestmaß zu beschränken. Hierdurch hätte nicht nur eine Konvergenz mit der EU-DSGVO hergestellt, sondern auch sichergestellt werden können, dass die Verarbeitung auf das erforderliche Minimum beschränkt bleibt. Der Terminus der exzessiven Verarbeitung stellt einen sprachlichen Fremdkörper innerhalb der Richtlinie dar, welcher den Ermessensspielraum der Mitgliedsstaaten bei der Umsetzung voraussichtlich erheblich erweitern wird.

Ernüchternd muss gesagt werden, dass die JI-Richtlinie ihrer Zielsetzung – eine umfassende Datenschutzkonzeption im Bereich der polizeilichen und justiziellen Zusammenarbeit zu schaffen – nicht gerecht werden kann. Problematisch ist insofern auch die Regelung des Artikels 59 der JI-Richtlinie, welcher bestimmt, dass bereits existente spezifische Datenschutzvorschriften im Bereich der polizeilichen und justiziellen Zusammenarbeit von der Richtlinie unberührt bleiben sollen. Innerhalb dieser Zusammenarbeit der Mitgliedsstaaten existiert eine Vielzahl solcher spezialgesetzlichen Rechtsakte. Nach dem Spezialitätsgrundsatz würde dies bedeuten, dass immer dann, wenn ein Rechtsakt spezifischere Regelungen als die Richtlinie enthält, letztere als allgemeinere Vorschrift (*lex generalis*) verdrängt und nicht mehr zur Anwendung kommen würde. Illustriert am Beispiel des Prümer Beschlusses würde dies zu folgender Situation führen: Der Prümer Beschluss enthält gesonderte Schutzvorschriften für besonders sensible Datenkategorien, u. a. für DNA-Profile und daktyloskopische Daten. Eine gesonderte Regelung für besonders sensible Daten ist in der Richtlinie nicht enthalten. Folglich wären die Vorschriften des Prümer Beschlusses als spezieller anzusehen und die Anwendbarkeit der JI-Richtlinie ausgeschlossen. Problematisch ist jedoch, dass innerhalb des Prümer Beschlusses der

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

von den Mitgliedsstaaten zu gewährleistende Mindeststandard auf das Schutzniveau des Abkommens des Europarates aus dem Jahre 1981 (!) samt Zusatzprotokoll²⁵ herabgesenkt wird. In einer Zeit weit vor Schaffung des Internets entstanden bleibt dessen Schutzniveau weit hinter dem der JI-Richtlinie zurück.

Offen bleibt, in welchem Verhältnis bereits bestehende Rechtsakte der polizeilichen und justiziellen Zusammenarbeit zur Richtlinie stehen und welcher datenschutzrechtliche Maßstab an die jeweiligen Datenverarbeitungen anzulegen sein wird. Ist ein Auseinanderfallen der Datenschutzniveaus zu befürchten? Werden Polizeibehörden gleichermaßen effektiv grenzüberschreitend Informationen austauschen können?

Artikel 61 Absatz 2 der Richtlinie sieht daher vor, dass alle derartigen bereits bestehenden Rechtsakte von der Kommission gesondert zu überprüfen und, falls erforderlich, im Rahmen eines zweiten Reformschrittes der Richtlinie anzupassen sind. Die schon lange bestehende Zersplitterung datenschutzrechtlicher Vorschriften im Bereich Polizei und Justiz wird daher auch nach Inkrafttreten der JI-Richtlinie fortauern. Um Rechtsunsicherheit zu vermeiden, sollte diese Überprüfung möglichst rasch erfolgen.

Durch die Entscheidung der Kommission, das Datenschutzreformpaket in zwei gesonderte Rechtsakte aufzugliedern, wurde die Möglichkeit verspielt, ein unionsweit gültiges, umfassendes Mindestschutzniveau zu schaffen. Trotz formaler Abschaffung der ehemaligen Säulenstruktur der EU werden sich der Datenschutz innerhalb der Europäischen Gemeinschaften und der Datenschutz im Bereich des Inneren und der Justiz auch weiterhin in zweierlei Geschwindigkeiten bewegen. Zudem offenbart der direkte Vergleich zwischen JI-Richtlinie und EU-DSGVO, dass das Schutzniveau der Richtlinie von dem der Verordnung in zahlreichen Bereichen nicht

nur abweicht, sondern dieses sogar abschwächt. Im Bereich der polizeilichen und justiziellen Zusammenarbeit werden besonders sensible Daten ausgetauscht, sodass es nur folgerichtig gewesen wäre, innerhalb der Richtlinie mindestens ein mit der Verordnung gleichwertiges Schutzniveau zu schaffen.

Was bleibt, ist der Beigeschmack eines Stückwerkes, welches einst als umfassende Datenschutzkonzeption angedacht war. Die europäische Datenschutzreform hat sich in ihrer Konzeption als umfassende Regenschirm-Gesetzgebung nunmehr zu einem bloßen Flickenteppich gewandelt. Dieser Flickenteppich mag zwar die Füße des Betroffenen wärmen, schützt aber nicht gleichermaßen vor dem Regen wie ein Regenschirm!

Das Inkrafttreten der JI-Richtlinie stellt einen bloßen Zwischenschritt für die Schaffung eines europäischen Mindestdatenschutzlevels im Bereich der polizeilichen und justiziellen Kooperation dar. Bereits jetzt steht fest, dass in den kommenden Jahren tiefgehende Umstrukturierungen und Folgereformen zu erwarten sind.

1.4 Die Rechtsprechung des Europäischen Gerichtshofs in Datenschutzfragen

Der Europäische Gerichtshof (EuGH) hat im Berichtszeitraum in mehreren Entscheidungen die Grundrechtsorientierung des Datenschutzes in Europa betont und damit die Tradition des Bundesverfassungsgerichts eindrucksvoll fortgeführt.

1.4.1 Urteil des EuGH vom 8. April 2014, C 293 und 594/12 (Vorratsdatenspeicherung)

Der EuGH hat mit dieser Entscheidung die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten für ungültig erklärt. Diese beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränke. Der Gerichtshof betonte, dass aus den auf Vorrat zu speichernden Telekommunikationsverkehrsdaten in ihrer Gesamtheit sehr genaue Schlüsse auf das Privatleben der be-

²⁵ Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, dem Zusatzprotokoll vom 8. November 2001 zu dem Übereinkommen und den Grundsätzen der Empfehlung Nr. R (87) 15 des Europarats über die Nutzung personenbezogener Daten im Polizeibereich.

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

treffenden Personen gezogen werden können, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld. Das Urteil liegt auf der Linie der bisherigen Rechtsprechung des Bundesverfassungsgerichts (vgl. Urteil vom 2. März 2010, 1 BvR 256/08) und bestätigt den hohen Grundrechtsschutz in der Europäischen Union auf der Grundlage der Europäischen Grundrechtecharta. Die Datenschutzbeauftragten des Bundes und der Länder haben die Entscheidung in einer Entschließung vom 25. April 2014 begrüßt (vgl. Anhang 6). Inzwischen ist – nachdem die zunächst geplante europäische Regelung nicht realisiert wurde – eine neue Rechtsgrundlage für die Vorratsdatenspeicherung auf nationaler Ebene geschaffen worden (siehe hierzu Kapitel 3.1).

1.4.2 Urteil des EuGH vom 13. Mai 2014, C 131/12 (Google Spain)

Auf Betreiben der spanischen Datenschutzaufsichtsbehörde und eines spanischen Staatsbürgers wurden in einem Vorlageverfahren die US-Firma Google und deren spanische Tochtergesellschaft verpflichtet, in den Treffern ihrer Suchmaschine den Link auf eine auch im Internet veröffentlichte Anzeige in einer spanischen Tageszeitung aus dem Jahr 1998 zu löschen; diese Anzeige betraf ein längst erledigtes Insolvenzverfahren des Spaniers. Dem Antrag auf Löschung der Zeitungsanzeige selbst im Internet wurde nicht stattgegeben.

Der Europäische Gerichtshof hat in dem Urteil wichtige Aussagen für das europäische Datenschutzrecht getroffen, die unter dem Schlagwort „Recht auf Vergessenwerden“ breite Resonanz gefunden haben:

- Das Grundrecht auf den Schutz personenbezogener Daten nach der Europäischen Grundrechtecharta gilt uneingeschränkt auch im Internet.
- Der Betreiber der Suchmaschine verarbeitet selbst (personenbezogene) Daten und ist hierfür im Sinne der Europäischen Datenschutzrichtlinie 95/46/EG verantwortlich. Durch die Tätigkeit einer Suchmaschine können die Grundrechte zusätzlich zur Herausgabe einer Internetseite beeinträchtigt werden. Dass die Betreiber von Internetseiten den Suchmaschinen den Zugriff technisch durch Ausschlussprotokolle verwehren können, ändert an der Verantwortung des Suchmaschinenbetreibers nichts.
- Die Suchmaschine wird auch „im Rahmen der Tätigkeiten“ der spanischen Niederlassung betrieben – selbst wenn die Datenverarbeitung außerhalb Europas stattfindet –, weil die Niederlassung die Aufgabe hat, Werbeflächen im Internet für den spanischen Markt zu verkaufen. Damit wurde das in der EU-Datenschutz-Grundverordnung vorgesehene Marktortprinzip praktisch vorweggenommen.
- Die Gefahr der detaillierten Profilbildung einer Person durch Suchmaschinen stellt einen potenziell schweren Eingriff in das Persönlichkeitsrecht des Betroffenen dar, der nicht allein mit dem wirtschaftlichen Interesse des Betreibers an der Verarbeitung der Daten gerechtfertigt werden kann.
- Anträge (auf Entfernen eines Links) können von der betroffenen Person unmittelbar an den für die Verarbeitung Verantwortlichen gerichtet werden, der dann sorgfältig ihre Begründetheit zu prüfen und die Verarbeitung der betreffenden Daten ggf. zu beenden hat. Wenn er den Anträgen nicht stattgibt, kann sich die betroffene Person an die Kontrollstelle (Datenschutzaufsichtsbehörde) oder das zuständige Gericht wenden.
- Da sich das Entfernen von Links auf das berechnete Interesse anderer am ungehinderten Informationszugang auswirken kann, ist im Einzelfall ein angemessener Ausgleich zu finden. Im Allgemeinen überwiegen die Interessen der durch Art. 7 und 8 der Grundrechtecharta geschützten Personen gegenüber dem Interesse der Internetnutzer; der Ausgleich kann in besonders gelagerten Fällen aber von der Art der betreffenden Information, von deren Sensibilität für das Privatleben der betroffenen Person und vom Interesse der Öffentlichkeit am Zugang zu der Information abhängen, das u. a. je nach der Rolle, die die betroffene Person im öffentlichen Leben spielt, variieren kann.
- Auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten kann im Laufe der Zeit nicht mehr den Bestimmungen der Europäischen Datenschutzrichtlinie entsprechen, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr erforderlich

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

sind. Das ist insbesondere der Fall, wenn sie diesen Zwecken in Anbetracht der verstrichenen Zeit nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen. Es ist nicht erforderlich, dass der betreffenden Person durch die Einbeziehung der Information in die Ergebnisliste (der Suchmaschine) ein Schaden entstanden ist.

Google bezeichnete die Entscheidung des EuGH in einer ersten Reaktion als „enttäuschend“. Kritische Stimmen, insbesondere aus den USA, vertraten die Auffassung, dass das Urteil das Recht auf Privatsphäre und informationelle Selbstbestimmung („Recht auf Vergessenwerden“) zu Lasten des Rechts auf Meinungsfreiheit und Informationsfreiheit („Recht auf Wissen“) überbetone. In den Medien wurde bereits über Löschanträge von Personen berichtet, über die im Internet Informationen im Zusammenhang mit Straftaten zu finden waren. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat als zuständige deutsche Aufsichtsbehörde auf seiner Internetseite mittlerweile Informationen zur Löschung von Google-Einträgen bereitgestellt²⁶. Zu beachten ist, dass Löschanträge direkt an Google und nicht etwa an den Hamburger Kollegen – und auch nicht an meine Dienststelle – zu richten sind.

1.4.3 Urteil des EuGH vom 6. Oktober 2015, C-362/14 (Safe Harbor)

Der Europäische Gerichtshof hat in einem viel beachteten Urteil vom 6. Oktober 2015 aufgrund einer Vorlage durch ein irisches Gericht im Klageverfahren des österreichischen Facebook-Nutzers Max Schrems gegen die irische Datenschutzaufsichtsbehörde die Angemessenheitsentscheidung der Europäischen Kommission vom 26. Juli 2000 für die Vereinigten Staaten von Amerika (sog. Safe-Harbor-Entscheidung) für ungültig erklärt und entschieden, dass die europäischen Datenschutzaufsichtsbehörden auch beim Vorliegen einer Angemessenheitsentscheidung der Kommission berechtigt und verpflichtet sind, die Angemessenheit des Daten-

*schutzniveaus in einem Drittstaat eigenständig zu prüfen*²⁷.

Bis dato hatten zahlreiche US-amerikanische Unternehmen, darunter alle großen Internetkonzerne, Safe-Harbor-Zertifizierungen erhalten, wenn sie sich gegenüber dem US-Handelsministerium verpflichtet hatten, die von der EU-Kommission vorgegebenen Datenschutzregelungen einzuhalten. Die deutschen Datenschutzbeauftragten hatten schon seit Jahren bemängelt, dass Safe Harbor mit seinem System der Selbstzertifizierung keinen ausreichenden Schutz für den Datentransfer in die USA biete²⁸. Der EuGH kam vor dem Hintergrund der Befugnisse der dortigen Sicherheitsbehörden u. a. zu dem Schluss, dass insbesondere „eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der (EU-Grundrechte)Charta garantierten Grundrechts auf Achtung des Privatlebens verletzt“ (Randnummer 93). Ebenso verletze „eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz“ (Randnummer 94).

Als unmittelbare Folge des Urteils ist ein Transfer personenbezogener Daten aus der EU und dem europäischen Wirtschaftsraum in die USA auf der Grundlage der Safe-Harbor-Entscheidung der Kommission ab sofort nicht mehr zulässig, da der EuGH auch keine Übergangsfristen eingeräumt hat. Ob die bisher alternativ eingesetzten Instrumente für den Datentransfer, etwa Standardvertragsklauseln oder Binding Corporate Rules (BCR), rechtlich noch zulässig sind, wird von den Datenschutzbehörden in der EU derzeit intensiv geprüft. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat ein erstes Positionspapier am

²⁶ vgl. https://www.datenschutz-hamburg.de/news/detail/article/informationen-zur-loeschung-von-google-eintraegen.html?tx_ttnews%5BbackPid%5D=200&cHash=193ff8064d2651f478dc11a6b997078b

²⁷ vgl. http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/15-10-06-EuGH-Safe-Harbor-Entscheidung-deutsch-C_0362_2014-DE-ARR.pdf

²⁸ vgl. 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Kap. 1.3.7, S. 26 f. m.w.N.; außerdem Entschließung vom 19. März 2015 (Anhang 22)

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

21. Oktober 2015 vorgelegt²⁹. Übermittlungen personenbezogener Daten in Drittstaaten, die weiterhin ausschließlich auf die aufgehobene Angemessenheitsentscheidung der Kommission gestützt werden, können von den Aufsichtsbehörden ab sofort untersagt werden.

In einer gemeinsamen Erklärung aller europäischen Datenschutzaufsichtsbehörden (Statement der Artikel-29-Datenschutzgruppe vom 15. Oktober 2015³⁰) haben sich diese zudem darauf geeinigt, dass sie Übermittlungen personenbezogener Daten in die USA auf der Grundlage der von § 4c des Bundesdatenschutzgesetzes zur Verfügung gestellten alternativen Transferinstrumente, d. h. insbesondere der Einwilligung Betroffener, der Standardvertragsklauseln der Europäischen Kommission sowie verbindlicher Unternehmensregelungen bis Ende Januar 2016 grundsätzlich nicht beanstanden werden, dass die Auswirkungen des Urteils des Europäischen Gerichtshofs vom 6. Oktober 2015 auf diese alternativen Transferinstrumente jedoch einer sorgfältigen rechtlichen Analyse bedürfen, an deren Ende ein einheitlicher Standpunkt aller europäischen Datenschutzaufsichtsbehörden zur gleichförmigen Umsetzung des Urteils sowie koordinierte Durchsetzungsmaßnahmen in den einzelnen Mitgliedsstaaten stehen sollten.

Nach dem Wegfall der Angemessenheitsentscheidung der Kommission ist es in erster Linie Sache der jeweiligen Exporteure in der EU zu prüfen, ob die Verwendung von Standardvertragsklauseln oder die Beachtung der Vorgaben verbindlicher Unternehmensrichtlinien unter Berücksichtigung aller mit dem jeweiligen Transfer im Zusammenhang stehender Umstände geeignet ist, ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Betroffenen sowie hinsichtlich der Ausübung der damit verbundenen Rechte im Sinne von Artikel 26 Absatz 2 Satz 1 der Richtlinie 95/46/EG zu bieten, oder ob zusätzliche technische, organisatorische oder recht-

liche Maßnahmen bis hin zur vorübergehenden Aussetzung oder endgültigen Beendigung des jeweiligen Transfers zu ergreifen sind. Bei der Erfüllung dieser Pflicht unterliegen die exportierenden Stellen in Europa der Aufsicht der europäischen Datenschutzaufsichtsbehörden. Diese müssen zudem entscheiden, wie sie mit den ihnen in den Rechtsakten der Europäischen Kommission sowie durch Artikel 28 Absatz 3 der Richtlinie 95/46/EG eingeräumten Befugnissen zur Aussetzung des Transfers personenbezogener Daten in Drittstaaten umgehen werden.

Die den Datenschutzaufsichtsbehörden in den Rechtsakten zu den Standardvertragsklauseln eingeräumten Aussetzungsbefugnisse könnten im Sinne einer abstrakten Betrachtungsweise so zu verstehen sein, dass die bloße rechtliche Möglichkeit eines Zugriffs US-amerikanischer Sicherheitsdienste nach amerikanischem Recht für eine Untersagung des betreffenden Transfers ausreichend ist. Im Sinne einer konkreten Betrachtungsweise könnte man die Untersagung oder Aussetzung einer Datenübermittlung in die USA stattdessen auch davon abhängig machen, ob im Einzelfall eine gewisse Wahrscheinlichkeit für einen tatsächlichen Zugriff auf die betroffenen Daten durch Sicherheitsdienste in den USA besteht und ggf. in diesem Zusammenhang auch die Menge und Qualität der Daten mitberücksichtigen. Dies würde es nahelegen, dass die Voraussetzungen für den Erlass von Verbots- oder Aussetzungsverfügungen zumindest im Hinblick auf den Transfer personenbezogener Daten an diejenigen US-amerikanischen Unternehmen und Anbieter von Cloud-Diensten, die nach Presseberichten am sog. PRISM-Programm teilgenommen haben und in diesem Zusammenhang personenbezogene Daten mit US-amerikanischen Sicherheitsdiensten ausgetauscht haben (u. a. Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL, Apple), vorliegen. Mit diesen Fragen sowie mit der notwendigen Analyse des US-amerikanischen Rechts beschäftigen sich zurzeit alle deutschen und europäischen Aufsichtsbehörden. Es bleibt zu hoffen, dass es gelingen wird, hierzu zeitnah einen gemeinsamen Standpunkt zu finden.

Als Reaktion auf das Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015 hat die Kommission in einer Mitteilung vom 6. November 2015 ange-

²⁹ vgl. <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/15-10-26-Positionspapier-DSK-zu-Safe-harbor.pdf>

³⁰ vgl. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

kündigt, dass sie ihre Verhandlungen mit den USA über eine Neuauflage des Safe-Habor-Abkommens intensiviert habe (Kom. [2015] 566 final³¹). Offenbar wurden dabei in letzter Zeit Fortschritte erzielt. So sind die Zugriffsrechte US-amerikanischer Sicherheitsbehörden durch zwei Änderungen des amerikanischen Rechts im Januar und Juni 2015 eingeschränkt worden. Außerdem haben die USA am 15. September 2015 einem Rahmenabkommen mit der EU zugestimmt, das EU-Bürgern im Bereich der Strafverfolgung ein Recht auf rechtliches Gehör einräumt. Dieses Rahmenabkommen muss allerdings erst noch durch nationale Gesetze in den USA umgesetzt werden. Die Kommission hat außerdem angekündigt, dass sie ihre Rechtsakte zu den übrigen Angemessenheitsentscheidungen kurzfristig dahingehend ändern wird, dass die den Aufsichtsbehörden darin eingeräumten Prüfungs- und Verbots- bzw. Aussetzungsrechte von den Aufsichtsbehörden in völliger Unabhängigkeit, d. h. ohne jede Bindung an Feststellungen der Kommission, ausgeübt werden können.

Der Europäische Gerichtshof hat mit seinem Urteil vom 6. Oktober 2015 die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt. Welche Auswirkungen dieses Urteil auf den Transfer personenbezogener Daten in die USA und andere Drittstaaten künftig haben wird, lässt sich zum gegenwärtigen Zeitpunkt noch nicht vollständig vorhersagen. Alle Beteiligten arbeiten jedoch mit Hochdruck daran, praktikable Lösungen zu finden, die allen betroffenen Interessen möglichst weitgehend gerecht werden.

1.5 Internationaler Datenverkehr

Sollen personenbezogene Daten aus der Europäischen Union oder dem europäischen Wirtschaftsraum in sonstige Länder, sog. Drittstaaten, transferiert werden, sind neben den Voraussetzungen für die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung gem. § 4 des Bundesdatenschutzgesetzes (BDSG), d. h. einer Einwilligung oder einem gesetzlichen Erlaubnissatz für den Umgang mit den Daten (sog. Zulässigkeitsvoraussetzungen der ers-

ten Stufe) die besonderen Voraussetzungen für eine Übermittlung der Daten in Drittstaaten nach § 4b und § 4c des Bundesdatenschutzgesetzes (sog. Zulässigkeitsvoraussetzungen der zweiten Stufe) zu prüfen.

Gem. § 4b Absatz 2 BDSG hat die Übermittlung in einen Drittstaat zu unterbleiben, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei der importierenden Stelle im Drittstaat ein angemessenes Datenschutzniveau nicht gewährleistet ist. Die Angemessenheit des Schutzniveaus wird gem. § 4b Absatz 3 des Bundesdatenschutzgesetzes unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Landesregeln und Sicherheitsmaßnahmen herangezogen werden.

Außer für die USA – mit dem zwischenzeitlich aufgehobenen Safe-Harbor-Rechtsakt – hat die Europäische Kommission auch für eine Reihe von anderen Staaten verbindlich festgestellt, dass dort ein im Sinne des § 4b des Bundesdatenschutzgesetzes angemessenes Datenschutzniveau gegeben ist. Eine solche Feststellung hat die Kommission bislang für Andorra, Argentinien, Kanada (mit Einschränkungen), die Färöer-Inseln, Guernsey, Isle of Man, Israel, Jersey, Neuseeland, die Schweiz und Uruguay getroffen. Bei einer Übermittlung in diese Länder sind die Voraussetzungen des § 4b des Bundesdatenschutzgesetzes bis zur förmlichen Aufhebung des entsprechenden Rechtsakts der Kommission durch den Europäischen Gerichtshof daher stets gegeben.

Sofern personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden sollen und keiner der in § 4c Absatz 1 des Bundesdatenschutzgesetzes aufgeführten Ausnahmetatbestände (zum Beispiel eine Einwilligung des Betroffenen) gegeben ist, kann die Aufsichtsbehörde entsprechende Datenübermittlungen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persön-

³¹ vgl. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

lichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Diese Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen (sog. Binding Corporate Rules) ergeben. Werden die von der EU-Kommission als ausreichende Garantien anerkannten sog. Standardvertragsklauseln gewählt, ist nach der bisherigen Praxis in Baden-Württemberg weder eine Genehmigung durch noch eine Anzeige bei der Datenschutzaufsichtsbehörde erforderlich. Derzeit gibt es drei solcher Standardvertragsklauseln:

- Standardvertragsklauseln für die Datenübermittlung (2001/497/EG),
- Alternative Standardvertragsklauseln für die Datenübermittlung (2004/915/EG),
- Standardvertragsklauseln für Auftragsdatenverarbeitung (2010/87/EU).

Der Text der diesbezüglichen Kommissionsentscheidungen und der dazu gehörigen Standardvertragsklauseln kann in der EU-Rechtsdatenbank <http://eur-lex.europa.eu> unter Angabe des Jahres und der Dokumentennummer abgerufen werden.

Anträge auf die Genehmigung eines Transfers personenbezogener Daten in Drittstaaten auf der Grundlage individueller Vertragsklauseln (sog. Ad-hoc-Verträge) sind im Berichtszeitraum bei meiner Dienststelle nicht eingegangen.

Es ist damit zu rechnen, dass aufgrund der Safe-Harbor-Entscheidung des EuGH vom 6. Oktober 2015 und vor allem im Zuge der Umsetzung der EU-Datenschutz-Grundverordnung das bisherige System des Datentransfers in Drittstaaten erheblichen Veränderungen unterworfen sein wird.

1.6 Aus der Dienststelle

„Datenschutz auf Schwäbisch“ – so war der Artikel einer renommierten Fachjournalistin überschrieben, der in der „Stuttgarter Zeitung“ am 24. September 2015 erschien. Darin legte die Autorin – offenbar in Anlehnung an das oft bemühte Bild der sparsamen Schwaben – dar, dass die amtlichen Datenschützer in Baden-Württemberg im bundesweiten Vergleich am schlechtesten ausgestattet seien; so stünden meiner Dienststelle pro Kopf der Bevölkerung nur

19 Cent zur Verfügung, während andere Länder über den mehrfachen Betrag verfügten. Insbesondere mit Blick auf die inzwischen verabschiedete Europäische Datenschutzreform (siehe hierzu Kapitel 1.2 und 1.3) seien die notwendigen Kontrollen bei Unternehmen und Behörden künftig kaum zu leisten. Bereits heute sei das „Risiko“, von einer Kontrolle überzogen zu werden, kaum geringer als die Chance eines Lottogewinns; ein IT-Unternehmen im Land könne es rechnerisch demnach nur alle 1.500 Jahre treffen.

Eigentlich halte ich von derartigen Statistiken und Vergleichen nicht viel. Wie so oft muss man sich die verglichenen Zahlen sehr genau anschauen, um sie wirklich vergleichen zu können. **Strukturelle Unterschiede** können das Bild leicht verzerren: Wenn etwa der Gebäudeunterhaltungsaufwand bzw. die Miete oder die Pensionsrückstellungen – anders als in Baden-Württemberg – dezentral budgetiert werden, ergeben sich bei den Haushaltsansätzen anderer Dienststellen zwangsläufig höhere Zahlen. Aus dem Haushalt kann man auch nur bedingt ablesen, ob beispielsweise wesentliche Querschnittsaufgaben im Bereich der Organisation, des Personalwesens, des Gebäudemanagements, des Fuhrparks oder der Beschaffung – um nur einige Beispiele zu nennen – von anderen Dienststellen miterledigt oder entsprechende Dienstleistungen von Dritten, womöglich ohne gesonderte Vergütung, erbracht werden. Bei kleineren Ländern schlägt die „Grundlast“ des Behördenbetriebs zudem stärker zu Buche als bei größeren Dienststellen und ist deswegen relativ „teuer“, ohne dass diese deswegen mehr Aufwand für Beratung und Kontrolle treiben können. Und so ärgerlich für uns bzw. erfreulich für ein Unternehmen das geringe Risiko sein mag, von einer Kontrolle überzogen zu werden, so würde andererseits auch eine (unrealistische) Verzehnfachung des Personals den zeitlichen Abstand zwischen etwaigen Kontrollen von IT-Unternehmen „nur“ auf 150 Jahre verringern, was immer noch zu selten wäre. Deswegen ist ja auch die Funktion der betrieblichen Datenschutzbeauftragten so wichtig, die über den Datenschutz in ihren Unternehmen zu wachen haben. Und deswegen haben wir auch die automatisierten Kontrollen der Webauftritte von Unternehmen (siehe Kapitel 11.4 und 11.5) und Kontrollen per Fragebogen (siehe Kapitel 10.11) verstärkt. Dennoch stimmt der Blick auf einige andere

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

Länder, die nach Bevölkerung und Fläche kleiner als Baden-Württemberg sind, nachdenklich und verdeutlicht, dass ausstattungsmäßig auch für meine Dienststelle noch „Luft nach oben“ besteht. Immerhin erhielt meine Dienststelle zur Verstärkung ihrer Kontrolltätigkeit im **Staatshaushaltsplan für 2015/2016** drei Neustellen, so dass der Personalbestand der Dienststelle im Berichtszeitraum von 29,5 Stellen auf 32,5 Stellen anwuchs. Ein weiterer personeller Zuwachs war für die Dienststelle – allerdings nicht für Aufgaben des Datenschutzes – mit dem (Artikel-)Gesetz zur Einführung der **Informationsfreiheit** verbunden, das am 30. Dezember 2015 in Kraft trat (GBl. S. 1201). Dessen Artikel 1 beinhaltet das „Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg“ (Landesinformationsfreiheitsgesetz – LIFG); § 12 LIFG bestimmt, dass die Aufgabe des oder der Landesbeauftragten für die Informationsfreiheit von dem oder der Landesbeauftragten für den Datenschutz wahrgenommen wird. Dementsprechend wurden meiner Dienststelle im Zweiten Nachtrag für den Staatshaushaltsplan 2015/2016, der im Dezember 2015 verabschiedet wurde, zwei Neustellen für die neue Aufgabe zugewiesen, so dass die Dienststelle nunmehr über insgesamt **34,5 Stellen** verfügt.

Leider hat der Landesgesetzgeber die Gelegenheit einer weiteren sinnvollen Aufgabenergänzung (und Personalaufstockung) für meine Dienststelle in Form einer Übertragung der **Zuständigkeit für die Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten**, die bei der Novellierung des Landesdatenschutzgesetzes (LDSG) im Jahr 2011 – sowohl im öffentlichen wie auch im nicht-öffentlichen Bereich – beim Regierungspräsidium Karlsruhe gebündelt worden war, verpasst. Nach dem Koalitionsvertrag für die 15. Legislaturperiode hätte dieses Vorhaben eigentlich längst erledigt sein sollen, denn dort war im Kapitel „Unabhängigen Datenschutz stärken“ (Seite 67) zu lesen, dass meine Dienststelle „den Status einer obersten Landesbehörde mit eigenen Sanktionsbefugnissen für die Verfolgung und Ahndung von Ordnungswidrigkeiten“ erhalten soll. Es hätte auch Sinn gemacht, die „Durchschlagkraft“ meiner Dienststelle in dieser Hinsicht frühzeitig zu erhöhen, weil mit Inkrafttreten der EU-Datenschutz-Grundverordnung (EU-DSGVO) ab 2018 die Aufsichtsbehörden umfassende Sanktionsbefugnisse erhalten werden und

es gut gewesen wäre, sich rechtzeitig darauf vorzubereiten zu können. Im September 2015 unternahm ich im Rahmen der Verbandsanhörung zum Entwurf des Gesetzes zur Einführung der Informationsfreiheit (vgl. LT-Drs. 15/7720) noch einen letzten Anlauf und schlug konkrete Formulierungen für eine entsprechende Zuständigkeitsübertragung vor. Da es sich um ein Artikelgesetz handelte, hätte der Entwurf gesetzestechnisch ohne weiteres ergänzt werden können; zudem hätte die Zuständigkeitsübertragung kostenneutral für den Landeshaushalt erfolgen können, indem die beim Regierungspräsidium Karlsruhe bisher eingesetzten Personalkapazitäten einfach zu meiner Dienststelle umgesetzt worden wären. Als mich Anfang November 2015 der Entwurf in der Fassung für die Landtagsberatungen erreichte, las ich dort zu meinem Erstaunen nicht nur, dass mein Vorschlag eine ganz andere Regelungsmaterie betreffe, sondern auch, dass verfassungsrechtliche Bedenken dagegen sprächen, einer völlig unabhängigen Stelle – wie es der Landesbeauftragte für den Datenschutz nun einmal ist – die Zuständigkeit für Bußgeldverfahren zu übertragen. In allen anderen Bundesländern und auf Bundesebene hat man derart schwerwiegende Bedenken offenbar nicht gehabt, denn dort ist die bzw. der jeweilige Landesbeauftragte – zumindest im nicht-öffentlichen, teilweise auch im öffentlichen Bereich – schon seit Jahren auch für die Verfolgung und Ahndung datenschutzrechtlicher Ordnungswidrigkeiten zuständig. Erstaunlich war aus meiner Sicht vor allem, dass die Landesregierung in dem von ihr selbst vorgelegten Gesetzentwurf ein Vorhaben aus der eigenen Koalitionsvereinbarung mit dem Odium der Verfassungswidrigkeit versah. Für eine Ablehnung hätte m. E. der Hinweis völlig gereicht, dass man das ohnehin schon überfällige LIFG im Hinblick auf das nahende Ende der Legislaturperiode nicht noch weiter verzögern wolle. So kann man sich selbst das Leben unnötig schwer machen, wenn man das Vorhaben später wieder aufgreifen will.

Unabhängig von der sinnvollen Übertragung der Bußgeldzuständigkeit, die alsbald vorgenommen werden sollte, halte ich eine personelle Kapazitätserhöhung auch wegen anderer Auswirkungen der 2018 in Kraft tretenden **Europäischen Datenschutz-Grundverordnung (EU-DSGVO)** für unausweichlich, und dies nicht erst im Frühjahr 2018,

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

sondern spätestens ab dem Haushaltsjahr 2017. Denn die baden-württembergischen Unternehmen werden ihren Beratungsbedarf bereits im Vorfeld geltend machen, weil sie sich auf neue Anforderungen wie etwa Folgenabschätzungen neuer IT-Verfahren einstellen und die Aufsichtsbehörden hierbei einbinden wollen. Die starke exportorientierte Wirtschaft und insbesondere die vielen leistungsfähigen mittelständischen Unternehmen des Landes sind auf eine kompetente Begleitung auf dem Weg in die neue europäische Datenschutzwelt angewiesen. Unabdingbar und aufwendig wird auch eine stärkere Kooperation der Datenschutzbehörden untereinander, auf nationaler wie auf internationaler Ebene, sein. Immerhin hat sich die Datenschutzkonferenz inzwischen etwas umbenannt und heißt nun „Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder“. Sie hat sich am 1. Oktober 2015 auch eine (vorläufige) **Geschäftsordnung** gegeben, die die internen Abläufe und Entscheidungsprozesse ihrer Gremien regelt und mit dem Anwendungsbeginn der EU-DSGVO wieder außer Kraft treten soll. Bis dahin sind sinnvolle Formen der Zusammenarbeit und der Entscheidungsfindung im Hinblick auf die Mitwirkung der deutschen Datenschutzbehörden im Europäischen Datenschutzausschuss zu finden. Die EU-DSGVO verpflichtet in Artikel 46 Absatz 2 die Mitgliedsstaaten, intern festzulegen, wer die Vertretung dort übernimmt und wie die übrigen Behörden die Regeln des Abstimmungsverfahrens (Kohärenzverfahren) nach Artikel 57 einhalten. Der interne Kooperationsmechanismus wird indessen für den öffentlichen Bereich nicht anwendbar sein, so dass hier weiterhin die Aufsichtsbehörde am Sitz der Behörde zuständig bleibt. Eine inländische Kooperation ist umso mehr jedoch im nicht-öffentlichen Bereich erforderlich, insbesondere muss gewährleistet sein, dass der deutsche Vertreter im Europäischen Datenschutzausschuss die Interessen der national zuständigen Aufsichtsbehörde vertritt bzw. diese dort selbst mit Stimmrecht auftreten kann.

Wegen der Herausforderungen durch die Europäische Datenschutzreform wird eine **stärkere internationale Ausrichtung** unserer Aktivitäten unausweichlich sein. Insbesondere sind die Mitarbeiterinnen und Mitarbeiter für den Umgang mit fremdsprachigen Texten und Gesprächspartnern – vor allem in englischer Sprache – fit zu machen. Bereits

heute treffen viele wichtige Dokumente der EU zunächst in Englisch ein und erst Wochen später in Deutsch. Ich habe deshalb einen entsprechenden Sprachkurs organisiert, der – zunächst – freiwillig angeboten wird und im Januar 2016 beginnt.

Die **Qualifikation der Mitarbeiter** und deren berufliches Fortkommen ist mir weiterhin ein besonderes Anliegen. Ihre in § 26 Absatz 4 Satz 4 LDSG „gewährleistete“ Einbeziehung in den allgemeinen Personalaustausch der Landesverwaltung hat sich auch im Berichtszeitraum eher als Programmsatz erwiesen³²; auch aus der seinerzeit angedachten Vereinbarung ist noch nichts geworden. Dabei ist im Hinblick auf die Stellenausstattung meiner Dienststelle weniger die Gewinnung von qualifiziertem Nachwuchs, d. h. von Berufsanfängern, als vielmehr die Gewinnung erfahrener Verwaltungsjuristen ein Problem, weil diese nicht abschätzen können, ob eine Verwendung in meiner Dienststelle für ihre weitere Karriere förderlich ist, und ihre bisherige Dienststelle in der Regel nicht geneigt ist, sie lediglich abzuordnen oder ihnen eine verbindliche Rückkehrzusage zu geben. So habe ich mir wiederholt Absagen qualifizierter Bewerber eingehandelt, weil sie Sorge hatten, beruflich in eine Sackgasse zu geraten; ich kann das gut nachvollziehen, aber auch nicht ändern. Umgekehrt habe ich wegen der kleinen Dienststelle Probleme, meine Mitarbeiter abzuordnen, weil ich auf deren Planstellen dann nur Angestellte befristet einstellen kann. Immerhin kann ich demnächst eine qualifizierte Mitarbeiterin in das Staatsministerium abordnen, nicht zuletzt, weil das Innenministerium bereit war, eine erfahrene Kollegin, die aus der Elternzeit zurückkehrt, zu meiner Dienststelle abzuordnen. Für diese kollegiale Unterstützung bedanke ich mich sehr; möge das Beispiel Schule machen. Dies gilt auch für die im Berichtszeitraum fortgesetzte Abordnung von zwei Mitarbeitern aus dem Polizeibereich bzw. aus dem Lehrerbereich, die in meiner Dienststelle kompetente Arbeit leisten und dank ihrer guten Vernetzung die Zusammenarbeit mit diesen großen Aufgabenbereichen der Landesverwaltung auch für uns erleichtern.

³² siehe hierzu bereits 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Kapitel 1.5, S. 38

32. Tätigkeitsbericht 2014/2015 - 1. Zur Situation

Was die Entwicklung der **Eingaben, Kontrollen und Beratungen** angeht, so haben sich die Zahlen nach einem Höhepunkt im Jahr 2014 auf hohem Niveau stabilisiert: Im Jahr 2014 gingen 1.110 Eingaben im öffentlichen und 1.710 Eingaben im nicht-öffentlichen Bereich ein. Im Jahr 2015 waren es in beiden Bereichen rund 10 % weniger, wobei die statistische Auswertung zum Redaktionsschluss teilweise noch andauerte. Die Kontrollen stiegen 2014 gegenüber dem Vorjahr im nicht-öffentlichen Bereich gegenüber dem Vorjahr signifikant an, was vor allem auf die in Kapitel 10.11. dargestellte Kontrollaktion bei Adresshändlern bzw. Markt- und Meinungsforschungsinstituten zurückzuführen war (von 11 auf 49). Im Jahr 2015 wurde etwa wieder das Niveau von 2013 erreicht. Im öffentlichen Bereich stiegen die Kontrollen von 10 im Jahr 2014 dagegen auf 17 im Jahr 2015 an. Die Zahl der Beratungen stieg 2014 gegenüber dem Vorjahr im öffentlichen Bereich um ca. 10 % an (auf 1.063), während sie im nicht-öffentlichen Bereich um ca. 5 % abnahm (auf 1.002). Im Jahr 2015 ergaben sich dagegen in beiden Bereichen Rückgänge (auf 788 bzw. 812), was aber auch auf Fehler bei der Erhebung im Zusammenhang mit einigen Personalwechseln zurückzuführen sein kann. Die reinen Fallzahlen berücksichtigen zudem nur unzureichend die unterschiedlichen Schwierigkeitsgrade der einzelnen Vorgänge. Zum Beispiel ist eine Beschwerde über eine Werbe-E-Mail in der Regel mit weniger Bearbeitungsaufwand verbunden als die Beschwerde über eine Videoüberwachungsanlage, die u. U. eine Ortsbesichtigung in einer weiter entfernten Stadt nach sich zieht. Und gerade in diesem Bereich ist die Anzahl der Beschwerden in den letzten Jahren erheblich angestiegen und hat sich von 2013 bis 2015 praktisch verdoppelt.

In diesem Zusammenhang sind auch die seit einigen Jahren verstärkt durchgeführten automatisierten **Kontrollen von Apps oder Webauftritten** von Unternehmen in Baden-Württemberg zu erwähnen, die in Kapitel 11.4 und 11.5 dieses Berichts dargestellt werden. Dabei wurden im Rahmen des OPEN Privacy Sweep 2014 rund zwei Dutzend Smartphone-Apps näher unter die Lupe genommen und im Hinblick auf datenschutzrechtliche Mängel überprüft. Bei der Kontrolle des Heartbleed Bugs 2014

wurden 11.000 Webauftritte hiesiger Unternehmen mit einer selbst entwickelten Prüfplattform untersucht. Auch diese neuartigen Kontrollen binden erhebliche personelle Kapazitäten und – wie sich dann herausgestellt hat – bleiben auch auf der Sachkostenseite nicht ohne Konsequenzen, denn förmliche Abmahnschreiben oder datenschutzrechtliche Verfügungen an tausende von Unternehmen können nicht ohne weiteres aus der sprichwörtlichen Portokasse gezahlt werden.

Dennoch bleibt die Verwirklichung einer einfach zu erstellenden und dennoch aussagekräftigen Statistik, am besten im Rahmen der technischen Erfassung der Posteingänge, ein wichtiger Merkposten für die Organisation meiner Dienststelle, auch im Interesse einer gerechten Verteilung der Arbeitsbelastung zwischen den Beschäftigten.

Die Bemühungen, den Dienstbetrieb weiter zu rationalisieren, waren im Berichtszeitraum unterschiedlich erfolgreich: Das Vorhaben, den IT-Betrieb der Dienststelle dem zentralen IT-Dienstleister der Landesverwaltung (BIT BW) zu übertragen, wurde nach einem Kostenvergleich wieder aufgegeben; außerdem war ein Know-How-Verlust für die eigene Kontrolltätigkeit nicht ganz auszuschließen. Dagegen wurde das Dienstreisemanagement der Dienststelle – ähnlich wie bereits bei den meisten anderen Landesbehörden – zum 1. Januar 2016 auf das Verfahren DRIVE BW des Landesamts für Besoldung und Versorgung umgestellt.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

2. Innere Sicherheit**2.1 Rechtsprechung****2.1.1 Wer filmt, darf gefilmt werden – gleiches Recht für alle?**

Unter Talion oder Talionsprinzip versteht man eine Rechtsfigur, nach der zwischen dem Schaden, der einem Opfer zugefügt wurde, und dem Schaden, der dem Täter zugefügt werden soll, ein Gleichgewicht angestrebt wird. Es wird angenommen, dass die Talion sich aus der mit nomadischem Sippenrecht verbundenen Blutrache entwickelt habe (Quelle: Wikipedia). Ganz so archaisch geht es heutzutage glücklicherweise nicht mehr zu. Jedoch klingt der Gedanke des „Wie du mir, so ich dir“ auch in dem Beschluss des Bundesverfassungsgerichts vom 24. Juli 2015 (1 BvR 2501/13, juris) an. Zugrunde lag eine Situation, wie sie bei Demonstrationen immer häufiger vorkommt: die Polizei verschafft sich unter Einsatz von Videotechnik Überblick über eine Versammlung, während Versammlungsteilnehmer ihrerseits mittels Smartphones Polizeibeamte im Einsatz fotografieren oder filmen. Nicht selten werden die Bilder oder Videos anschließend veröffentlicht. Dass dies bei den betroffenen Beamten auf wenig Gegenliebe stößt, ist nachvollziehbar.

Im Rahmen einer Versammlung, die von der Polizei per Video beobachtet wurde, erweckte eine Versammlungsteilnehmerin den Anschein, als fotografiere sie die Einsatzbeamten. Einer dieser Beamten führte daraufhin bei dem Begleiter der Versammlungsteilnehmerin eine Identitätskontrolle durch, indem er sich den Personalausweis aushändigen ließ. Nach Auffassung des Bundesverfassungsgerichts war er hierzu allerdings nicht berechtigt gewesen.

Die dem Beschluss des Bundesverfassungsgerichts zugrundeliegende Bestimmung des niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung findet ihre Entsprechung in § 26 des baden-württembergischen Polizeigesetzes (PolG):

§ 26

Personenfeststellung

(1) Die Polizei kann die Identität einer Person feststellen,

1. um im einzelnen Falle eine Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren oder eine Störung der öffentlichen Sicherheit oder Ordnung zu beseitigen, [...].

(2) Die Polizei kann zur Feststellung der Identität die erforderlichen Maßnahmen treffen. Sie kann den Betroffenen insbesondere anhalten und verlangen, dass er mitgeführte Ausweispapiere vorzeigt und zur Prüfung aushändigt. [...].

Das Bundesverfassungsgericht weist zu Recht darauf hin, dass die Feststellung der Identität einer Person durch Befragen und die Aufforderung, dass sie mitgeführte Ausweispapiere zur Prüfung aushändigt, einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Eine allgemeine Verpflichtung, sich ohne Grund auf amtliche Aufforderung auszuweisen oder sonstige Angaben zu Personalien zu machen, gibt es nicht. Auch wenn mit § 26 PolG eine bereichsspezifische gesetzliche Grundlage für solche Eingriffe besteht, muss jeweils im konkreten Einzelfall die Bedeutung und Tragweite des Rechts auf informationelle Selbstbestimmung hinreichend berücksichtigt werden. Für die Rechtsanwendung bedeutet dies, dass das anzuwendende Gesetz stets so auszulegen ist, dass abschreckende Effekte im Hinblick auf den Gebrauch des Grundrechts möglichst gering gehalten werden.

„Hiergegen verstieße es, wenn das Anfertigen von Lichtbildern oder Videoaufnahmen eines Polizeieinsatzes unter Verweis auf die bloße Möglichkeit einer nachfolgenden strafbaren Verletzung des Rechts am eigenen Bild (nach § 22 Satz 1, § 33 Abs. 1 KunstUrhG) genügen sollten, um polizeiliche Maßnahmen wie eine Identitätsfeststellung gem. [§ 26 Absatz 1 Nummer 1 PolG] durchzuführen. Wer präventivpolizeiliche Maßnahmen bereits dann gewärtigen muss, wenn sich nicht ausschließen lässt, dass sein Verhalten Anlass zu polizeilichem Einschreiten bietet, wird aus Furcht vor polizeilichen Maßnahmen auch zulässige Aufnahmen (zur grundsätzlichen Zulässigkeit des Filmens und Fotografierens polizeilicher Einsätze vgl. BVerwGE 109, 203 <210 f.>)

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

und mit diesen nicht selten einhergehende Kritik an staatlichem Handeln unterlassen. Beabsichtigt die Polizei, wegen Lichtbildern und Videoaufnahmen präventivpolizeilich – sei es durch ein Film- oder Fotografierverbot (vgl. BVerwGE 143, 74 <77 ff.>), sei es wie hier durch eine Identitätsfeststellung – einzuschreiten, ergibt sich aus den durch die Maßnahme jeweils betroffenen Grundrechten – hier Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG – die Anforderung einer konkreten Gefahr für ein polizeiliches Schutzgut. Dies ist eine Frage der tatsächlichen Umstände im Einzelfall. Dementsprechend geht die verwaltungsrechtliche Rechtsprechung grundsätzlich in verfassungskonformer Auslegung der §§ 22, 23 KunstUrhG davon aus, dass unzulässige Lichtbilder nicht auch stets verbreitet werden (vgl. BVerwGE 109, 203 <211>). Gehen die Sicherheitsbehörden demgegenüber davon aus, dass im Einzelfall die konkrete Gefahr besteht, eine solche unzulässige Verbreitung sei ebenfalls zu befürchten, bedarf es hierfür hinreichend tragfähiger Anhaltspunkte. Dem genügen die vom Beschwerdeführer mit der Verfassungsbeschwerde angegriffenen Entscheidungen mit Blick auf die streitgegenständliche Identitätsfeststellung nicht“ (BVerfG, a.a.O.).

Das Argument, man habe schon deshalb von einer Veröffentlichung der Aufnahmen im Internet abgesehen dürfen, weil ein anderer Grund, die Aufnahmen anzufertigen, nicht ersichtlich gewesen sei, ließ das Gericht im vorliegenden Fall nicht gelten. Es werde dabei verkannt, dass der Anlass für die Aufnahmen hier ausdrücklich darin gelegen habe, dass die Polizei selbst Bild- und Tonaufnahmen der Teilnehmer einer öffentlichen Versammlung angefertigt habe. Wenn es sich bei der Anfertigung der Aufnahmen lediglich um eine bloße Reaktion auf die seitens der Polizei gefertigten Bild- und Tonaufzeichnungen – etwa zur Beweissicherung mit Blick auf etwaige Rechtsstreitigkeiten – handle, könne dies allein nicht Grundlage für polizeiliche Maßnahmen sein.

Es gibt keine allgemeine Verpflichtung, sich ohne Grund auf amtliche Aufforderung auszuweisen oder sonstige Angaben zu Personalien zu machen. Die polizeiliche Identitätsfeststellung greift in das Recht auf informationelle Selbstbestimmung ein und bedarf einer verfassungsrechtlichen Rechtfertigung im Einzelfall. Beabsichtigt die Polizei, wegen der Anfertigung von Lichtbildern oder Videoaufnahmen Maß-

nahmen zur Identitätsfeststellung zu ergreifen, muss mit Rücksicht auf die jeweils betroffenen Grundrechte ein polizeiliches Schutzgut konkret gefährdet sein; hierzu bedarf es hinreichender tragfähiger Anhaltspunkte.

2.1.2 Automatische Kennzeichenlesesysteme der Polizei

Mit automatischen Kennzeichenlesesystemen soll die Polizei in die Lage versetzt werden, verdachtslos die amtlichen Kennzeichen aller an dem Gerät vorbeifahrenden Fahrzeuge zu erfassen und sie mit einem Fahndungsbestand abzugleichen, um Hinweise zur Auffindung von Personen oder Sachen zu erlangen. In Baden-Württemberg findet sich seit November 2008 eine die Zulässigkeit solcher Systeme regelnde Bestimmung in § 22a PolG. Von dieser Regelung wurde nach Angabe des Innenministeriums aber noch kein Gebrauch gemacht. Grund hierfür sind die mit dieser Vorschrift verbundenen verfassungsrechtlichen Probleme.

Die Regelung der automatischen Kennzeichenlesesysteme hat meine Dienststelle seit Jahren immer wieder beschäftigt und war daher auch schon wiederholt Gegenstand der Tätigkeitsberichte, zuletzt im 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, S. 44 f. Auch in dieser Berichtsperiode hatte ich mich wieder mit ihr zu befassen.

Denn vor dem Bundesverfassungsgericht, das bereits mit Urteil vom 11. März 2008 (BVerfGE 120, 378-433) die damaligen Regelungen in Hessen und Schleswig-Holstein für verfassungswidrig erklärt hatte, sind nach wie vor noch mehrere Verfassungsbeschwerden anhängig, die die Regelungen verschiedener Bundesländer, darunter auch die baden-württembergische, betreffen (1 BvR 2795/09 u. a.). Das Bundesverfassungsgericht hat den Datenschutzbeauftragten des Bundes und der Länder Gelegenheit zu einer Stellungnahme gegeben, die ich Anfang des Jahres 2015 wahrnahm.

Meiner Stellungnahme zeitlich unmittelbar vorangegangen war das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2014 (6 C 7.13, NVwZ 2015, S. 906-908) zur bayerischen Regelung des Einsatzes automatischer Kennzeichenlesesysteme in Artikel 33 Absatz 2 Satz 2 bis 5 des bayerischen Polizeiaufgabengesetzes. Dem Urteil lag die Klage ei-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

nes Kraftfahrzeugführers zugrunde, der im Wege der vorbeugenden Unterlassungsklage verhindern wollte, dass das Kennzeichen seines Fahrzeuges von den in Bayern seit 2006 verwendeten automatischen Kennzeichenlesesystemen der Polizei erfasst und mit Fahndungsbeständen abgeglichen wird. Dabei konnte der Kläger nicht geltend machen, dass sein Kennzeichen in einem der abzugleichenden Fahndungsbestände enthalten sei. Das Verwaltungsgericht München hatte die Klage bereits 2009 abgewiesen, der Bayerische Verwaltungsgerichtshof die hiergegen gerichtete Berufung des Klägers mit Urteil vom 17. Dezember 2012 (10 BV 09.2641, DuD 2013, S. 465–470) zurückgewiesen. Der Verwaltungsgerichtshof hatte hierzu drei mögliche Fallkonstellationen unterschieden, nämlich den Nichttreffer-Fall, in dem der Abgleich des erkannten Kfz-Kennzeichens mit dem Fahndungsbestand keine Übereinstimmung ergibt, den unechten Treffer-Fall, in dem der maschinelle Abgleich zu Unrecht eine Übereinstimmung mit dem Fahndungsbestand ergibt, weil das Kennzeichen des passierenden Fahrzeuges durch das Lesegerät falsch erkannt wurde, und den echten Treffer-Fall, in dem zu Recht eine Übereinstimmung mit dem Fahndungsbestand angezeigt wird. Der Verwaltungsgerichtshof hatte entschieden, dass im Nichttreffer-Fall vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichts vom 11. März 2008 kein Eingriff in das informationelle Selbstbestimmungsrecht des Klägers vorliege, weil das Kennzeichen zwar kurzfristig erfasst und abgeglichen, anschließend aber unverzüglich anonym und spurlos wieder gelöscht werde. Bei einem unechten Treffer liege aber jedenfalls deswegen ein Eingriff vor, weil das Kennzeichen für den sachbearbeitenden Polizeibeamten, also für eine Person, einsehbar sei. Denn ausschlaggebend für den Grundrechtseingriff sei, dass durch das Aufscheinen des Kennzeichens und dessen Kenntnisnahme durch eine Person die Möglichkeit der Herstellung eines Personenbezugs entstehe. Die Eingriffswahrscheinlichkeit sei auch hinreichend, weil derartige unechte Treffer-Fälle nach Angaben der bayerischen Polizei bei acht Millionen Scanvorgängen im Monat in ca. 40–50.000 Fällen bei nur ca. 500–600 echten Treffern vorkämen. Der Eingriff beruhe aber auf einer verfassungsgemäßen gesetzlichen Grundlage. Soweit unbestreitbar ein Eingriff im echten Trefferfall vorliege, habe der Kläger kein Rechtsschutzbedürfnis, da sein Kfz-Kennzeichen nicht in einer der Fahndungslisten enthalten sei, die

vorbeugende Unterlassungsklage aber eine konkrete Eintrittswahrscheinlichkeit des Eingriffs voraussetze.

Das Bundesverwaltungsgericht wies auch die Revision des Klägers gegen dieses Urteil mit – vom unechten Treffer-Fall abgesehen – ähnlichen Erwägungen zurück. Abweichend von der Vorinstanz sah es aber selbst im unechten Treffer-Fall keinen Eingriff, so dass es auf die Verfassungsmäßigkeit der Rechtsgrundlage gar nicht mehr eingehen musste. Zwar werde das erfasste Kennzeichen in dieser Konstellation durch den Polizeibeamten, der mit dem visuellen Abgleich betraut ist, zur Kenntnis genommen. Das allein stelle aber noch keinen Eingriff dar. Denn das behördliche Interesse an dem Datum sei in diesem Stadium nur ein systembezogenes Korrekturinteresse. Der Inhaber des tatsächlich erfassten Kennzeichens habe insoweit nicht mehr hinzunehmen als eine lediglich kurzzeitige Wahrnehmung der Buchstaben-Zahlen-Kombination des Kennzeichens durch den Polizeibeamten, der seinerseits nicht über die rechtliche Befugnis verfüge – und auch der Sache nach keinen Anlass hätte –, eine Abfrage aus dem Fahrzeugregister vorzunehmen. Die Anonymität des Inhabers bleibe folglich gewahrt. Dies entspreche auch der Ansicht des Bundesverfassungsgerichts, das auch in der Entscheidung vom 11. März 2008 den unechten Trefferfall keiner gesonderten Würdigung unterzogen habe.

In meiner Stellungnahme bin ich der Ansicht des Bundesverwaltungsgerichts nicht gefolgt (wobei sich allerdings auch die prozessuale Lage bei der Verfassungsbeschwerde teilweise anders darstellt). Vielmehr kann aus meiner Sicht schon dem Nichttreffer-Fall eine Eingriffsqualität zukommen. Die zugegebenermaßen inzwischen durch mehrere Entscheidungen gefestigte Rechtsprechung des Bundesverfassungsgerichts, auch bei einer letztlich auf einen Eingriff zumindest in die allgemeine Handlungsfreiheit gerichteten Datenverarbeitung wie den polizeilichen oder strafprozessualen Ermittlungen eine Betroffenheit im Recht auf informationelle Selbstbestimmung dann zu verneinen, wenn das kurzfristig erfasste personenbezogene Datum nach dem unverzüglichen maschinellen Abgleich sofort spurlos wieder gelöscht werde, halte ich schon wegen der schwierigen Abgrenzbarkeit der Begriffes der Kurzfristigkeit und der Spurenlosigkeit für über-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

prüfungsbedürftig. Bedenken habe ich auch unter dem Gesichtspunkt, dass eine der Erfassung nachfolgende Löschung die Erfassung nicht ungeschehen macht, was insbesondere dann deutlich wird, wenn es aufgrund eines Hard- oder Software-Fehlers nach der Erfassung oder auch aufgrund einer Manipulation faktisch bei der Speicherung verbleibt. Auch verschließt sich das Bundesverfassungsgericht durch die Verneinung der Eingriffsqualität die Prüfung der Erforderlichkeit der zwischenzeitlich vorgenommenen Datenverarbeitung. Unabhängig von der Frage des Festhaltens an dieser Rechtsprechung ergibt sich aber die Eingriffsqualität auch im Nichttreffer-Fall, wenn der Abgleich nicht mit bereits vorab auf lokalen Speichermedien abgelegten Fahndungsdateien, sondern unmittelbar online mit dem aktuellen Fahndungsbestand des Bundeskriminalamts erfolgen soll. Diese Lösung wurde im Rahmen der Gesetzesbegründung zur baden-württembergischen Regelung sogar als der Normalfall der vorgesehenen Praxis dargestellt (LT-Drs. 14/3165, S. 46 und 52); das Bundesverwaltungsgericht musste sich in seiner Entscheidung aufgrund der Feststellungen der Vorinstanzen hingegen nicht mit dieser Variante befassen, weil nach diesen in Bayern nur abgegrenzte lokale (Offline-)Systeme zur Anwendung kommen. Bei einer Online-Abfrage aber wird eine Reihe von Datenverarbeitungen vorgenommen: Zunächst wird ein Bild des Kennzeichens aufgenommen (Datenerhebung), aus dem Bild die Buchstaben- und Ziffernfolge ausgelesen (Datennutzung) und das Bild sowie der gewonnene Text gespeichert (Speicherung). Danach erfolgt eine Übermittlung des aus dem aufgezeichneten Bild herausgelesenen Kennzeichens an das Bundeskriminalamt. Dort wird das Kennzeichen mit den Datenbeständen abgeglichen (Datennutzung; zu allem s. Belz/Mußmann/Kahlert/Sander, Polizeigesetz für Baden-Württemberg, 8. Auflage 2015, § 22a PolG Rn. 2). Außerdem erfolgt dort für jede einzelne Abfrage eine Protokollierung nach § 11 Absatz 6 des Bundeskriminalamtgesetzes, die für zwölf Monate vorwiegend zum Zwecke der Datenschutzkontrolle, der Datensicherheit und der Aufrechterhaltung des ordnungsgemäßen Betriebs gespeichert bleibt, gegebenenfalls aber auch zur Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person verwendet werden kann. Dem steht das Protokollierungsverbot aus § 22a Absatz 3 Satz 2 PolG nicht entgegen, das sich – schon wegen des Vorranges des Bundes-

rechts gem. Art. 31, 70 ff. des Grundgesetzes – nur auf die Protokollierung bei der Landespolizei erstrecken kann.

Auch im unechten Trefferfall kann nach meiner Einschätzung die Eingriffsqualität entgegen der Ansicht des Bundesverwaltungsgerichts nicht in Frage gestellt werden. Denn in diesem Fall wird das Kennzeichen des Halters sowie Zeit, Ort und Richtung der Fahrt durch einen Polizeibeamten zielgerichtet zur Kenntnis genommen und mit der – tatsächlich unzutreffenden – Information i. V. gebracht, dass es sich dabei um ein polizeilich ausgeschriebenes Fahrzeug handle. Selbst wenn sich nach einer Überprüfung der Fehler herausstellt, ist nach der Kenntnisnahme durch einen Menschen jedenfalls nicht mehr „rechtlich und technisch gesichert, dass die Daten anonym bleiben und sofort spurlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden“.

Unstreitig liegt schließlich beim echten Trefferfall ein Eingriff in das informationelle Selbstbestimmungsrecht vor. Anders als im Fall der vorbeugenden Unterlassungsklage muss der Beschwerdeführer jedenfalls bei der Verfassungsbeschwerde nach der Rechtsprechung des Bundesverfassungsgerichts auch nicht geltend machen, dass der Treffer-Fall in Bezug auf seine Person deswegen wahrscheinlich ist, weil ein ihm zugewiesenes Kfz-Kennzeichen auf einer der abzugleichenden Fahndungslisten stehe.

Vor diesem Hintergrund wird das Bundesverfassungsgericht zunächst die Frage der Gesetzgebungskompetenz des Landesgesetzgebers für die Maßnahme zu überprüfen haben. Darüber hinaus habe ich Bedenken hinsichtlich der ausreichenden Bestimmtheit der Vorschrift. Insbesondere halte ich die Bezugnahme auf „Kontrollen nach § 26 Absatz 1 PolG“ in § 22a Absatz 1 PolG für nicht hinreichend normenklar. Die Vorschrift ist aber auch insoweit nicht bestimmt genug, als sie die zulässige Dauer, Häufigkeit und räumliche Dichte des Einsatzes von Kennzeichenlesegeräten nicht hinreichend nachvollziehbar regelt. Die Formulierungen, der Einsatz dürfe „nicht flächendeckend“ (§ 22a Absatz 1 Satz 3 Nummer 1 PolG; s. hierzu auch schon BVerfG, Urteil vom 11. März 2008, Absatz-Nr. 92, 144, 146 und 174), bzw. „nicht dauerhaft“ (Nummer 2) oder „nicht längerfristig“ erfolgen, sind – ohne dass die Regelungsmaterie eine konkretere Festlegung aus-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

schließen würde – derart unbestimmt, dass sie kaum justiziabel erscheinen und ihre Anwendung nicht vorhersehbar ist. Der Gesetzgeber hat es hier versäumt, die wesentlichen Entscheidungen zur höchsten zulässigen Dichte und Dauer der Kontrollen selbst zu regeln.

Weitere Bedenken habe ich hinsichtlich der Erforderlichkeit der Eingriffsbefugnis. Grundsätzliche Bedenken gegen die Erforderlichkeit der Regelung bestehen deswegen, weil die nunmehr seit über sechs Jahren in Kraft befindliche Vorschrift in Baden-Württemberg kein einziges Mal angewandt wurde (s. zuletzt die Stellungnahme der Landesregierung vom 16. April 2014 zu meinem 31. Tätigkeitsbericht, LT-Drs. 15/5302, S. 17), ohne dass dies daran liegen würde, dass die Tatbestandsvoraussetzungen des § 22a PolG bislang nicht erfüllt gewesen wären. Auch die in aller Regel geringen Fahndungserfolge der die Technik praktizierenden Länder lassen Zweifel an der Erforderlichkeit, zumindest aber an der Verhältnismäßigkeit der Maßnahme aufkommen. Ferner beschränkt sich – die generelle Erforderlichkeit der Eingriffsermächtigung unterstellt – die Regelung in § 22a PolG auch deswegen nicht auf das zur Zweckerreichung Erforderliche, weil im Normtext nicht sichergestellt wird, dass die Datenerhebung zu den in Absatz 1 genannten Zwecken nur zur Durchführung des Datenabgleichs nach § 22a Absatz 2 PolG erfolgt; die Ermächtigung zum Datenabgleich nach § 22a Absatz 2 PolG ist vielmehr als eigenständige – nicht notwendig auf die Erhebung nach Absatz 1 folgende – Eingriffsbefugnis formuliert; eine Frist für die Durchführung des Datenabgleichs wird nicht bestimmt. Außerdem regeln die Vorschriften in Absatz 2 lediglich abstrakt-generell den Umfang der in den Abgleich mit einzubeziehenden Dateien, ohne dass auf den jeweiligen in § 22a Absatz 1 PolG genannten Zweck der Maßnahme abgestellt würde. Der Gesetzgeber hat außerdem versäumt, als verbindliche organisatorische Maßnahme festzuschreiben, dass die Kontrollkräfte bis zum Datenabgleich keine Kenntnis vom ausgelesenen Kraftfahrzeugkennzeichen nehmen dürfen (s. hierzu aber die Erfahrungen des Hessischen Datenschutzbeauftragten, die dieser in seinem 40. Tätigkeitsbericht 2011, S. 193 f., schildert). In der Regelung wird außerdem kein Vorrang der offenen Erhebung normiert, von der nur bei Gefährdung des Zwecks der Maßnahme abgesehen werden kann.

Insgesamt scheint mir schließlich unter dem Gesichtspunkt der Verhältnismäßigkeit im engeren Sinne der vom Bundesverfassungsgericht geforderte Stichprobencharakter der automatischen Kennzeichenerfassung (vgl. Urt. vom 11. März 2008, Absatz-Nr. 174) nicht hinreichend sichergestellt.

Das Bundesverfassungsgericht wird zu entscheiden haben, inwieweit die geschilderten Mängel des Gesetzestextes durch Auslegung korrigiert werden können oder die Verfassungswidrigkeit der Norm begründen.

Ein Termin zur mündlichen Verhandlung über die Verfassungsbeschwerden gegen die Regelungen zur automatisierten Kennzeichenerfassung ist noch nicht bestimmt. Bereits mit Nichtannahmebeschluss vom 4. Juni 2014 – 1 BvR 1443/08 – hat die 3. Kammer des Ersten Senats immerhin angedeutet, dass die Regelung der automatisierten Kennzeichenerfassung in § 32 Absatz 5 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung „gravierende verfassungsrechtliche Fragen aufwirft“, die diesbezügliche Verfassungsbeschwerde allerdings aus prozessualen Gründen nicht zur Entscheidung angenommen. Die Entwicklung der verfassungsrechtlichen Rechtsprechung hierzu bleibt daher weiterhin spannend.

2.1.3 Strategische Fernmeldeüberwachung

Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 8./9. Oktober 2014 in ihrer Entschließung „Effektive Kontrolle von Nachrichtendiensten herstellen!“ (vgl. Anhang 8) die Notwendigkeit einer wirksamen Kontrolle der Nachrichtendienste und Sicherheitsbehörden u. a. auch damit begründet, dass der Individualrechtsschutz für die Betroffenen in diesem Bereich faktisch eingeschränkt sei. Als Beleg dafür, wie richtig diese Forderung ist, kann das Urteil des Bundesverwaltungsgerichts vom 28. Mai 2014 (6 A 1/13, BVerwGE 149, 359–373) ins Feld geführt werden.

Die Entscheidung behandelt die Frage, ob und unter welchen Voraussetzungen eine Einzelperson verwaltungsgerichtlichen Rechtsschutz gegen die Anordnung einer strategischen Beschränkung von internationalen Telekommunikationsbeziehungen durch den Bundesnachrichtendienst erreichen kann. Rechtsgrundlage für derartige Beschränkungen ist

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – Art. 10-Gesetz (G 10). Bei der strategischen Beschränkung des Telekommunikationsverkehrs wird nicht der Telekommunikationsverkehr einer einzelnen Person, sondern es werden anlasslos bestimmte Übertragungswege überwacht. Beschränkungen sind nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um gesetzlich näher bestimmte Gefahren rechtzeitig zu erkennen und ihnen zu begegnen (§ 5 Absatz 1 Satz 3 G 10). Dabei darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Es dürfen keine Suchbegriffe verwendet werden, die anhand von Identifizierungsmerkmalen zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen, oder die den Kernbereich der privaten Lebensgestaltung betreffen. Dies gilt nicht für Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden (§ 5 Absatz 2 G 10). Wer geschäftsmäßig Telekommunikationsdienste erbringt, hat der berechtigten Stelle auf Anordnung die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen (§ 2 Absatz 1 Satz 3 G 10). Der dazu verpflichtete Betreiber des in der Anordnung bezeichneten Übertragungsweges (Telekommunikationsleitung) leitet den Datenstrom in Gestalt einer Verdoppelung dem Bundesnachrichtendienst zu. Damit stehen die Telekommunikationsverkehre dem Bundesnachrichtendienst zur Verfügung, der sie dann nach einer ersten technischen Selektion, bei der Inlandsverkehre aus den erfassten Telekommunikationsverkehren ausgeschieden werden sollen, anhand der angeordneten Suchbegriffe auf sogenannte Treffer durchsucht, die dann ihrerseits auf ihre nachrichtendienstliche Relevanz geprüft werden.

Geklagt hatte ein Rechtsanwalt mit der Begründung, er habe häufig per E-Mail mit Kollegen, Mandanten und anderen Personen im Ausland kommuniziert, vielfach in Angelegenheiten, die dem Anwaltsgeheimnis unterlegen hätten. Er müsse damit rechnen, dass diese Auslandskommunikation von strategischen Beschränkungsmaßnahmen nach § 5 G 10 betroffen gewesen sei, und insofern davon ausgehen, dass auch seine eigene, insbesondere anwalt-

liche E-Mail-Korrespondenz erfasst und auf nachrichtendienstliche Relevanz hin ausgewertet worden sei.

Das Bundesverwaltungsgericht hat die Klage als unzulässig abgewiesen. Für den konkreten Fall räumte es zwar ein, es könne nicht ausgeschlossen werden, dass auch vom Kläger versandte oder an ihn gerichtete E-Mails von der strategischen Beschränkung des Telekommunikationsverkehrs erfasst worden seien. Entscheidend sei jedoch, dass über diese bloße Möglichkeit hinaus eine Erfassung von Telekommunikationsverkehren unter Beteiligung des Klägers nicht mit an Sicherheit grenzender Wahrscheinlichkeit habe festgestellt werden können. Nachweislich hätte sich jedenfalls kein Telekommunikationsverkehr des Klägers unter denjenigen befunden, die sich im Ergebnis als nachrichtendienstlich relevant erwiesen hätten und vom Bundesnachrichtendienst insoweit weiterverarbeitet worden seien. Nicht mehr zu ermitteln gewesen sei dagegen, ob ein Telekommunikationsverkehr des Klägers zwar zunächst erfasst, anhand angeordneter Suchbegriffe selektiert, unverzüglich auf nachrichtendienstliche Relevanz überprüft und sodann aber, weil diese Prüfung negativ verlaufen sei, als irrelevant gem. § 6 Absatz 1 Satz 2 G 10 unverzüglich gelöscht worden sei. Aufklärungsbemühungen scheiterten daran, dass die Protokolldateien über die Erfassung und den Abgleich mit angeordneten Suchbegriffen als auch über die Löschung erhobener personenbezogener Daten entsprechend den gesetzlichen Vorgaben gelöscht worden waren und damit nicht mehr zur Verfügung standen.

Die danach verbleibende Wahrscheinlichkeit für eine Erfassung hat das Bundesverwaltungsgericht als nicht so hoch beurteilt, dass sie als überwiegend hätte eingestuft werden müssen und ihm damit die erforderliche Überzeugung dafür hätte vermitteln können, dass die Voraussetzungen eines konkreten Rechtsverhältnisses erfüllt seien. Ein Aspekt war dabei die gesetzliche Maßgabe, dass nur ein geringer Bruchteil aller Telekommunikationsverkehre von der strategischen Beschränkung erfasst wird. Strategische Beschränkungen gem. § 5 Absatz 1 G 10 wiesen fragmentarischen Charakter auf. Sie seien zum einen auf die Übertragungswege beschränkt, die in der Anordnung bezeichnet würden. Zum anderen werde der Telekommunikationsverkehr dadurch wirksam begrenzt, dass nur 20 % der Kapazi-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

tät aller beantragten und angeordneten Übertragungswege überwacht werden dürften. Die Beschränkung auf einen Anteil der Gesamtkapazität aller Übertragungswege zwingt mithin zur Auswahl aus den angeordneten Übertragungswegen, die jeweils gleichzeitig überwacht werden könnten.

Als Ergebnis trifft das Bundesverwaltungsgericht eine Beweislastentscheidung: Die verbleibenden erheblichen Zweifel daran, ob der Telekommunikationsverkehr des Klägers von der strategischen Beschränkung nach § 5 G 10 erfasst und damit das streitige Rechtsverhältnis begründet worden sei, gingen zulasten des Klägers. Dies entspreche der allgemeinen Regel, nach der es zulasten des Beteiligten gehe, der sich auf eine Norm berufe, wenn die tatsächlichen Voraussetzungen dieser Norm nicht geklärt werden könnten. Dies gelte auch, wenn sich die tatsächlichen Voraussetzungen nicht klären ließen, von denen die Zulässigkeit der erhobenen Klage abhängt. Eine Beweislastumkehr wegen Beweisvereitelung aufgrund der Löschung überprüfter, aber irrelevanter Verkehre scheidet aus. Denn dieses Vorgehen des Bundesnachrichtendienstes habe Vorschriften entsprochen, die verfassungsrechtlich nicht zu beanstanden seien, insbesondere mit dem Gebot effektiven Rechtsschutzes aus Artikel 19 Absatz 4 des Grundgesetzes (GG) in Einklang stünden. Der Gesetzgeber sei insbesondere nicht gehalten gewesen, in Fällen der unverzüglichen Prüfung und anschließenden unverzüglichen Löschung erfasster Telekommunikationsverkehre (§ 6 Absatz 1 Satz 6 G 10) eine Mitteilungspflicht einzuführen, um auf diese Weise die Möglichkeiten nachträglichen Rechtsschutzes zu verbessern. Eine solche Mitteilungspflicht würde massenhafte Recherchezwänge auslösen und dadurch in beträchtlicher Weise den Eingriff vertiefen. Auch die gesetzlichen Lösungsregeln im Art. 10-Gesetz seien für die Betroffenen offenkundig in erheblichem Maße grundrechtsschonend und stünden daher trotz ihrer Auswirkungen auf spätere Rechtsschutzmöglichkeiten mit Artikel 19 Absatz 4 GG im Einklang.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste ist weiterhin dringend geboten. Neben

den parlamentarischen Kontrollinstanzen sollten hierbei grundsätzlich auch die unabhängigen Datenschutzbehörden des Bundes und der Länder einbezogen werden.

2.1.4 Quod non legitur, non creditur

Mit dieser aus dem römischen Recht stammenden Prozessmaxime „Was nicht gelesen wird, wird nicht geglaubt“ musste die Polizei des Landes eine leidvolle Erfahrung machen. Was war geschehen?

Im Zusammenhang mit seinem Engagement gegen die friedliche Nutzung der Atomkraft in Atomkraftwerken waren gegen einen Bürger in einzelnen Fällen strafrechtliche Ermittlungsverfahren eingeleitet worden. Die zuständigen Polizeidirektionen speicherten aus diesen Ermittlungsverfahren sowie aus weiteren polizeilichen Maßnahmen im Zusammenhang mit Demonstrationen stammende Daten über den Betroffenen u. a. in der Arbeitsdatei Politisch Motivierte Kriminalität³³ (AD PMK). Nachdem ein Auskunftersuchen des Betroffenen eingegangen war, kam man im Zuge der Vorbereitung einer Antwort wohl zum Ergebnis, dass bezüglich einzelner Vorgänge die Speichervoraussetzungen mittlerweile nicht mehr vorlagen. Die entsprechenden Daten wurden gelöscht und die diesen Datenspeicherung zugrunde liegenden Akten wurden vernichtet. Übrig blieben nur noch Dateiausdrucke, die vor der Löschung gefertigt und für Zwecke der Datenschutzkontrolle und zur Dokumentation der Sachbearbeitung zur Vorgangsakte genommen worden waren. Im erstinstanzlichen Verfahren beantragte der Betroffene bei dem Verwaltungsgericht u. a., gegenüber dem Land Baden-Württemberg festzustellen, dass die Speicherung der Daten in den polizeilichen Auskunftssystemen von Anfang an rechtswidrig gewesen sei. Das Verwaltungsgericht wies die Feststellungsklage mangels Feststellungsinteresses noch als unzulässig zurück. Im Berufungsverfahren sah der Verwaltungsgerichtshof Baden-Württemberg dies anders und gab dem Kläger in der Sache Recht (Urteil vom 10. Februar 2015 – 1 S 554/13 –,

³³ Mit dem Themenkomplex der Arbeitsdatei Politisch Motivierte Kriminalität haben sich mein Amtsvorgänger und ich in mehreren Tätigkeitsberichten befasst (vgl. 26. Tätigkeitsbericht 2005, LT-Drs. 13/4910, S. 16 ff.; 27. Tätigkeitsbericht 2006, LT-Drs. 14/650, S. 33 ff.; 28. Tätigkeitsbericht 2007, LT-Drs. 14/2050, S. 17 ff.; 30. Tätigkeitsbericht 2010/2011, LT-Drs. 15/955, S. 71 f.).

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

DVBI 2015, S. 506–510). Das Gericht hielt die in der Vorgangsakte noch vorhandenen Dateiausdrucke nicht für ausreichend, um die Rechtmäßigkeit der Speicherung belegen zu können. Das Land trage die materielle Beweislast für das Vorliegen der Speichervoraussetzungen, insbesondere der Wiederholungsgefahr. Zur Begründung führte es Folgendes aus (Leitsatz, verkürzt):

„Die gesetzlichen Voraussetzungen für die Zulässigkeit der Speicherung, Veränderung und Nutzung personenbezogener Daten aus Ermittlungsverfahren durch den Polizeivollzugsdienst nach § 38 Abs. 1 PolG ... räumen der Behörde kein Ermessen ein. Bei der Beurteilung der für eine rechtmäßige Datenspeicherung erforderlichen Wiederholungsgefahr (§ 38 Abs. 1 S 2 und 3 PolG a.F.) steht dem Polizeivollzugsdienst allerdings ein Prognosespielraum zu. Die die Wiederholungsgefahr ... begründenden Anhaltspunkte sind in einer auf den Einzelfall bezogenen, auf schlüssigen, verwertbaren und nachvollziehbar dokumentierten Tatsachen beruhenden Entscheidung festzuhalten. Fehlt es an einer solchen Dokumentation der Wiederholungsgefahr, ist die Datenspeicherung rechtswidrig. Dies gilt auch für die Dokumentation der Gefahr der künftigen Begehung von Straftaten nach § 37 Abs. 1 i. V. m. § 20 Abs. 3 Nr. 1 PolG“.

Weiter heißt es in den Entscheidungsgründen:

„Eine ausreichende Dokumentation der Wiederholungsgefahr ist in den vorgelegten Akten, von denen der Beklagte in der mündlichen Verhandlung vor dem Senat versichert hat, sie seien vollständig, nicht feststellbar. Die materielle Beweislast für das Vorliegen einer ausreichenden Dokumentation der die Wiederholungsgefahr stützenden Umstände trägt der Beklagte“.

Grundsätzlich ist es zwar so, dass es einer Behörde nicht zum Nachteil, etwa im Sinne einer Beweislastumkehr, angerechnet werden kann, wenn sie sich gesetzeskonform verhält. Dies gilt auch dann, wenn eine Behörde ihrer gesetzlichen Verpflichtung zur Löschung von Daten nachkommt und dies zur Folge hat, dass ein Bürger nachträglich ein rechtswidriges Verhalten der Behörde nicht mehr nachweisen kann. Denn *„die gesetzlichen Lösungsregeln ...*

sind für die Betroffenen offenkundig in erheblichem Maße grundrechtsschonend und stehen daher trotz ihrer Auswirkungen auf spätere Rechtsschutzmöglichkeiten mit Art. 19 Abs. 4 GG im Einklang“ (Bundesverwaltungsgericht, BVerwGE 149, S. 359–373). Allerdings wird sich die Behörde dann den Vorwurf der Beweisvereitelung vorhalten lassen müssen, wenn sie ohne nennenswerten Verwaltungsaufwand und ohne dadurch eventuelle Grundrechtseingriffe zu vertiefen in der Lage wäre, den Betroffenen durch entsprechende Mitteilungen die Möglichkeit einzuräumen, dem Nachteil der Nichterweislichkeit seiner Behauptungen zu entgehen. In solchen Fällen könnte eine Mitteilungspflicht verfassungsrechtlich geboten sein. Auch in der datenschutzrechtlichen Kommentarliteratur wird überwiegend die Auffassung vertreten, die verantwortliche Stelle könne sich nicht durch die Löschung von Daten, die zum Zeitpunkt des Auskunftersuchens noch gespeichert sind, dem Auskunftsanspruch entziehen.

Das Innenministerium Baden-Württemberg habe ich um Stellungnahme gebeten, welche Konsequenzen es aus dem Urteil des Verwaltungsgerichtshofs Baden-Württemberg zu ziehen gedenkt. Hierauf hat es folgende Verfahrensweise vorgeschlagen:

Sofern sich im Rahmen der Bearbeitung eines Auskunftsantrags herausstellt, dass die Daten in den polizeilichen Dateien aufgrund fehlender Speichereberechtigung zu löschen sind, werden die elektronischen Dateien vollständig ausgedruckt. Die Ausdrucke werden zur Vorgangsakte genommen und die elektronischen Dateien werden gelöscht. Die Vorgangsakte sowie der Aktenrückhalt zu dem entsprechenden Ermittlungsverfahren (Ermittlungsakte sowie der entsprechende Teil der Kriminalakte) werden gem. § 46 Absatz 1 Satz 2 PolG i.V. mit § 23 Absatz 4 Nummer 1 und § 24 Absatz 1 Nummer 2, Absatz 2 Satz 1 des Landesdatenschutzgesetzes (LDSG) gesperrt. Die gesperrten Unterlagen werden bei dem oder der behördlichen Datenschutzbeauftragten der Dienststellen ausschließlich für Zwecke der Datenschutzkontrolle gesondert aufbewahrt.

Der antragstellenden Person wird sodann umfassend Auskunft zu allen über sie gespeicherten Daten erteilt. Gleichzeitig erfolgt der Hinweis, dass die unrechtmäßig gespeicherten Daten aus den elektronischen Dateien gelöscht wurden, jedoch gesperrt

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

als Dateiausdruck für weitere drei Monate aufbewahrt werden. Die Mitteilung erfolgt schriftlich und wird der antragstellenden Person gemäß den Vorschriften des Landesverwaltungszustellungsgesetzes förmlich zugestellt. Wird keine Überprüfung durch ein Gericht oder durch den Landesbeauftragten für den Datenschutz eingeleitet und wird ferner kein Einwand gegen die Löschung der betroffenen Daten vorgebracht, werden diese nach Ablauf der genannten Frist endgültig vernichtet. Auch darauf wird die antragstellende Person bereits im Rahmen der förmlich zuzustellenden Mitteilung ausdrücklich hingewiesen.

Dieser vorgeschlagenen Verfahrensweise habe ich zugestimmt. Mit der Löschung der Daten in den polizeilichen Dateien wird zum einen sichergestellt, dass die Möglichkeit eines landesweiten Zugriffs durch die Polizeidienststellen hierauf entfällt. Andererseits wird den Interessen der Betroffenen dadurch Rechnung getragen, dass anhand der Dateiausdrucke und des Aktenrückhalts eine nachträgliche Rechtsprüfung möglich bleibt. Gleichzeitig könnte sich dadurch auch das Risiko einer Beweislastumkehr zulasten des Landes vermindern. Durch die Aufbewahrung der Unterlagen mit alleiniger Zugriffsbefugnis durch die oder den behördliche/n Datenschutzbeauftragte/n wird auch dem notwendigen Sicherheitsbedürfnis bezüglich der gesperrten Daten hinreichend Rechnung getragen.

Die Negativprognose als Voraussetzung für die Speicherung personenbezogener Daten in den polizeilichen Dateien bedarf einer auf den Einzelfall bezogenen, auf schlüssigen, verwertbaren und nachvollziehbar dokumentierten Tatsachen beruhenden Begründung, die zu dokumentieren ist. Wird anlässlich der Bearbeitung eines Auskunftsantrags festgestellt, dass Daten zu löschen sind, bedarf es besonderer Maßnahmen, um dem Rechtsschutzanspruch des Antragstellers einerseits, aber auch dessen Interesse an der Nichtauffindbarkeit in den polizeilichen Dateien andererseits angemessen Rechnung zu tragen.

2.1.5 Wie man sich irren kann!

„Ich bin nicht entmutigt, denn jeder erkannte Irrtum ist ein weiterer Schritt nach vorn“ – dieser Satz von Thomas Alva Edison (amerik. Erfinder, 1847–1931)

kam mir in den Sinn, als ich die Begründung des Urteil des Verwaltungsgerichts Karlsruhe vom 26. August 2015 (– 4 K 2107/11 –, juris) las. Zum Hintergrund:

Im 30. Tätigkeitsbericht 2010/2011 (LT-Drs. 15/955 S. 72) hatte ich über den Einsatz eines Verdeckten Ermittlers des Landeskriminalamts Baden-Württemberg berichtet. Zur datenschutzrechtlichen Bewertung führte ich seinerzeit aus: „Soweit sich dies anhand der Akten beurteilen ließ, dürften die gesetzlichen Voraussetzungen sowohl hinsichtlich der Personen als auch hinsichtlich der vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erfüllt gewesen sein. Daher konnte ich gegen diese Maßnahme keine durchgreifenden datenschutzrechtlichen Bedenken geltend machen“. Die nunmehr vom Verwaltungsgericht Karlsruhe getroffene Entscheidung hat zwar gezeigt, dass ich damals falsch lag. Andererseits hat sie deutlich die Defizite dieses Polizeieinsatzes benannt und dadurch klare Hinweise für die Praxis gegeben, die jetzt auch Maßstab für künftige Kontrollen meiner Dienststelle sein werden.

Bemängelt hat das Gericht zunächst, dass die an die Anordnung des Einsatzes Verdeckter Ermittler zu stellenden formalen Voraussetzungen nicht erfüllt gewesen seien. Die entsprechenden Regelungen in §§ 22 und 20 PolG haben folgenden Wortlaut (Auszug):

<p>§ 22 Besondere Mittel der Datenerhebung</p> <p>(1) Besondere Mittel der Datenerhebung sind: [...]</p> <p>4. der Einsatz von Polizeibeamten unter Geheimhaltung ihrer wahren Identität (Verdeckte Ermittler) [...]</p> <p>(3) Der Polizeivollzugsdienst kann personenbezogene Daten durch besondere Mittel der Datenerhebung</p> <p>1. zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit und Freiheit einer Person oder für bedeutende fremde Sach- und Vermögenswerte über die in § 20 Abs. 2 genannten Personen oder</p> <p>2. zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung über die in § 20 Abs. 3 Nr. 1</p>

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

und 2 genannten Personen erheben, wenn andernfalls die Wahrnehmung seiner Aufgaben gefährdet oder erheblich erschwert würde.

(6) Der Einsatz von Mitteln nach Absatz 1 [...] bedarf der Anordnung durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts.

§ 20
Befragung und Datenerhebung

(2) Die Polizei kann Daten der in den §§ 6 oder 7 genannten Personen sowie anderer Personen erheben, soweit dies zur Abwehr einer Gefahr oder zur Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung erforderlich ist und die Befugnisse der Polizei nicht anderweitig geregelt sind.

(3) Der Polizeivollzugsdienst kann Daten über
1. Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie künftig Straftaten begehen,
2. Kontakt- und Begleitpersonen einer der in Nummer 1 genannten Personen, ...

Insbesondere die doch recht kargen formalen Vorgaben des § 22 Absatz 6 PolG füllte das Verwaltungsgericht mit Leben, indem es unter Hinweis auf die hohe Intensität des Eingriffs in das informationelle Selbstbestimmungsrecht weitere verfahrensmäßige Vorkehrungen als Voraussetzung dafür benannte, dass eine am Maßstab des Bestimmtheitsgrundsatz orientierte Einsatzanordnung Bestand haben kann.

Neben dem bereits gesetzlich geregelten Behördenleitervorbehalt bedarf es danach einer hinreichenden Bestimmung des eingesetzten Mittels: „Allein die in der Einsatzanordnung vom ... und deren Folgeanordnungen aufgenommene abstrakte Bezeichnung des Mittels „verdeckter Ermittler“ ist für eine hinreichende Bestimmung des besonderen Mittels i.S. des § 22 Abs. 1 Nr. 4 PolG nicht ausreichend“. Die grundsätzlich in Schriftform zu ergehende Einsatzanordnung muss nach Auffassung des Gerichts die Zielperson benennen und Angaben über die Anzahl der als Verdeckte Ermittler eingesetzten Personen sowie darüber enthalten, ob es sich bei diesen – wie vom Gesetz vorgeschrieben – um Poli-

zeibeamte handelt. Des Weiteren muss sie Aufschluss über die Identität der Betroffenen geben, d. h. konkret müssen die Namen der jeweiligen Polizeibeamten angegeben werden.

Nach Auffassung des Verwaltungsgerichts war die Einsatzanordnung, die diese formalen Kriterien nicht erfüllte, allein deshalb bereits rechtswidrig. Dass sie daneben auch materiell fehlerhaft war, sei hier nur am Rande erwähnt. Es hätten – so das Gericht – in der Begründung die wesentlichen tatsächlichen Gründe gefehlt, die den Anordnungsberechtigten zu der Entscheidung bewogen hätten. Zum einen seien keine hinreichenden Fakten genannt, aus denen sich eine konkrete Gefahr für die öffentliche Sicherheit und Ordnung herleiten ließe (§ 22 Absatz 3 Nummer 1 PolG). Zum anderen seien, auch unter Heranziehung der Akten, weder tatsächliche Anhaltspunkte noch Indizien dafür ersichtlich, dass es sich bei dem Betroffenen um eine Person handelt, die Straftaten begehen wird (§ 22 Absatz 3 Nummer 2 PolG).

Alles in allem kann ich der Entscheidung uneingeschränkt Positives abgewinnen. Sie schafft einmal mehr Klarheit, unter welchen formalen und materiellen Voraussetzungen polizeiliche Maßnahmen in grundrechtssensiblen Bereichen zulässig sind. Die künftige polizeiliche Praxis wie auch Kontrollmaßnahmen meiner Dienststelle werden sich daran ausrichten haben.

In der schriftlichen Anordnung des Einsatzes von Verdeckten Ermittlern nach § 22 Absatz 6 PolG ist die Zielperson zu benennen oder zumindest zu umschreiben. Die Anordnung muss angeben, wie viele Verdeckte Ermittler tätig werden, ob es sich dabei um Polizeibeamte handelt und wer konkret als Verdeckter Ermittler eingesetzt wird. In einer Begründung sind die wesentlichen tatsächlichen Gründe darzulegen, die den Anordnungsberechtigten zu der Entscheidung bewogen haben. Außerdem wird eine Frist für die Dauer des Einsatzes zu bestimmen sein.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

2.2 Datenverarbeitung durch Sicherheits- und Ordnungsbehörden**2.2.1 Die Antiterrordatei – Neue Strategien zur Effektivierung der Kontrollpraxis**

Die Antiterrordatei³⁴ (ATD) ist eine gemeinsame Datenbank von 38 deutschen Sicherheitsbehörden. Neben dem Bundeskriminalamt (BKA), der Bundespolizei, dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst und dem Zollkriminalamt nehmen die Länderpolizeien und die Landesämter für Verfassungsschutz gleichermaßen teil. Ziel der Datei ist es, bereits im Vorfeld zu erkennen, ob ein bestimmtes Verhalten typischerweise dem eines potenziellen Attentäters ähnelt. Darüber hinaus soll verhindert werden, dass jemand von einer Behörde verfolgt, von einer anderen aber geduldet oder vielleicht sogar gefördert wird. Diese sog. Verbunddatei wurde auf der Rechtsgrundlage des Antiterrordateigesetzes (ATDG) zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland errichtet und ist als Index-Datei ausgestaltet.

Mit Urteil vom 24. April 2013³⁵ erklärte das Bundesverfassungsgericht (BVerfG) Teile des Antiterrordateigesetzes (ATDG) für verfassungswidrig (vgl. hierzu auch 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Kap. 2.4.2, S. 62f.). Das BVerfG führte aus, dass die Gesamtstruktur der ATD zwar verfassungsgemäß sei, Teile von ihr jedoch hinsichtlich ihrer Ausgestaltung im Einzelnen den verfassungsrechtlichen Anforderungen nicht genügen würden. So würde die Regelung der Datei den Verhältnismäßigkeitsgrundsatz im engeren Sinne nicht vollständig wahren, da sie hinsichtlich der zu erfassenden Daten sowie deren Nutzungsmöglichkeiten nicht normenklar und in der Sache nicht hinreichend begrenzt ausgestaltet sei.³⁶ U. a. wurde kritisiert, dass Kontaktpersonen im Grunddatensatz gespeichert und zu weitgehende Recherchemöglichkeiten im Rahmen der sogenannten Inverssuche eröffnet würden und dass angesichts der nur eingeschränk-

ten Möglichkeiten individuellen Rechtsschutzes datenschutzrechtliche Kontrollen nur mangelhaft ausgestaltet seien. Es liege in der Natur der Sache, dass die an der ATD beteiligten Sicherheitsbehörden verdeckt arbeiten; der Betroffene könne daher nur unter erschwerten Bedingungen Rechtsschutz im Falle einer rechtswidrigen Datenspeicherung und -verarbeitung erhalten. In der Großzahl der Fälle würden Betroffene somit keinerlei Kenntnis erhalten, ob sie in der ATD gespeichert sind und welche Daten von ihnen vorhanden sind. Das Bundesverfassungsgericht hat deshalb den Kontrollen der Datenschutzbehörden im Rahmen der ATD großes Gewicht beigemessen, weil die Kontrolle aufgrund einer Beschwerde eben nur ausnahmsweise sichergestellt werden könne. Effektive Kontrollen seien nur durch sachlich, personell und kompetenzmäßig ausreichend ausgestattete Datenschutzaufsichtsbehörden sowie anhand einer qualitativ hochwertigen Dokumentation möglich. Eine vollständige Protokollierung von Zugriffen und Änderungen auf die Daten sei für letzteres zwingend.

Das Urteil des Bundesverfassungsgerichts verpflichtete den Gesetzgeber zu einer Nachbesserung des ATDG bis Anfang 2015 und führte zu einer Neuregelung der beanstandeten Vorschriften. Durch das novellierte ATDG werden die Datenschutzbeauftragten von Bund und Ländern verpflichtet, mindestens alle zwei Jahre die von den Ländern in die ATD eingegebenen Datensätze zu kontrollieren. Es ist vorgesehen, dass Landes- und Bundesbeauftragte für den Datenschutz zusammenarbeiten. Bereits im Jahre 2007 – also direkt nach Einführung der ATD – hatten meine Mitarbeiter in mehrtägigen Kontrollbesuchen beim Landeskriminalamt (Abteilung Staatsschutz) und beim Landesamt für Verfassungsschutz die technischen Rahmenbedingungen und die veranlassten Datenspeicherungen in der ATD überprüft.³⁷ Um dem neuen Gesetzesrahmen und dem Prüfauftrag entsprechen zu können, wurde in meiner Dienststelle dank der Unterstützung des Landtags 2015 eine zusätzlich Planstelle geschaffen. Regelmäßige, wiederkehrende Kontrollen der ATD sind somit jedenfalls personell voraussichtlich gesichert.

Bislang bestehen zwischen den jeweiligen Landesdatenschutzbehörden hinsichtlich der Prüfpraxis und der methodischen Herangehensweise im Rahmen

³⁴ Zum Gesamtkonzept der ATD vgl. 27. Tätigkeitsbericht 2006, LT-Drs. 14/650, S. 10, und 28. Tätigkeitsbericht, LT-Drs. 14/2050, S. 12, sowie 31. Tätigkeitsbericht, LT-Drs. 15/4600, S. 62 ff.

³⁵ BVerfGE 133, S. 277; NJW 2013, S. 1335.

³⁶ Hierzu auch 31. TB, LT-Drs. 15/4600, S. 62 ff.

³⁷ vgl. 28. Tätigkeitsbericht, LT-Drs. 14/2050, S. 12 ff.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

der ATD erhebliche Unterschiede: Während einige zur Überprüfung der ATD primär den bei den Landesbehörden befindlichen Aktenrückhalt verwendeten und die ATD-Protokolle lediglich unterstützend herangezogen (so verfahren auch wir), nahmen andere die Protokollierungsdateien des BKA als Ausgangspunkt ihrer Kontrollen. Diese Vorgehensweise führte insbesondere durch die Masse der zu sichtenden Protokolldaten zu teils erheblichen Problemen in der Kontrollpraxis.

Beim BKA sind sowohl der Datenbankserver als auch der Protokollserver der ATD installiert. Auf dem Protokollserver des BKA werden sogenannte Reports zur Ausweisung bestimmter Auswertungskriterien programmiert. Zum Zwecke der Überprüfung haben die Landesdatenschutzbehörden bislang die Möglichkeit, zwischen insgesamt elf verschiedenen Reports zu wählen, welche wiederum über zusätzlich einstellbare Parameter eine individuell bestimmbare Verfeinerung der Protokollauswertungen ermöglichen. Reports sind beispielsweise nach den Kriterien „neu angelegte Objekte“, „geänderte Objekte“, „gelöschte Objekte“, „angesehene Objekte“ oder aber auch nach dem Kriterium „Suchanfragen“ erstellbar. Momentan gestalten sich die Bereitstellung und die Auswertung der beim BKA gespeicherten Protokolle durch die Datenschutzbehörden als extrem zeit- und arbeitsintensiv. So berichteten mir Kollegen, welche die Kontrolle der ATD anhand der Protokolldateien begonnen hatten, dass sich der Seitenumfang der übersandten Protokoll-Reports im fünfstelligen Bereich bewege.

Die Ursache hierfür ist in der Datenbankarchitektur der ATD zu finden: So wird die ATD von den jeweiligen Systemen der teilnehmenden Sicherheitsbehörden gespeist. Ohne auf Details einzugehen kann vereinfacht gesagt werden, dass die Quelldateien der beteiligten Sicherheitsbehörden der Länder im Vergleich zu den in die ATD gespeisten Daten ein Datenplus enthalten. Dies entspricht der Funktion der ATD als bloßem Instrument zur Informationsanbahnung. So betonte auch das Bundesverfassungsgericht mit Verweis auf das zwischen Polizei und Verfassungsschutz zu beachtende Trennungsprinzip, dass die ATD keinesfalls den Charakter eines zentralen, für alle beteiligten Behörden frei zugänglichen Datenpools haben dürfe. Sämtliche Änderungen und Löschungen in den Quelldateien werden somit nicht nur in den landeseigenen Systemen,

sondern zusätzlich auch auf dem Protokollserver des BKA protokolliert. Dies selbst dann, wenn Datenfelder der Quelldatei geändert werden, welche selbst nicht in die ATD hineingespiegelt worden sind. Hierdurch steigt die Masse der übermittelten Protokolle immens an, obwohl die eigentlichen ATD-relevanten Datenfelder nicht von einer Änderung betroffen waren. Für die Aufsichtsbehörden kann dies bedeuten, sich geduldig durch tausende Protokollseiten zu arbeiten, auch wenn diese keinerlei Änderungen der ATD-Daten beinhalten.

Um eine Effektivierung der Kontrollpraxis und ein genaueres Prüfungsvorgehen zu erreichen, trafen sich im Dezember 2015 Vertreter aller Landesdatenschutzbehörden und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) mit dem BKA. Für das Jahr 2016 ist geplant, die Zusammenarbeit mit dem BKA zu intensivieren, um den Datenschutzbehörden user- bzw. kontrollzweckgerechtere Reports liefern zu können. Es wird zu klären sein, ob und gegebenenfalls welche weiteren Reports bereitgestellt werden sollten und auf welchem Wege dies technisch umgesetzt werden kann. Schwachstellen der bereits vorhandenen Reports sollen hierbei genutzt werden, um erforderliche Anpassungen vornehmen zu können.

Um zukünftig eine länderübergreifend einheitliche Prüfpraxis der ATD-Protokolldaten zu erzielen, kamen die Landesdatenschutzbehörden und die BfDI überein, dass man sich im ersten Quartal 2016 zunächst auf ein standardisiertes Reportpaket einigen werde. Dies ist nicht zuletzt aufgrund der wiederkehrenden Kontrollpflicht sinnvoll. Zudem würde eine solche Standardisierung die Arbeit des BKA erheblich erleichtern und zur schnelleren Beantwortung von Anfragen führen. Neben der Bereitstellung eines standardisierten Reports wird es den Ländern jedoch auch weiterhin möglich bleiben, individuelle Abfragen der Protokolle anfordern zu können. Spezifische Prüfungen der ATD durch meine Dienststelle sind zukünftig also auch weiterhin möglich.

Mit Blick auf die nunmehr normierte Prüfpflicht der Datenschutzbeauftragten wird meine Dienststelle im Jahr 2016 entsprechende Prüfungen bei den an der ATD beteiligten Behörden durchführen.

Um die Antiterrordatei effektiv prüfen zu können, bedarf es einer intensiven Vorbereitung der tech-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

nisch-organisatorischen Grundlagen. Dies setzt eine enge Zusammenarbeit der Datenschutzaufsichtsbehörden untereinander, aber auch insgesamt mit dem Bundeskriminalamt voraus. Erste Abstimmungsprozesse wurden bereits eingeleitet. Sie sollen mit Nachdruck weitergeführt werden.

2.2.2 Precogs oder Precobs – die Zukunft der Verbrechensverhinderung?

In meinem 31. Tätigkeitsbericht 2012/2013 hatte ich noch unter Hinweis auf den Science-Fiction-Thriller „Minority Report“ und den Versuch der Polizei in einigen Städten der USA, mit Hilfe moderner Datenanalyse vorherzusagen, wo und wann Verbrechen geschehen, um vorher da zu sein und den Täter verhaften zu können, meiner Hoffnung Ausdruck verliehen, dass die Polizei hierzulande sich diesbezüglich zurückhält (LT-Drs. 15/4600, S. 18). Es kam anders! Seit dem 30. Oktober 2015 ist die Verbrecherjagd per Computer auch im Alltag der Polizei Baden-Württemberg angekommen.

In dem erwähnten Film werden drei sogenannte „Precogs“ mit Medikamenten in einem Zustand zwischen Traum und Wachen gehalten, der für ihre hellseherischen Fähigkeiten besonders günstig ist. In ihren Visionen sehen sie künftige Morde voraus. Die Namen von Täter und Opfer werden in Holzkugeln graviert. Ganz so weit ist man hierzulande zwar noch nicht. Dass Polizeibeamte unter Drogeneinfluss hellseherische Fähigkeiten entwickeln, dürfte in absehbarer Zukunft weder erwünscht noch zu erwarten sein. Computerprogrammen scheint man solche Fähigkeiten schon eher zuzutrauen: Vorhang auf für „Precobs“ („Pre Crime Observation System“), eine Statistiksoftware, mit deren Hilfe man sich erhofft, Einbrüche voraussehen zu können. Die Polizei Baden-Württemberg will dieses Verfahren zunächst im Rahmen eines Pilotbetriebs bei den Polizeipräsidien Stuttgart und Karlsruhe testen, um herauszufinden, ob es hält, was die Hersteller versprechen. Die Hoffnung ist, damit einen bedeutenden Schritt hin zur Verbesserung der Situation im Bereich des Deliktsfelds Wohnungseinbruchdiebstahl (WED)/ Tageswohnungseinbruch (TWE) zu machen. Diese Delikte stellen die Polizei tatsächlich vor große Probleme.

Wie der Antwort des Innenministeriums auf eine parlamentarische Anfrage vom Frühjahr 2015 (LT-

Drs. 15/6620 vom 18. März 2015) zu entnehmen ist, stiegen die in der Polizeilichen Kriminalstatistik (PKS) registrierten Fallzahlen beim Wohnungseinbruchdiebstahl zwischen 2010 und 2014 kontinuierlich von 7.844 auf 13.483 an. Die Aufklärungsquote ging dabei geringfügig auf 14 Prozent zurück. Weiter heißt es in der Stellungnahme:

„Als weiterer Baustein zur Bekämpfung, insbesondere zur Unterstützung von präventiven Präsenz- und Fahndungsmaßnahmen, wird aktuell Einsatz unterstützende Software geprüft. Im kriminologischen Zusammenhang wird dies als „Predictive Policing“ bezeichnet. Durch computergestützte Auswertung verschiedener polizeilicher, nicht personenbezogener Daten sollen räumlich-zeitliche Tatwahrscheinlichkeiten antizipiert werden. Aktuell wurde das Landeskriminalamt mit der Erstellung eines Fachkonzepts beauftragt; in einem nächsten Schritt soll die Software in einem Pilotprojekt getestet werden.“

Dieser nächste Schritt folgte auf dem Fuß: bereits Anfang Mai 2015 fand eine Besprechung zwischen dem Landeskriminalamt und meiner Dienststelle statt, in der das Landeskriminalamt die bereits sehr konkreten Planungen vorstellte. Zusammengefasst kann die Funktionsweise der Prognosesoftware wie folgt beschrieben werden (vgl. LT-Drs. 15/6816 vom 29. April 2014):

„Die Prognosesoftware soll in Fällen des Wohnungseinbruchdiebstahls anhand bestimmter Tatmerkmale [sog. Trigger] erkennen, ob es sich um Fälle handelt, die einem Wiederholungstäter bzw. einer entsprechenden Tätergruppierung zugerechnet werden können. Grundlage der Berechnung sind statistische Falldaten aus der polizeilichen Vorgangsbearbeitung, soziodemographische Daten, Wetterdaten und aktuelle kriminologische und kriminalistische Erkenntnisse, wie die Near-Repeat- und Rational-Choice-Theorien. Die Verarbeitung personenbezogener Daten ist nicht beabsichtigt. Die Berechnungen stützen sich auf Prognosealgorithmen, die zunächst im Rahmen einer vorgelagerten Simulationsstudie mit Daten aus der Vergangenheit optimiert werden. Im Wirkbetrieb sollen auf der Grundlage von tagesaktuellen Datensätzen induktiv Vorhersagen für die nächsten sieben Tage getroffen werden können, die von einem polizeilichen Sachbearbeiter im Hinblick auf ihre Plausibilität bewertet

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

werden. In der Folge können in den betroffenen Gebieten zielgerichtet polizeiliche Maßnahmen, wie beispielsweise präventive Präsenz- und Fahndungsmaßnahmen, geplant und durchgeführt werden“.

Die Behauptung, das Programm komme ohne personenbezogene Daten aus, war aus meiner Sicht allerdings nicht ganz zutreffend. Aus dem Vortrag eines Mitarbeiters des Bayerischen Landeskriminalamts, das das Verfahren Precobs bereits seit einiger Zeit einsetzt, war mir nämlich bekannt, dass dem beileibe nicht so ist. Denn insbesondere die dort verwendeten Tatortdaten (genaue Adresse, Diebesgut, Tatörtlichkeit und Taträumlichkeit, z. T. auch Namensinitialen) ließen durchaus eine Identifizierung der Opfer zu und wiesen damit Personenbezug auf. Auch wenn dies zum einen Daten sind, die der Polizei im Rahmen der Fallbearbeitung ohnehin bekannt und deren Datenschutzrisiken aufgrund fehlender Recherchierbarkeit gering sind, hielt ich es doch für angezeigt, nach Wegen zu suchen, um die (erwarteten) Vorteile des Softwareeinsatzes auch ohne personenbezogene Daten zu erreichen. Erfreulicherweise erklärte sich das Landeskriminalamt ohne Wenn und Aber bereit, diesbezüglich mit dem Softwarehersteller in Kontakt zu treten – mit Erfolg, wie sich zeigen sollte.

In der aktuellen Version der Software, die in Baden-Württemberg zum Einsatz kommt, ist vorgesehen, die Tatortdaten nicht konkret, sondern jeweils bezogen auf bestimmte Geoparzellen oder sog. Polygone anzugeben. Konkret heißt das, dass sämtliche Informationen fünf potenziellen Opferhaushalten oder zumindest einem gewissen geographischen Bereich von ca. 50–60 m Kantenlänge zugeordnet werden und damit der Personenbezug beseitigt wird. Damit scheint mir ein guter Kompromiss zwischen fachlicher Notwendigkeit einerseits und dem Interesse von Straftatenopfern andererseits erreicht worden zu sein, nicht zusätzlich zu den ohnehin erlittenen Schäden auch noch in den polizeilichen Systemen „verarbeitet“ zu werden. Die Funktionsweise des Verfahrens wurde meinen Mitarbeitern und mir inzwischen im Echtbetrieb vorgeführt. Dabei konnte ich mich davon überzeugen, dass die besprochenen Modifikationen tatsächlich vorgenommen worden waren und das System nun ohne personenbezogene Daten arbeitet.

Neben der lobend hervorzuhebenden konstruktiven Art und Weise, in der das Landeskriminalamt früh-

zeitig das Beratungsangebot meiner Dienststelle in Anspruch genommen hat, sehe ich es auch als positiv an, dass das Pilotprojekt, das auf sechs Monate angelegt ist, durch eine angesehene Forschungseinrichtung wissenschaftlich begleitet werden soll. Ob Predictive Policing künftig zu einem Standardbaustein im Rahmen der Kriminalitätsanalyse und Einsatzplanung werden wird, ist deshalb derzeit noch offen.

Auch wenn Precobs insgesamt gesehen datenschutzrechtlich unbedenklich erscheint, dürfen gleichwohl die Risiken für das Persönlichkeitsrecht nicht aus dem Blick verloren werden, die mit dem zunehmenden Einsatz von Massendatenanwendungen verbunden sind. In ihrer Konferenz am 18./19. März 2015 in Wiesbaden haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung „Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten“ hierauf hingewiesen (vgl. Anhang 16).

2.2.3 Gut gemeint ist nicht immer gut

Jede Behörde wünscht sich engagierte Mitarbeiterinnen und Mitarbeiter. Den Spruch des Tages: „Nimm nicht das, was Du kriegen kannst, sondern kämpfe um das, was Du haben willst“ nahm sich indes eine Mitarbeiterin des Landeskriminalamts Baden-Württemberg zu sehr zu Herzen und schoss dabei übers Ziel hinaus. Dies führte dazu, dass ich mich mit folgender Angelegenheit befassen durfte:

Der Rechtsamtsleiters einer Kleinstadt wandte sich an mich und fragte, was ich davon halte, dass das Landeskriminalamt die Stadt per E-Mail aufgefordert hatte, ihm zu einer Liste italienischer Gastronomiebetriebe jeweils Auskünfte über Geschäftsinhaber, Betreiber, Konzessionsträger, eventuelle Stellvertreter sowie deren Familien zu erteilen. Dem Amtsleiter kam dies merkwürdig vor. Auf seine telefonische Nachfrage bei der Verfasserin des Schreibens, auf welche Rechtsgrundlage sich das Landeskriminalamt dabei stütze, habe ihm die Gesprächspartnerin, trotz mehrfacher Versuche, keine zufriedenstellende Antwort geben können, sondern das Gespräch schließlich mit den Worten beendet: „Dann lassen Sie's, wir kommen auch ohne Ihre Daten aus!“.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Auf die daraufhin unvermeidliche Nachfrage meinerseits beim Landeskriminalamt, was der Hintergrund dieses Auskunftersuchens gewesen sei, wurde ich auf das dortige Auswerteprojekt „Italienische Gastronomiebetriebe“, kurz: APIG, aufmerksam gemacht. Bei diesem ging es im Wesentlichen darum, Zusammenhänge zwischen organisierter Kriminalität und italienischer Gastronomie festzustellen. Bei einem Besuch des Landeskriminalamts wurde meinen Mitarbeitern das Projekt näher vorgestellt. Ohne an dieser Stelle auf Einzelheiten einzugehen, führte die Diskussion rasch zu der Kernfrage, auf welche Rechtsgrundlage das Projekt denn nun eigentlich gestützt werde. Das Landeskriminalamt führte die Berechtigung zu solchen Initiativmittlungen auf § 20 Absatz 3 PolG zurück. Dieser hat folgenden Wortlaut:

§ 20
Befragung und Datenerhebung

[...]

(3) Der Polizeivollzugsdienst kann Daten über

1. Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie künftig Straftaten begehen,
2. Kontakt- und Begleitpersonen einer der in Nummer 1 genannten Personen,
3. Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie Opfer von Straftaten werden,
4. Personen im räumlichen Umfeld einer in besonderem Maß als gefährdet erscheinenden Person oder
5. Zeugen, Hinweisgeber oder sonstige Auskunftspersonen erheben, soweit dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist.

Hauptziel der Maßnahmen war nach Aussage des Landeskriminalamts ausschließlich die Gewinnung von Ermittlungsansätzen, um irgendwann zu einem späteren Zeitpunkt Ermittlungsverfahren einleiten und Straftäter der Strafverfolgung zuführen zu können. Damit lag folgendes Problem auf dem Tisch:

Der Verwaltungsgerichtshof Baden-Württemberg hatte sich in seinem Urteil vom 15. Mai 2014 (1 S 815/13, NVwZ-RR 2015, S. 26–31) mit der Frage befasst, wie der Begriff der vorbeugenden Bekämpfung von Straftaten in § 22 Absatz 2 und 3 PolG vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichts zur Telekommunikationsüberwachung nach dem Niedersächsischen Gesetz über

die öffentliche Sicherheit und Ordnung (§ 33 a Absatz 1 Nummer 2 und 3 NdsSOG a.F.; Urt. v. 27. Juli 2005 – 1 BvR 668/04 – BVerfGE 113, 348) auszulegen sei.

§ 22 Absatz 2 und 3 PolG hat folgenden Wortlaut (gekürzt):

§ 22
Besondere Mittel der Datenerhebung

[...]

(2) Der Polizeivollzugsdienst kann personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Lichtbildern und Bildaufzeichnungen von den in § 20 Abs. 2 genannten Personen zur Abwehr einer erheblichen Gefahr oder von den in § 20 Abs. 3 Nr. 1, 2 und 4 genannten Personen zur vorbeugenden Bekämpfung von Straftaten erheben, wenn andernfalls die Wahrnehmung seiner Aufgaben gefährdet oder erheblich erschwert würde.

(3) Der Polizeivollzugsdienst kann personenbezogene Daten durch besondere Mittel der Datenerhebung

[...]

2. zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung über die in § 20 Abs. 3 Nr. 1 und 2 genannten Personen erheben, wenn andernfalls die Wahrnehmung seiner Aufgaben gefährdet oder erheblich erschwert würde.

Der Verwaltungsgerichtshof kam zum Ergebnis, dass das bisher in Rechtsprechung und Literatur in Bezug auf das baden-württembergische Polizeigesetz herrschende duale Begriffsverständnis der vorbeugenden Straftatenbekämpfung im Sinne der (präventiven) Verhinderungsvorsorge wie auch der (repressiven) Strafverfolgungsvorsorge nicht mehr aufrechterhalten zu sei. Die in § 22 Absatz 2 und 3 PolG geregelten verdeckten Observationsmaßnahmen seien hinsichtlich ihrer repressiven Zielrichtung der vorbeugenden Bekämpfung von Straftaten bereits durch den Bund in der Strafprozessordnung umfassend geregelt worden (§ 100 f, § 100 h StPO). Der Bund habe insoweit von seiner konkurrierenden Gesetzgebungskompetenz nach Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes abschließend Gebrauch gemacht. § 22 Absatz 2 und 3 PolG könne daher nur Bestand haben, wenn der Begriff der vorbeugenden Bekämpfung von Straftaten verfas-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

sungskonform dahingehend ausgelegt werde, dass er nur die Verhütung von Straftaten (Verhinderungsvorsorge) umfasst: *„Die Verhütung von Straftaten erfasst nur Maßnahmen, die drohende Rechtsgutverletzungen von vornherein und in einem Stadium verhindern sollen, in dem es noch nicht zu strafwürdigem Unrecht gekommen ist [...]. Hauptzweck ist nicht das Sammeln von Beweismitteln für ein mögliches, künftiges Strafverfahren, sondern das Verhindern der Straftat zu einem Zeitpunkt, zu dem die Strafbarkeitsschwelle noch nicht überschritten ist, in der Regel also im Planungs- oder Vorbereitungsstadium“.*

Angesichts dieser (geänderten) Rechtsprechung stellte sich die Frage, ob auch der in § 20 Absatz 3 PolG verwendete Begriff der vorbeugenden Bekämpfung von Straftaten einschränkend auszulegen ist und welche Konsequenzen dies für das Auswerteprojekt, das sich gerade auf diese Bestimmung stützte, hat. Die Entscheidungsgründe des Urteils könnten so verstanden werden, dass der Verwaltungsgerichtshof das für die Auslegung des § 22 PolG gefundene Ergebnis auch auf andere Bestimmungen des Polizeigesetzes mit Bezug zur vorbeugenden Verbrechensbekämpfung erstrecken will. Hiervon ausgehend dürfte der in § 20 Absatz 3 PolG verwendete Begriff der vorbeugenden Straftatenbekämpfung (verfassungskonform) nur im Sinne der Verhinderungsvorsorge, also rein präventiv verstanden werden. Dies allerdings war weder Haupt- noch Nebenzweck des Projekts APIG. Das hierzu um Stellungnahme gebetene Innenministerium Baden-Württemberg neigte dagegen der Auffassung zu, die Entscheidung des Verwaltungsgerichtshofs zu § 22 PolG könne nicht verallgemeinert werden. Vielmehr müsse jede Vorschrift gesondert betrachtet und daraufhin überprüft werden, ob der Bund von seiner (konkurrierenden) Gesetzgebungskompetenz im Bereich der Strafverfolgungsvorsorge abschließend Gebrauch gemacht habe. Allerdings müsse dies noch vertieft geprüft werden. Eventuell erforderliche Änderungen des Polizeigesetzes seien derzeit nicht realisierbar. Das Landeskriminalamt jedenfalls zog die Konsequenzen aus der unsicheren Rechtslage und teilte mit, dass es das Projekt eingestellt und die Daten gelöscht habe.

„Das Gegenteil von gut ist gut gemeint.“ (Kurt Tucholsky) – mit ihrer Aktion hat die engagierte Polizeibedienstete, die von ihrer Arbeit so begeis-

tert war, dass sie sich weder durch interne Zuständigkeiten noch durch die formalen Kriterien der Konzeption des Landeskriminalamts bremsen ließ, nicht nur für erhebliche Verwirrung gesorgt, sondern unbeabsichtigt auch ein juristisches Problem ins Scheinwerferlicht gerückt, mit der Folge, dass die Rechtmäßigkeit bestimmter polizeilicher Maßnahmen künftig kritischer zu hinterfragen sein wird.

Mit der Feststellung, die polizeilichen Maßnahmen, um die es in dem Rechtsstreit ging, seien rechtswidrig gewesen, weil sie nicht primär auf die Verhütung von Straftaten, sondern auf die Strafverfolgungsvorsorge ausgerichtet waren und daher rechtgrundlos erfolgten, ließ es der Verwaltungsgerichtshof in der angesprochenen Entscheidung allerdings nicht bewenden. Vielmehr zog er die Verfassungsmäßigkeit des § 22 PolG an sich in Zweifel. So sei die Datenerhebung nach § 20 Absatz 3 Nummer 1 PolG lediglich an die Voraussetzung geknüpft, dass tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person künftig Straftaten begehen werde. Die Situation bei solchen Vorfeldermitteilungen sei aber durch eine hohe Ambivalenz der potenziellen Bedeutung einzelner Verhaltensumstände geprägt. Bei polizeilichen Maßnahmen im Vorfeld der Gefahrenabwehr und der Strafverfolgung müssten die Bestimmtheitsanforderungen deshalb spezifisch an dieser Vorfeldsituation ausgerichtet werden. Die in einer Vorfeldsituation bestehenden Schwierigkeiten der Abgrenzung eines harmlosen Verhaltens von dem in eine Straftatenbegehung mündenden Verhalten müssten in der Ermächtigung durch einschränkende Tatbestandsmerkmale bewältigt werden. Dem genüge § 22 PolG nicht. Fazit des Gerichts: *„Überträgt man diese – sehr hohen – Anforderungen an die Bestimmtheit polizeilicher Ermächtigungsgrundlagen im Vorfeld einer Gefahr und des Anfangsverdachts einer Straftat auf die hier herangezogene Ermächtigungsgrundlage des § 22 PolG, wird man ebenfalls von der Verfassungswidrigkeit der Norm ausgehen müssen“.* Dass daneben auch noch die Frage aufgeworfen wird, ob denn § 22 Absatz 1 Nummer 2 Alt. 2 PolG (verdeckter Einsatz technischer Mittel zur Aufzeichnung des nicht öffentlich gesprochenen Wortes auf Tonträger) verfassungsrechtlichen Anforderungen genüge, da keinerlei verfahrensmäßige Absicherungen (Richter-, Behördenleitervorbehalt) vorgesehen sind, und bemängelt wird, dass § 22 PolG keine Pflicht zur Do-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

kumentation enthalte, was eine aus dem Grundrecht auf informationelle Selbstbestimmung abgeleitete Notwendigkeit darstelle, rundet das Bild einer verfehlten gesetzlichen Regelung ab.

Die Frage, welche Maßnahmen der vorbeugenden Straftatenbekämpfung auf der Grundlage der entsprechenden Vorschriften des Polizeigesetzes zulässig sind, bedarf einer kritischen Überprüfung. Die Entscheidung des Verwaltungsgerichtshofs Baden-Württemberg macht einmal mehr deutlich, dass eine Novellierung des Polizeigesetzes – auch in diesem Punkt – dringend erforderlich ist. Dass daneben auch das Landesverfassungsschutzgesetz nicht den verfassungsrechtlichen Anforderungen entspricht, habe ich schon seit Jahren vergeblich kritisiert. Es ist höchste Zeit, auch einmal ein „Sicherheitspaket“ zur Schaffung verfassungskonformer Rechtsgrundlagen für die Tätigkeit der Sicherheitsbehörden in Baden-Württemberg zu schnüren.

2.2.4 Der Kriminalaktennachweis – gehören Daten aus Ermittlungsverfahren wegen des Verdachts der exhibitionistischen Handlung in diese bundesweite Datei?

Nachdem sich Eingaben häuften, bei denen die Datenspeicherung aus strafrechtlichen Ermittlungsverfahren durch die Landespolizei in der beim Bundeskriminalamt geführten Verbunddatei „Kriminalaktennachweis (KAN)“ zu beanstanden war, entschloss ich mich, die Handhabung vor Ort zu kontrollieren. Da die in KAN eingestellten personenbezogenen Daten von allen Polizeien der Länder und des Bundes sowie der Zolldienststellen automatisiert abgerufen werden können, kann die Aufnahme in diese Datei durchaus folgenreich sein. In den beanstandeten Fällen ging es allerdings häufig um Straftaten von eher geringem Unrechtsgehalt, bei denen die KAN-Relevanz zu Unrecht bejaht worden war. Bei der Kontrolle fielen in dieser Hinsicht Ermittlungsverfahren wegen des Verdachts der exhibitionistischen Handlung im Sinne von § 183 StGB auf. Den Grund dafür vermute ich in internen Zielvorgaben des Innenministeriums, die gleich zu mehreren rechtlichen Fehleinschätzungen bei der Behandlung dieser Ermittlungsverfahren verleiten. Beispielsweise sei einer der von uns kontrollierten Fälle genannt, in dem die Polizeidienststelle die Daten

eines Ermittlungsverfahrens wegen des Verdachts einer exhibitionistischen Handlung gemäß § 183 StGB in die bundesweite Datei KAN eingestellt hatte. Das Verfahren war von der Staatsanwaltschaft später nach § 170 Absatz 2 StPO eingestellt worden, weil sich ein für die Anklageerhebung hinreichender Tatverdacht nicht ergeben habe. Außerdem wurde der Beschuldigte von der Polizei erkenndienstlich behandelt; ihm wurde – auf freiwilliger Basis – eine DNA-Speichelprobe entnommen. Sein DNA-Identifizierungsmuster wurde in die DNA-Analyse-Datei eingestellt. Der Fall wurde sowohl in das landesweite Abrufsystem POLAS als auch in die bundesweite KAN-Datei aufgenommen. Als Speicherdauer bis zur Aussonderungsprüfung wurde in der KAN-Datei eine Frist von 10 Jahren, in POLAS sogar eine solche von 20 Jahren festgesetzt.

Die Einstellung in die Verbunddatei KAN hielt ich für unzulässig: Der Straftatbestand des § 183 StGB ist erfüllt, wenn „ein Mann [...] eine andere Person durch eine exhibitionistische Handlung belästigt“. Die maximale Strafdrohung beträgt ein Jahr Freiheitsstrafe. Es handelt sich um ein relatives Antragsdelikt, d. h. es ist nur auf Antrag der belästigten Person verfolgbar, so lange nicht die Staatsanwaltschaft wegen eines besonderen öffentlichen Interesses an der Strafverfolgung eine Verfolgung von Amts wegen für geboten erachtet. Bei dem genannten Beispiel handelte es sich allenfalls um einen Verdacht der exhibitionistischen Handlung von deutlich unterdurchschnittlichem Gewicht, da schon die sexuelle Motivation des Beschuldigten nicht sicher festgestellt werden konnte.

In die Verbunddatei KAN sind aber nach der aufgrund von § 34 des Bundeskriminalamtsgesetzes (BKAG) erlassenen Errichtungsanordnung und den zugehörigen Rahmenrichtlinien für den Kriminalaktennachweis (KAN-Rahmenrichtlinien) nur personenbezogene Daten von Beschuldigten oder Tatverdächtigen bestimmter Ermittlungsverfahren aufzunehmen: Nur Beschuldigte, gegen die wegen des Verdachts schwerer Straftaten oder von Straftaten mit überregionaler Bedeutung ermittelt wurde, und Beschuldigte oder Verurteilte, bei denen aufgrund von § 81g Absatz 1 StPO die Speicherung eines DNA-Identifizierungsmusters in der DNA-Analyse-datei erfolgt ist, sollen hier auftauchen.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Um die Einordnung des Ausgangsfalls bewerten zu können, müssen wir uns daher die Zugangskriterien zur KAN-Relevanz nach den KAN-Rahmenrichtlinien genauer ansehen:

4. Zugangskriterien gemäß der KAN-Rahmenrichtlinien

4.1 Schwere Straftaten

Verbrechen und Vergehen, die in § 100a StPO genannt sind

4.2 Straftaten gemäß § 81g StPO (DNA-Identifizierung)

Straftaten, bei denen gemäß § 81g StPO die Speicherung eines DNA-Identifizierungsmusters in der DNA-Analyse-Datei erfolgt ist [...]

4.3 Sonstige Straftaten mit überregionaler Bedeutsamkeit

Als überregional bedeutsam werden Straftaten eingestuft, wenn Verdacht besteht auf gewohnheits-, gewerbs- oder bandenmäßige Begehung.

Gewohnheitsmäßig handelt, wer durch wiederholte Tatbegehung erkennen lässt, dass eine kriminelle Neigung vorliegt. [...]

Triebtäterschaft, d. h. es liegt eine Triebfähigkeit von solcher Stärke vor, dass der Täter ihr nicht widerstehen kann, unabhängig vom Delikt.

Planmäßige überörtliche Begehung, d. h. wenn nach einer vom Täter oder von anderen Personen entworfenen, nicht unbedingt auf Dauer abgestellten Gesamtvorstellung vorgegangen wird und die Tat außerhalb des Wohn- oder Aufenthaltsortes des Beschuldigten oder Tatverdächtigen begangen wird. [...]

Die Einstufung, ob eine Straftat unter Berücksichtigung der o. a. Kriterien überregional bedeutsam ist, erfolgt nach dem Sachbearbeiterprinzip.

Welches dieser KAN-Zugangskriterien der Sachbearbeiter im jeweiligen Fall angenommen hat, lässt sich leider in Baden-Württemberg der KAN-Datei selbst nicht entnehmen. Zwar sieht Nummer 4 der bundesweiten KAN-Richtlinien vor, dass die jeweils zutreffenden Zugangskriterien anhand der Einzelmerkmale gemäß den Nummern 4.1, 4.2 und 4.3 in der Datei KAN zu dokumentieren sind. Nach den landesspezifischen Ergänzungen hierzu für die Polizei Baden-Württemberg entfällt jedoch diese sinnvolle Dokumentationsverpflichtung „bis zur Einführung eines entsprechenden Datenfeldes“ in der hier verwendeten Software. Daher sind wir bei der Über-

prüfung der vom Sachbearbeiter angenommenen Gründe für die Einstellung in den KAN-Verbund auf eine Einsichtnahme in die Akten und ggf. – falls sich dort kein entsprechender Vermerk findet – sogar auf Vermutungen angewiesen.

Eine exhibitionistische Handlung ist ersichtlich keine schwere Straftat im Sinne von Nummer 4.1 der Rahmenrichtlinien. Im Regelfall wird eine exhibitionistische Handlung aber auch keine Straftat mit überregionaler Bedeutsamkeit im Sinne des Zugangskriteriums Nummer 4.3 der KAN-Rahmenrichtlinie sein. Nur aufgrund besonderer Umstände, die einer sorgfältigen Einzelfallprüfung bedürfen, kann ausnahmsweise eine solche überregionale Bedeutsamkeit angenommen werden. In Betracht kann dies bei exhibitionistischen Handlungen allenfalls unter dem Gesichtspunkt der gewohnheitsmäßigen Begehung, der Triebtäterschaft oder des reisenden Täters kommen. Dabei ist allerdings der geringe Unrechtsgehalt der einzelnen Tat angemessen zu berücksichtigen. Im Allgemeinen wird eine einfache exhibitionistische Handlung ohne weitere Indizien auf wiederholte überörtliche Begehungsweise, besondere Triebtäterschaft oder Neigung zu Gewalt den KAN-Kriterien der überregionalen Bedeutung nicht genügen. In unserem konkreten Fall waren derartige Anhaltspunkte nicht ersichtlich.

Daher blieb nur das Zugangskriterium nach Nummer 4.2 der Richtlinien: Demnach sind auch solche Straftaten KAN-relevant, bei denen gemäß § 81g StPO eine Speicherung des DNA-Identifizierungsmusters in der DNA-Analyse-Datei erfolgt ist oder aufgrund bereits bestehender Speicherung nicht erfolgen konnte, obwohl die Voraussetzungen für eine Speicherung vorgelegen hätten.

Aber waren Voraussetzungen für eine Speicherung nach § 81g StPO tatsächlich gegeben? Diese Vorschrift lautet wie folgt:

§ 81g StPO

(1) Ist der Beschuldigte einer Straftat von erheblicher Bedeutung oder einer Straftat gegen die sexuelle Selbstbestimmung verdächtig, dürfen ihm zur Identitätsfeststellung in künftigen Strafverfahren Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters sowie des Geschlechts

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind. Die wiederholte Begehung sonstiger Straftaten kann im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen. [...]

Die Vorhaltung eines DNA-Profiles zur Aufklärung künftiger Straftaten setzt danach hinreichende Anhaltspunkte dafür voraus, dass der Beschuldigte künftig eine Straftat von erheblicher Bedeutung gemäß § 81 Absatz 1 Satz 1 StPO oder gemäß § 81g Absatz 1 Satz 2 StPO mehrere Straftaten, deren wiederholte Begehung im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen, begehen wird. Eine Straftat von erheblicher Bedeutung ist dabei eine solche, die mindestens dem Bereich der mittleren Kriminalität zuzuordnen ist, den Rechtsfrieden empfindlich stört und geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung empfindlich zu beeinträchtigen. Die Prognose weiterer exhibitionistischer Handlungen reicht dafür regelmäßig nicht aus: Schon angesichts des Strafmaßes von höchstens einem Jahr Freiheitsstrafe kann in der Regel nicht von einem Delikt ausgegangen werden, welches mindestens der mittleren Kriminalität entspricht. Auch genügt die allgemeine kriminalistische Wahrscheinlichkeit von ca. 1–2 Prozent, mit der bei einem exhibitionistischen Straftäter mit einem späteren sexuellen oder sonstigen Gewaltdelikt zu rechnen sein soll, nicht als Indiz für die Prognose weiterer Straftaten von erheblicher Bedeutung.³⁸

Darüber hinaus spricht gegen die Zulässigkeit einer Speicherung des DNA-Profiles, dass nach § 81g Absatz 1 Satz 1 StPO die Feststellung des DNA-Identifizierungsmusters einer Identitätsfeststellung in zukünftigen Strafverfahren voraussichtlich dienlich sein wird, also zur Identifizierung des Täters beiträgt. Dies wird bei Ermittlungsverfahren wegen § 183 StGB regelmäßig nicht der Fall sein, da DNA-

Spuren weder am Opfer noch am Tatort zu erwarten sind.

Die Voraussetzungen des § 81g StPO waren im Beispielsfall daher nicht gegeben. Das war übrigens in einem polizeilichen Aktenvermerk sogar ausdrücklich so festgestellt worden: Daraus ging hervor, dass von einer DNA-Erhebung abzusehen sei, da die rechtlichen Voraussetzungen nicht vorgelegen hätten. Es habe sich nicht um eine Straftat von erheblicher Bedeutung oder eine Straftat gegen die sexuelle Selbstbestimmung gehandelt. Auch sei die Tat keine wiederholt begangene sonstige Straftat gewesen, welche insgesamt genommen im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichgestanden hätte.

Allerdings war dem Beschuldigten bereits vor Anfertigung dieses Vermerks im Rahmen seiner Vernehmung mit seinem Einverständnis eine freiwillige Speichelprobe entnommen worden. Deswegen wurde der Beschuldigte trotz des zitierten Vermerks an die DNA-Analyse-Datei gemeldet. Die Erstellung des DNA-Identifizierungsmusters und dessen Speicherung wurden – im glatten und unaufgelösten Widerspruch zu dem oben wiedergegebenen Vermerk – von der Qualitätsvorprüfung damit begründet, dass eine Straftat gegen die sexuelle Selbstbestimmung vorliege und sich eine Wiederholungsgefahr für eine Straftat von erheblicher Bedeutung aus einem negativen sozialen Umfeld ergebe.

Offensichtlich war daher die Einstellung in die DNA-Analyse-Datei der Grund für die Annahme, die Falldaten seien auch in die KAN-Verbunddatei zu übernehmen. Zur Einstellung in die DNA-Analyse-Datei war es aber gekommen, weil der Beschuldigte freiwillig eine DNA-Probe abgegeben hatte.

Dies führt erneut ein Problem vor Augen, auf das ich bereits im 28. Tätigkeitsbericht 2007 (LT-Drs. 14/2050, S. 28 ff.) hingewiesen habe, dass nämlich die Prüfung der Voraussetzungen für eine Erstellung des DNA-Identifizierungsmusters zur Vorsorge für die Verfolgung künftiger Straftaten oftmals mangelhaft erfolgt. Insbesondere die Möglichkeit der Probenentnahme aufgrund einer Einwilligung des Betroffenen verführt geradezu dazu, die übrigen Tatbestandsvoraussetzungen im Falle der Einwilligung des Betroffenen nicht mehr gründlich zu prüfen. Hinzu kommt, dass die Polizeidienststellen durch

³⁸ LG Bremen, Beschluss vom 23. Oktober 2006 - 11 Qs 318/06; Schmitt in Meyer-Goßner, StPO, 57. Aufl. 2014, § 81g StPO Rn. 7b; Ritzert in Beck'scher-Onlinekommentar zur StPO, Edition 21, Stand 15. Januar 2015, § 81g StPO Rn. 4.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

interne Führungsinstrumente dazu angehalten werden, eine hinreichende Menge an Fällen in die DNA-Analyse-Datei einzustellen: Mittels einer sogenannten „Balanced Scorecard“ wird den regionalen Polizeipräsidien eine Quote für die Entnahme von Speichelproben bei Beschuldigten über 14 Jahren, auch auf freiwilliger Basis, vorgeschrieben, deren Nichteinhaltung entsprechend kritisiert wird. Vor diesem Hintergrund dürften die Dienststellen noch mehr geneigt sein, die Beschuldigten zur freiwilligen Abgabe einer DNA-Probe zu bewegen, allein um die vorgegebenen Quoten zu erfüllen.

Es ist aber festzuhalten, dass tatsächlich die oben beschriebenen rechtlichen Voraussetzungen des § 81g StPO unabdingbar sind: Sie müssen also auch dann vorliegen, wenn der Beschuldigte in die Probenerhebung, Erstellung des DNA-Identifizierungsmusters und dessen Speicherung einwilligt.³⁹ In erfreulicher Deutlichkeit kommt dies in einem Urteil des Verwaltungsgerichts Hannover vom 23. September 2013 (10 A 2028/11, juris) zum Ausdruck:

„Denn die Einwilligung ersetzt zwar gem. § 81 g Abs. 3 Satz 1 und 2 StPO die richterliche Entscheidung bzw. ermöglicht die Anordnung der Entnahme der Körperzellen durch die Staatsanwaltschaft und ihre Ermittlungspersonen auch ohne Gefahr im Verzug. Damit ersetzt sie aber schon nach dem Wortlaut der Vorschrift nur formelle Voraussetzungen, nicht aber auch die tatbestandlichen Anforderungen. Die Bedeutung und die Tragweite der durch eine solche Anordnung betroffenen Grundrechte der körperlichen Unversehrtheit (Art. 2 Abs. 2 GG) und der informationellen Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) gebieten, die Vorschrift insofern restriktiv auszulegen und nicht über ihren Wortlaut hinaus zu dehnen. Insbesondere die Negativprognose ist deshalb eine unverzichtbare Voraussetzung für die Erstellung eines molekulargenetischen Identifizierungsmusters für Zwecke künftiger Strafverfahren [weitere Nachweise]. Auch der Anspruch auf effektiven Rechtsschutz gegenüber der öffentlichen Gewalt aus Art. 19 Abs. 4

GG verbietet es, die Entnahme und molekulargenetische Untersuchung von Körperzellen und die Speicherung des gewonnenen DNA-Identifizierungsmusters allein aufgrund der Einwilligung des Betroffenen als rechtmäßig anzusehen. Denn wenn die richterliche Prüfung der tatbestandlichen Voraussetzungen nach § 81 g Abs. 3 StPO bei einer schriftlichen Einwilligung des Betroffenen unterbleibt, gibt die verwaltungsgerichtliche Prüfung der Speichervoraussetzungen im Rahmen eines Lösungsbegehrens dem Betroffenen die Möglichkeit, noch nachträglich gerichtlichen Rechtsschutz zu erlangen und den mit der Entnahme und Untersuchung von Körperzellen verbundenen Eingriff in seine Grundrechte zwar nicht vollends (dazu BVerfG, Beschluss vom 10.3.2009 – 2 BvR 400/09 –, juris Rn. 10; Beschluss vom 23.1.2013 – 2 BvR 2392/12 –, juris Rn. 10), aber wenigstens weitestmöglich rückgängig machen zu lassen. Wäre dem Verwaltungsgericht infolge der Einwilligung die Prüfung der tatbestandlichen Voraussetzungen verwehrt, liefe auch diese letzte Rechtsschutzmöglichkeit leer.“

Dem ist eigentlich nichts hinzuzufügen! Die Einhaltung dieser gesetzlichen Voraussetzungen muss auch in der Praxis den Vorrang vor ministeriellen Zielvorgaben behalten!

Die Einstellung von Beschuldigten einer exhibitionistischen Handlung in die KAN-Verbunddatei stellt daher nach meinen Feststellungen regelmäßig einen Folgefehler dar, der auf einer unzulässigen Erhebung des DNA-Identifizierungsmusters beruht.

Exkurs: Nur zur Abgrenzung sei klargestellt, dass anders als die Erhebung des DNA-Identifizierungsmusters die Durchführung erkennungsdienstlicher Behandlungen gemäß § 81b StPO bei Ermittlungsverfahren wegen des Verdachts exhibitionistischer Handlungen häufig zulässig sein wird, da hierfür weniger hohe Voraussetzungen vorliegen müssen: Es muss eine Wiederholungsgefahr bestehen und die erhobenen Daten müssen für die Aufklärung der zu erwartenden weiteren Straftaten dienlich sein. Bei exhibitionistischen Handlungen wird sich eine Gefahr der Wiederholung zumindest in Bezug auf weitere exhibitionistische Handlungen begründen lassen, wenn von einer entsprechenden Sexualpräferenz ausgegangen werden kann. Zur Aufklärung weiterer exhibitionistischer Handlungen wird eine

³⁹ vgl. nur Senge in Karlsruher Kommentar zur StPO, 7. Auflage 2013, § 81g StPO Rn. 16 und unseren 28. Tätigkeitsbericht 2007, LT-Drs. 14/2050, S. 30.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

erkennungsdienstliche Behandlung auch mit gewisser Wahrscheinlichkeit dienlich sein, da bei diesem Delikt typischerweise keine Bekanntschaft zwischen Opfer und Täter besteht und für die Identifizierung des Täters z. B. die Vorlage von Lichtbildern erforderlich sein kann. Auch die Verhältnismäßigkeit wird bei einem Ermittlungsverfahren wegen des Verdachts einer exhibitionistischen Handlung gemäß § 183 StGB nicht generell zu beanstanden sein.

Im Beispielsfall – und in den meisten anderen kontrollierten Fällen der Ermittlungen wegen des Verdachts exhibitionistischer Handlungen – wurde eine Speicherdauer in INPOL (KAN) von zehn Jahren und im landesweiten Auskunftssystem POLAS sogar von 20 Jahren festgesetzt.

Abgesehen davon, dass die Aufnahme in die Verbunddatei KAN in diesen Fällen ohnehin schon unzulässig war und regelmäßig einen Folgefehler der unzulässigen Speicherung des DNA-Identifizierungsmusters darstellte, ist darauf hinzuweisen, dass die Festlegung der Speicherfrist eine Entscheidung ist, die anhand der Umstände des Einzelfalls zu treffen ist. So heißt es unter Nummer 8.1.1 der KAN-Errichtungsanordnung (Hervorhebung nicht original):

Nach § 32 Absatz 3 BKAG dürfen Aussonderungsprüffristen ... bei Erwachsenen zehn Jahre und bei Jugendlichen fünf Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist.

Auch die KAN-Rahmenrichtlinien führen hierzu unter Nummer 7 „Prüffristen/Speicherungsdauer“ ausdrücklich aus, dass jede eingebende Stelle für sich im Rahmen einer Einzelfallprüfung die Aussonderungs- und Prüffristen festlegt. Hieraus ergibt sich, dass auch bei Bejahung der KAN-Relevanz nicht gleichsam automatisch die genannten Höchstfristen festzusetzen sind, sondern dass im Einzelfall nach dem Verhältnismäßigkeitsprinzip kürzere Fristen zu bestimmen sind.

Überdies gehen kürzere Überprüfungsfristen nach dem Recht des Landes der für die Datenspeicherung verantwortlichen Dienststelle – mit der Ausnahme aus § 32 Absatz 9 Satz 2, Absatz 7 Satz 3 BKAG – grundsätzlich vor.

Das Gebot der Einzelfallprüfung ergibt sich aber auch noch einmal deutlich aus dem Landesrecht: Für die Speicherdauer nach dem Polizeigesetz ist bei „Straftaten nach dem Dreizehnten Abschnitt des Strafgesetzbuchs“ zwar eine maximale Überprüfungsfrist von 20 Jahren gemäß § 38 Absatz 4 Satz 3 Nummer 1 PolG möglich. Die Maximalfrist setzt aber voraus, dass Anhaltspunkte dafür bestehen, dass die betroffene Person künftig weitere Sexualstraftaten, Menschenhandel oder sexuell motivierte Tötungs- oder Körperverletzungsdelikte begehen wird. Diese Frist wird auch nicht durch § 5 der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes (DVO PolG) modifiziert. Von der 20-Jahre-Frist und der Unanwendbarkeit des § 5 DVO PolG ausgenommen sind die Fälle der §§ 183a, 184, 184d und 184e StGB, nicht aber Fälle des § 183 StGB.

Allerdings ist bei der Speicherung potenzieller Sexualstraftäter im vorgenannten Sinn die Einschränkung aus § 38 Absatz 4 Satz 4 PolG zu beachten: Danach sind für Fälle von Straftaten mit geringer Bedeutung kürzere Fristen festzulegen. In Fällen des Verdachts einer exhibitionistischen Handlung ist – schon angesichts des Strafrahmens und des relativen Antragserfordernisses – eine solche Prüfung stets erforderlich. Dafür spricht auch, dass die nach Tatbestand und Strafdrohung vergleichbare Sexualstraftat des Erregens öffentlichen Ärgernisses aus § 183a StGB von der zwanzigjährigen Höchstfrist des § 38 Absatz 4 Satz 3 PolG ausdrücklich ausgenommen ist mit der Folge, dass diese Ermittlungsverfahren § 5 DVO unterfallen. Dies hat für Ermittlungsverfahren nach § 183a StGB die Folge, dass regelmäßig höchstens fünf Jahre als Speicherfrist festgelegt werden dürfen, in Fällen von geringer Bedeutung sogar nur drei Jahre. Angesichts der Ähnlichkeit der bundesgesetzlich geregelten Strafbarkeitsvoraussetzungen und Rechtsfolgen können auch polizeirechtlich Ermittlungsverfahren wegen des Verdachts einer exhibitionistischen Handlung und der Erregung eines öffentlichen Ärgernisses nicht völlig unterschiedlich behandelt werden. Daher werden auch für Ermittlungsverfahren wegen des Verdachts exhibitionistischer Handlungen über die Regelung in § 38 Absatz 4 Satz 4 PolG die Maßstäbe des § 5 DVO PolG zum Vergleich heranzuziehen sein, so dass entsprechend auch für diese Ermittlungsverfahren regelmäßig für die Speicherung in den Landessystemen eine Frist von höchstens fünf

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Jahren, bei Fällen von geringer Bedeutung sogar nur von drei Jahren festzusetzen sein wird.

Freilich sind die Systeme so eingestellt, dass die Vergabe der jeweils abstrakt-generell zulässigen Höchstfrist vorgeschlagen wird und diese Vorgabe bei Festsetzung einer kürzeren Frist manuell abgeändert werden muss. Bei Speicherungen in der KAN-Datei ist demgemäß bei Erwachsenen eine Speicherdauer von zehn Jahren voreingestellt. Und auch bei Speicherungen in POLAS werden nach Nummer 13.4 der Dienstanweisung POLAS-BW (Stand: 01/2014) Standardlaufzeiten vorgegeben, die zwar manuell überschrieben werden können, aber in der Praxis häufig ohne Einzelfallprüfung übernommen werden. Als Standard-Laufzeit ist bei Sexualdelikten mit KAN-Relevanz – unter die aus den genannten Gründen auch die exhibitionistische Handlung oft fehlerhaft subsumiert wird – eine Frist sogar von 240 Monaten vorgesehen.

Die systemseitige Vorgabe der jeweiligen Höchstfrist verleitet mithin dazu, die Einzelfallprüfung zu vernachlässigen und jeweils die Höchstfrist für das Aussonderungsprüfdatum vorzusehen.

Was ist das Fazit? Bei den überprüften Ermittlungsverfahren wegen des Verdachts der exhibitionistischen Handlung ließ sich nahezu durchgängig die tatsächlich bejahte KAN-Relevanz rechtlich nicht begründen, wobei die mangelnde Dokumentation der Zugangskriterien im Landessystem die Prüfung noch erschwerte. Für die Annahme einer überregionalen Bedeutung im Sinn der KAN-Rahmenrichtlinie Nummer 4.3 ließen sich hinreichende Anhaltspunkte regelmäßig nicht ausmachen. Vielfach wurden zu Unrecht DNA-Identifizierungsmuster nach § 81g StPO erhoben, und zwar typischerweise nicht aufgrund eines richterlichen Beschlusses, sondern auf Basis einer Einwilligung, die gleichwohl die DNA-Speicherung nicht rechtfertigte. Als Ursache für diese Neigung, auch bei dem Verdacht exhibitionistischer Handlungen trotz fehlender rechtlicher Voraussetzungen DNA-Identifizierungsmuster auf Basis einer Einwilligung einzuholen, vermute ich die Zielvorgabe des Innenministeriums durch eine „Balanced Scorecard“. Mutmaßlich aufgrund der Einholung des DNA-Identifizierungsmusters wurden die Fälle der exhibitionistischen Handlung – gleichsam als Folgefehler – auch als KAN-relevant eingestuft. Dabei wurde für die Speicherung in der Ver-

bunddatei zudem aufgrund der systemseitigen Voreinstellungen – ohne ausreichende Prüfung der Verhältnismäßigkeit im Einzelfall – eine zehnjährige Prüfungsfrist vergeben. Noch dramatischer wirkten sich die systemseitigen Voreinstellungen für die Speicherung in Landessystem POLAS-BW aus, indem hier die vorgegebene zwanzigjährige Frist übernommen wurde, obwohl bei zutreffender Prüfung nach § 38 Absatz 4 Satz 4 PolG höchstens eine fünfjährige, in Fällen von geringer Bedeutung sogar nur eine dreijährige Frist hätte bestimmt werden müssen.

Daher sehe ich bei der Datenspeicherung von Ermittlungsverfahren wegen des Verdachts der exhibitionistischen Handlungen gemäß § 183 StGB folgenden Handlungsbedarf:

- 1. Delikte nach § 183 StGB sind wegen Ihrer Vergleichbarkeit mit Straftaten nach 183a StGB als Straftaten von geringer Bedeutung gemäß § 38 Absatz 4 Satz 4 PolG zu behandeln, weshalb verkürzte Speicherfristen für den Datenbestand in POLAS von drei oder fünf Jahren festzulegen sind.*
- 2. Um bei zukünftigen datenschutzrechtlichen Kontrollen des KAN-Datenbestandes nicht mehr auf Mutmaßungen angewiesen zu sein, ist die systemseitige, verpflichtende Dokumentation der Zugangskriterien für den KAN in Baden-Württemberg einzuführen.*
- 3. Da im Regelfall eine einfache exhibitionistische Handlung ohne weitere Indizien auf wiederholte überörtliche Begehungsweise, besondere Triebtäterschaft oder Neigung zu Gewalt im Allgemeinen den KAN-Kriterien nicht genügt, sind Ermittlungsverfahren wegen § 183 StGB, die als KAN-relevant eingestuft wurden, von den verantwortlichen Stellen systematisch zu überprüfen.*
- 4. Die Vorhaltung eines DNA-Profiles gemäß § 81g StPO bei Beschuldigten, gegen die ausschließlich wegen des Verdachts der exhibitionistischen Handlungen ermittelt wird, halte ich regelmäßig für rechtswidrig und sehe einen Zusammenhang mit der Zielvorgabe der „Balanced Scorecard“, die für die regionalen Polizeipräsidien eine Quote für die Entnahme von Speicherproben bei Beschuldigten über 14 Jahren, auch auf freiwilliger Basis, vorsieht. Daher halte ich eine Überprüfung dieses Führungsinstru-*

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

ments und seiner Umsetzung für dringend geboten.

5. *Es ist sicherzustellen, dass bei der Festsetzung von Aussonderungsprüffristen eine individuelle fallbezogene Einzelfallprüfung stattfindet und nicht aufgrund der systemseitigen Voreinstellungen gleichsam automatisch die jeweiligen Höchstfristen übernommen werden.*

2.2.5 Steht der Datenschutz sich selbst im Wege?

Mitunter kann der Eindruck entstehen, dass Vorschriften, die das informationelle Selbstbestimmungsrecht sicherstellen sollen, das Gegenteil bewirken. So in einem Fall, mit dem sich meine Dienststelle zu befassen hatte.

Ein Bürger fragte bei der Polizei nach, was sie über ihn in ihren polizeilichen Systemen speichere. In der Antwort erfuhr er, dass er im Computergestützten Vorgangsbearbeitungssystem der Polizei namens ComVor u. a. als Beschuldigter im Zusammenhang mit einem Verstoß gegen das Kraftfahrzeugsteuergesetz (KraftStG) gespeichert sei (zu ComVor siehe auch 29. Tätigkeitsbericht 2008/2009, LT-Drs 14/5500, S. 138 f.). Zugrunde lag dem, dass der Betroffene ein mit einem roten Kennzeichen versehenes Kraftfahrzeug entgegen § 16 der Fahrzeug-Zulassungsverordnung (FZV) geführt hatte. Dabei war er von einer Polizeistreife erwischt worden.

Grundsätzlich müssen Kraftfahrzeuge, wenn sie im öffentlichen Verkehrsraum in Betrieb genommen werden, zum Verkehr zugelassen sein (§ 3 Absatz 1 FZV). Eine Ausnahme von dieser Regel enthält § 16 Absatz 1 FZV. Danach dürfen auch nicht zum Verkehr zugelassene Fahrzeuge zu Prüfungs-, Probe- und Überführungsfahrten in Betrieb gesetzt werden, wenn sie entweder ein sogenanntes Kurzzeitkennzeichen oder ein Kennzeichen mit roter Beschriftung auf weißem rot gerandetem Grund (rotes Kennzeichen) führen.

Nachdem die Polizei das Strafverfahren zunächst eingeleitet und einen entsprechenden Vorgang in ComVor angelegt hatte, gab sie es mit Blick darauf, dass es sich um eine Steuerstraftat gem. § 370 Absatz 1 Nummer 2 der Abgabenordnung (AO) i. V. mit § 1 Absatz 1 Nummer 3 und § 2 Absatz 5 Satz 1 KraftStG handelte, an das zuständige Finanzamt ab.

Denn nach § 386 Absatz 1 Satz 1 AO ermittelt beim Verdacht einer Steuerstraftat nicht die Polizei, sondern die Finanzbehörde den Sachverhalt. In ComVor blieb der Vorgang aber weiter gespeichert und sollte erst nach fünf Jahren gelöscht werden.

Die Speicherung von Daten über Ermittlungsverfahren in ComVor dient der Durchführung des Strafverfahrens und der Vorgangsverwaltung. Daher dürfen Vorgänge in ComVor höchstens so lange gespeichert bleiben, bis das betroffene Delikt verjährt ist. Die Fristen für die Verfolgungsverjährung der einzelnen Straftaten sind in ComVor systemseitig eingearbeitet. Spätestens mit Erreichen der Verfolgungsverjährung werden die Vorgänge automatisiert gelöscht, weil die Daten dann weder für die Durchführung des Strafverfahrens noch für die Vorgangsverwaltung weiter erforderlich sind. Allerdings wurde auch eine Funktion geschaffen, um personenbezogene Daten in Vorgängen manuell zu löschen, wenn deren Speicherung bereits vor Erreichen der Verfolgungsverjährung nicht mehr erforderlich ist. Dies ist vor allem dann der Fall, wenn nach rechtskräftigem Abschluss eine Mitteilung über den Ausgang des Strafverfahrens (MAV) eingeht. Nach § 482 Absatz 2 StPO i.V. mit Nummer 11 der Anordnung über die Mitteilung in Strafsachen (MiStrA) ist die Staatsanwaltschaft verpflichtet, die Polizei in Bezug auf den Ausgang des Verfahrens zu unterrichten. In diesen Fällen ist der Speicherzweck „Vorgangsbearbeitung“ entfallen und der Sachbearbeiter muss den „Löschbutton“ betätigen.

Im oben geschilderten Fall lag die Verjährungsfrist gem. § 369 Absatz 2, § 370 Absatz 1 AO i.V. mit § 78 Absatz 3 Nummer 4 StGB bei fünf Jahren. Insofern entsprach die in ComVor festgelegte Überprüfungsfrist den für ComVor festgelegten Löschrufen. Der Punkt war nun der, dass die Polizei keine Chance hatte zu erfahren, ob und ggf. wann und mit welchem Ergebnis das Verfahren rechtskräftig abgeschlossen wurde. Denn die Finanzbehörden weigern sich unter Berufung auf das Steuergeheimnis nach § 30 Absatz 1 AO mit Recht, die Polizei über den Ausgang der bei ihnen geführten Steuerstrafverfahren zu informieren. Eine Mitteilungspflicht gegenüber der Polizei, wie sie für die Staatsanwaltschaft gilt, besteht für die Finanzbehörden nicht. Kann es nun sein, dass das Steuergeheimnis, das ja gerade (auch) den Schutz des informationellen Selbstbestimmungsrechts bezweckt, hier verhindert,

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

dass Daten in polizeilichen Systemen vor Ablauf der Verjährungsfrist gelöscht werden? Die Polizei hatte sich zunächst auf diesen Standpunkt gestellt.

Der Widerspruch ist allerdings nur ein scheinbarer. Denn auch ohne eine Mitteilung über den Ausgang eines Steuerstrafverfahrens ist die Polizei nicht nur nicht gehindert, persönliche Daten von Beschuldigten aus ihrem Vorgangsbearbeitungssystem zu löschen, sie ist sogar dazu verpflichtet! Eigentlich muss sie nur das zu ComVor erarbeitete Fachkonzept Datenschutz konsequent anwenden. Denn dieses sieht eine manuelle Löschung der Daten vor Ablauf der Verjährungsfrist des zugrunde liegenden Delikts allgemein dann vor, *wenn die Speicherung nicht mehr erforderlich ist*. Der Eingang einer MAV ist diesbezüglich nur als Regelbeispiel genannt. Nicht mehr erforderlich ist eine weitere Speicherung aber immer auch und gerade dann, wenn eine Mitteilung über den Verfahrensabschluss nicht mehr zu erwarten ist, weil die speichernde Polizeidienststelle mit Abgabe des Verfahrens auch die Zuständigkeit hierfür verliert. Steuerstraftaten sind nur ein Beispiel hierfür. Weitere Beispiele hierfür sind die Abgabe an die Bundespolizei in den Fällen des § 12 des Bundespolizeigesetzes, an die Zollverwaltung in den Fällen des § 14 des Schwarzarbeitsbekämpfungsgesetzes oder an sonstige außerpolizeiliche Ermittlungspersonen der Staatsanwaltschaft (vgl. § 152 des Gerichtsverfassungsgesetzes und die hierzu ergangene Verordnung der Landesregierung über die Ermittlungspersonen der Staatsanwaltschaft), sofern diese (ausnahmsweise) die Endsachbearbeitung vornehmen. Gleiches gilt bei der Abgabe wegen örtlicher Unzuständigkeit an eine Polizeidienststelle außerhalb des Landes (bei Abgaben innerhalb der Landespolizei übernimmt dagegen die neu zuständige Polizeidienststelle die Bearbeitung in ComVor).

Dem im Ausgangsfall zuständigen Polizeipräsidium habe ich demzufolge geraten, den Vorgang aus ComVor zu löschen, was dieses dann auch anstandslos tat, zumal die Mindestspeicherdauer von zwölf Monaten bereits abgelaufen war.

Der Grundsatz der Erforderlichkeit als zeitliche Grenze für das Vorhalten von Daten im Vorgangsbearbeitungssystem der Polizei ComVor verbietet ein schematisches Vorgehen. Immer dann, wenn

aufgrund der Besonderheiten des Einzelfalls nicht damit zu rechnen ist, dass die Polizei eine Mitteilung über den Verfahrensausgang erhält, ist zu prüfen, ob der Vorgang vor Ablauf der im System hinterlegten Lösungsfristen manuell zu löschen ist.

2.2.6 Ende gut, alles gut?

Im 29. Tätigkeitsbericht 2009 (LT-Drs. 14/5500 S. 37) und im 30. Tätigkeitsbericht 2010/2011 (LT-Drs. 15/955 S. 62) hatte ich meine grundsätzlichen Bedenken gegen die sog. Prüffallregelung des § 38 Absatz 2 des Polizeigesetzes (PolG) dargestellt. Die reine Verdachtsspeicherung für bis zu zwei Jahre ohne eine Prognose zur Wiederholungsgefahr führt immer wieder zu Ergebnissen, die selbst wohlmeinende Vertreter einer harten Haltung auch bei Bagatelldelikten ins Grübeln kommen lassen müssen. Folgender Fall, mit dem sich meine Mitarbeiter befassen mussten, mag als Beispiel hierfür gelten:

Einem jungen Mann war vorgeworfen worden, zu später Stunde einen Sonnenschirm im Außenbereich einer Gaststätte umgestoßen und damit eine Sachbeschädigung begangen zu haben. Ein Nachbar gab an, den Betroffenen als Täter wiedererkannt zu haben. Gegenüber der Polizei benannte der Betroffene dagegen drei Personen, die bezeugen könnten, dass er sich zu keiner Zeit an dem Tatort aufgehalten habe. Dem ging die Polizei allerdings nicht nach und legte den Vorgang der Staatsanwaltschaft vor. Diese stellte postwendend das Verfahren nach § 170 Absatz 2 StPO unter Verweis auf den Privatklageweg ein. Auf einen Antrag, die über ihn im polizeilichen Auskunftssystem POLAS gespeicherten Daten zu löschen, teilte die Polizei dem Betroffenen mit, einer Löschung stehe § 38 Absatz 2 PolG entgegen. Es bestehe trotz Verfahrenseinstellung durch die Staatsanwaltschaft ein Resttatverdacht, der die Datenspeicherung für einen Zeitraum bis zu zwei Jahren rechtfertige.

Nachdem mich der Betroffene um Unterstützung seines Antrags auf Datenlöschung gebeten hatte, wandte ich mich an die zuständige Polizeidienststelle. In meiner Bitte um Stellungnahme räumte ich ein, dass eine Speicherung personenbezogener Daten zur vorbeugenden Straftatenbekämpfung nach § 38 Absatz 2 PolG zwar grundsätzlich zulässig sei, wenn sich im Falle einer Verfahrenseinstellung

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

durch die Staatsanwaltschaft aus den Gründen der Einstellungsverfügung nicht positiv ergebe, dass die Einstellung deshalb erfolgt sei, weil der Betroffene die Tat nicht oder nicht rechtswidrig begangen habe. Allerdings wies ich deutlich darauf hin, dass letztlich allein die Polizei die datenschutzrechtliche Verantwortung für die in ihrem polizeilichen Informationssystem gespeicherten Daten trage. Im Zweifel sei sie gehalten, die Einstellungsverfügung der Staatsanwaltschaft zu hinterfragen, bevor sie über die weitere Speicherung entscheide (so: Bundesverwaltungsgericht, BVerwGE 137, S. 113–123). Die eigenverantwortliche und kritische Prüfung, ob personenbezogene Daten bei einer Verfahrenseinstellung weiter gespeichert werden sollen, ist aus meiner Sicht vor allem in Ermittlungsverfahren wegen Bagatelldelikten notwendig. In diesen Fällen erfolgt die Verfahrenseinstellung vielfach allein unter Berufung auf ein mangelndes öffentliches Interesse, ohne dass der Frage, ob der Beschuldigte überhaupt als Täter in Frage kommen kann, auch nur ansatzweise nachgegangen wurde. Gerade in solchen Fällen, in denen eine Person allein deshalb als sog. „Prüfball“ quasi auf Vorrat gespeichert wird, weil sie eine Straftat lediglich begangen haben *könnte*, wird die Verfassungsmäßigkeit des § 38 Absatz 2 PolG auch in der Literatur zu Recht in Zweifel gezogen.⁴⁰

Auf die Bitte, die drei angebotenen Alibizeugen, von denen die Staatsanwaltschaft bei ihrer Entscheidung keine Kenntnis gehabt hatte, zu vernehmen und auf der Grundlage der hierdurch gewonnen Erkenntnisse erneut zu prüfen, ob sich ein Resttatverdacht tatsächlich begründen lasse, verwies die Polizeidienststelle zunächst auf eine – mir im Übrigen nicht bekannte – Dienstanweisung, die besage, dass an sich allein die Einstellungsverfügung der Staatsanwaltschaft ausreiche, um den für die Speicherung ausreichenden Tatverdacht zu begründen. Man habe insoweit keinen Ermessenspielraum. Sollte ich dies anders sehen, werde um eine entsprechende Mitteilung gebeten. Eine Antwort hierauf konnte ich mir dann doch nicht verkneifen. Denn die Frage, ob eine Datenspeicherung zur vorbeugenden Straftatenbekämpfung erforderlich ist, ist keine Frage des Ermessens, sondern eine Sachfrage, nämlich ob ein Resttatverdacht besteht oder nicht. Dies hat die Polizei eigenverantwortlich zu prüfen und in

der Folge auch die datenschutzrechtliche Verantwortung zu übernehmen, wenn sie personenbezogene Daten in ihren polizeilichen Systemen speichert. Nachdem ich insoweit insistiert hatte, schrieb die Polizeidienststelle abschließend, aufgrund der Widersprüche der Zeugenaussagen habe man, dem Grundsatz „in dubio pro reo“ folgend, die Löschung der Daten des Betroffenen veranlasst. Warum nicht gleich so? Was bleibt, ist die sicher nicht unbegründete Vermutung, dass in den polizeilichen Dateien noch viele ähnlich gelagerte Fälle schlummern. Es ist zu wünschen, dass die Polizei, vor allem auch in Fällen, in denen das Verfahren unter Verweis auf die Privatklage eingestellt wird, sich ihre eigene datenschutzrechtliche Verantwortung stärker ins Bewusstsein ruft und nicht schematisch alle Fälle über einen Kamm schert. Nötig ist vielmehr ein verantwortungsbewusster, auf die Umstände des Einzelfalls bezogener Umgang mit den Speicherbefugnissen, die für die Betroffenen immer einen gravierenden Eingriff in ihre Freiheitsrechte bedeuten.

Die Verfahrenseinstellung durch die Staatsanwaltschaft nach § 170 Absatz 2 StPO aufgrund mangelnden öffentlichen Interesses oder eines Verfahrenshindernisses enthebt die Polizei nicht ihrer Verpflichtung zur Prüfung des Resttatverdachts als Voraussetzung für die weitere Speicherung.

2.2.7 Warum darf die Polizei die Daten von Fußballfans in verschiedenen Sportdateien speichern?

Nach gewaltsamen Ausschreitungen speichert die Polizei Baden-Württemberg Daten von Teilnehmern an diesen Ausschreitungen in verschiedenen Dateien des Landes und des Bundes. Eine solche Datenspeicherung erfolgt nicht nur dann, wenn strafrechtliche Ermittlungen eingeleitet werden, sondern auch bei polizeirechtlichen Maßnahmen, wie beispielsweise bei Platzverweisen oder Gewahrsamsnahmen.

Für Baden-Württemberg werden Erkenntnisse aus der gewaltgeneigten Sportszene, insbesondere aus dem Bereich Fußball, in der „Arbeitsdatei Szenekundige Beamte“ (SKB-Datenbank) zusammengeführt. Sie ermöglicht die Dokumentation fantypischer Verhaltensweisen auch unterhalb der Schwelle bedeutender Ordnungswidrigkeiten. Damit dient diese

⁴⁰ vgl. insbesondere Belz/Mußmann, Polizeigesetz, 7. Auflage 2009, § 38 Rn. 17

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

der Polizei als Grundlage für die Beantragung und den Erlass von verwaltungsgerichtlich überprüfbar, präventivpolizeilichen Maßnahmen, die gewalttätige Auseinandersetzungen bei oder im Zusammenhang mit Sportveranstaltungen verhindern sollen.

Die SKB-Datenbank wird von den sog. „Szenekundigen Beamten“ geführt. Szenekundige Beamte sind dauerhaft eingerichtete Organisationseinheiten bei den Polizeipräsidien in Baden-Württemberg, in deren Zuständigkeitsbereich ein Sportverein mit einer zur Gewalt bereiten bzw. Gewalt suchenden Problemfanzene ansässig ist. Das Aufgabenspektrum der SKB-Beamten umfasst neben der Durchführung von Ermittlungsverfahren gegen Fans auch jede Art der Erkenntnisgewinnung über aktuelle Entwicklungen in den Fanszenen beispielsweise dadurch, dass die Beamten bei den Spielen selbst im Stadion sind und den ständigen Kontakt mit dem Verein, den Ordnungsdiensten und Fanbetreuern halten.

Bei der auf Bundesebene eingerichtete Verbunddatei „Gewalttäter Sport“ liegt die Schwelle für die Datenspeicherung höher: hier werden im Wesentlichen eingeleitete bzw. abgeschlossene Ermittlungsverfahren, die im Zusammenhang mit Sportveranstaltungen stehen, sowie bestimmte Verstöße gegen das Versammlungsgesetz, das Waffengesetz sowie das Sprengstoffgesetz erfasst. Personenfeststellungen, Platzverweise und Gewahrsamnahmen werden nur dann gespeichert, wenn Tatsachen die Annahme rechtfertigen, dass die Betroffenen anlassbezogene Straftaten von erheblicher Bedeutung begehen werden. Ist ein Erwachsener oder Jugendlicher erstmalig in der Datei „Gewalttäter Sport“ gespeichert, erfolgt im Regelfall frühestens nach fünf Jahren eine Überprüfung, ob die Daten ausgesondert werden können.

Die in der SKB-Datenbank gelisteten Personen, die als „aktive“ Fans mit Potenzial für Ausschreitungen eingestuft werden, können grundsätzlich ebenfalls für fünf Jahre gespeichert werden.

Zusammen mit gewonnenen Erkenntnissen werden in der SKB-Datenbank verschiedene Statusbezeichnungen für die Fans vergeben, die verschieden lange Speicherfristen nach sich ziehen. Beispielsweise wird für einen Erwachsenen, der als „Tatverdächtiger“ einer Straftat gilt, eine fünfjährige Speicherfrist gem. § 38 Absatz 2 und 3 PolG vergeben, während für eine erwachsene Person, die i.S. der

§§ 6 und 7 PolG als potentieller Störer bei Fußballspielen eingeschätzt wird, eine dreijährige Speicherfrist vergeben wird. Im Ergebnis werden in der Datenbank personenbezogene Gefahrenprognosen gespeichert. Des Weiteren wird die SKB-Datenbank jährlich zum Ende der Fußball-Bundesligasaison überprüft. Wird eine Person über einen Zeitraum von zwei Jahren in der Datenbank als „inaktiv“ geführt, so werden deren Daten auch vor Ablauf der genannten fünf Jahre gelöscht. Die Entscheidung über eine Löschung von Daten obliegt dabei der datenschutzrechtlich verantwortlichen Polizeidienststelle.

Damit die Polizei ihre Pflicht zur „Datenpflege“ wahrnehmen kann, müssen ihr die dafür relevanten Informationen zugehen. Wenn nun eine Person in der jährlich überprüften SKB-Datenbank gelöscht wird, stellt dies eine relevante Information für die Prüfung der weiteren Speicherung in der Verbunddatei „Gewalttäter Sport“ dar.

Hier setzt meine datenschutzrechtliche Kritik an: Es gibt derzeit keine Verpflichtung, dass die Information über die Löschung einer Person in der SKB-Datenbank des Landes an die zuständige Stelle für die Speicherung in der auf Bundesebene betriebenen Verbunddatei „Gewalttäter Sport“ weitergeleitet wird, falls die Person in dieser Datei noch gespeichert sein sollte. Weshalb diese Unterrichtung bisher nicht erfolgt, hat einen einfachen Grund: Die Speicherung in der Datei „Gewalttäter Sport“ erfolgt nach dem sog. „Tatort-Prinzip“, d. h. dort, wo es zu den gewaltsamen Ausschreitungen kommt, wird die zuständige Polizeidienststelle die Fandaten in die Verbunddatei eingeben und ist damit die „verantwortliche Stelle“. Dies kann aber eine Dienststelle sein, die nicht den Heimatverein des jeweiligen Fans betreut und kann natürlich auch außerhalb von Baden-Württemberg liegen.

Zur Veranschaulichung möchte ich das Beispiel eines Petenten aus Stuttgart anführen, der zusammen mit 162 weiteren Fans vor der Bundesligabegegnung der Fußballclubs „Karlsruher SC“ und „VfB Stuttgart“ am 1. März 2009 in Karlsruhe in Gewahrsam genommen worden war. Die formelle Rechtmäßigkeit der Maßnahme wurde durch das Verwaltungsgericht Karlsruhe mit Urteil vom 11. Oktober 2011 bestätigt. Damit war auch die Eingabe seiner personenbezogenen Daten sowohl in die SKB-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Datenbank durch das Polizeipräsidium Stuttgart als auch in die Verbunddatei „Gewalttäter Sport“ durch das Polizeipräsidium Karlsruhe zunächst zulässig. Bereits in der Fußballsaison 2010/2011 wurde der nicht wieder auffällig gewordene Petent mit dem Status „inaktiv“ in der SKB-Datenbank geführt und dann mit Ende der Saison durch das Polizeipräsidium Stuttgart dort gelöscht. Über die Löschung wurde das Polizeipräsidium Karlsruhe, als für den Eintrag in der Verbunddatei verantwortliche Stelle, nicht informiert. Erst auf ein im Jahr 2013 an das Polizeipräsidium Karlsruhe gerichtetes Auskunftersuchen bezüglich der Datenspeicherung in der Verbunddatei „Gewalttäter Sport“ hin wurden die Daten des Petenten auch dort gelöscht. Mit der Löschung in der SKB-Datenbank war hier die weitere Speicherung des Petenten in der Verbunddatei entbehrlich geworden. Dennoch blieb der Petent noch über ein Jahr nach der Löschung in der SKB-Datenbank in der bundesweiten Verbunddatei gespeichert.

Bei vergleichbaren Fällen haben meine Mitarbeiter – nachdem sie die Auskunft erhalten haben, dass der Petent aus der SKB-Datenbank gelöscht wurde – die für die Speicherung der Person in der Datei „Gewalttäter Sport“ zuständige Polizeidienststelle hierüber unterrichtet. Dies war stets der Anlass für die Löschung der Person in der Verbunddatei.

Für meine Position wird mir seitens des Innenministeriums Baden-Württemberg grundsätzlich Verständnis entgegengebracht. Derzeit bemüht sich eine vom „Unterausschuss Führung, Einsatz und Kriminalitätsbekämpfung“ (UA FEK) eingesetzte Bund-Länder-Arbeitsgruppe der Innenministerkonferenz um Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei „Gewalttäter Sport“ und damit um eine Neuausrichtung dieser Verbunddatei. In dieser Arbeitsgruppe wurde ein Wechsel vom „Tatortprinzip“ zum „Vereinsortprinzip“ bei der Datenerfassung diskutiert und zunächst fachlich favorisiert. Gegenstimmen sprechen sich aber für die Beibehaltung des Tatortprinzips aus und machen dafür anderweitige, rechtliche Gründe geltend. Eine abschließende Entscheidung wurde noch nicht getroffen, allerdings scheint es für einen Wechsel zu einem anderen Datenerfassungsprinzip derzeit keine Mehrheit zu geben.

Auch wenn mein Anliegen von der Polizei Baden-Württemberg erfreulicherweise positiv aufgenommen

men und vom Innenministerium auf der Arbeitstagung der Polizeiführer und Szenekundigen Beamten weitergegeben wurde, bleibt doch das Bedauern, dass sich an dem Problem im Ergebnis wenig ändert.

Jedenfalls soweit es die polizeilichen Dienststellen im Lande in der Hand haben, sollte mit der Prüfung des Datenbestandes in der SKB-Datenbank auch eine Prüfung der Erforderlichkeit der weiteren Datenspeicherung in der Verbunddatei „Gewalttäter Sport“ einhergehen und gegebenenfalls die Löschung der dortigen Daten veranlasst werden.

2.2.8 Stadionverbote – Was passiert, wenn die Polizei sich geirrt hat?

Stadionverbote werden oft dann gegen Fans erlassen, wenn die Polizei dem Stadionbetreiber bzw. dem Sportverein mitteilt, dass gegen die betroffene Person strafrechtlich ermittelt wird, beispielsweise wegen des Verdachts des Landfriedensbruchs. Mitunter handelt es sich dabei aber um Tatvorwürfe, die vom Beschuldigten bestritten werden oder aber bei denen das Strafverfahren später von der Staatsanwaltschaft eingestellt wird. So nimmt es nicht Wunder, dass sich wegen solcher Datenübermittlungen durch die Polizei an private Stellen schon viele Fußballfans an mich gewandt haben.

Kommt es vor, während oder nach einer Sportveranstaltung zu Ausschreitungen innerhalb oder außerhalb der Platzes bzw. der Halle, übermittelt die Polizei, dort im Regelfall die sog. „Szenekundigen Beamten“, die in diesem Zusammenhang erhobenen personenbezogenen Daten regelmäßig an die Stadionbetreiber bzw. Sportvereine. Nur in wenigen Fällen, so zum Beispiel bei Vorfällen im Fanreiseverkehr, werden die Daten über die Landesinformationsstelle Sparteinsätze beim Innenministerium Baden-Württemberg (LIS) an die Zentrale Informationsstelle Sparteinsätze im Bund (ZIS) übermittelt. Von dort werden die Daten unter bestimmten Voraussetzungen an den Deutschen Fußball-Bund (DFB) bzw. an die Deutsche Fußball Liga (DFL) weitergesteuert.

Das Aufgabenspektrum der Szenekundigen Beamten wird durch eine Dienstanweisung des Innenministeriums Baden-Württemberg festgelegt. Davon umfasst sind u. a. „die anlassbezogene Initiierung sowie Überwachung der Einhaltung von örtlichen, ligaweiten und bundesweit wirksamen Stadionver-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

boten im Zusammenarbeit mit den Sicherheitsbeauftragten der Vereine sowie den zuständigen Sport-Verbänden unter Beteiligung der Landesinformationsstelle für Sporeinsätze Baden-Württemberg“. In den von meiner Dienststelle geprüften Fällen wurden Stadionverbote vor allem dann veranlasst, wenn Ermittlungsverfahren gegen die Petenten eingeleitet worden waren.

Grundsätzlich ist der Polizeivollzugsdienst nach § 44 Absatz 1 Nummer 2 PolG ermächtigt, personenbezogene Daten an die Stadionbetreiber zu übermitteln:

§ 44
Datenübermittlung an Personen oder Stellen
außerhalb des öffentlichen Bereichs

(1) Die Polizei kann von sich aus personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies erforderlich ist

[...]

2. zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl ...

Der private Empfänger, also der Stadionbetreiber und dessen Sicherheitsdienst, soll mit Hilfe der übermittelten Daten befähigt werden, effektiv Maßnahmen zur Beseitigung erheblicher Gefahren für das Gemeinwohl treffen zu können, so z. B. durch Stadionverbote. Wenn – wie bei den gewaltsamen Auseinandersetzungen zwischen Fußballfans und der Polizei oder verschiedenen Fanggruppierungen untereinander – eine unbestimmte Zahl von Betroffenen der Gefahr von Körperverletzungsdelikten ausgesetzt ist oder Einrichtungen in Stadien durch Vandalismus bedroht sind, ist diese erhebliche Gefahr für das Gemeinwohl gegeben.

Allerdings bat ich das Innenministerium Baden-Württemberg um Abhilfe, als mich die Eingabe eines Fußballfans auf zwei grundlegende Probleme bei der Datenübermittlung durch die Polizei aufmerksam machte:

Ein Petent war im Oktober 2011 zusammen mit 56 weiteren Fußballfans in einem Reisebus zu einem Spiel in Fürth unterwegs, als die Gruppe auf einer Autobahnrastanlage auf einen Bus mit 47 Fußball-

fans einer anderen – in der Sprache der Fans „verfeindeten“ – Fanggruppierung traf. Ein Teil der Fanggruppe, mit der der Petent unterwegs war, verhielt sich sofort aggressiv und drang in den anderen Bus ein. Es kam zu Körperverletzungen und es wurden Fanartikel, sog. „Trophäen“, entwendet. Noch am gleichen Tag nahm die zuständige Kriminalpolizei die Ermittlungen auf.

Im Dezember 2011 wurde dem Petenten vom DFB mitgeteilt, dass gegen ihn ein bundesweites Stadionverbot erlassen worden sei, da ein Ermittlungsverfahren wegen Landfriedensbruch, Körperverletzung und Raub gegen ihn geführt werde.

Als der Petent daraufhin bei der zuständigen Polizeidienststelle Auskunft über die ihn betreffende Datenverarbeitung verlangte, wurde ihm mitgeteilt, dass er in dem Ermittlungsverfahren als „Zeuge“ geführt werde und keine Daten zu ihm im Auskunftssystem der Polizei Baden-Württemberg (POLAS) gespeichert würden. Nicht mitgeteilt wurde ihm hingegen, dass die Polizeidienststelle bereits im Oktober 2011 der ZIS bzw. dem DFB die personenbezogenen Daten aller an dieser sog. „Drittortauseinandersetzung“ beteiligten Personen (nebst Sachverhalt) übermittelt hatte. Hier waren die ZIS bzw. der DFB die Empfänger, da es sich um ein Vorkommnis auf dem Reiseweg der Fans gehandelt hatte. Letzteres hätte ihm aber nach der für die Erteilung der Auskunft maßgeblichen Bestimmung in § 21 Absatz 1 Nummer 1 und Nr. 3 LDSG gesagt werden müssen. Die Vorschrift hat folgenden Wortlaut:

§ 21
Auskunft

(1) Dem Betroffenen ist von der speichernden Stelle auf Antrag unentgeltlich Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,

[...]

3. [...] die Empfänger oder Gruppen von Empfängern, an die die Daten übermittelt werden sollen.

Aber nicht nur das. Im vorliegenden Fall musste die Tatbeteiligung von knapp 100 Personen, die sich zufälligerweise auf einer Raststätte getroffen hatten, in Zusammenarbeit mit drei Polizeidienststellen aus zwei Bundesländern geklärt werden. Daher dauer-

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

ten die Ermittlungen an, was grundsätzlich nachvollziehbar ist. Erst nach einer Reihe von Zeugenbefragungen wurde klar, dass der Tatverdacht wegen Landfriedensbruch gegen den Petenten keinen Bestand hatte. Damit änderte sich sein Status im Ermittlungsverfahren von dem eines „Beschuldigten“ zu dem eines „Zeugen“. Damit war aber auch der Grund für das Stadionverbot entfallen. In so unübersichtlich gelagerten Fällen wird es unvermeidbar sein, dass die Polizei zunächst Daten von Personen mitteilt und dass gegen diese Betroffenen in der Folge dann auch Stadionverbote erlassen werden, bei denen sich später herausstellt, dass diese nicht an den Straftaten beteiligt waren oder deren Tatbeitrag nicht bewiesen werden kann.

Spätestens aber mit der Statusänderung hätte dem „Heimatverein“ des Fans mitgeteilt werden müssen, dass gegen diesen nicht mehr ermittelt wird und er allenfalls als Zeuge in Betracht kam. Nur durch eine solche Berichtigung hätte die Berechtigung des Stadionverbots überprüft und zurückgenommen werden können. § 22 LDSG regelt insoweit:

§ 22
Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. [...]

(2) Von der Berichtigung unrichtiger Daten sind die Empfänger der Daten zu verständigen, soweit dies zur Wahrung schutzwürdiger Interessen des Betroffenen oder zur Erfüllung der Aufgaben der verantwortlichen Stelle oder des Empfängers erforderlich erscheint; dies gilt nicht, wenn dies einen unverhältnismäßigen Aufwand erfordern würde.

Der Pflicht zur Berichtigung nach § 22 LDSG stand im Übrigen § 46 Absatz 2 PolG nicht entgegen.

§ 46
Löschung, Sperrung und Berichtigung von Daten

[...]

(2) Auf die vom Polizeivollzugsdienst zur vorbeugenden Bekämpfung von Straftaten gespeicherten personenbezogenen Daten finden §§ 22 und 24 des Landesdatenschutzgesetzes insoweit keine Anwen-

dung, als der Betroffene die Richtigkeit der gespeicherten Daten bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

Denn im vorliegenden Fall stand fest, dass die zunächst zur Person des Petenten gespeicherte Beschuldigteneigenschaft unrichtig war.

Um zukünftige Missverständnisse dieser Art zu vermeiden, habe ich das Innenministerium gebeten, in der einschlägigen Verwaltungsvorschrift „Führungs- und Einsatzanordnung Fußball Baden-Württemberg (FEA Fußball)“ die Pflicht zu Berichtigung bereits übermittelter Daten festzuschreiben. Mit einer solchen Mitteilung können Fußballvereine und Stadionbetreiber prüfen, ob zunächst verhängte Stadionverbote wieder aufzuheben sind.

Der aktualisierte Entwurf der FEA Fußball soll zur Datenübermittlung durch die Polizei Folgendes klarstellen:

„Werden im Zusammenhang mit der Beantragung von bundesweit wirksamen Stadionverboten bzw. Stadionverboten mit Gültigkeit in der Oberliga Baden-Württemberg Daten von Betroffenen an Vereine bzw. Verbände übermittelt, so ist im Falle eines Statuswechsels der betroffenen Person (z. B. vom Beschuldigten zum Zeugen), dieser Statuswechsel dem Verein bzw. Verband gem. § 48 PolG i. V. mit § 22 LDSG ebenfalls mitzuteilen, damit zeitgerecht gegebenenfalls das Stadionverbot in angemessener Dauer ausgesprochen bzw. zurückgenommen werden kann.“

2.2.9 Das Nationale Waffenregister –
Kontrollbesuche bei den Waffenbehörden

Zum Thema Nationales Waffenregister (NWR) hatte ich bereits in der Vergangenheit berichtet (30. Tätigkeitsbericht 2010/2011, LT-Drs. 15/955 S. 55, und 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, S. 57). Um einen ersten Eindruck von der Arbeit mit diesem Register zu bekommen, haben Mitarbeiter meiner Dienststelle insgesamt vier Waffenbehörden in Baden-Württemberg kontrolliert.

Nach den Anschlägen von Paris am 13. November 2015 hat die Europäische Union erneut die EU-weite Kontrolle von Feuerwaffen verschärft. Bereits am 18. November verabschiedete die Europäische

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Kommission ein aus mehreren Maßnahmen bestehendes Paket: u. a. wird es damit künftig schwieriger, Feuerwaffen in der Europäischen Union zu erwerben und in legalem Besitz befindliche Waffen können noch besser zurückverfolgt werden.

Eine solche Verschärfung hatte die Europäische Kommission bereits mit der Richtlinie 91/477/EWG des Rates vom 18. Juni 1991 über die Kontrolle des Erwerbs und des Besitzes von Waffen in der Fassung der Richtlinie 2008/51/EG des Europäischen Parlaments und des Rates vom 21. Mai 2008 angestoßen. Damals verpflichtete die Europäische Union die Mitgliedstaaten, spätestens bis zum 31. Dezember 2014 ein computergestütztes Waffenregister auf nationaler Ebene einzuführen. In diesem Waffenregister sind für mindestens 20 Jahre Typ, Modell, Fabrikat, Kaliber, Seriennummer sowie Namen und Anschriften des Lieferanten und der Person, die die Waffe erwirbt oder besitzt, zu registrieren und zu speichern.

Neu am NWR, das vom Bundesamt für Verwaltung (BVA) geführt wird, ist nicht nur die Umstellung auf ein deutschlandweites elektronisches Verfahren, sondern auch die Einführung des Datenformats „XWaffe“. Dies ist ein bundesweit gültiger Standard für die Speicherung von Daten, die im Zusammenhang mit Waffen gesetzlich verarbeitet werden müssen. Der Standard soll helfen, die bisherigen Datenbestände genauer zu erfassen und den länderübergreifenden Zugriff zu ermöglichen. Zusätzlich werden im NWR nun auch die Daten von Waffenherstellern sowie -händlern erfasst, da diese nach dem Waffengesetz ebenfalls verschiedene Nachweispflichten zu erfüllen haben.

Schätzungen zu Folge sind für Baden-Württemberg mehr als 725.000 Waffen im NWR eingetragen (s. LT-Drs. 15/4782). Für deren Überwachung sind in unserem Bundesland derzeit 149 Waffenbehörden zuständig. Damit stellt das Land mehr als ein Viertel der ca. 550 deutschen Waffenbehörden. In Anbetracht der doch sehr speziellen Materie könnte eine gewisse Bündelung auf Behördenebene meines Erachtens durchaus sinnvoll sein.

Um das in Baden-Württemberg äußerst breite Spektrum an Waffenbehörden in der Kontrolle widerspiegeln zu können, wurden hinsichtlich Größe und Zuständigkeit unterschiedliche Behörden für die

Kontrollbesuche ausgewählt: die eines Stadtkreises mit ca. 2.800 Waffenbesitzern, eines Landkreises mit ca. 7.500 Waffenbesitzern (im Landkreis sind weitere sechs Waffenbehörden zuständig), einer Großen Kreisstadt mit ca. 600 Waffenbesitzern und einer Stadt unterhalb der Größenordnung einer Großen Kreisstadt mit ca. 300 Waffenbesitzern. Zusätzlich wurde eine Polizeidienststelle im Hinblick auf die Nutzung des NWR für polizeiliche Zwecke kontrolliert.

Um die Einführung des NWR bei den Kommunen zu erleichtern, wurde den Waffenbehörden des Landes ein kostenfreier Anschluss an das Verfahren „Online-Sicherheitsüberprüfungen“ (OSiP-BW) angeboten. Davor war es üblich, die für Erteilung waffenrechtlicher Erlaubnisse notwendigen Abfragen schriftlich bei der örtlich zuständigen Polizeidienststelle zu stellen. Jetzt können Behörden mittels OSiP-BW ihre Anfragen unmittelbar an das Landeskriminalamt Baden-Württemberg richten. Die Bearbeitungszeit der Vorgänge soll damit verkürzt werden.

Zur Vorbereitung der Kontrollbesuche forderte ich nicht nur die Protokolle zu Abrufen aus dem NWR vom BVA, sondern eben auch die Protokolle zu Abrufen aus OSiP-BW von der Datenzentrale Baden-Württemberg sowie zu Abrufen aus dem Bundeszentralregister (BZR) vom Bundesamt für Justiz (BfJ) an. Dabei fielen zunächst die relativ wenigen Abfragen aus OSiP-BW auf. Vor Ort wurde hierzu erklärt, dass Anfragen zur Sicherheitsüberprüfung häufig nach wie vor schriftlich gestellt würden, da Probleme mit der Anbindung des Verfahrens OSiP-BW an das Programm-Modul „Registerauskunft“ der Condition WorkOffice Software "Waffenverwaltung" – eines speziellen Programmsystems zur Waffenverwaltung – bestünden. Wahrscheinlich dürfte es sich dabei aber um Einführungsschwierigkeiten gehandelt haben, da eine andere Stadt in Baden-Württemberg, die OSiP-BW bereits seit 2012 einsetzt, ihre Sicherheitsüberprüfungen problemlos abarbeiten konnte.

Erfreulicherweise konnten meine Mitarbeiter feststellen, dass die Verwaltungsverfahren zur Erteilung waffenrechtlicher Erlaubnisse keine Abweichungen von dem gesetzlich vorgegebenem Rahmen erkennen ließen. Hierzu wurden mit Einverständnis von Waffenbesitzern die Aus- bzw. Eintragungen von

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Waffen aus deren Waffenbesitzkarte einschließlich aller notwendigen Verfahrensschritte nachverfolgt.

Der Antrag auf Erteilung einer waffenrechtlichen Erlaubnis wird häufig schriftlich gestellt. Ein persönliches Erscheinen des zukünftigen Waffenbesitzers ist meistens erst im Zusammenhang mit der Aushändigung der Waffenbesitzkarte erforderlich. Dem Erlass eines Waffenverbots geht im Regelfall eine Meldung der Polizei mit entsprechenden Hinweisen voraus. Diese erfolgt nach keinem standardisierten Katalog, so z. B. wenn bestimmte Straftaten oder Ordnungswidrigkeiten begangen wurden, sondern dann, wenn nach der subjektiven Einschätzung des polizeilichen Sachbearbeiters eine solche Meldung angezeigt ist. Das Ergebnis kann dann nicht nur die Entziehung waffenrechtlicher Erlaubnisse, sondern auch die Verhängung eines „präventiven“ Waffenverbots sein, das bei möglichen zukünftigen Anträgen der betroffenen Person zu berücksichtigen ist.

Bei der Kontrolle der technischen und organisatorischen Maßnahmen konnten lediglich kleinere Mängel festgestellt werden:

Im Rahmen der Sachbearbeitung wurden bei allen kontrollierten Behörden allgemeine Schreiben verfasst, die personenbezogene Daten beinhalteten. Für die Erstellung der Dokumente bestand in der Anwendung des Programmsystems zur Waffenverwaltung eine Schnittstelle zu einem gängigen Textverarbeitungsprogramm. Wenn mit der auf dem Terminalserver installierten Textverarbeitung gearbeitet wurde, war es möglich, solche Dokumente auf dem Terminalserver oder auf eingebundenen Netzlaufwerken zu speichern. Dazu wurden die erstellten Schreiben vom Arbeitsplatz-PC bzw. vom Dateiserver der Behörde an den Terminalserver durchgereicht. Bei den Kontrollen zeigte sich, dass keine schriftlichen Vorgaben hinsichtlich der Speicherung der Dokumente existierten. Hier habe ich empfohlen, den Speicherort, die Speicherdauer und die Löschung von Schriftgut der Waffenbehörde zu regeln. Dies könnte z. B. durch eine Dienstanweisung geschehen.

Weiter wurde festgestellt, dass Änderungshinweise des BVA zu Daten aus dem NWR nicht selten in einem allgemeinen elektronischen Postfach des Ordnungsamts eingingen. Der Amtsleiter leitete die Hinweise dann an die zuständigen Waffensachbe-

arbeiter weiter. Da in dem Postfach neben den Änderungshinweisen des BVAs auch andere Nachrichten an das Ordnungsamt auflaufen dürften, war zu vermuten, dass auch weitere, für das Waffenrecht nicht zuständige Mitarbeiter darauf zugreifen konnten. Daher habe ich empfohlen, ein Funktionspostfach für die Waffenbehörde anzulegen und beim BVA zu veranlassen, dass Datenänderungshinweise ausschließlich an dieses Postfach übermittelt werden.

Bei jeder Kontrolle nahmen meine Mitarbeiter die Aufbewahrung der Waffenakten gesondert in Augenschein. Dazu ließen sie sich die Sortiermerkmale und die Maßnahmen zur Sicherung der Akten vor unbefugten Zugriffen erläutern. Dabei wurden unterschiedliche Arbeitsweisen festgestellt: so wurden z. B. in einem Fall die Waffenakten in den Diensträumen der Behörde in einem abschließbaren Aktenrollschrank aufbewahrt, während in einem anderen Fall Verwahräume, zu denen nur die Mitarbeiter der Waffenbehörde Zugang hatten, zur Verfügung standen. Solange nur den Mitarbeiter der Waffenbehörde der Zugang zu den verschließbaren Aktenschränken möglich war, konnte die Sorgfaltspflicht in Bezug auf die Sicherheit bei der Aktenaufbewahrung als erfüllt angesehen werden.

Im Zusammenhang mit den Maßnahmen zur Sicherung der Akten wurde auch die Dauer der Aktenaufbewahrung angesprochen. Dabei wurde festgestellt, dass regelmäßig keine Aussonderungsfristen festgelegt waren. § 44a des Waffengesetzes (WaffG) sagt dazu:

§ 44a

Behördliche Aufbewahrungspflichten

(1) Die für die Ausführung dieses Gesetzes zuständigen Behörden haben alle Unterlagen, die für die Feststellung der gegenwärtigen und früheren Besitzverhältnisse sowie die Rückverfolgung von Verkaufswegen erforderlich sind, aufzubewahren.

(2) Die Aufbewahrungspflicht bezieht sich sowohl auf eigene Unterlagen als auch auf nach § 17 Abs. 6 Satz 2 und 3 der Allgemeinen Waffengesetz-Verordnung vom 27. Oktober 2003 (BGBl. I S. 2123), die zuletzt durch Artikel 2 des Gesetzes vom 26. März 2008

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

(BGBl. I S. 426) geändert worden ist, übernommene Waffenherstellungs- und Waffenhandelsbücher.

(3) Für die Waffenherstellungsbücher beträgt die Aufbewahrungsfrist mindestens 30 Jahre. Für alle anderen Unterlagen einschließlich der Einfuhr- und Ausfuhrzeichnungen beträgt die Aufbewahrungsfrist mindestens 20 Jahre.

Diese Regelung zielt auf eine verbesserte Nachverfolgbarkeit von Waffen und bestimmt deshalb nur Mindestfristen von 20 Jahren für besitzverhältnisrelevante Unterlagen und 30 Jahren für verkaufswegerelevante Unterlagen. Vor dem Hintergrund des § 23 Absatz 2 LDSG, wonach personenbezogene Daten in Akten dann zu löschen sind, wenn die speichernde Stelle im Einzelfall feststellt, dass die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist, habe ich empfohlen, dass auch hier eine Dienstanweisung erlassen wird, die die Aufbewahrungsdauer der Akten und ggf. die Andienung ausgesonderter Akten gegenüber dem Landesarchiv festlegt.

Des Weiteren haben meine Mitarbeiter eine Reihe von Beobachtungen gemacht, von denen sich erst bei einer längeren Nutzung des NWR herausstellen wird, ob diese im Einklang mit den datenschutzrechtlichen Vorschriften stehen:

Zunächst bereitete es Probleme, die Protokolldaten des BZR nachzuvollziehen. In den Ausdrucken wurden Registereinträge gefunden, bei denen z. B. das Aktenzeichen aus den Buchstaben „A–Z“, einem Bindestrich und einer Zahl oder aus der Bezeichnung „31.05“ bestand. Wenn bei Anfragen keine individuellen Aktenzeichen verwendet werden, ist die Prüfung der Erforderlichkeit des Abrufs erschwert. Hier hielte ich es für hilfreich, wenn das verantwortliche BfJ die Angabe des Aktenzeichens in einem Pflichtfeld mit vorgegebenem Format zur Voraussetzung für die Abfrage machen würde.

Bei dem Vergleich der Protokolldaten des BZR mit denen des NWR ergab sich, dass Einzelanfragen aus dem NWR protokolliert wurden, für Sammelanfragen, wie diese zum Beispiel bei den wiederkehrenden Zuverlässigkeitsüberprüfungen von Jägern gemacht werden, aber keine entsprechenden Protokolleinträge gefunden werden konnten. Hier stellt

sich die Frage nach dem Grund für eine solche unterschiedliche Verfahrensweise.

Das von den Waffenbehörden zur Bearbeitung ihrer Vorgänge eingesetzte Programmsystem ermöglicht die Suche nach einer Waffe beispielsweise an Hand der Seriennummer oder Teilen davon. Hierbei wurden im Allgemeinen mehrere Waffen gefunden. Aus der Protokollierung des NWR ergab sich, dass, selbst wenn nur eine Waffe gefunden wurde, vom Programmsystem der aktuelle Besitzer, aber auch alle ehemaligen Inhaber dieser Waffe im NWR aufgerufen wurden. Ich bezweifle, dass die Übermittlung der Daten ehemaliger Besitzer, der sog. „Historienaufruf“, in jedem Fall erforderlich ist, zumal diese Daten häufig nicht in die Zuständigkeit der jeweiligen Behörde fallen dürften.

Die Umsetzung des neuen Formats „XWaffe“ bedeutete für die Waffenbehörden, dass im Prinzip jeder Datensatz überprüft werden musste. Dieses Format lässt keine Ungenauigkeiten z. B. bei den Namen des Waffenbesitzers oder bei der Bezeichnung einer Waffe zu. In der Praxis war zu erfahren, dass die Kontrolle und Überarbeitung der Datensätze zum einen die Bearbeitung der Vorgänge verzögerte und zum anderen von Waffenbehörde zu Waffenbehörde verschieden weit fortgeschritten war. Eine Behörde erklärte aufgrund einer vorübergehenden Personalverstärkung, dass 99 % des dortigen Bestandes diesem Standard entsprächen. Die anderen Waffenbehörden sahen sich erst innerhalb des vom BVA vorgegebenen Zeitraums bis Ende 2017 in der Lage, die notwendigen Arbeiten vollständig abzuschließen.

Übereinstimmend wurde von den Waffenbehörden berichtet, dass sie aufgrund der mit der Einrichtung des NWR verbundenen zusätzlichen Aufgaben ihren gesetzlichen Verpflichtungen zur Regelüberprüfung nach § 4 WaffG, wonach die Inhaber von waffenrechtlichen Erlaubnissen mindestens alle drei Jahre zu überprüfen sind, nicht nachkommen könnten. Bei einer Waffenbehörde wurde die Regelüberprüfung nach fünf Jahren angegangen.

Als Ergebnis der Kontrollaktion ist festzuhalten, dass meine Mitarbeiter bei den Verwaltungsverfahren in den Waffenbehörden keine Abweichungen von dem gesetzlich vorgegebenen Rahmen erkennen konnten, dass aber kleinere Mängel bei den technischen und organisatorischen Maßnahmen

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

festzustellen waren. Inwieweit sich die Erwartungen der Europäischen Union an eine verbesserte Kontrolle von Schusswaffen in Privatbesitz durch die Einführung von elektronischen Waffenregistern in den Mitgliedstaaten erfüllen, lässt sich vermutlich erst im Jahr 2017 sagen, da weiterhin noch mit Einführungsproblemen gerechnet werden muss.

Den Waffenbehörden empfehle ich,

- im Rahmen einer Dienstanweisung den Umgang mit allgemeinen Schreiben, so z. B. den Speicherort, die Speicherdauer sowie die Löschung von Schriftgut der Waffenbehörde, zu regeln,
- ein Funktionspostfach für die Waffenbehörde einzurichten, dieses für Änderungshinweise o. ä. dem BVA mitzuteilen und den Zugriff auf dieses elektronische Postfach nur Mitarbeitern der Waffenbehörde zu eröffnen,
- sicherzustellen, dass nur die Mitarbeiter der Waffenbehörde Zugang zu den verschließbaren Aktenschränken haben,
- eine Dienstanweisung zur Aufbewahrung von Waffenakten zu erlassen, die die Aufbewahrungsdauer der Akten und ggf. die Andienung ausgesonderter Akten gegenüber dem Landesarchiv festlegt.

2.2.10 Glückssache!

Wer träumt nicht davon, über Nacht reich zu werden? Die Teilnahme an Glücksspielen begreifen viele als Chance, diesen Traum Wirklichkeit werden zu lassen. Dass dieser Traum dann nicht selten zum Albtraum wird, zeigen einschlägige Forschungsergebnisse. Danach steht fest, dass Glücksspiele in ein krankhaftes Suchtverhalten münden können. Spielsucht kann wegen der drohenden Verschuldung der Betroffenen und der mit der Sucht nicht selten verbundenen Folge- und Begleitkriminalität zu schwerwiegenden Folgen nicht nur für die Spieler selbst, sondern auch für ihre Familien und die Gemeinschaft führen. Die Bekämpfung der Glücksspielsucht, der Jugend- und Spielerschutz und der Schutz vor Folge- und Begleitkriminalität sind deshalb als überragend wichtige Gemeinwohlziele anerkannt. Studien belegten dabei, dass das Suchtpotential bei Geldspielgeräten unter allen Gewinnspielen am höchsten sei. Dem entgegenzuwirken ist

deshalb ein berechtigtes und anerkennenswertes Anliegen auch des Landesgesetzgebers.

Mit dem Glücksspielstaatsvertrag (GlüStV) haben die Länder einen bundesweit einheitlichen Rahmen zur Regelung des Glücksspiels geschaffen. Die konkrete Umsetzung erfolgte im Landesglücksspielgesetz (LGlüG). Sowohl der Glücksspielstaatsvertrag als auch das Landesglücksspielgesetz enthalten auch Regelungen zum Schutz von spielsuchtgefährdeten Spielern vor sich selbst. So können gegen diese, sei es auf eigenen Antrag oder „von Amts wegen“, sog. Spielersperrungen verhängt werden. Ist eine Spielersperre verhängt, darf kein Spieleanbieter der Person die Teilnahme am Glücksspiel ermöglichen. Um dies zu gewährleisten und um bestehende Sperrungen wirksam überprüfen zu können, gibt es Sperrdatenbanken, in denen alle Personen erfasst sind, gegen die solche Sperrungen verhängt wurden.

Bis zum Jahr 2012 unterhielten die Spielbankunternehmen und die Lottoanbieter der Länder ein dezentral vernetztes Sperrsystem (Zentrales Sperrsystem der Deutschen Spielbanken – ZSDS). Jeder Glücksspieleanbieter führte seine eigene, lokale Sperrdatenbank. Diese war mit den Sperrdatenbanken aller anderen Anbieter vernetzt, so dass bei einer neuen Sperre bzw. der Aufhebung einer bestehenden Sperre die entsprechenden Daten mit allen angeschlossenen Datenbanken synchronisiert wurden. Somit konnten alle angeschlossenen Spieleanbieter aktuell auf alle bundesweit vorhandenen Sperrdaten zugreifen.

Mit dem Ersten Glücksspieländerungsstaatsvertrag (Erster GlüÄndStV⁴¹) wurde dieses dezentrale durch ein übergreifendes Sperrsystem abgelöst, das zentral von der zuständigen Behörde des Landes Hessen, vertreten durch das Hessische Ministerium des Innern und für Sport, geführt wird und das den bundesweiten Sperrabgleich für die Spielbanken und Veranstalter von Sportwetten und Lotterien mit besonderem Gefährdungspotenzial ermöglicht (Spielersperrsystem OASIS). Die Etablierung der zentralen Sperrdatei ist derzeit allerdings noch nicht abgeschlossen. Die Mehrzahl der Spielanbieter in den

⁴¹ <http://www.vdai.de/regelwerke/GlueStV/1-GlueAendStV.pdf>

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Bundesländern arbeitet nach wie vor im Rahmen des dezentralen Sperrsystems zusammen.

Im Zuge der landesrechtlichen Umsetzung des Ersten Glücksspieländerungsstaatsvertrags hat der Landesgesetzgeber mit § 43 Absatz 1 LGLüG erstmals auch Spielhallen zur Teilnahme an dem übergreifenden Sperrsystem verpflichtet und dies wie folgt geregelt:

Die die Erlaubnis innehabende Person hat dafür zu sorgen, dass sich in der Spielhalle keine Personen unter 18 Jahren oder gesperrte Spielerinnen und Spieler aufhalten. Dies ist durch Einlasskontrollen sicherzustellen, bei denen die Personalien der Gäste festgestellt und mit der zentral geführten Sperrdatei nach [...] § 23 Absatz 1 [GlüStV] abgeglichen werden.

Ergänzend bestimmt § 45 LGLüG:

Für die Entgegennahme von Anträgen auf Selbstsperrungen gilt § 4 Absatz 3.

§ 4 Absatz 3 LGLüG verpflichtet dazu, eingereichte Anträge auf Selbstsperrung unverzüglich „an die mit der Durchführung des staatlichen Glücksspiels nach § 9 Absatz 4 beauftragte juristische Person“ weiterzuleiten, die die betroffene Person unverzüglich sperrt. Juristische Person im Sinne dieser Vorschrift ist die Staatliche Toto-Lotto GmbH (kurz: Lottogesellschaft).

Gegen die Verpflichtung zur Teilnahme an dem übergreifenden Sperrsystem (und weitere Bestimmungen des Landesglücksspielgesetzes) erhoben einzelne Spielhallenbetreiber Verfassungsbeschwerden zum Staatsgerichtshof für das Land Baden-Württemberg. Mit Urteil vom 17. Juni 2014 (– 1 VB 15/13 –, juris) stellte dieser fest, dass der Glücksspielstaatsvertrag einen Zugriff von Spielhallenbetreibern auf die zentrale Sperrdatei nach § 23 GlüStV nicht vorsehe. Soweit § 43 Absatz 1 Satz 2 LGLüG die Spielhallenbetreiber gleichwohl zu einem solchen Datenabgleich verpflichte, verstoße er gegen die von der Verfassung des Landes Baden-Württemberg garantierte Berufsfreiheit und sei deshalb verfassungswidrig. Im Klartext: Die Länder hatten im Glücksspielstaatsvertrag von 2007 offenbar

schlichtweg vergessen, eine Rechtsgrundlage für eine Aufnahme der Spielhallen in das länderübergreifende Sperrsystem zu schaffen!

Die Entscheidung, dass Spielhallen nicht in das übergreifende Sperrsystem einbezogen werden dürfen, bedeutet aber zugleich, dass auch die in § 45 LGLüG geregelte Pflicht zur Übermittlung von bei Spielhallen eingereichten Anträgen auf Selbstsperrung an die Lottogesellschaft von vornherein nicht bestand. Denn § 45 LGLüG kann nur im Kontext mit der beabsichtigten Einbeziehung der Spielhallen in das übergreifende Sperrsystem verstanden werden (so auch die Gesetzesbegründung, vgl. LT-Drs. 15/2431 S. 109). Dementsprechend hat auch das Ministerium für Finanzen und Wirtschaft Baden-Württemberg im Oktober 2014 die nachgeordneten Behörden verpflichtet, dafür Sorge zu tragen, dass solche Übermittlungen künftig unterbleiben. Und auch die Lottogesellschaft hat nach eigenem Bekunden die ihr nach der Staatsgerichtshofsentscheidung durch Spielhallen übersandten Sperranträge nicht weiter bearbeitet.

Bis zum Zeitpunkt der Entscheidung des Staatsgerichtshofs waren der Lottogesellschaft aber bereits ca. 1.500 Selbstsperranträge übermittelt worden. In allen Fällen waren gegen die Betroffenen Spielersperrungen verhängt worden. In die Diskussion zwischen verschiedenen Landesministerien, wie mit der aufgrund des Gerichtsurteils entstandenen neuen Situation umzugehen sei, wurde auch meine Dienststelle einbezogen. Dabei ging es um die Frage, wie aus datenschutzrechtlicher Sicht mit den bereits verarbeiteten Sperranträgen umzugehen sei. Denn klar ist, dass nicht nur die Speicherung der erhaltenen Spielerdaten, sondern auch deren weitere Verarbeitung durch die Lottogesellschaft und insbesondere die Verfügung von Spielersperrungen, die faktisch eine Übermittlung der jeweiligen Daten an die Verbundteilnehmer darstellt, datenschutzrechtlich relevante Sachverhalte betrifft, die auf ihre Rechtmäßigkeit zu überprüfen waren.

Denn neben dem Aspekt des Schutzes vor einer Selbstgefährdung sind im Rahmen des Sperrsystems auch die Datenschutzgrundrechte der betroffenen Spieler zu beachten. Diesbezüglich führt der Staatsgerichtshof aus (a.a.O., Abs.-Nr. 407 ff.):

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

„Aus der allgemeinen Zielbestimmung in § 1 GlüStV, die u. a. als Ziel die Bekämpfung von Glücksspielsucht festlegt, kann sich insoweit nichts anderes ergeben. Sie ist nicht in der Lage, eine Rechtsgrundlage für Grundrechtseingriffe zu bieten.

Entgegen der Meinung der Landesregierung sind auch weder § 23 Abs. 2 GlüStV noch § 28 GlüStV geeignet, eine hinreichend bestimmte Rechtsgrundlage für den Datenabgleich und den Zugriff der Spielhallen auf die Daten der zentralen Sperrdatei darzustellen oder die Länder zum Erlass entsprechender Regelungen zu ermächtigen. [...].

Wenn sich aus diesen Normen [...] die Möglichkeit ergeben soll, dass einzelne Länder durch abweichende Regelungen ihre Spielhallen auf die zentrale Sperrdatei zugreifen lassen können, hätte dies im Glücksspielstaatsvertrag – und damit nachfolgend von allen Landtagen – selbst hinreichend bestimmt geregelt werden müssen. Denn eine solche Auslegung von § 23 Abs. 2 und § 28 GlüStV würde zu einem Eingriff in das Recht auf informationelle Selbstbestimmung der gesperrten Spieler führen.

[...] Zwischen Datenspeicherung und Verwendungszweck besteht ein unauflösbarer verfassungsrechtlicher Zusammenhang. Daten dürfen von vornherein nur zu bestimmten, bereichsspezifischen, präzise und normenklar festgelegten Zwecken gespeichert werden, so dass bereits bei der Speicherung hinreichend gewährleistet ist, dass die Daten nur für solche Zwecke verwendet werden, die das Gewicht der Datenspeicherung rechtfertigen. [...] Diese materielle Verknüpfung darf auch im Zusammenspiel von Bund und Ländern nicht aufgebrochen werden [...]. Entsprechendes muss für die Zusammenarbeit der Länder aufgrund staatsvertraglicher Grundlage gelten. Auch hier dürfen einzelne Länder nicht in einem Umfang auf gemeinsam erhobene Daten zugreifen oder zu einem Zugriff verpflichtet, der nicht präzise vom Staatsvertrag geregelt ist“.

Auch das Bundesverfassungsgericht hat in seinem Nichtannahmebeschluss vom 16. Juli 2015 (– 1 BvR 1014/13 –, juris) darauf hingewiesen, dass die Verarbeitung personenbezogener Daten im Rahmen des Spielersperrsystems datenschutzrechtlichen Anforderungen genügen muss.

Zur Klärung der schwierigen Rechtsfragen führten meine Mitarbeiter mehrere Gespräche mit der Lottogesellschaft und statteten dieser auch einen Besuch vor Ort ab. Als vorläufiges Ergebnis lässt sich Folgendes festhalten:

Zunächst ist erfreulich, dass mit der Lottogesellschaft Einigkeit jedenfalls in den Fällen erzielt werden konnte, in denen die ihr zugesandten Selbstsperrerkklärungen keinerlei Hinweis darauf ergaben, dass die Betroffenen von einer Übermittlung an die Lottogesellschaft wussten oder diese gar wollten und dass sie damit den Wunsch verbunden hätten, in ein übergreifendes Sperrsystem aufgenommen zu werden. Drei markante Beispiele hierzu, die bei der Stichprobenprüfung der bei der Lottogesellschaft gespeicherten Anträge zufällig herausgegriffen wurden:

- Ein von der Spielhalle offenbar selbst entwerfener, als „Selbstsperrformular“ überschriebener Vordruck enthielt lediglich die Personalien des Spielers einschließlich seiner Unterschrift sowie den Stempel der Spielhalle.
- Ein Spieler schrieb handschriftlich an die Spielhalle: „Hiermit erteile ich mir [Name] mit sofortiger Wirkung ein Hausverbot ein Jahr, bis 30.05.14“. Die Spielhalle antwortete schriftlich und bestätigte das Hausverbot. Weiter schrieb sie: „Als weiterführende Maßnahme empfehlen wir Ihnen, sich eventuell auch bundesweit über das Sperrsystem der Spielbanken sperren zu lassen“.
- Ein „Antrag auf Spielsperre für Baden-Württemberg“ hatte folgenden Wortlaut: „Hiermit beantrage ich [persönliche Angaben], mich für die Dauer von mindestens einem Jahr ab Zugang der Spielsperre vom Spiel in der Spielhalle [Bezeichnung der Spielhalle] auszuschließen. [...] Die erhobenen Daten [...] sind nur von der Spielhalle mit der Funktion des Abgleichs der Spielersperrliste beauftragten Person einzusehen, somit geschützt aufzubewahren und werden nach Aufhebung der Sperre gelöscht“.

In allen Fällen – vergleichbare weitere wurden festgestellt – verhängte die Lottogesellschaft eine Spielsperre, nachdem ihr die Schreiben von den Spielhallen zugesandt worden waren. Insoweit akzeptierte die Lottogesellschaft unsere Auffassung, wonach für die weitere Speicherung der Unterlagen

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

und die Eingabe in das Sperrsystem keine Rechtfertigung besteht. Sie erklärte sich auch bereit, unserem Vorschlag zu folgen und den Betroffenen schriftlich anzubieten, die Spielersperre aufrecht zu erhalten. Damit könnte, nach entsprechender datenschutzkonformer Aufklärung, der bisherige rechtlose Zustand bereinigt werden. Für den Fall, dass keine nachträgliche Genehmigung erfolgt, soll die Sperre aufgehoben, der entsprechende Aktenrückhalt für einen gewissen Zeitraum gesperrt und anschließend vernichtet werden. Ein aus meiner Sicht gutes Ergebnis!

Noch nicht abschließend geklärt sind die Fälle, in denen auf den Anträgen die Lottogesellschaft irgendwie erwähnt wird (Beispiel: „An die Spielhalle [...] oder an die Staatliche Toto-Lotto-GmbH oder über jede Toto- und Lotto-Annahmestelle“) oder in denen sie sogar – bei entsprechender Verwendung des eigenen Sperrantragsformulars der Lottogesellschaft, das über das Internet bezogen werden kann und von einzelnen Spielhallen auch verwendet wird – ausdrücklich an die Lottogesellschaft adressiert sind. Hier verweist die Lottogesellschaft auf die Rechtsprechung des Bundesgerichtshofs, wonach der Spieleanbieter mit der Entgegennahme eines Selbstsperrantrags eine vertragliche Verpflichtung eingehe, den Spieler vor den aufgrund seiner Spielsucht zu befürchtenden wirtschaftlichen Schäden zu bewahren. Sie befürchtet Schadensersatzansprüche, wenn sie die Betroffenen nicht vom Spielbetrieb ausschließt.

Ob solche vertraglichen Verpflichtungen in allen Fällen zustande gekommen sind, in denen die Lottogesellschaft im Antrag auf Spielersperre benannt ist, erscheint fraglich. Etwa wenn ein Spieler in einem Antrag handschriftlich vermerkt: „Der Grund, ich möchte da nicht mehr hingehen“. Hier kann mit Fug und Recht in Frage gestellt werden, ob daraus der Wille abgeleitet werden kann, mit der Lottogesellschaft einen Vertrag abzuschließen – der Antrag wurde schließlich in einer Spielhalle gestellt! Wir hatten der Lottogesellschaft vorgeschlagen, auch in diesen Fällen wie oben dargestellt zu verfahren und die Betroffenen anzuschreiben. Dies würde weniger Aufwand bedeuten, da nicht jeder Antrag einzeln überprüft werden müsste, und würde letztlich zu einer datenschutz- wie zivilrechtlich sauberen Lösung führen. Ob sich die Lottogesellschaft dazu durchringen kann, bleibt abzuwarten. Wir sind dies-

bezüglich mit ihr weiter im Gespräch, zumal auch die Frage der datenschutzgerechten Ausgestaltung der Sperrantragsformulare noch nicht abschließend zu unserer Zufriedenheit geklärt ist.

Mit dem Gesetz vom 1. Dezember 2015 zur Änderung des Landesglücksspielgesetzes (GBI. S. 1033) hat der Gesetzgeber die Konsequenzen aus dem Urteil des Staatsgerichtshofs gezogen. So wird die Pflicht der Spielhallen in § 43 Absatz 1 LGlüG zum Datenabgleich mit der zentralen Sperrdatei aufgehoben. Der die Übermittlungspflicht der Spielhallen für Selbstsperranträge regelnde § 45 wird ersetzt durch eine Regelung, die Spielhallenbetreiber zur Führung jeweils eigener Sperrdateien verpflichtet.

Die datenschutzrechtlichen Fragen im Zusammenhang mit den Sperranträgen aus Spielhallen sind noch nicht abschließend geklärt. Auch die künftige, den datenschutzrechtlichen Anforderungen an eine informierte Einwilligung in die Datenverarbeitung Rechnung tragende Gestaltung der von der von der Lottogesellschaft bereitgestellten Sperrantragsformulare bedarf weiterer Gespräche. Unabhängig davon ist festzuhalten, dass das ursprüngliche Ziel des Glücksspielstaatsvertrages, Spielsüchtige mit Hilfe eines bundesweiten Sperrsystems auch dann vor sich selbst zu schützen, wenn sie in der Spielhalle eines anderen Betreibers oder in einem anderen Bundesland spielen wollen, erst dann erreicht werden kann, wenn der Glücksspielstaatsvertrag der Länder entsprechend geändert wird. Ob dies noch geschehen wird, ist angesichts der vielfältigen Kritik daran und der grundsätzlichen Reformvorschläge einiger Länder allerdings fraglich.

2.3 Die Verfassungsschutzreform

Quieta non movere – dieser dem römischen Historiker Sallust zugeschrieben Satz wurde vom deutschen Reichskanzler Otto von Bismarck im April 1891 in Friedrichsruh in einem Schreiben an den Vorstand der Konservativen Partei, deren Abgeordneter er war, wie folgt zitiert: „Es gibt ein altes, gutes politisches Sprichwort: Quieta non movere, das heißt, was ruhig liegt, nicht stören, und das ist echt konservativ: eine Gesetzgebung nicht mitmachen, die beunruhigt, wo das Bedürfnis einer Änderung nicht vorliegt“. Auch wenn nicht bezweifelt wird, dass aufgrund der Empfehlungen und Erkenntnisse

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

der Bund-Länder-Kommission Rechtsextremismus und der NSU-Untersuchungsausschüsse des Deutschen Bundestags und einiger Länderparlamente das Bedürfnis nach Änderungen an der Struktur und der Arbeitsweise der Sicherheitsbehörden besteht, wäre zu wünschen gewesen, dass der Gesetzgeber bei der aktuellen Reform der Verfassungsschutzbehörden etwas zurückhaltender ans Werk gegangen wäre. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte schon frühzeitig hierauf hingewiesen (Entschließung vom 7./8. November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“, 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Anhang 9).

Stattdessen hat der Deutsche Bundestag am 3. Juli 2015 das von der Bundesregierung eingebrachte „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (Bundestagsdrucksache [BT-Drs.] 18/4654, 18/5051) verabschiedet, das wesentliche Forderungen des Datenschutzes unberücksichtigt lässt. Trotz inhaltlicher Bedenken hat der Bundesrat von einer Anrufung des Vermittlungsausschusses abgesehen (Bundesratsdrucksache [BR-Drs.] 382/15 Beschluss). Das Gesetz ist am 21. November 2015 in Kraft getreten (BGBl. I S. 1938).

Inhaltlich geht es bei dem Gesetz vor allem um ein verbessertes Zusammenwirken der Verfassungsschutzbehörden von Bund und Ländern. Hierzu erhält das Bundesamt für Verfassungsschutz (BfV) eine Koordinierungsaufgabe und seine operativen Zuständigkeiten werden auf sämtliche, auch nicht länderübergreifende gewaltorientierte Bestrebungen ausgedehnt. Um die Informationsflüsse zu verbessern, werden künftig alle relevanten Informationen zwischen den Verfassungsschutzbehörden ausgetauscht. Die bisherige bloße Indexfunktion der Verbunddatei NADIS (Nachrichtendienstliches Informationssystem) der Verfassungsschutzbehörden wird um Volltextdateien ergänzt; damit werden die Möglichkeiten der Datenspeicherung und der Volltextrecherche sowie der Führung elektronischer Akten erweitert.

Das Gesetz ist in vielerlei Hinsicht datenschutzrechtlich frag- und kritikwürdig. Dies betrifft vor allem die erweiterten Auswertungs- und Analysekompetenzen des BfV sowie die neue Datenbankstruktur.

Die erweiterten Kompetenzen nach § 5 Absatz 2 des Bundesverfassungsschutzgesetzes (BVerfSchG), die sich auf alle von §§ 3 und 4 BVerfSchG erfassten Bestrebungen erstreckt, hat auch der Bundesrat kritisch angesprochen. Das Gesetz regelt nicht, mit welchen Mitteln das BfV die Daten auswerten kann; die vertiefte softwaregestützte Analyse unstrukturierter Daten nach dem Vorbild von „Big Data“ ist zu befürchten. Wie der Abgleich personenbezogener Daten in diesem Auswertesystem begrenzt werden soll, bleibt unklar. Überdies lässt das Gesetz in § 6 BVerfSchG unbegrenzte Volltextdateien in NADIS zu. Derartige Erweiterungen sind von den Datenschutzbeauftragten bereits 2010 abgelehnt worden (Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden“, LT-Drs. 15/955, Anhang 11). Für gewalttätige Bestrebungen sind schon jetzt erweiterte Speichermöglichkeiten erlaubt; NADIS-neu geht jedoch über die bisherige Hinweisdatei weit hinaus und lässt künftig die Recherche auch zu Randpersonen zu, die keiner gewalttätigen Bestrebungen angehören und zu denen bisher keine eigenständige Personenakte angelegt werden durfte. Das kommt m. E. einem Paradigmenwechsel gleich. Aus datenschutzrechtlicher Sicht fehlen hierzu normenklare und bereichsspezifische Eingriffsschwellen, die der Gesetzgeber selbst festlegen sollte; die im Entwurf vorgesehene Vollprotokollierung aller Zugriffe vermag dieses Defizit nicht auszugleichen. Kritisch zu bewerten ist ferner die weiterhin fehlende Regelung des Einsatzes nachrichtendienstlicher Mittel im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung; auch hier hat der Gesetzgeber die Gelegenheit nicht genutzt, die Eingriffsintensität nachrichtendienstlicher Maßnahmen insgesamt hinreichend zu differenzieren. Die Vorschriften zur Übermittlung personenbezogener Daten dürften überdies der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Trennungsprinzip zwischen Polizei und Nachrichtendiensten widersprechen. Statt verfassungskonformer Begrenzungen werden im Gesetz neue Befugnisse geschaffen; der Grundsatz der Zweckbindung wird weiter aufgeweicht. Verfassungsrechtlich bedenklich erscheint zudem, dass die in Artikel 87 Absatz 1 des Grundgesetzes verankerte Zentralstellenfunktion von Bundesbehörden, die bisher im Wesentlichen als Koordinierungsaufgabe verstanden wurde, in unzulässiger Weise ausgedehnt wird.

32. Tätigkeitsbericht 2014/2015 - 2. Innere Sicherheit

Dass die Länder nun eigene Kompetenzen Bundesbehörden überlassen, ist eigentlich nur mit dem großen öffentlichen Druck zu erklären, der nach der Aufdeckung der NSU-Mordserie auf allen Sicherheitsbehörden lastet; der Bund hat diese Situation nicht ungeschickt ausgenutzt.

Trotz deutlich vorgetragener Kritik sowohl seitens der Sachverständigen im Rahmen der öffentlichen Anhörung zum Gesetzentwurf als auch seitens der unabhängigen Datenschutzbehörden, die nachträglich nochmals durch eine Entschließung am 30. September/1. Oktober 2015 („Verfassungsschutzreform bedroht die Grundrechte“, vgl. Anhang 26) bekräftigt wurde, wurde das Gesetz unverändert in Kraft gesetzt. Dies bedeutet einen weiteren Schritt in Richtung einer Aushöhlung des Rechts auf informationelle Selbstbestimmung im sensiblen Bereich geheimdienstlicher Tätigkeit.

3. Justiz

3.1 Vorratsdatenspeicherung

Trotz heftiger Proteste – auch von Datenschützern – ist die Vorratsdatenspeicherung, allerdings in einer gegenüber den Vorläuferregelungen deutlich reduzierten Form, nunmehr eingeführt worden.

Am 16. Oktober 2015 verabschiedete der Bundestag das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“, mit dem die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr wieder eingeführt wird. Neben dem Entwurf der Regierungsfractionen (BT-Drs. 18/5088) hatte die Bundesregierung hierzu einen textidentischen Entwurf in den Bundesrat eingebracht (BR-Drs. 249/15). Am 6. November 2015 beschloss der Bundesrat, den Vermittlungsausschuss nicht anzurufen (BR-Drs. 492/15). Am 17. Dezember 2015 wurde das neue Gesetz im Bundesgesetzblatt veröffentlicht (BGBl. I S. 2218 f.) und trat einen Tag später in Kraft. Damit geriet ein jahreslanges zähes Ringen um die Vorratsdatenspeicherung an sein vorläufiges Ende. Künftig werden zehn Wochen lang die Rufnummern sowie Zeitpunkt und Dauer eines Anrufs und bei Internetverbindungen die IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe gespeichert werden. Bei Mobilfunkverbindungen sind auch die Standortdaten für vier Wochen zu speichern. E-Mails sind dagegen von der Speicherung ausgenommen. Die Speicherung von Inhalten sieht das Gesetz ebenfalls nicht vor. Allerdings ist kurz vor Verabschiedung des Gesetzes bekannt geworden, dass Mobilfunkbetreiber auch die Inhalte von SMS-Nachrichten speichern, weil es angeblich nicht möglich sei, diese von den Stammdaten zu trennen.

Mit Urteil vom 2. März 2010 (1 BvR 256/08 und andere, BVerfGE 125, 260–385) hatte das Bundesverfassungsgericht die damaligen Regelungen zur Vorratsdatenspeicherung für nichtig erklärt. Es bewertete die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kenne.

Vier Jahre später, am 8. April 2014 (C-293/12, Celex-Nr. 62012CJ0293), erklärte der Europäische Gerichtshof die europäische Richtlinie zur Vorrats-

speicherung von Telekommunikationsverkehrsdaten (Richtlinie 2006/24-EG), die ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete, für ungültig. In dieser Entscheidung wies der Europäische Gerichtshof u. a. darauf hin, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstelle und diese in der europäischen Grundrechtecharta verbrieften Rechte nur eingeschränkt werden dürften, soweit dies absolut notwendig sei. Der Europäische Gerichtshof kritisierte insbesondere die unzureichenden Vorgaben und fehlenden Konkretisierungen in der Richtlinie. Er führte in seiner Entscheidung beispielsweise aus, dass die Richtlinie zwar dem Ziel der Bekämpfung schwerer Kriminalität dienen solle, aber kein Zusammenhang zwischen den zu speichernden Daten und einer Bedrohung der öffentlichen Sicherheit verlangt werde. Außerdem sei die Datenspeicherung weder in räumlicher Hinsicht noch mit Blick auf einen bestimmten Personenkreis, der etwa in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, beschränkt. Darüber hinaus bemängelte der Europäische Gerichtshof, dass die Richtlinie keine Ausnahme für Berufsgeheimnisträger vorsah.

Die Datenschutzbeauftragten des Bundes und der Länder, die die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt hatten, begrüßten diese Entscheidung ebenso wie die nachfolgende Absichtserklärung der Bundesregierung, zunächst kein neues Gesetz zur Speicherung von Verkehrsdaten einführen zu wollen, sondern etwaige Diskussionen auf europäischer Ebene abwarten zu wollen (Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25. April 2014: „Ende der Vorratsdatenspeicherung in Europa“, vgl. Anhang 6). Obwohl die EU-Kommission verlautbart hatte, dass vorläufig keine weitere Regelungsabsicht auf europäischer Ebene bestehe, lag bereits im Mai 2015 ein Gesetzentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vor. Einen gleichlautenden, von den Regierungsfractionen eingebrachten Gesetzentwurf hat der Bundestag nun – mit wenigen Änderungen – verabschiedet.

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

So sieht die vom Bundestag beschlossene Fassung – im Gegensatz zum Ausgangsentwurf – vor, dass das Gesetz hinsichtlich der Auswirkungen auf Strafverfolgung und Gefahrenabwehr, der für Wirtschaft und Verwaltung verursachten Kosten sowie der Einhaltung der datenschutzrechtlichen Regelungen wissenschaftlich evaluiert werden soll. Dass eine Evaluierung vorzunehmen ist, begrüße ich ausdrücklich. Dass der ursprüngliche Entwurf der Bundesregierung keine Evaluation vorgesehen hatte, hatten die Datenschutzbeauftragten des Bundes und der Länder bereits in einer Umlaufentschließung vom 9. Juni 2015 („Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken“, vgl. Anhang 24) kritisiert. Die weiteren in der Umlaufentschließung geäußerten verfassungsrechtlichen und europarechtlichen Bedenken sind dagegen aufrecht zu erhalten:

Auch das verabschiedete Gesetz greift unabhängig von einem konkreten Verdacht erheblich in die Grundrechte aller ein. Denn die Speicherung von Verkehrsdaten kann ebenso aussagekräftig sein wie die Speicherung von Inhalten. Aus der Gesamtheit der gespeicherten Verkehrsdaten, zum Beispiel wie oft kommuniziert wer mit wem von welchem Ort aus und auf welchem Wege, können Rückschlüsse auf das Leben der Betroffenen gezogen werden, wie etwa Gewohnheiten des täglichen Lebens, regelmäßige Aufenthaltsorte, soziale Beziehungen und dergleichen.

Derart eingriffsintensive Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, müssen einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Dass das Gesetz den Anforderungen genügt, die das Bundesverfassungsgericht und der Europäische Gerichtshof in ihren vorgenannten Entscheidungen hierzu präzisiert haben, ist zumindest fraglich.

So sind Berufsheimnisträger nicht von der Speicherung ausgenommen, lediglich den Zugriff auf diese Daten sieht das Gesetz nicht vor. Auch die Vorgabe des Europäischen Gerichtshofs, hinsichtlich der Datenarten, der Speicherfristen und der Verwendungszwecke zu differenzieren, ist im Gesetz nur unzureichend umgesetzt. Darüber hinaus wurde bislang nicht hinreichend begründet, dass die Speicherung von Telekommunikationsdaten erfor-

derlich ist. Bereits im Jahre 2011 hatten sowohl das Max-Planck-Institut für europäisches und internationales Strafrecht (Freiburg) als auch der Wissenschaftliche Dienst des Deutschen Bundestages in Gutachten die Wirksamkeit der Vorratsdatenspeicherung in Frage gestellt.

Letztendlich wird auch über die Neuauflage der Vorratsdatenspeicherung das Bundesverfassungsgericht entscheiden. Kritiker haben bereits Verfassungsbeschwerden angekündigt.

3.2 Einführung der Elektronischen Akte im Strafverfahren

Bereits seit einigen Jahren gibt es Bestrebungen, im Strafverfahren die Elektronische Akte einzuführen. Die elektronische Aktenführung wird nicht nur die derzeitigen Rahmenbedingungen grundsätzlich verändern, sie birgt auch erhebliche Gefahren für das Recht auf informationelle Selbstbestimmung.

Bislang gibt es einerseits Papierakten. Sie dienen dazu, die einzelnen Fälle zu bearbeiten und das Vorgehen der Behörden zu dokumentieren. Andererseits verfügen die am Strafverfahren beteiligten Stellen über elektronische Dateisysteme. Jede Stelle betreibt ein eigenes Vorgangsverwaltungssystem, in dem die Stammdaten des Verfahrens, beispielsweise Angaben über Beschuldigte, Geschädigte, Zeugen, Verteidiger und zum Tatvorwurf, gespeichert sind. Vor allem die Polizei verfügt bereits heute über weitergehende Dateisysteme, die nicht nur für die Bearbeitung des konkreten Falles genutzt werden, sondern beispielsweise auch eine schnelle und umfassende Recherche für andere Strafverfahren ermöglichen. Derzeit ist die elektronische Datenverarbeitung der am Strafverfahren beteiligten Stellen, von eng definierten Schnittstellen abgesehen, die den Austausch mit den Systemen der anderen Stellen ermöglichen, strikt voneinander getrennt. Die gesetzlichen Regelungen dazu, welche Daten überhaupt dateimäßig erfasst werden dürfen, sind außerdem relativ eng gefasst.

Diese Begrenzungen der elektronischen Datenverarbeitung sind auf das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 (BVerfGE 65, 1 ff.) zurückzuführen. Bereits damals hatte das Bundesverfassungsgericht ausgeführt, dass sich aus den mit der elektronischen Datenver-

arbeitung verbundenen Möglichkeiten besondere Gefahren für das Recht auf informationelle Selbstbestimmung ergeben. Um diese Gefahren einzudämmen, hat das Bundesverfassungsgericht besondere Vorgaben für die elektronische Datenverarbeitung aufgestellt und dem Gesetzgeber aufgegeben, diesen durch restriktive gesetzliche Regelungen Rechnung zu tragen.

Diese vom Bundesverfassungsgericht vorgegebenen Begrenzungen der elektronischen Datenverarbeitung dürfen durch die Einführung der elektronischen Strafakte nicht ausgehöhlt werden. Der Gesetzgeber steht daher in der Pflicht, durch entsprechende Regelungen den Schutz des informationellen Selbstbestimmungsrechts auch nach Einführung der elektronischen Strafakte zu gewährleisten. So darf die elektronische Strafakte zum Beispiel nicht umfassend elektronisch recherchierbar und auswertbar sein. Es darf ebenfalls nicht ermöglicht werden, dass die Daten ohne weiteres in andere Verfahren überführt werden können. Darüber hinaus sind zahlreiche weitere Fragen zu klären, wie etwa, welche Stelle die elektronische Akte „führen“ wird und die datenschutzrechtliche Verantwortung trägt, welche Stelle und welche Mitarbeiter welche Zugriffsberechtigungen haben sollen usw.

Vor Einführung der elektronischen Strafakte muss der Gesetzgeber genau regeln, innerhalb welcher Grenzen die Strafverfolgungsbehörden die gespeicherten Daten verwenden dürfen und wie dies durch eng auszugestaltende technisch-organisatorische Maßnahmen sicherzustellen ist.

3.3 Öffentlichkeitsfahndung in sozialen Netzwerken

Strafverfolgungsbehörden haben ein großes Interesse daran, soziale Netzwerke zur Öffentlichkeitsfahndung zu nutzen. Dies ist aus datenschutzrechtlicher Sicht äußerst problematisch.

Die strafprozessuale Öffentlichkeitsfahndung richtet sich nach den gesetzlichen Bestimmungen der §§ 131 bis 131c StPO. Aufgrund ihrer technikoffenen Formulierung kommen diese Vorschriften als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Bei Erlass dieser Vorschriften dürfte der Gesetzgeber allerdings von der Nutzung klassischer Methoden für die Öffent-

lichkeitsfahndung ausgegangen sein. Die Nutzung sozialer Netzwerke für die Öffentlichkeitsfahndung führt im Vergleich hierzu zu weitaus gravierenderen Eingriffen in die Persönlichkeitsrechte der Betroffenen. Die Daten sind nicht nur weltweit recherchierbar, sie können mit geringem Aufwand weiter verbreitet, kopiert und auf anderen Webseiten veröffentlicht werden. Die Löschung einer einmal veröffentlichten Ausschreibung wird dadurch erheblich erschwert, oftmals sogar unmöglich. Hierdurch kann zum einen die Resozialisierung von Straftätern beeinträchtigt werden, zum anderen kann aber auch die Rechtsstellung von Betroffenen, die ohne Verschulden in eine Fahndung einbezogen werden, erheblich gefährdet werden. Da das Internet nichts „vergisst“, kann der einmal entstandene Ansehensverlust nicht wieder ausgeglichen werden. Die Persönlichkeitsrechte von Betroffenen können außerdem durch Kommentare von Nutzern der sozialen Netzwerke erheblich beeinträchtigt werden. Durch öffentliche Spekulationen, verleumderische Kommentare usw. können zufällig verdächtige Personen einer regelrechten Hetzjagd ausgesetzt sein. So kam es im Zusammenhang mit einem Mordfall im Jahr 2012 im Internet zu einem Aufruf zur Lynchjustiz gegen eine irrtümlich unter Mordverdacht stehende Person.

Auf Bitte der Justizministerkonferenz, sich zum Thema Öffentlichkeitsfahndung in sozialen Netzwerken zu äußern, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer 87. Konferenz am 27. und 28. März 2014 eine Entschließung verabschiedet („Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“, vgl. Anhang 4). In dieser forderte sie dazu auf, die Nutzung sozialer Netzwerke zum Zweck der Öffentlichkeitsfahndung wegen der damit verbundenen besonderen Gefahren nur unter engen Voraussetzungen zuzulassen. In der Entschließung sind u. a. folgende Punkte genannt:

- Da Rückmeldungen über Kommentierungsfunktionen für die Ermittlungsbehörden aufgrund der vorgenannten Risiken (Aufruf zu Hetzjagden usw.) weder geeignet noch erforderlich sind, darf nur auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückgegriffen werden.
- Der Gesetzgeber sollte in den Vorschriften der Strafprozessordnung zur Öffentlichkeitsfah-

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

derung klarstellen, dass diese im Hinblick auf den Verhältnismäßigkeitsgrundsatz für die Öffentlichkeitsfahndung im Internet nur eingeschränkt anwendbar sind. Zumindest müssen die besonderen Voraussetzungen der Fahndung im Internet in Umsetzungsvorschriften konkretisiert werden.

- Es muss klargestellt werden, dass die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten haben, und dass eine Öffentlichkeitsfahndung in sozialen Netzwerken nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht kommt.
- Es ist klarzustellen, dass die Staatsanwaltschaft bereits im Antrag auf richterliche Anordnung der Maßnahme konkrete Angaben zur Art, dem Umfang und der Dauer der Öffentlichkeitsfahndung machen muss, wie zum Beispiel, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.
- Es ist weiter sicherzustellen, dass die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden und dass die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerken erfolgt.

Zwischenzeitlich zeichnet sich ab, dass zur Festlegung eines bundesweiten Standards für die Öffentlichkeitsfahndung in sozialen Netzwerken die Anlage B der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) geändert werden wird. Ich gehe davon aus, dass dabei die meisten der von der Datenschutzkonferenz angesprochenen Punkte berücksichtigt werden. Allerdings ist nicht damit zu rechnen, dass auch die Forderung der Datenschutzkonferenz, zu Zwecken der Öffentlichkeitsfahndung nur auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, umgesetzt werden wird. Es scheint vielmehr auf eine Regelung hinauszulaufen, nach der im Einzelfall zu prüfen ist, ob von der Bereitstellung etwaiger Kommentierungsfunktionen abgesehen wird und – soweit die Kommentierungsfunktion freigeschaltet wird

– die Kommentare der Nutzer rund um die Uhr durch die Strafverfolgungsbehörden zu überwachen sind.

3.4 Auskunftsanspruch für Grundstückseigentümer

Aufgrund des durch Gesetz vom 1. Oktober 2013 (BGBl. I S. 3719) neu eingefügten § 12 Absatz 4 der Grundbuchordnung (GBO) kann ein Grundstückseigentümer grundsätzlich Auskunft darüber verlangen, wer in die ihn betreffenden Grundbucheintragungen Einsicht genommen hat. In Baden-Württemberg ist diese Bestimmung – aufgrund einer Verordnung der Landesregierung vom 29. Juli 2014 – jedoch erst ab dem 1. Januar 2018 anzuwenden.

Vor der Rechtsänderung beschränkten sich die Auskunftsansprüche von Grundstückseigentümern über Einsichtnahmen auf automatisierte Abrufe. Für Einsichtnahmen beim Grundbuchamt selbst existierten keine entsprechenden Auskunftsansprüche. Auch eine Protokollierung über Einsichtnahmen war – anders als bei automatisierten Abfragen – nicht vorgesehen.

Durch § 12 Absatz 4 GBO wird der Auskunftsanspruch der Grundstückseigentümer über Einsichtnahmen in sie betreffende Grundbucheintragungen erheblich erweitert.

3.5 Neuordnung des Notariatswesens

Im Bereich der Notariate wird es in den nächsten Jahren zu weitreichenden Veränderungen kommen, die auch datenschutzrechtliche Auswirkungen haben können.

Baden-Württemberg wird – wie in der Bundesnotarordnung vorgesehen – zum 1. Januar 2018 seine staatlichen Notariate auflösen. Der hiermit verbundene Regelungs- und Organisationsbedarf dürfte – nicht nur aus datenschutzrechtlicher Sicht – immens sein. So ist im Zusammenhang mit der Auflösung der staatlichen Notariate zum Beispiel sicherzustellen, dass die Übergabe und Fortführung von laufenden Vorgängen durch die ab dem 1. Januar 2018 zuständigen Stellen und die Verwahrung von abgeschlossenen Vorgängen datenschutzrechtlichen Anforderungen genügen.

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

Auf Bundesebene gibt es darüber hinaus Bestrebungen, die Aufbewahrung von Notariatsunterlagen neu zu strukturieren und bei der Bundesnotarkammer ein zentrales elektronisches Urkundenarchiv zu errichten, in dem die langfristige Aufbewahrung von Notariatsunterlagen künftig in elektronischer Form erfolgen soll. Dieses elektronische Urkundenarchiv soll die Führung einer elektronischen Urkundensammlung, eines Urkundenverzeichnisses und eines Verwahrungsverzeichnisses durch die Notare ermöglichen. Die mit dieser Thematik befasste Arbeitsgruppe hat hierzu einen Entwurf erarbeitet, den mir das Justizministerium im Jahr 2014 zur Stellungnahme vorgelegt hat.

Die in diesem Entwurf vorgesehene Neuordnung der Aufbewahrung von Notariatsunterlagen wirft eine Vielzahl datenschutzrechtlicher Fragen und Probleme auf. So soll das zentrale elektronische Urkundenarchiv zwar bei der Bundesnotarkammer eingerichtet und von dieser betrieben werden. Für die dort von den bundesweit tätigen Notaren „aufbewahrten“ Unterlagen und die darin gespeicherten personenbezogenen Daten sollen jedoch die jeweiligen Notare verantwortlich bleiben. Wie die Notare dieser Verantwortung gerecht werden sollen, ist angesichts dessen, dass sie keinen Einfluss auf den Betrieb des Urkundenarchivs und damit darauf haben, wie mit „ihren“ dort gespeicherten Dokumenten umgegangen wird, nicht ersichtlich. Es ist daher sicherzustellen, dass die verantwortlichen Stellen auch die Möglichkeit haben, ihrer Verantwortung nachzukommen.

Dem meiner Dienststelle vorgelegten Entwurf war außerdem nicht immer eindeutig zu entnehmen, welche Stelle für welchen Datenverarbeitungsvorgang verantwortlich sein soll. Auch dies ist aus datenschutzrechtlicher Sicht eindeutig zu regeln.

Der Entwurf sah darüber hinaus vor, dass die Landesbeauftragten für den Datenschutz keine Kontrollbefugnisse mehr über die Notare haben sollen. Von den vorgebrachten Argumenten, die ich alle nicht für stichhaltig halte, möchte ich beispielhaft die folgenden nennen:

So wird im Entwurf vorgetragen, dass eine doppelte Kontrolle des Datenschutzes durch Dienstaufsicht und Landesdatenschutzbeauftragte unnötig und im Hinblick auf das notarielle Berufsgeheimnis und das Recht der Betroffenen auf informationelle Selbstbestimmung problematisch sei.

Hierzu ist festzustellen, dass die „doppelte Kontrolle“ der Normalfall ist. Öffentliche Stellen unterliegen grundsätzlich der Dienstaufsicht (und regelmäßig der Fachaufsicht) und unabhängig hiervon der Kontrolle der Landesdatenschutzbeauftragten. Auch die Kontrolle von öffentlichen Stellen des Landes, deren Mitarbeiter Berufsgeheimnisträger sind, gehört für meine Dienststelle zum Alltag und ergibt sich aus § 28 Absatz 2 Satz 1 LDSG. In dieser Vorschrift ist geregelt, dass sich die Kontrolle des Landesdatenschutzbeauftragten auch auf personenbezogene Daten erstreckt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Inwiefern eine doppelte Kontrolle gerade bei den Notaren unnötig sein sollte, erschließt sich mir insofern nicht.

Mit dem Entzug der Kontrollbefugnis würde den von einer notariellen Datenverarbeitung Betroffenen das Recht abgesprochen werden, sich an den Landesdatenschutzbeauftragten zu wenden (§ 27 LDSG). Dies kann – anders als im Entwurf ausgeführt – nicht mit dem Recht der Betroffenen auf informationelle Selbstbestimmung begründet werden. Ganz im Gegenteil wäre der vorgesehene Entzug der Möglichkeit, sich an den Landesdatenschutzbeauftragten zu wenden, für das informationelle Selbstbestimmungsrecht der Betroffenen höchst problematisch.

Falls die dem Notargeheimnis unterliegenden Daten vollständig der Kontrolle der Landesdatenschutzbeauftragten entzogen werden sollten, hätte dies außerdem zur Folge, dass diese Daten, obwohl es sich um besonders schutzwürdige Daten handelt, künftig weniger Schutz erfahren würden als „normale“ personenbezogene Daten.

Das Justizministerium, dem ich meine Bedenken und Anregungen vorgetragen habe, hat diese an die mit der Erarbeitung des Gesetzentwurfs befasste Arbeitsgruppe weitergeleitet und zugesagt, meine Dienststelle über den weiteren Verlauf der Arbeiten an dem Entwurf zu unterrichten.

Sowohl die mit der Auflösung der staatlichen Notariate verbundenen Aufgaben als auch die mit der Einführung eines zentralen elektronischen Urkundenarchivs zu klärenden datenschutzrechtlichen Fragen sind aus datenschutzrechtlicher Sicht ausgesprochen anspruchsvoll. Meine Dienststelle wird die im Notariatswesen in den nächsten Jahren anstehenden Veränderungen aufmerksam verfolgen.

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

3.6 Kontrollen bei Notariaten

Mitarbeiter meiner Dienststelle haben im Berichtszeitraum anlasslose Kontrollbesuche bei zwei staatlichen Notariaten im württembergischen Rechtsgebiet durchgeführt. Dort haben sie sich vor allem darüber informiert, wie die Entsorgung von datenschutzrechtlich relevanten Unterlagen organisiert worden ist.

Zunächst ist in diesem Zusammenhang auf eine württembergische Besonderheit hinzuweisen: Bis zur Auflösung der staatlichen Notariate zum 1. Januar 2018 (siehe Kapitel 3.5) sind die Gemeinden des württembergischen Rechtsgebiets, in deren Gebiet ein staatliches Notariat seinen Sitz hat, u. a. verpflichtet, die erforderlichen Diensträume samt Einrichtungsgegenständen zur Verfügung zu stellen und die Diensträume zu reinigen. Zur Reinigung der Diensträume gehört auch die Altpapierentsorgung. Diese gesetzliche Regelung hat teilweise seltsame Auswirkungen.

So ist der Notar zwar für die datenschutzgerechte Aufbewahrung der Notariatsunterlagen, die oftmals sensible personenbezogene Daten enthalten, verantwortlich. Die Verpflichtung, das Notariat mit Räumlichkeiten und Mobiliar auszustatten, die dem Notar eine datenschutzgerechte Aufbewahrung seiner Unterlagen ermöglichen, liegt dagegen bei der jeweiligen Gemeinde. Kommt die Gemeinde ihrer Ausstattungspflicht nicht in angemessenem Umfang nach und führt dies etwa dazu, dass die in Notariatsunterlagen gespeicherten personenbezogenen Daten nur unzureichend vor unberechtigten Zugriffen geschützt sind, trifft hierfür den Notar die datenschutzrechtliche Verantwortung. Andererseits ist die Gemeinde ab Aushändigung für die datenschutzgerechte Entsorgung des datenschutzrelevanten Altpapiers des Notariats verantwortlich, ohne jedoch vom Inhalt der zu entsorgenden Unterlagen Kenntnis nehmen zu dürfen.

Auch im Rahmen der beiden Kontrollbesuche ist diese rechtliche Konstruktion relevant geworden. In beiden der von meinen Mitarbeitern kontrollierten Notariate war die Aufbewahrung des datenschutzrelevanten Altpapiers bis zur Übergabe an die zuständigen Mitarbeiter der Gemeinde zunächst unzureichend. In einem der Notariate wurde das Altpapier in offenen Behältnissen gesammelt, auf die nicht nur

unzuständige Mitarbeiter des Notariats, sondern theoretisch auch Besucher hätten zugreifen können. Auch im zweiten Notariat wurde das datenschutzrelevante Altpapier in offenen Behältnissen gesammelt. Durch die Standorte dieser Behältnisse bestand zwar nicht die Gefahr, dass Besucher oder unzuständige Mitarbeiter auf die zur Vernichtung vorgesehenen Unterlagen zugreifen konnten, allerdings bestand die Möglichkeit, dass Mitarbeiter des externen Reinigungsdienstes, die nicht für die Entsorgung/Vernichtung des Altpapiers zuständig waren, vom Inhalt dieser Unterlagen Kenntnis nehmen. In dem zwischen der zuständigen Gemeinde und der externen Reinigungsfirma bestehenden Vertrag war zwar vorgesehen, dass die Mitarbeiter der Reinigungsfirma auf das Datengeheimnis verpflichtet werden. Angesichts der Sensibilität der in einem staatlichen Notariat anfallenden personenbezogenen Daten war diese Maßnahme meiner Ansicht nach jedoch nicht ausreichend, um den Anforderungen des § 9 Absatz 2 LDSG zu genügen, wonach technisch-organisatorische Maßnahmen erforderlich sind, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Zwischenzeitlich wurden beiden Notariaten von der jeweils zuständigen Gemeinde Datencontainer zur Verfügung gestellt, die die datenschutzgerechte Aufbewahrung des für die Vernichtung bestimmten datenschutzrelevanten Altpapiers ermöglichen.

Von einem der kontrollierten Notariate wurden meine Mitarbeiter bereits bei Ankündigung des Kontrollbesuchs gebeten, das Notariat in einer datenschutzrechtlichen Angelegenheit zu unterstützen. In diesem Notariat, das in einem mehrstöckigen Gebäude untergebracht ist, in dem neben dem Notariat verschiedene Dienstleister Büro- bzw. Geschäftsräume haben, die von einem gemeinsamen Treppenhaus abgehen, seien vor einigen Jahren bei einem Einbruchversuch die vom Treppenhaus abgehenden Stockwerkstüren des Notariats aufgebrochen worden. Dabei seien Schäden an den Metallrahmen im Bereich der Schließmechanismen verursacht worden. Die Schäden seien bis zum Zeitpunkt des Kontrollbesuchs, trotz regelmäßiger Aufforderungen durch das Notariat an die zuständige Gemeinde, nur provisorisch repariert worden. Das Notariat war der Ansicht, der sich meine Mitarbeiter während des Kontrollbesuchs anschlossen, dass diese Türen, die

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

zwar noch abschließbar waren, nicht geeignet seien, einen unberechtigten Zugang zum Notariat effektiv zu verhindern. Dem Wunsch des Notariats um Unterstützung bin ich nachgekommen und habe mich an die zuständige Gemeinde gewandt. Die Stockwerkstüren sind zwischenzeitlich repariert.

Rechtlich bewerte ich diesen Vorgang folgendermaßen:

Die Gemeinde ist zwar verpflichtet, dem staatlichen Notariat angemessene Diensträume zur Verfügung zu stellen, also solche, die eine den datenschutzrechtlichen Anforderungen entsprechende Verwahrung der Akten ermöglichen. Trotz dieser Verpflichtung liegt die datenschutzrechtliche Verantwortung für die sichere Aufbewahrung der in einem Notariat verwahrten Schriftstücke und damit auch dafür, dass das Notariat vor einem unberechtigten Eindringen und vor unberechtigten Zugriffen auf personenbezogene Daten in angemessener Weise geschützt ist, aber dennoch beim jeweiligen Notar. Insofern hätte das Notariat sich nicht mit regelmäßigen Beschwerden an die ausstattungspflichtige Gemeinde begnügen dürfen. Es hätte vielmehr Maßnahmen ergreifen müssen, beispielsweise die Einschaltung der Kommunalaufsicht, die zu einer zeitnahen Beseitigung der Schäden geführt hätten.

Die Verpflichtung der Gemeinden, die staatlichen Notariate mit angemessenen Räumen auszustatten, ändert nichts daran, dass der jeweilige Notar die datenschutzrechtliche Verantwortung für die von ihm verwahrten personenbezogenen Daten trägt.

3.7 Kaputte Schlösser am Aktenschrank

Anfang Januar 2015 wies ein Bürger meine Dienststelle darauf hin, dass er im Wartezimmer eines Notariats unverschlossene Aktenschränke bemerkt habe, in denen Unterlagen und Akten aufbewahrt worden seien. Die Schranktüren seien leicht geöffnet gewesen, weshalb die Möglichkeit bestanden hätte, dass Besucher die dort gelagerten Unterlagen einsehen oder sogar entwenden konnten.

Auf Nachfrage meiner Dienststelle räumte das Notariat ein, dass an einem Aktenschrank im Wartezimmer, in dem Urkunden und Nachlassakten aus dem Vorjahr aufbewahrt worden seien, kurz vor Jahresende 2014 zwei Schlösser kaputt gegangen seien, so dass man die betroffenen Schranktüren nicht

mehr hätte verschließen können. Die in dem Schrank aufbewahrten Unterlagen seien im Januar 2015 in die Registratur abgegeben worden. Die defekten Schränke würden künftig nicht mehr genutzt werden. Von einer sofortigen Reparatur habe das Notariat angesichts der kurzen Zeit bis zur Abgabe der Akten an die Registratur und der Tatsache, dass das Notariat Ende 2017 geschlossen werde, abgesehen.

Dass diese – wenn auch nur kurzzeitig erfolgte – Art der Aufbewahrung von Schriftstücken mit sensiblen personenbezogenen Daten, die Zugriffe durch unbefugte Dritte ermöglichte, datenschutzrechtlichen Anforderungen nicht entsprach, bedarf keiner näheren Ausführungen. Meine Dienststelle hat das Notariat auf die Verpflichtung hingewiesen, technisch-organisatorische Maßnahmen zu treffen, um solche Zugriffe zu verhindern.

Aufgrund der Sensibilität der in Notariaten anfallenden personenbezogenen Daten sind hohe Anforderungen an die technisch-organisatorischen Maßnahmen zu stellen, die zur Gewährleistung einer datenschutzgerechten Datenverarbeitung zu treffen sind.

3.8 Unberechtigte Informationsweitergabe zwischen Gerichtsvollziehern

Die kollegial gemeinte Warnung vor säumigen Schuldnern kann datenschutzrechtlich problematisch sein.

Durch die Eingabe eines registrierten Inkassodienstleisters habe ich von folgendem Vorgang Kenntnis erhalten:

Eine Gerichtsvollzieherin hatte dem Inkassodienstleister, in dessen Auftrag sie tätig geworden war, Gerichtsvollzieherkosten in Rechnung gestellt. Da der Inkassodienstleister diese Kostenrechnung für unbegründet hielt, hatte er sie zunächst nicht beglichen und der Gerichtsvollzieherin per E-Mail mitgeteilt, weshalb er die Kostenrechnung für fehlerhaft halte. Die Gerichtsvollzieherin leitete diese E-Mail unter dem Betreff „Kostenwarnung“ ungekürzt und ebenfalls per E-Mail an einen Gerichtsvollzieherkollegen eines anderen Amtsgerichts weiter, der mit der zugrunde liegenden Angelegenheit nicht das Geringste zu tun hatte. Ihrer Bitte, die E-Mail des

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

Inkassodienstleisters allgemein den Gerichtsvollziehern im Land bekanntzugeben, kam der so Angeschriebene nach, indem er die E-Mail der Gerichtsvollzieherin und die angeschlossene E-Mail des Inkassodienstleisters ebenfalls unter dem Betreff „Kostenwarnung“ an eine große Zahl von Gerichtsvollzieherkollegen im Land weiterleitete.

Das war allerdings des Guten zu viel: Die Vermutung, dass ein Kostenschuldner sich weigern könnte, in künftigen Verfahren – in wessen Zuständigkeit diese auch immer liegen mögen – gewisse Kosten zu zahlen, berechtigt nicht dazu, diesen Kostenschuldner auf Vorrat bei einer Vielzahl von Gerichtsvollzieherkollegen (und damit auch bei Kollegen, die nie mit diesem Kostenschuldner zu tun haben werden) mit derartigen „Kostenwarnungen“ anzuschwärzen. Dies ist weder vorgesehen noch zur Aufgabenerledigung erforderlich. So hat ein Gerichtsvollzieher zum Beispiel die Möglichkeit, von einem Auftraggeber einen Vorschuss zu erheben, bei Meinungsverschiedenheiten zwischen Kostenschuldner und zuständigem Gerichtsvollzieher sieht das Gerichtsvollzieherkostengesetz Rechtsbehelfe vor und die zwangsweise Einziehung fälliger Gerichtsvollzieherkosten ist in der Justizbeitragsordnung ausdrücklich geregelt.

Sowohl die Weiterleitung der E-Mail des Inkassodienstleisters durch die Gerichtsvollzieherin an einen Kollegen als auch die Übermittlung der E-Mail durch diesen an eine Vielzahl von Gerichtsvollziehern des Landes Baden-Württemberg erfolgten damit ohne Übermittlungsbefugnis und waren rechtswidrig.

Ich habe diese Datenschutzverstöße dem Justizministerium gegenüber förmlich beanstandet. Dieses hat sich meiner Rechtsauffassung angeschlossen und verschiedene Maßnahmen ergriffen. So hat es zum Beispiel die Präsidenten der Oberlandesgerichte gebeten, die Gerichtsvollzieher an die Voraussetzungen zu erinnern, die nach den Vorgaben des Datenschutzes bei der Verarbeitung personenbezogener Daten zu beachten sind, und ihnen mitzuteilen, dass der Austausch sog. „Kostenwarnungen“ zwischen Gerichtsvollziehern unzulässig ist. Außerdem will es sich mit den Gerichtsvollziehern darüber austauschen, wie das Fortbildungsangebot im Bereich Datenschutz ergänzt werden kann. Das Justizministerium wird weiterhin die Gerichtsvollzieherausbildung daraufhin überprüfen, ob der Vermitt-

lung des Datenschutzes mehr Raum gegeben werden sollte, und die Ausbildungsleiter für das Thema Datenschutz sensibilisieren.

Wenn die Gerichtsvollzieher dem Thema Datenschutz künftig mehr Aufmerksamkeit widmen, hat die voreilige „Kostenwarnung“ letztlich doch noch Gutes bewirkt.

3.9 Aufbewahrungsfrist für die Handakten des Rechtsanwalts

„Quod non est in actis, non est in mundo“ – „was nicht in den Akten ist, ist nicht in der Welt“. Dieses Sprichwort beschreibt eigentlich das strenge Schriftlichkeitsprinzip im Prozessrecht, wie es vor der Einführung des Mündlichkeitsgrundsatzes in der Folge der französischen Revolution galt: Nur das schriftlich Dokumentierte war danach vom Richter bei der Urteilsfindung zu berücksichtigen. Es provoziert durch seine offensichtliche Fiktion, weil selbstverständlich auch nicht aktenmäßig Dokumentiertes real geschehen sein kann. Der Satz gilt aber in jedem Fall in seiner Umkehrung: Was in Akten gespeichert ist, bleibt in der Welt. Das kann gerade dann eine Belastung darstellen, wenn die Akten unangenehme Vorfälle dokumentieren. Und weil man Rechtsanwälte oft – wenn nicht gar in aller Regel – in nicht allzu angenehmen Situationen aufsucht, ist das Anliegen von Mandanten grundsätzlich nachvollziehbar, bei allem Vertrauen in die Verschwiegenheit und Integrität des aufgesuchten Anwalts irgendwann einmal die Angelegenheit nach deren Abschluss ganz „aus der Welt zu schaffen“ und für eine Löschung der in den Handakten dokumentierten Informationen über sich zu sorgen.

Dementsprechend werfen immer wieder Petenten die Frage auf, wann ein Rechtsanwalt nach Abschluss eines Mandats die in seiner EDV und in seinen Handakten enthaltenen personenbezogenen Daten zu löschen hat bzw. wie lange er Handakten aufbewahren muss oder darf.

Zur Beantwortung der Frage ist zunächst festzustellen, dass auf die in der EDV gespeicherten oder in den Handakten des Rechtsanwalts abgelegten personenbezogenen Daten das Bundesdatenschutzgesetz (BDSG) Anwendung findet: Ein Rechtsanwalt ist eine nicht-öffentliche Stelle im Sinne der § 1 Absatz 2 Nummer 3, § 2 Absatz 4 Satz 1, §§ 27 ff.

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

BDSG, die Erfassung mittels EDV stellt gem. § 1 Absatz 2 Nummer 3, § 3 Absatz 2 Satz 1, § 27 Absatz 1 BDSG eine Erhebung bzw. Verarbeitung mittels einer Datenverarbeitungsanlage dar, und durch Einordnung der Unterlagen in einen Handaktenapparat werden nicht automatisierte Dateien im Sinne der § 1 Absatz 2 Nummer 3, § 3 Absatz 2 Satz 2, § 27 Absatz 1 und 2 BDSG erzeugt. Die Datenverarbeitung dient dabei nicht ausschließlich persönlichen oder familiären Tätigkeiten (§ 1 Absatz 2 Nummer 3, § 27 Absatz 1 Satz 2 BDSG).

Die Anlegung von Handakten erfolgt im Rahmen eines rechtsgeschäftlichen Schuldverhältnisses, des Mandatsverhältnisses, und zwar für eigene Geschäftszwecke (§ 28 Absatz 1 Nummer 1 BDSG). Eine Löschung der zulässig erhobenen Daten hat gem. § 35 Absatz 2 Nummer 3 BDSG dann zu erfolgen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Bei Anwendung dieser Regelung ist allerdings zunächst zu beachten, dass einzelne Vorschriften bestimmte Aufbewahrungspflichten für den Rechtsanwalt vorsehen, die Unterlagen betreffen, die Teil der Handakten eines Rechtsanwalts darstellen können. So bestimmt das Steuerrecht in § 147 der Abgabenordnung, dass Geschäftsbriefe sechs Jahre und Buchungsbelege – hier vor allem Kostenrechnungen gegenüber dem Mandanten – zehn Jahre ab dem Ende des Kalenderjahres ihrer Entstehung aufzubewahren sind. Außerdem gilt für Rechtsanwälte das Geldwäschegesetz (GWG), wenn sie für ihren Mandanten an der Planung oder Durchführung von folgenden Geschäften mitwirken:

- Kauf und Verkauf von Immobilien oder Gewerbebetrieben,
- Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten,
- Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten,
- Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel,
- Gründung, Betrieb oder Verwaltung von Treuhandgesellschaften, Gesellschaften oder ähnlichen Strukturen,

oder wenn sie im Namen und auf Rechnung des Mandanten Finanz- oder Immobilientransaktionen

durchführen (§ 2 Absatz 1 Nummer 7 GWG). Dann haben sie Unterlagen, die sie in Erfüllung ihrer geldwäscherechtlichen Sorgfaltspflichten erheben (insbesondere Unterlagen zur Identifizierung von Vertragspartnern und zu den wirtschaftlich Berechtigten einer Transaktion, aber auch Unterlagen zu den Transaktionen selbst und der Herkunft von Vermögen) nach § 8 GWG fünf Jahre lang ab dem Schluss des Kalenderjahres aufzuheben, in dem die Geschäftsbeziehung zum Mandanten endete.

Eine grundlegende Bestimmung über die berufsrechtlichen Pflichten des Rechtsanwalts bei der Führung und Aufbewahrung von Handakten enthält die Bundesrechtsanwaltsordnung (BRAO): Die Regelung des § 50 Absatz 2 BRAO schreibt vor, dass der Rechtsanwalt die Handakten auf die Dauer von fünf Jahren nach Beendigung des Auftrags aufzubewahren hat. Diese Verpflichtung erlischt jedoch schon vor Beendigung dieses Zeitraumes, wenn der Rechtsanwalt den Auftraggeber aufgefordert hat, die Handakten in Empfang zu nehmen, und der Auftraggeber dieser Aufforderung binnen sechs Monaten, nachdem er sie erhalten hat, nicht nachgekommen ist. Auch diese Vorschrift regelt die Aufbewahrung der Handakte jedoch nicht abschließend. Für erstrittene (Original-)Titel – also gerichtliche Entscheidungen, Vergleiche u. a., aus denen der Mandant die Zwangsvollstreckung betreiben kann – werden über § 50 Absatz 2 BRAO hinaus längere Aufbewahrungspflichten gegenüber dem Mandanten (nämlich bis zur Undurchsetzbarkeit des Titels) angenommen. Vor allem aber betrifft die Bestimmung des § 50 Absatz 2 BRAO nur die Frage, wie lange – vorbehaltlich einer anderen konkreten Vereinbarung zwischen Anwalt und Mandat – der Anwalt gegenüber dem Mandanten zur Aufbewahrung *verpflichtet* ist, nicht jedoch diejenige, wie lange der Rechtsanwalt zur Aufbewahrung der Handakte datenschutzrechtlich *berechtigt* ist.

Für die Frage der Dauer der Aufbewahrungsbefugnis bleibt es mithin bei der Bestimmung des § 35 Absatz 2 Nummer 3 BDSG, der zufolge darauf abzustellen ist, wie lange die Kenntnis des Inhalts der Handakten noch für die Erfüllung eigener Geschäftszwecke des Rechtsanwalts (§ 28 Absatz 1 BDSG) erforderlich ist. Hierzu ist – außer den genannten Aufbewahrungspflichten – zu berücksichtigen, dass der Rechtsanwalt noch nach Beendigung des Mandats Haftungsansprüchen seines Mandan-

32. Tätigkeitsbericht 2014/2015 - 3. Justiz

ten wegen einer tatsächlichen oder vermeintlichen Fehlberatung ausgesetzt sein kann. Im Falle eines Haftungsprozesses trifft den Rechtsanwalt dabei regelmäßig die Obliegenheit darzulegen, welchen Rat er gegeben hat und welche Belehrung durch ihn erfolgt ist. Um dieser Darlegungsobliegenheit im Rahmen eines eventuellen Haftungsprozesses nachkommen zu können, kann die Aufbewahrung der Handakten noch bis zum Ablauf der Verjährung erforderlich sein. Für die Verjährung von (Haftungs-) Ansprüchen gegen den Rechtsanwalt gelten die Vorschriften aus den §§ 195 und 199 des Bürgerlichen Gesetzbuchs (BGB). Danach beginnt eine dreijährige Verjährungsfrist mit dem Schluss desjenigen Jahres, in dem der geschädigte Mandant nach Entstehen des Anspruchs von diesem Kenntnis erlangt oder nur aufgrund grober Fahrlässigkeit die Existenz des Anspruchs übersieht (§§ 195, 199 Absatz 1 BGB). Unabhängig von der Kenntnismöglichkeit des Mandanten tritt die Verjährung spätestens zehn Jahre nach Entstehung des Anspruchs ein (§ 199 Absatz 3 Nummer 1 BGB), wobei der Anspruch in diesem Sinne erst „entstanden“ ist, wenn ein Schaden eingetreten ist. Es sind aber auch Fälle vorstellbar, in denen aus einer anwaltlichen Pflichtverletzung ein Schaden des Mandanten erst lange nach Abschluss des Mandats eintritt; beispielsweise wird angenommen, dass dann, wenn die Pflichtverletzung des Anwalts in einer unklaren Vertragsgestaltung bestand, der Schaden erst entsteht, sobald der Vertragsgegner aus dem vermeintlich günstigeren Vertragsinhalt Rechte gegen seinen Vertragspartner herleitet. Für diesen Fall bestimmt § 199 Absatz 3 Nummer 2 BGB, dass die Verjährung spätestens mit Ablauf von 30 Jahren ab der anwaltlichen Pflichtverletzung eintritt.

Vor diesem Hintergrund wird Rechtsanwälten in der Literatur regelmäßig dazu geraten, die Handakten zur Abwehr von etwaigen Haftungsansprüchen mindestens zehn Jahre lang ab Beendigung des Mandats (so Christian Dahns, NJW-Spezial 2008, S. 414) bzw. ab dem Jahresende der Beendigung des Mandats (so Jürgen Bestellmeyer in einer Empfehlung der Rechtsanwaltskammer München⁴²), aufzuheben. Dem ist auch meines Erachtens grundsätzlich zu folgen, wobei entsprechend § 35 Absatz 3

Nummer 1 und 2 BDSG eine Sperrung der Daten (also eine Kennzeichnung und Separierung zur Einschränkung ihrer Nutzung, § 3 Absatz 4 Nummer 4 BDSG) zu erfolgen hat, wenn die Handakten ausschließlich noch zur Abwehr eventueller Haftungsansprüche vorgehalten werden (vgl. Dix, in: Simitis, BDSG, 8. Auflage 2014, § 35 Rn. 38 am Ende).

Vor Eintritt der Verjährung besteht eine Löschungspflicht nur dann, wenn eine Haftung des Rechtsanwalts aus anderen Gründen als der Verjährung ausgeschlossen werden kann, beispielsweise weil der Mandant den Rechtsanwalt durch Verzicht von einer Haftung freistellt, um die Löschung der Unterlagen zu erreichen. Dann sind – außer Originaltiteln, die der Mandant in diesem Falle aber sich aushändigen lassen wird – nur noch solche Unterlagen beim Anwalt aufzubewahren, für die eine steuer- oder geldwäscherechtliche Aufbewahrungspflicht besteht. Daneben bleibt der Rechtsanwalt noch zur Aufbewahrung des Haftungsverzichts selbst – aus dem ggf. auch der Umfang des Verzichts und damit ein Hinweis auf den Inhalt des damaligen Vertrages hervorgehen kann – berechtigt. Hinsichtlich dieser weiter aufzubewahrenden Daten kann der Mandant bei Verzicht auf Haftungsansprüche allerdings stets eine Sperrung gem. § 35 Absatz 3 Nummer 1 BDSG mit dem Ziel verlangen, dass sie nur noch für den jeweils mit der Aufbewahrungspflicht bzw. der Aufbewahrungsberechtigung verfolgten Zweck verwendet werden.

Rechtsanwälte dürfen die Handakten nach Abschluss des Mandats grundsätzlich noch so lange speichern, wie ihre Haftung wegen etwaiger Beratungsfehler in Betracht kommt. Der Mandant kann durch einen Haftungsverzicht für einen Großteil der Unterlagen eine frühere Löschung bewirken. Ob ein zur Verkürzung der Aufbewahrungsdauer erklärter Haftungsverzicht freilich auch im Hinblick auf die damit möglicherweise verbundenen (finanziellen) Nachteile sinnvoll ist, bleibt der eigenverantwortlichen Risikoabwägung des Mandanten vorbehalten.

⁴² Im Internet abrufbar unter <http://rak-muenchen.de/fileadmin/downloads/04-Berufsrecht/01-Berufsrecht/Aufbewahrungsfristen.pdf>

32. Tätigkeitsbericht 2014/2015 - 4. Steuern und Statistik

4. Steuern und Statistik

Zensus 2011 – und kein Ende!

Man soll den Tag nicht vor dem Abend loben: In meinem 30. Tätigkeitsbericht konnte ich noch die erfreuliche Botschaft verkünden „Volkszählung Zensus 2011: Ohne wesentliche Datenschutzmängel“ (LT-Drs. 15/955 S. 132). Nun haben sich hinsichtlich der beim Zensus verwendeten Hilfsmerkmale, also der Namen und Anschriften der Auskunftspflichtigen sowie weiterer personenbezogener Daten, im Zusammenhang mit den von über 140 baden-württembergischen Kommunen gegen die Feststellung der sie betreffenden Zensusergebnisse erhobenen Klagen doch noch gravierende Probleme ergeben. Einige Kommunen versuchten, beispielsweise in verwaltungsgerichtlichen Eilverfahren, eine über die vom Zensusrecht statuierten Zeitgrenzen hinaus fortdauernde Speicherung dieser Hilfsmerkmale zu erzwingen, damit diese Daten u. U. zur Begründung der Anliegen verwendet werden können, welche diese Kommunen mit ihren jeweiligen Klagen im Hauptsacheverfahren verfolgen. Konkret geht es darum, dass die klagenden Gemeinden mit dem sie betreffenden Datenmaterial aus dem Zensus 2011 nachweisen wollen, dass der ihre amtliche Einwohnerzahl feststellende Bescheid des Statistischen Landesamts fehlerhaft ist.

Diese Versuche waren bislang erfolgreich. Die von § 19 Absatz 1 Satz 3 des Zensusgesetzes 2011 (ZensG 2011) gesetzte äußerste Zeitgrenze für die Speicherung der Hilfsmerkmale, der 9. Mai 2015 (vier Jahre nach dem von § 1 Absatz 1 ZensG 2011 festgesetzten Berichtszeitpunkt 9. Mai 2011), ist überschritten. Die danach zu löschenden Daten werden beim Statistischen Landesamt Baden-Württemberg noch auf Bandkassetten mit für den Katastrophenfall angefertigten Sicherungskopien von XML- und Bilddateien gescannter Fragebögen sowie deren Metadaten und Sicherungen des Fileservers weiterhin gespeichert.

Aus Sicht des Datenschutzes war zunächst klar, dass das Statistische Landesamt die gesetzliche Löschungsverpflichtung in jedem Fall zu beachten hatte. Hatte doch das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1–71) deutlich zum Ausdruck gebracht, dass erst die vom Recht auf informationel-

le Selbstbestimmung geforderte und gesetzlich abzusichernde Abschottung der Statistik durch Anonymisierung der Daten und deren Geheimhaltung, soweit sie zeitlich begrenzt noch einen Personenbezug aufweisen, den Zugang der staatlichen Organe zu den für die Planungsaufgaben erforderlichen Informationen öffne. Nur unter dieser Voraussetzung könne und dürfe vom Bürger erwartet werden, die von ihm zwangsweise verlangten Auskünfte zu erteilen. „Dürften personenbezogene Daten, die zu statistischen Zwecken erhoben wurden, gegen den Willen oder ohne Kenntnis des Betroffenen weitergeleitet werden, so würde das nicht nur das verfassungsrechtlich gesicherte Recht auf informationelle Selbstbestimmung unzulässig einschränken, sondern auch die vom Grundgesetz selbst in Art. 73 Nr. 11 vorgesehene und damit schutzwürdige amtliche Statistik gefährden“. Zur Sicherung des Rechts auf informationelle Selbstbestimmung seien „Löschungsregelungen für solche Angaben erforderlich, die als Hilfsangaben (Identifikationsmerkmale) verlangt wurden und die eine Deanonymisierung leicht ermöglichen würden“. Und nachdem das Bundesverwaltungsgericht noch kürzlich festgestellt hatte, dass die Beachtung gesetzlicher Lösungsfristen nicht zu einer Beweislastumkehr führen könne (BVerwGE 149, 359–373), sah ich zunächst auch kein unvertretbares Prozessrisiko. Gestärkt sah ich mich auch durch den im Rahmen eines Eilverfahrens ergangenen Beschluss des Verwaltungsgerichts Freiburg (Breisgau) vom 20. Mai 2015 (3 K 922/15, juris), in dem das Verwaltungsgericht unter Verweis auf eine Reihe weiterer verwaltungsgerichtlicher Entscheidungen aus anderen Bundesländern feststellte, dass die nach ihrem Wortlaut eindeutige Vorschrift des § 19 ZensG eine weitere Aufbewahrung von Daten nicht zulasse:

„Angesichts des klaren Wortlauts von § 19 ZensG 2011 besteht keine Möglichkeit, von der Lösungs-vorschrift abzuweichen. [...] begegnet es keinen rechtlichen Bedenken, dass der Gesetzgeber – trotz der augenscheinlichen Möglichkeit, dass sich Gemeinden gegen die Feststellung der Einwohnerzahl wenden – die Löschung der Hilfsmerkmale zwingend und zudem spätestens zum 09.05.2015 angeordnet hat. Damit hat er dem Recht der Bürger auf informationelle Selbstbestimmung gegenüber dem Interesse der durch die Feststellung der amtlichen Einwohnerzahl betroffenen Gemeinden an der gerichtlichen Überprüfung der ihnen gegenüber organ-

32. Tätigkeitsbericht 2014/2015 - 4. Steuern und Statistik

genen Feststellungsbescheide den Vorrang eingeräumt. Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es enthält auch das Gebot der frühestmöglichen Vernichtung und Löschung von Daten (vgl. BVerfG, Urt., v. 15.12.1983 – 1 BvR 209/83 u. a. –, BVerfGE 65,1; BVerfG, Beschl. v. 24.09.1987 – 1 BvR 970/87 –, NJW 1987, 2805 = DVBl 1987, 1207). Vor diesem Hintergrund war der Gesetzgeber unter Beachtung des ihm zukommenden gesetzgeberischen Spielraums nicht verpflichtet, im Interesse der Gewährung effektiven Rechtsschutzes zugunsten betroffener Gemeinden die Aufbewahrung und Speicherung der die Gemeinden betreffenden Daten bis zum Eintritt der Bestandskraft von Bescheiden über die Feststellung ihrer amtlichen Einwohnerzahl zu ermöglichen. Dass dadurch die Überprüfung der Feststellungsbescheide nicht mehr im vollem Umfang möglich ist, begegnet aus Sicht der Kammer keinen Bedenken“ (a.a.O., Abs.-Nr. 7).

Diese aus meiner Sicht zutreffend begründete Auffassung wurde jedoch nicht von allen Gerichten geteilt. Insbesondere vertrat das Oberverwaltungsgericht für das Land Nordrhein-Westfalen in einem Beschluss vom 3. Juni 2015 (4 B 458/15, DVBl 2015, 1063–1067) die Auffassung, es komme „ernsthaft in Betracht“, die Fristbestimmungen des § 19 Abs. 1 Satz 3 und Abs. 2 ZensG 2011 dahingehend verfassungskonform teleologisch zu reduzieren, dass Erhebungsdaten aus dem Zensus 2011 erst dann zu löschen sind, wenn sie zur Gewährung effektiven Rechtsschutzes nicht mehr benötigt werden. „Die als Folge dieser Rechtsauffassung eintretende zeitweilige Perpetuierung der mit dem Zensus verbundenen Eingriffe in die Grundrechte der Einwohner auf informationelle Selbstbestimmung dürfte ebenfalls gerechtfertigt sein“ (im Ergebnis ebenso: Oberverwaltungsgericht für das Land Schleswig-Holstein, Beschluss vom 15. Juli 2015 – 4 MB 14/15 –, juris). Von daher war es für mich nachvollziehbar, dass das Statistische Landesamt die Hilfsmerkmale bis zum Abschluss der aktuellen gerichtlichen Verfahren in seinem Datentresorraum unter Verschluss

zunächst weiter speichern und erst dann löschen wollte.

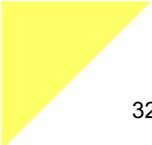
Mittlerweile hat das Bundesverfassungsgericht mit Beschluss vom 26. August 2015 (2 BvF 1/15, NVwZ 2015, S. 1524–1528) im Verfahren der abstrakten Normenkontrolle § 19 ZensG 2011 mit Hinweis auf den offenen Ausgang des Verfahrens und die erwarteten Nachteile für die betroffenen Gemeinden, falls das Normenkontrollverfahren später Erfolg hätte, bis zur Entscheidung in der Hauptsache, längstens für die Dauer von sechs Monaten, außer Vollzug gesetzt. Damit wird eine Perpetuierung der Verletzung der Auskunftspersonen in ihrem Recht auf informationelle Selbstbestimmung, das auch ein Recht auf frühestmögliche Löschung personenbezogener Daten umfasst, hingenommen.

Aus Sicht des Datenschutzes ist es außerordentlich bedauerlich, dass beim Bürger zunehmend der Eindruck entstehen muss, er könne sich auf die zum Schutz seines Rechts auf informationelle Selbstbestimmung eingeführten Verfahrenssicherungen immer weniger verlassen, wenn selbst gesetzlich klar definierte Löschungspflichten letztlich doch nur noch Abwägungsgesichtspunkte darstellen. Ähnliches gilt bezüglich des Zweckbindungsgrundsatzes, wie etwa der Blick auf einen Beschluss des Verwaltungsgerichtshofs Baden-Württemberg vom 7. August 2015 (1 S 1239/15, DVBl 2015, S. 1383–1388) zeigt: dort ging es um die Herausgabe von E-Mails sowie E-Mail-Entwürfen einer ehemaligen Ministerin an einen Untersuchungsausschuss. Die fraglichen Dokumente waren beim Ministerium nur noch in Form von Sicherungskopien vorhanden. Zwar stellte der Verwaltungsgerichtshof fest, dass die Sicherungskopien wohl bereits seit Längerem zu löschen gewesen wären und die fortdauernde Speicherung rechtswidrig sei. Gleichwohl sah es keinen grundsätzlichen Hinderungsgrund für den Zugriff durch den Untersuchungsausschuss. In den Entscheidungsgründen liest sich dies dann so: „Folge dieses rechtswidrigen Unterlassens der Datenlöschung nach Abschluss der Umressortierung ist jedoch nicht, dass nachfolgend ein Untersuchungsausschuss auf noch vorhandene Daten nicht zugreifen kann. Solche Daten dem Zugriff eines Untersuchungsausschusses von vornherein zu entziehen, käme einem Beweisverwertungsverbot gleich, das im deutschen Recht jedoch nicht die typische Folge davon ist, dass ein Beweismittel auf rechtswidrige

32. Tätigkeitsbericht 2014/2015 - 4. Steuern und Statistik

Weise gewonnen wurde. ... Einem Untersuchungsausschuss ist der Zugriff auf Akten nicht schon dann verwehrt, wenn sich in den Akten Ergebnisse vorausgegangener Grundrechtseingriffe finden und die Kenntnisnahme seitens des Untersuchungsausschusses einen neuen Eingriff darstellen würde“. Noch circa ein Jahr zuvor hatte der Verwaltungsgerichtshof Folgendes festgestellt: „Eine Wiederherstellung der Originaldateien aus der Sicherungskopie heraus ist von den Zwecken der Datensicherung und des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage i. S. d. § 15 Abs. 4 LDSG nicht mehr gedeckt und daher unzulässig, wenn der Zweck, zu dem die Originaldateien nach § 15 Abs. 1 LDSG gespeichert wurden, inzwischen weggefallen ist und daher nicht mehr erfüllt werden kann (Zweckerreichung)“ (Urteil vom 30. Juli 2014 – 1 S 1352/13 –, ESVGH 65, 71–90).

Um hier einem Vertrauensverlust der Bürgerinnen und Bürger in die Verlässlichkeit der zu ihrem Schutz geschaffenen Instrumentarien entgegen zu wirken, ist es aus meiner Sicht unerlässlich, dass die öffentlichen Stellen peinlich genau darauf achten, ihren Löschungsverpflichtungen zeitgerecht nachzukommen.



32. Tätigkeitsbericht 2014/2015 - 4. Steuern und Statistik

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

5. Kommunales und andere Verwaltungsbereiche

5.1 Haushaltsbefragung in einer Kommune

Nicht enden wollende Verkehrsstaus und massive Parksuchverkehre im städtischen Bereich stellen nach wie vor ein großes Problem dar. Eine im Regierungsbezirk Stuttgart gelegene Große Kreisstadt sah sich deshalb veranlasst, eine Haushaltsbefragung zum Mobilitätsverhalten ihrer Bürger durchzuführen. Die Anfrage eines Bürgers der Stadt gab Anlass, die Sache genauer anzuschauen.

Für die Verkehrserhebung hatte die Stadt Fragebögen an jeden Haushalt verteilen lassen. Abgesehen davon, dass in diesen Fragebögen der Hinweis fehlte, bei den Adressen der Abfahrts- und Zielorte nicht auch die Hausnummer mitzuteilen, erschienen die erfragten Daten zum Mobilitätsverhalten grundsätzlich nicht personenbezogen und im Großen und Ganzen dem Zweck der Erfassung, nämlich zu erfahren, wer wann von wo wohin fährt, dienlich. Ein Personenbezug liegt dagegen häufig dann vor, wenn es sich bei der Abfahrtsadresse um ein Einfamilienhaus handelt, oder wenn im Fragebogen nur zwei Fahrten angegeben werden, die morgens und abends stattfinden. Hierbei handelt es sich häufig um die Fahrt von und zum Arbeitsplatz. Dass mit diesen Angaben ganz nebenbei auch noch der Rückschluss auf den Arbeitgeber möglich sein könnte, ist meiner Auffassung nach ebenso bedenklich. Für ganz besonders kritisch halte ich es, wenn im Rahmen einer Haushaltsbefragung zu verkehrsplanerischen Zwecken auch Fragen zur Lebensführung gestellt werden. Gedacht war offenbar daran, anhand der Antworten hierauf die befragten Bürger gewissen „Typen“ unterschiedlicher Lebensführung zuzuordnen. Obwohl meine Mitarbeiter der Stadt ausreichend Gelegenheit gegeben haben darzustellen, welchen Einfluss beispielsweise die Antwort auf die Frage, wie viel man denn ausgeben, wenn man Essen gehen, mit dem Mobilitätsverhalten zu tun habe, ist es der Stadt bis heute nicht gelungen, mich davon zu überzeugen, dass diese Daten im Rahmen der Befragung tatsächlich erforderlich waren. Genauso wenig hilfreich dürften Antworten auf die Frage sein, ob man es gerne habe, wenn etwas los sei, einen eher ruhigeren Lebensstil bevorzuge oder sein Leben nach religiösen Grundsätzen ausrichte. Aber selbst wenn die Klassifizierung zur Er-

hebung des Mobilitätsverhaltens genutzt werden könnte, ist sie meiner Auffassung nach in der durchgeführten Form datenschutzrechtlich fragwürdig, da der Bürger gar nicht darüber aufgeklärt wurde und daher nicht wissen konnte, ob und ggf. welche Konsequenzen es für ihn haben würde, wenn er wahrheitsgetreu Angaben macht. Die Transparenz der Datenverarbeitung war damit meiner Meinung nach nicht gewährleistet.

Ich machte meine Kritik an der Verkehrserhebung aber nicht nur am Fragebogen, sondern auch an der Abwicklung der Befragung über das Internet fest, die als Alternative zur schriftlichen Beantwortung angeboten worden war. Die einzige Maßnahme, um feststellen zu können, ob ein über das Internet abgegebener Fragebogen von einem Bürger der Stadt herrührte, bestand darin, dass eine Nummer, die auf dem an den Haushalt verteilten Fragebogen stand, eingegeben werden musste. Die Nummern, das ergab sich bei der Kontrolle, wurden laufend vergeben. Sofern es bei der Zustellung nicht zu einer Durchmischung der Fragebögen kam, wurden damit laufend durchnummerierte Fragebögen an benachbarte Haushalte ausgegeben. Es wäre daher für Unbefugte ein Leichtes gewesen, an der Befragung mit der mutmaßlichen Nummer des Nachbarn teilzunehmen. Eine weitere Beurteilung der Verarbeitung personenbezogener Daten bei der Befragung über das Internet war nicht möglich, da Unterlagen, die einen Eindruck von dem Verfahren hätten geben können, nicht vorhanden waren oder meiner Dienststelle nicht vorgelegt wurden. Mit der Durchführung der elektronischen Erfassung hatte die Stadt zudem ein externes Unternehmen beauftragt, wobei technische Maßnahmen zur Gewährleistung der Vertraulichkeit im Rahmen der Transportkontrolle hiervon nicht umfasst waren. Dementsprechend konnte die Stadt auch nicht Auskunft geben, ob die Daten zwischen den Betroffenen und dem Rechner der Beratungsfirma verschlüsselt übertragen werden. Der Auftrag konnte jedenfalls den Anforderungen an einen Vertrag zur Auftragsdatenverarbeitung nach § 7 Absatz 2 LDSG nicht genügen.

Zwar waren zum Zeitpunkt der Kontrolle die Daten bereits erhoben, aber wie das Verfahren im Weiteren ablaufen würde, war bestenfalls nebulös. Weder war festgelegt, welche Auswertungen konkret durchgeführt werden, noch war bestimmt, wie und mit welcher Software die Daten verarbeitet werden

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

sollten. Bei der Kontrolle erklärte die Stadt, dass man sich auf die konzeptionellen und technischen Details bisher nicht festgelegt habe. Eine schriftliche Konzeption der Verarbeitung gebe es nicht. Abgesehen von diesem bemerkenswerten Einzelfall halte ich es grundsätzlich bei jedem Verfahren für erforderlich, dass rechtzeitig konzeptionell und technisch geklärt wird, welche Daten von wem zu welchem Zweck mit welcher Software verarbeitet werden, bevor mit der Erhebung personenbezogener Daten überhaupt begonnen wird.

Auf Grund der festgestellten Mängel hat sich die Stadt von der Notwendigkeit einer umfangreichen Überarbeitung ihrer bisherigen Konzeption überzeugen lassen und die Auswertung neu ausgerichtet. Ich werde die weiteren Fortschritte beobachten.

5.2 Wenn einer eine Reise tut – die Übernachtungssteuer

Mit Wirkung zum 1. Januar 2010 wurde im Rahmen des Wachstumsbeschleunigungsgesetzes der Mehrwertsteuersatz für Beherbergungsleistungen von neunzehn auf sieben Prozent gesenkt. Die hieraus resultierenden Steuerausfälle will eine baden-württembergische Stadt durch Einführung einer sog. „Übernachtungssteuer“ kompensieren.

„Wenn einer eine Reise tut, so kann er [nicht nur] was erzählen“⁴³, sondern muss seit dem 1. Januar 2014 bei Besuch einer baden-württembergischen Stadt auch mit der Erhebung einer örtlichen Abgabe für seine Übernachtungen in einem Beherbergungsbetrieb rechnen. Dies jedenfalls dann, wenn der Aufenthalt rein privaten Zwecken dient und eine Berufsbedingtheit des Aufenthaltes nicht nachgewiesen werden kann. Mit Urteil vom 11. Juni 2015 (2 S 2555/13) stellte der Verwaltungsgerichtshof Baden-Württemberg rechtskräftig fest, dass die Erhebung der sog. Übernachtungssteuer auf Basis der städtischen Übernachtungssteuersatzung dem Normenkontrollantrag standhält und wirksam ist. Interessenverbände für Hotellerie und Gastronomie, Beherbergungsbetreiber und Anbieter von Hotelportalen sind über den ihnen entstehenden (Formular-) Mehraufwand empört und befürchten einen Rück-

gang der Gästezahlen. Doch auch betroffene Reisende haben sich an mich gewandt und um rechtliche Prüfung des städtischen Vorgehens gebeten. Bereits im letzten Tätigkeitsbericht (LT-Drs. 15/4600, S. 79) hatte ich über eine Eingabe wegen der Übernachtungssteuer berichtet. Innerhalb des Berichtszeitraumes habe ich mich erneut mit der Thematik befasst: Diesmal aus der datenschutzrechtlichen Perspektive eines Arbeitgebers, welcher im Rahmen einer stichprobenartigen Kontrolle der städtischen Steuerbehörde zur Auskunft über einen Aufenthalt seines Arbeitnehmers aufgefordert wurde.

Was bisher geschah: Seit dem 1. Januar 2014 haben die Betreiber der Beherbergungsbetriebe für jeden Gast die Steuer abzuführen, wenn keine Befreiungsgründe vorliegen. Bei jedem Check-In eines Gastes sind sie insofern angehalten, diesen nach dem Grund seines Aufenthaltes zu befragen. Hierbei können sich die Beherbergungsbetreiber bereitgestellter städtischer Formularvordrucke bedienen. Erfolgt eine Übernachtung aus beruflichen Gründen, so kann der Gast u. a. durch Vorlage einer Arbeitgeberbescheinigung oder aber auch durch Ausfüllen eines Formulars geltend machen, dass er von der Steuerpflicht befreit sei. Bei der Arbeitgeberbescheinigung bestätigt der Arbeitgeber für die darin namentlich genannten Mitarbeiter, dass die Übernachtung seiner Mitarbeiter ausschließlich beruflichen Zwecken diene. Der Gast ist insofern angehalten, vor Reiseantritt von seinem Arbeitgeber eine Bescheinigung ausstellen zu lassen. Hat der Gast hingegen nicht die Möglichkeit, vor Reiseantritt eine Arbeitgeberbescheinigung einzuholen, so kann er vor Ort durch Ausfüllen eines entsprechenden Formulars auch selbst bestätigen, dass die Übernachtung beruflich notwendig sei (sog. Eigenbescheinigung). In beiden Konstellationen wird auf eine Erhebung der Übernachtungssteuer verzichtet; der Gast bezahlt den regulären Preis für die Übernachtung, der Beherbergungsbetrieb muss an die Steuerbehörde keine Abgaben abführen. Besteht kein beruflicher Bezug, so hat der Beherbergungsbetrieb die Steuer als Aufpreis auf den regulären Übernachtungspreis direkt vom Gast einzuziehen und diese dann entsprechend an die Steuerbehörde abzuführen. Die Übernachtungssteuer ist somit als indirekte Steuer ausgestaltet, d. h., dass die Person, welche die Steuer schuldet (sog. Steuerschuldner, der Beherbergungsbetrieb), und die Person, welche die

⁴³ Matthias Claudius, Urians Reise um die Welt in: Jost Perfahl (Hrsg.): Matthias Claudius. Sämtliche Werke. Winkler-Verlag, München: 1976, S. 345-348.

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

Steuer wirtschaftlich trägt (sog. Steuerträger, der Gast), nicht personenidentisch sind. Vielmehr wird die Steuer vom Steuerschuldner auf eine andere Person – hier den jeweiligen Gast – abgewälzt.

Ein Petent teilte meiner Dienststelle mit, dass einer seiner Arbeitnehmer aus beruflichen Gründen in der „Übernachtungssteuer“-Stadt übernachtet habe. Beim Ausfüllen der Eigenbescheinigung habe sein Arbeitnehmer angegeben, dass der Aufenthalt berufsbedingt erfolge, aber – entgegen der Formulargestaltung – keine Angaben zum konkreten Zweck des Aufenthaltes gemacht. Der Beherbergungsbetrieb verzichtete daraufhin auf die Erhebung der Übernachtungssteuer. Es dauerte nicht lange, bis die Stadt als zuständige Steuerbehörde den Petenten aufforderte zu bestätigen, dass der Aufenthalt seines Arbeitnehmers berufsbedingt erfolgte. Darüber hinaus sollte er angeben, aus welchen beruflichen Gründen der Aufenthalt des Arbeitnehmers konkret notwendig gewesen sei. Der Petent befürchtete die Offenbarung von Betriebsgeheimnissen und fragte meine Dienststelle, ob er als Arbeitgeber zur Auskunft verpflichtet sei und – falls eine solche Pflicht bestehe – wo die Grenzen der Auskunftspflicht gegenüber der Steuerbehörde zu ziehen seien.

Nicht nur die städtische Satzung, sondern auch die Vorschriften der Abgabenordnung ermächtigen die Steuerbehörden dazu, Auskünfte von sog. Dritten einzuholen.⁴⁴ Dritte sind Personen, welche selbst nicht Beteiligte des Besteuerungsverfahrens sind und auch nicht stellvertretend für Beteiligte auftreten. Dabei ist die Steuerbehörde angehalten, erforderliche Informationen zunächst von den konkret am Steuerverfahren Beteiligten einzuholen, bevor schließlich eine Einbeziehung von Dritten erfolgen kann (Subsidiaritätsgrundsatz). Zur Feststellung eines für die Besteuerung erheblichen Sachverhalts haben Dritte – hierzu zählen eben auch Arbeitgeber des Herbergsgastes – die erforderlichen Auskünfte

zu erteilen, wenn deren Heranziehung aufgrund hinreichend konkreter Umstände oder aufgrund der allgemeinen Erfahrung im Einzelfall geboten ist. Die Steuerbehörde darf sich zur Sachaufklärung aller Beweismittel bedienen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhaltes für erforderlich hält.⁴⁵ Gleichwohl ist sie angehalten, das Beweismittel auszuwählen, welches sich für den Zweck, den Sachverhalt umfassend aufzuklären, am besten eignet (Prinzip des bestmöglichen Beweises). Zu prüfen war insofern, ob die vom Arbeitgeber geforderten Auskünfte zur Feststellung eines steuerlich erheblichen Sachverhaltes tatsächlich erforderlich waren.

Bestätigung des beruflichen Bezugs

Grundsätzlich besteht ein allgemeines Risiko, dass Beherbergungsgäste sich selbst wahrheitswidrig einen berufsbedingten Aufenthalt bescheinigen, um der Erhebung der Steuer zu entgehen und sich dadurch einen finanziellen Vorteil zu verschaffen. Derartige bewusste Falschangaben würden zu einer Steuerverkürzung – sprich dem Ausfall der Übernachtungssteuer – führen. Bei vollständigem Verzicht auf eine Kontrollmöglichkeit bestünde die Gefahr, dass der Regelungszweck der Satzung leerliefe (sog. strukturelles Vollzugsdefizit). Dies würde dem Gebot der Steuergerechtigkeit widersprechen, wonach der Staat die gesetzlich vorgesehene Besteuerung gegenüber jedermann gleichmäßig durchzusetzen versucht, um Ungleichbehandlung und Wettbewerbsverzerrungen zu Lasten einzelner – gegenüber der Wirtschaft und dem Bürger – zu verhindern.

Die Bestätigung des beruflichen Bezugs des Aufenthaltes durch den Arbeitgeber ist hier ein geeignetes Mittel zur wirksamen Ermittlung des relevanten Steuersachverhalts. Im Falle der Übernachtungssteuer hängt die Erhebung einzig und allein davon ab, ob der jeweilige Gast dem Beherbergungsbetrieb freiwillig offenbart, ob seine Übernachtung aus rein privaten Gründen erfolgt. Denn die steuererhebende Stelle selbst hat über den steuerbegründenden privaten Charakter der jeweiligen Übernachtung in aller Regel keine eigenen Erkenntnisse. Insofern sind die in der Satzung vorgesehenen Kontrollmöglichkeiten erforderlich, um nicht nur die Steuerehrlichkeit, sondern auch eine Gleichheit der Steuerbelastung zu gewährleisten. Die allgemeine Nachfrage

⁴⁴ Rechtsgrundlage der Auskunftspflicht Dritter ist § 11 der Übernachtungssteuersatzung (ÜSS) i. V. mit § 3 Absatz 1 Nummer 3 Buchstabe a des Kommunalabgabengesetzes (KAG) sowie §§ 92 und 93 der Abgabenordnung (AO). Die Auskunftspflicht des Arbeitgebers gegenüber der Stadt als „andere Person“ i.S. des § 93 Absatz 1 Satz 1 AO ergibt sich daraus, dass (auch) er nach § 5 Absatz 3 ÜSS, § 3 Absatz 1 Nummer 2 Buchstabe a KAG und § 33 Absatz 1 AO unter den Begriff des Steuerpflichtigen fällt.

⁴⁵ Seer in Tipke/Kruse, Kommentar AO, § 92 Rn. 5f.

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

bei dem Arbeitgeber, ob der Aufenthalt des Arbeitnehmers aus beruflichen Gründen erfolgte, ist datenschutzrechtlich somit zulässig.

Zweck des berufsbezogenen Aufenthaltes

Unzulässig war jedoch die weitergehende Frage gegenüber dem Arbeitgeber, welchem konkreten Zweck der berufsbedingte Aufenthalt des Arbeitnehmers diene. Zur Überprüfung des jeweiligen Steuerfalles sind solche zusätzlichen Informationen jedenfalls nicht zwingend erforderlich. Die allgemeine Rückfrage beim Arbeitgeber nach der beruflichen Notwendigkeit reicht hier völlig aus.

Nachdem ich die Stadt aufgefordert hatte, zukünftig von weiteren Nachfragen bezüglich des Zwecks berufsbedingter Aufenthalte gegenüber dem Arbeitgeber abzusehen, wurde mir von der verantwortlichen Stelle mitgeteilt, dass zwischenzeitlich die Anfragepraxis gegenüber Arbeitgebern zur Überprüfung von Eigenbescheinigungen geändert worden sei. Bereits seit April 2015 würden Arbeitgeber nur noch um eine generelle Bestätigung der beruflichen Veranlassung der Übernachtung des Beschäftigten gebeten werden. Von der Frage nach dem konkreten Zweck des berufsbedingten Aufenthalts werde seitdem abgesehen.

Es ist damit zu rechnen, dass auch weitere Städte und Gemeinden entsprechende Satzungen zur Erhebung von Übernachtungssteuern erlassen werden.

5.3 Inkrafttreten des Bundesmeldegesetzes – Chance auf Stärkung des Grundrechts auf informationelle Selbstbestimmung vertan

Bereits in den letzten Tätigkeitsberichten habe ich mich mit dem neuen Bundesmeldegesetz befasst, das nunmehr am 1. November 2015 in Kraft getreten ist. Erstmals gibt es somit bundesweit einheitliche und unmittelbar geltende melderechtliche Vorschriften. Leider hat der Gesetzgeber die Gelegenheit versäumt, das Grundrecht auf informationelle Selbstbestimmung im Meldewesen nachhaltig zu stärken. Hinzu kommt, dass das neue Bundesmeldegesetz in Teilen sogar zu Verschlechterungen der bisher geltenden Regelungen führt.

Eine Verschlechterung stellt etwa die Wiedereinführung der Mitwirkungspflicht des Vermieters bei der

Anmeldung von Mietern dar. Diese Mitwirkungspflicht war erst 2002 abgeschafft worden und feiert nun in verschärfter Form ihre Wiedergeburt. Grund der damaligen Streichung waren erhebliche Zweifel daran, auf diese Weise Scheinanmeldungen verhindern zu können. Warum der Gesetzgeber von seiner ehemaligen Auffassung abgewichen ist und nunmehr die Mitwirkungspflicht des Vermieters wieder als wesentlichen Beitrag zur Vermeidung von Scheinanmeldungen verstehen will, bleibt zunächst sein Geheimnis. Ob und in welcher Form Scheinanmeldungen in den Melderegistern gespeichert sind, ist nicht bekannt. Es fehlt auch ein empirischer Nachweis, dass die Wiedereinführung der Mitwirkungspflicht des Vermieters tatsächlich geeignet ist, Scheinanmeldungen zu verhindern.

Als Beispiel für eine vergebene Chance kann die Hotelmeldepflicht angeführt werden, deren Abschaffung für deutsche Gäste auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vergeblich gefordert wurde, da es sich hier um eine nicht zu rechtfertigende Datenspeicherung auf Vorrat handelt. Hotelgäste werden nun also weiterhin als potenzielle Straftäter diskriminiert und in ihrem Persönlichkeitsrecht verletzt.

Auch wurde die Forderung der Datenschutzkonferenz nicht aufgegriffen, dass Melderegisterauskünfte in besonderen Fällen wie Auskünfte an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen zu Wahlwerbungszwecken oder an Mandatsträger, Presse oder Rundfunk im Zusammenhang mit Alters- und Ehejubiläen nur mit Einwilligung der Meldepflichtigen zulässig sein sollten. Hier bleibt es dabei, dass die Betroffenen ein Widerspruchsrecht haben, falls sie Übermittlungen zu solchen Zwecken nicht wünschen. Widersprechen die Betroffenen nicht, darf die Meldebehörde bei Vorliegen der jeweiligen Voraussetzungen die entsprechenden Meldedaten übermitteln. Deshalb ist es wichtig, dass die Betroffenen ihre Rechte insofern kennen.

Ein Thema, das auch im Melderecht seinen Niederschlag findet, sind Auskunftersuchen von Polizei und Staatsanwaltschaft, die an Krankenhäuser gerichtet sind. Das neue Bundesmeldegesetz regelt in § 32 die besondere Meldepflicht in Krankenhäusern. Näheres hierzu kann diesem Tätigkeitsbericht in Kapitel 7.3.3 entnommen werden.

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

Bei Meldedaten handelt es sich um Pflichtangaben, die Betroffene gegenüber den Meldebehörden machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei ihrer Verwendung.

5.4 Die Karawane zieht weiter – Datenschutz im kommunalen Bereich

Im Berichtszeitraum war meine Dienststelle mit einem Fall im kommunalen Bereich befasst, welcher nahezu mustergültig verschiedene datenschutzrechtliche Problemlagen offenbarte.

5.4.1 Datenübermittlungen an externe Energieberater

Durch eine Eingabe wurde meine Dienststelle im Februar 2014 auf eine Initiative aufmerksam, welche den klangvollen Namen „Energiekarawane“ trägt. Dabei handelt es sich, so deren Selbstdarstellung im Internet, um ein von einem Bundesministerium gefördertes regionales, aber länderübergreifendes Gemeinschaftsprojekt zweier Gesellschaften mit beschränkter Haftung zur „Aufklärung und Motivation für das Thema Energieeffizienz“. Dazu sollen „Hausbesitzer in ausgewählten Wohnvierteln über Möglichkeiten des energetischen Sanierens und der Energieeinsparung informiert“ werden, indem ein sog. Energieberater interessierte Bürger zur kostenlosen Erstberatung besucht und vor Ort über die wirksamsten Energiesparmaßnahmen aufklärt.

Dieses umwelt- und energiepolitisch durchaus sinnvolle Projekt war in datenschutzrechtlicher Hinsicht leider problematisch. Der Bürgermeister einer Gemeinde im Regierungsbezirk Karlsruhe hatte, wie meinem Amt von betroffenen Bürgern mitgeteilt wurde, Hauseigentümer seiner Gemeinde unter dem energischen Betreff „Die Energiekarawane kommt!“ nicht nur schriftlich über das Projekt informiert, sondern auch sinngemäß angekündigt, dass ihre „Kontaktdaten“ von der Gemeinde „an die von uns beauftragten Energieberater“ weitergegeben werden, falls die Betroffenen dem nicht innerhalb einer relativ knapp bemessenen Frist von ca. zwei Wochen ausdrücklich widersprechen.

Nach dem für baden-württembergische Gemeinden geltenden datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt gem. § 4 Absatz 1 LDSG (siehe dazu auch die weiteren Ausführungen in Kapitel 5.4.4)

brauchte die Gemeinde für die Weitergabe der personenbezogenen Kontaktdaten die vorherige und grundsätzlich schriftliche (vgl. § 4 Absatz 3 Satz 1 LDSG) Einwilligung der jeweiligen Betroffenen oder eine Erlaubnis, die sich aus dem Landesdatenschutzgesetz oder einer anderen Rechtsvorschrift ergibt. Das Schreiben des Bürgermeisters und die später erhaltenen Informationen ließen nicht erkennen, auf welche Rechtsgrundlage die Gemeinde die Weitergabe der Kontaktdaten stützen wollte. Für die von der Gemeinde offenbar in Betracht gezogene Widerspruchslösung war keine Rechtsgrundlage ersichtlich. Um eine unzulässige Weitergabe der Hauseigentümer an private Energieberater zu verhindern, riefen meine Mitarbeiter umgehend im Rathaus an und klärten die Gemeinde umfassend über die bestehenden rechtlichen Probleme auf.

Hierbei wurde schnell deutlich, dass sich die Gemeinde im Vorfeld keine hinreichenden Gedanken über die datenschutzrechtliche Zulässigkeit einer solchen Datenweitergabe gemacht hatte und auch keine Rechtsgrundlage dafür nennen konnte. Eine passende Rechtsvorschrift war in der Tat nicht ohne weiteres ersichtlich. Da bis zu diesem Zeitpunkt noch keine Daten weitergegeben worden waren, nahm die Gemeinde aufgrund unserer Kritik zunächst von einer Datenübermittlung Abstand. Dagegen hatten wir natürlich nichts einzuwenden und nahmen zunächst an, dass unsere Intervention erfolgreich gewesen war.

Innerhalb weniger Tage änderte die Gemeinde jedoch ihre Meinung und teilte uns mit, dass sie nun doch Kontaktdaten an die Energieberater übermitteln werde. Nach wie vor ließ die Gemeinde offen, auf welche Rechtsvorschriften sie die Datenübermittlung stützen wollte. Meine Dienststelle forderte die Gemeinde daher auf, umgehend eine umfassende schriftliche Stellungnahme abzugeben. Zudem wurde die Gemeinde gebeten, bis zum Abschluss der datenschutzrechtlichen Prüfung von der Übermittlung personenbezogener Daten an die Energieberater abzusehen. Jedoch zeigte sich die Gemeinde hiervon unbeeindruckt und beratungsresistent: Sie übermittelte die Kontaktdaten an die externen Energieberater, soweit die Betroffenen dem nicht im Vorfeld widersprochen hatten.

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

Als schließlich eine schriftliche gemeindliche Stellungnahme einging, war auch dieser keine Rechtsgrundlage zu entnehmen. Unsere Fragen waren nur sporadisch beantwortet worden. Nicht nur wegen dieser Verletzung der Unterstützungspflicht, sondern auch wegen der unzulässigen Datenübermittlung beanstandete ich schließlich das Vorgehen der Gemeinde und informierte außerdem die Aufsichtsbehörde.

Nun kam Bewegung in den Fall: Die Beanstandung führte zu einer zweiten Stellungnahme der Gemeinde: Diesmal stützte sie ihr Vorgehen u. a. auf Rechtsnormen, die meine Dienststelle bereits im Rahmen der vorangegangenen, intensiven datenschutzrechtlichen Beratung als nicht anwendbar erklärt hatte. Da keine neuen Umstände vorgebracht wurden, hielt ich an meiner Rechtsauffassung fest. Des Weiteren bat die Gemeinde um eine Unterrichtung über Datenschutzfragen zur Vermeidung künftiger Pannen. In der Folge führten meine Mitarbeiter einen ganztägigen Informations-, Beratungs- und Kontrollbesuch bei der Gemeinde durch. Dabei wurde zunächst die gemeindliche Datenverarbeitung im Zusammenhang mit der Energiekarawane auf der Grundlage der dort vorliegenden Akten eingehend geprüft, erörtert und ins Reine gebracht. Darüber hinaus wurden die von der Gemeinde aufgebrachten weiteren Themen abgehandelt und dabei (nochmals) mit einigem Aufwand versucht, auch datenschutzrechtliches Grundlagenwissen zu vermitteln. Meine Mitarbeiter teilten mir im Nachgang mit, dass sie bei dem Besuch den Eindruck gewonnen hatten, diesmal mit ihrer Beratungstätigkeit durchgedrungen zu sein.

Der vorliegende Fall bietet Gelegenheit, auf einige Punkte einzugehen, die allgemein im kommunalen Bereich von Bedeutung sind.

5.4.2 Notwendigkeit der Vermittlung datenschutzrechtlicher Grundlagen

Es zeigt sich immer wieder, dass Gemeinden, insbesondere mit relativ geringer Verwaltungskraft, grundlegende datenschutzrechtliche Kenntnisse vermissen lassen.

Bereits in meinem letzten Tätigkeitsbericht (LT-Drs. 15/4600, S. 77, Kapitel 5.1) habe ich darauf hingewiesen, dass nicht nur Kontrollen sein müssen, sondern auch (präventive) Beratung wichtig ist. Vor

allem kleineren Gemeinden sollten verstärkt Angebote zur Vermittlung datenschutzrechtlicher Grundlagen unterbreitet werden. Hier sehe ich auch die Aufsichtsbehörden gefordert. Meine Dienststelle hat in der letzten Zeit im Rahmen ihrer Ressourcen auf Anfrage bei einzelnen Kommunen entsprechende Schulungen durchgeführt. Für größer angelegte Schulungskampagnen fehlen meiner Dienststelle bisher jedoch die notwendigen Kapazitäten.

Es ist erforderlich, dass auch kleine, verwaltungsschwache Gemeinden über hinreichende datenschutzrechtliche Kenntnisse verfügen.

5.4.3 Behördliche Datenschutzbeauftragte

Es ist bedauerlich, dass es die derzeitige Rechtslage (vgl. § 10 Absatz 1 Satz 1 LDSG) in das Ermessen der Kommunen in Baden-Württemberg stellt, ob sie einen behördlichen Datenschutzbeauftragten bestellen oder nicht.

Die Bestellung eines behördlichen Datenschutzbeauftragten sollte für alle öffentlichen Stellen, so auch die Kommunen, verpflichtend werden, um endlich datenschutzrechtliches Fachwissen zu bündeln und den immer wieder anzutreffenden Wissenslücken zumindest teilweise abzuhelpfen. Meine Erfahrung zeigt, dass das Datenschutzniveau im kommunalen Bereich bemerkenswert steigt, wenn (bislang freiwillig bestellte) behördliche Datenschutzbeauftragte eingebunden werden. Kleinere Gemeinden, deren Mittel nicht ausreichen, einen eigenen behördlichen Datenschutzbeauftragten zu bestellen, können übrigens auf der Grundlage von § 10 Absatz 2 Satz 3 LDSG gemeinsam mit anderen Gemeinden einen behördlichen Datenschutzbeauftragten bestellen. Oder sie nutzen die von § 10 Absatz 2 Satz 2 LDSG eröffnete Möglichkeit, einen Bediensteten ihrer Aufsichtsbehörde, also etwa des zuständigen Landratsamts oder Regierungspräsidiums, mit deren Zustimmung zum Beauftragten für den Datenschutz zu bestellen.

Die Bestellung behördlicher Datenschutzbeauftragter dürfte mit Inkrafttreten der Europäischen Datenschutz-Grundverordnung im Jahr 2018 ohnehin rechtlich verpflichtend werden (vgl. Artikel 35 Nummer 1 Buchstabe a in der endgültigen Fassung vom 15. Dezember 2015). Die Behörden in Baden-Würt-

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

temberg sollten sich rechtzeitig darauf einstellen und bis dahin von den nach § 10 Absatz 2 Satz 2 und 3 LDSG eröffneten Möglichkeiten Gebrauch machen.

5.4.4 Datenschutzrechtliches Verbot mit Erlaubnisvorbehalt

Das Verbot mit Erlaubnisvorbehalt ist eine der Säulen des Datenschutzrechts (vgl. z. B. § 4 Absatz 1 LDSG). Sollen personenbezogene Daten ohne Einwilligung des datenschutzrechtlich Betroffenen verarbeitet werden, ist eine Rechtsvorschrift für die jeweilige Datenverarbeitung erforderlich. Dabei ist von der verantwortlichen Stelle im Voraus für jedes einzelne Datum zu prüfen, ob die vorgesehene Datenverarbeitung zulässig ist. Obwohl diese „Basics“ auch im kommunalen Bereich hinreichend bekannt sein sollten, entsteht immer wieder der Eindruck, dass personenbezogene Daten unbedacht und geradezu naiv verarbeitet werden. Oftmals nehmen die Kommunen keine Prüfung vor, ob es für ihr Handeln eine Rechtsgrundlage gibt. In Einzelfällen scheinen manche Kommunen noch nicht einmal im Bilde zu sein, ob sie überhaupt Daten mit Personenbezug verarbeiten und welche Vorschriften von ihnen hierbei zu beachten sind.

Außerdem hat sich eine öffentliche Stelle stets zu fragen, ob die geplante Verarbeitung personenbezogener Daten wirklich erforderlich ist oder ob die Aufgabe auch mit einem milderem Mittel erfüllt werden kann, das weniger oder gar nicht in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen eingreift. Der datenschutzrechtliche Erforderlichkeitsbegriff ist dabei in einem strengen Sinne zu verstehen. Dies bedeutet, kurz gesagt: Eine Datenverarbeitung ist erforderlich, wenn ohne sie die konkret anstehende dienstliche Aufgabe nicht erledigt werden kann. Dagegen reicht es für das Vorliegen der datenschutzrechtlichen Erforderlichkeit nicht aus, wenn eine Datenverarbeitung lediglich als bequem, üblich oder günstig erscheint, um später u. U. davon profitieren zu können.

Auch der Erforderlichkeitsgrundsatz wird im kommunalen Bereich nicht immer hinreichend beachtet. Insbesondere bei der Wahrnehmung von sogenannten freiwilligen Aufgaben tragen die Gemeinden teilweise vor, dass eine Datenverarbeitung alleine bereits deshalb zulässig sei, weil diese der Aufgaben-

erfüllung diene. Eine Prüfung, ob es für die Aufgabenerfüllung wirklich erforderlich ist, bestimmte personenbezogene Daten zu verarbeiten (oder eventuell Sachinformationen ohne Personenbezug ausreichend sind), findet nicht in jedem Fall statt.

Die aus Sicht des Datenschutzes wichtigen Prinzipien der Datenvermeidung und Datensparsamkeit stehen in unmittelbarem Zusammenhang mit diesem strengen datenschutzrechtlichen Erforderlichkeitsbegriff.

5.5 Bebauungspläne – Öffentliche Auslegung von Einwendungen

Personenbezogene Daten sind nur dann datenschutzgerecht gelöscht, wenn deren Löschung unwiederbringlich ist und die Daten nicht mehr – auch nicht mit Hilfsmitteln – wieder hergestellt werden können.

Im Rahmen der Aufstellung von Bebauungsplänen haben Bürgerinnen und Bürger in zwei Stufen die Möglichkeit, sich zu beteiligen: Dies ist in der ersten Stufe die frühzeitige Öffentlichkeitsbeteiligung und in der zweiten Stufe die öffentliche Auslegung. Im Rahmen des Verfahrens der öffentlichen Auslegung stellte eine Gemeinde im Großraum Stuttgart auf ihrer Internetseite eine sog. Abwägungstabelle ein. Innerhalb der Tabelle waren sämtliche Einwendungen aufgelistet, welche im Zusammenhang mit einem Bebauungsplan eingegangen waren. Vor Einstellen des Dokuments hatte die Gemeinde in dem elektronischen Dokument die Namen und Adressen von Personen, die Einwendungen vorgebracht haben, zwar digital geschwärzt. Es stellte sich jedoch heraus, dass diese Daten durch Kopieren und Einfügen in ein Word-Dokument wieder hergestellt werden konnten und somit nicht unwiederbringlich gelöscht waren. Kein Wunder, dass sich einige Betroffene bei mir beschwerten. Durch technische Unterstützung meiner Dienststelle gelang es der Gemeinde schließlich, die genannten Daten in der Abwägungstabelle so zu löschen, dass eine Umgehung der Schwärzungsfunktion nicht mehr möglich war. Diese bereinigte Fassung wurde sodann in das Internet eingestellt. Eine Wiederherstellung von Namen und Adressen war damit nicht mehr möglich.

Die Schwärzungsfunktion in Word ist unzuverlässig und deshalb für eine datenschutzgerechte Löschung

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

nicht geeignet, wenn entsprechende Dokumente der Öffentlichkeit über das Internet zugänglich gemacht werden sollen. Insbesondere bei Umwandlung eines Word-Dokumentes in ein PDF-Dokument werden die geschwärzten Daten gespeichert und können mittels „kopieren und einfügen“ wiederhergestellt werden. Hier ist entsprechende Sorgfalt geboten.

5.6 Fundsachen mit elektronischem Speicher

Immer wieder fragen mich Kommunen, welche datenschutzrechtlichen Grenzen zu beachten sind, wenn Smartphones oder Tablets (oder allgemeiner Fundsachen mit elektronischem Speicher) weiterveräußert oder aber an ehemalige Eigentümer herausgegeben werden.

Die zunehmende Verbreitung von mobilen Geräten zur Kommunikation und Datenverarbeitung führt naturgemäß dazu, dass immer mehr Smartphones verlorengehen. Nach einer Umfrage des Branchenverbandes BITKOM vom August 2015 ist fast jedem vierten Handy- oder Smartphone-Besitzer sein Mobilgerät schon einmal ungewollt abhandengekommen. Der Verlust von Handys oder Smartphones sei zum alltäglichen Phänomen geworden, meint der Branchenverband und rät schon wegen der zahlreichen persönlichen oder beruflichen Daten auf den Geräten zu wirksamen Sicherheitsvorkehrungen wie Zugriffssperre und Verschlüsselung. Hilfreich sei es auch, für den Fall eines Verlustes die sog. Serien- bzw. IMEI-Nummer des Mobiltelefons zu notieren, schon weil diese für eine Diebstahlsanzeige bei der Polizei benötigt werde. Die fünfzestellige Zahl befindet sich übrigens häufig auf einem Aufkleber unter dem Akku und kann auch über die Eingabe der Zeichenfolge *#06# auf der Tastatur abgefragt werden.

Der Schutz vor ungewolltem Geräte- und damit Datenverlust ist aber nur die eine Seite des Problems. Mindestens ebenso gewichtig ist die Frage, wie mit den aufgefundenen Geräten datenschutzkonform von den Fundbehörden umzugehen ist. Aufgrund mehrerer Anfragen hat sich meine Dienststelle im Berichtszeitraum auch mit diesem nicht ganz trivialen Thema befasst und die Rechtslage gegenüber früheren Aussagen neu bewertet:

Gem. § 973 Absatz 1 BGB erwirbt der Finder einer verloren gegangenen Sache nach dem Ablauf von

sechs Monaten ab Fundanzeige oder Ablieferung bei der zuständigen Behörde Eigentum an der Fundsache. Damit erlöschen gleichzeitig sonstige, bis dahin bestehende Rechte an der Sache. Anderes gilt, wenn die Fundsache in den Geschäftsräumen oder den Beförderungsmitteln einer öffentlichen Behörde oder einer dem öffentlichen Verkehr dienenden Verkehrsanstalt gefunden wurde: Hier ist ein originärer Eigentumserwerb ausgeschlossen (§ 978 Absatz 1 Satz 2 BGB).

Sobald die Voraussetzungen für die Aufbewahrung gefundener Sachen entfallen sind, entsteht ein öffentlich-rechtlicher Herausgabeanspruch gegenüber der Fundbehörde analog § 985 BGB. Die Sachen sind an den Empfangsberechtigten oder gem. § 973 BGB an den Finder herauszugeben. Das Eigentumsrecht umfasst auch sämtliche auf dem Datenträger gespeicherte Daten. Einwirkungen auf eine Sache, die den Eigentümer daran hindern, mit dieser seinem Wunsch entsprechend zu verfahren, können eine Eigentumsverletzung darstellen.

Datenschutzrechtliche Vorschriften, aus denen sich ein Zurückbehaltungsrecht der Fundbehörde ergeben könnte, sind nicht ohne weiteres ersichtlich. Das Landesdatenschutzgesetz (LDSG) regelt allein den Umgang mit personenbezogenen Daten. Es enthält jedoch keine Vorschriften darüber, ob und ggf. wie eine datenschutzrechtlich verantwortliche Stelle unmittelbar auf fremdes Eigentum an Sachen einwirken könnte. So ist bereits fraglich, ob eine Fundbehörde bei einem in Verwahrung genommenen Datenträger als verantwortliche Stelle im Sinne des § 3 Absatz 3 LDSG angesehen werden kann. Denn danach ist verantwortliche Stelle jede Stelle, die personenbezogene Daten „für sich selbst“ verarbeitet. Bezugspunkt der Verantwortlichkeit ist somit der Umgang mit personenbezogenen Daten für eigene Zwecke. In der bloßen Verwahrung eines abgegebenen Datenträgers kann jedoch kaum von einer solchen eigenzweckbezogenen Verarbeitung durch die Fundbehörde ausgegangen werden. Gesetzlich geregelten Eigentümerbefugnissen können allgemeine datenschutzrechtliche Grundsätze nicht mit Erfolg entgegen gehalten werden. Hierfür wäre vielmehr eine normenklare gesetzliche Grundlage erforderlich, die jedoch nicht ersichtlich ist.

Auch stellt sich die Frage, ob die Fundbehörde überhaupt berechtigt ist, die für sie fremden Daten

32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

des Verlierers zu löschen, um etwa dem Finder ein „datenfreies“ Handy aushändigen zu können. Eine solche Löschung der Daten käme grundsätzlich erst dann in Betracht, wenn sichergestellt ist, dass der Datenträger nicht mehr an den Verlierer herausgegeben werden kann. Dieser Zeitpunkt fällt zeitlich mit dem Eigentumserwerb des Finders zusammen (sechs Monate nach Ablieferung). Eine vorherige Datenlöschung würde insofern gegen § 23 Absatz 4 Nummer 1 LDSG verstoßen.

Für die teilweise geübte Praxis, die Herausgabe der Fundsache von der Zahlung der Kosten für eine Datenlöschung durch ein Privatunternehmen abhängig zu machen, ist keine Rechtsgrundlage ersichtlich.

Im Ergebnis lässt sich feststellen, dass eine rechtlich belastbare Begründung, die Herausgabe eines elektronischen Datenträgers an den Finder nach dessen gesetzlichem Eigentumserwerb zu verweigern, nicht ersichtlich ist. Allgemeine datenschutzrechtliche Erwägungen reichen hierfür nicht aus, normenklare Datenschutzregelungen existieren insoweit nicht. Die Fundbehörden sollten in Erwägung ziehen, jedenfalls dann, wenn sich die gespeicherten Daten ohne großen technischen Aufwand mit eigenen Mitteln oder im Wege der Auftragsdatenverarbeitung löschen lassen, diese vor der Herausgabe an den Finder zu veranlassen. Ist dies nicht möglich, etwa weil der Zugriff auf die Daten mittels technischer Maßnahmen gesichert ist, ist der Datenträger mitsamt den Daten herauszugeben, auch wenn dies aus Sicht des Datenschutzes unbefriedigend ist.



32. Tätigkeitsbericht 2014/2015 - 5. Kommunales und andere Verwaltungsbereiche

6. Verkehr

6.1 Datenschutz rund um das Kraftfahrzeug: Automatisiertes und vernetztes Fahren, Elektromobilität und Pkw-Maut

Automobil 4.0, das Automobil als Datenschleuder, als rollender Computer oder als Smartphone auf Rädern, als Teil des Internets der Dinge, unterwegs auf der Datenautobahn – kaum eine Woche vergeht inzwischen ohne Berichterstattung über neue Entwicklungen in der Kraftfahrzeugtechnik. In den Schlagzeilen spiegelt sich dabei einerseits die Begeisterung für die Möglichkeiten, die die neuen Technologien zu bieten versprechen, andererseits die Sorge vor einer überhandnehmenden Beobachtung und Überwachung der Verkehrsteilnehmer wider. Diese Entwicklungen, aber auch die Elektromobilität und die Pkw-Maut werfen zahlreiche datenschutzrechtliche Fragen auf.

Bereits in meinem letzten Tätigkeitsbericht (31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, S. 84 ff.) habe ich auf die technischen Entwicklungen bei Kraftfahrzeugen, insbesondere die Trends zu deren Vernetzung und zum automatisierten Fahren, und die darauf beruhenden Gefahren für das Recht auf informationelle Selbstbestimmung hingewiesen. Das Thema hat seitdem noch einmal mächtig „Fahrten aufgenommen“, und zwar sowohl in technischer Hinsicht als auch mit Blick auf die gesellschaftliche Wahrnehmung und Diskussion.

Die technische Entwicklung und die Verbreitung neuer Technologien und Geschäftsideen sind erneut weiter vorangeschritten. Die Vernetzung und das automatisierte Fahren waren Hauptthemen der Internationalen Automobilausstellung (IAA) 2015. Anfang Oktober 2015 ließ sich der Ministerpräsident vom Autopiloten eines Lastkraftwagens auf der A 8 von der Raststätte Denkendorf zum Stuttgarter Flughafen und zurück fahren. Sein Stellvertreter begleitete wenige Tage später den Versuch des vollautomatischen Einparkens eines Elektrokleinwagens in einem Stuttgarter Parkhaus mit spiralförmiger Auffahrt⁴⁶ – um nur zwei Beispiele für diesbe-

zügliche Nachrichten zu nennen. Immer mehr Sensorik dient immer weiteren Assistenzsystemen. Der Internetanschluss im Kraftfahrzeug, die Möglichkeit der Einbindung des Smartphones in das Fahrzeug, das Angebot von Zusatzdiensten aus dem Fahrzeug über diese Schnittstellen, aber auch der Fernzugriff über das Internet bzw. das Smartphone auf Fahrzeugdaten einschließlich der Fahrzeugortung werden immer selbstverständlicher. Mehr und mehr Versicherer bieten auch für in Deutschland zugelassene Kraftfahrzeuge sogenannte pay-as-you-drive-Tarife an, bei denen aufgrund einer Auswertung der Fahr- und Bewegungsdaten die tatsächliche oder vermeintliche Risikoneigung bei der Kraftfahrzeugnutzung ermittelt wird und diese als Faktor bei der Bestimmung der konkreten Beitragshöhe zugrunde gelegt wird. Beim „Tanken“ von Elektrofahrzeugen an öffentlichen Ladesäulen werden ebenfalls Daten erhoben, die Rückschlüsse auf den Aufenthaltsort und die Fahrgeohnheiten des Nutzers zulassen. Im Hinblick auf die Datensicherheit beunruhigten schließlich verschiedene in der Presse veröffentlichte demonstrative Hackerszenarien die Öffentlichkeit, namentlich Anfang 2015 die Öffnung von Fahrzeugtüren von mit „connected drive“ ausgestatteten BMW-Fahrzeugen durch Hacker im Auftrag des ADAC⁴⁷ und im Sommer 2015 die Fremdsteuerung eines Jeep Cherokee in Amerika⁴⁸.

Die Europäische Union treibt weiterhin die Entwicklung zur Vernetzung voran. Zu dem bereits im letzten Tätigkeitsbericht erwähnten europäischen eCall – einem einheitlichen, in Kraftfahrzeugen fest eingebauten System, das im Falle eines über die Kfz-Sensorik festgestellten schweren Unfalls oder im Fall der individuellen Notruf-Auslösung einen bestimmten Datensatz über die einheitliche Rufnummer 112 an die Notrufstelle übermittelt und eine Sprechverbindung zu dieser aufbaut – wurden die europäischen Vorschriften inzwischen insoweit vervollständigt, als nach längeren Verhandlungen im Rahmen des Trilogs zwischen Parlament, Rat und Kommission am 29. April 2015 die Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung

⁴⁶ S. <http://www.e-mobilbw.de/de/aktuelles/meldungen/meldungen-detail/automatisches-parken-und-laden-in-der-stuttgarter-innenstadt-301.html>.

⁴⁷ Hierzu <http://www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html>.

⁴⁸ S. <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG verabschiedet wurde. Danach werden ab dem 31. März 2018 Typenzulassungen für Fahrzeuge der Klassen M1 (Pkw und Wohnmobile) und N1 (Lastkraftwagen bis 3,5 Tonnen zulässiger Gesamtmasse) nur noch erteilt, wenn die Fahrzeuge mit dem bordeigenen eCall-System ausgestattet sind. Die datenschutzrechtliche Forderung, das eCall-System im Fahrzeug abschaltbar auszugestalten, hat sich im EU-Rechtssetzungsverfahren im Interesse der Effektivität des Notrufs nicht durchgesetzt; immerhin wurde aber den Herstellern auferlegt, dafür Sorge zu tragen, dass das auf dem Notruf 112 basierende bordeigene eCall-System nicht zurückverfolgbar ist und dass keine dauerhafte Verfolgung erfolgt. Außerdem wurden der Umfang der Speicherung von und der Zugriff auf die Daten im Fahrzeug sowie der zu übermittelnde Datensatz begrenzt und eine strenge Zweckbindung vorgeschrieben (Art. 6 der Verordnung). Der Hersteller kann zwar alternativ auch ein eigenes bzw. drittanbieterbasiertes Notrufsystem vorsehen; dem Fahrzeughalter muss aber jederzeit das Recht gewährt werden, auf das Hersteller- bzw. Drittanbietersystem zugunsten des europäischen eCalls zu verzichten. Der Landesgesetzgeber hat die europäische Gesetzgebung zum eCall zum Anlass genommen, die Vorschriften in § 35 des Feuerwehrgesetzes über die Entgegennahme von Anrufen über Notrufe die Rufnummer 112 auch auf „Meldungen“ zu erstrecken.⁴⁹

Darüber hinaus hat die Europäische Kommission inzwischen die Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern um einen Kranz delegierter Verordnungen ergänzt, nämlich außer in Bezug (a) auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes (Nr. 305/2013 vom 26. November 2012), (b) auf die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lastkraftwagen und andere gewerbliche Fahrzeuge (Nr. 885/2013 vom 15. Mai 2013), (c) auf Daten und Verfahren für die möglichst unentgeltliche Bereitstellung eines Mindestniveaus allgemeiner für die Stra-

ßenverkehrssicherheit relevanter Verkehrsinformationen für die Nutzer (Nr. 886/2013 vom 15. Mai 2013), nunmehr auch (d) hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationen (Nr. 2015/962 vom 18. Dezember 2014). Insbesondere in den Erwägungsgründen für die zuletzt genannte delegierte Verordnung wird deutlich, dass die EU hier an die Verarbeitung auch von Daten aus Fahrzeugsensoren denkt (Erwägungsgrund 8). Dies schließt die Verarbeitung personenbezogener Daten ein: Diese sollen zwar grundsätzlich – aber nur „so weit möglich“ – unwiderruflich anonymisiert werden; im Übrigen seien das europäische und jeweilige nationale Datenschutzrecht einzuhalten.

Die nationale Gesetzgebung hat dagegen nach meiner Kenntnis keine weiteren Vorschriften mit Bezug zur Datenverarbeitung in Ergänzung zum Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (s. auch dazu bereits mein 31. Tätigkeitsbericht 2012/2013, a.a.O. S. 84 f.) erlassen. Ein Beeinträchtigung des Datenschutzes im motorisierten Straßenverkehr kam hier aus anderer Richtung: Mit dem Infrastrukturabgabengesetz (InfrAG) vom 8. Juni 2015 (BGBl. S. 904) – also der landläufig als „Pkw-Maut“ bezeichneten Abgabe – soll nicht nur ein neues Infrastrukturabgaberegister beim Kraftfahrtbundesamt errichtet werden, aus dem zu Überwachungszwecken im Wege des automatisierten Abrufverfahrens Übermittlungen erfolgen dürfen, wobei sowohl zur Erhebung, Mahnung und Beitreibung als auch zur Kontrolle – und damit auch in die jeweilige Datenverarbeitung – Private einbezogen werden. Sondern vor allem soll durch Kennzeichenlesegeräte zu Zwecken der Kontrolle der Abgabentrachtung eine automatisierte massenhafte Erfassung der amtlichen Kennzeichen der die betroffenen Bundesfernstraßen nutzenden Kraftfahrzeuge und deren Abgleich mit dem Infrastrukturabgaberegister durchgeführt werden, obwohl zumindest hinsichtlich aller in der Bundesrepublik zugelassenen Fahrzeuge die Erhebung der Abgabe ohnehin über die Verarbeitung der Steuer- und Zulassungsdaten sichergestellt ist. Die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014 „Keine PKW-Maut auf Kosten des Datenschutzes!“ (vgl. Anhang 12) konnte zwar eine Verkürzung der Speicherdauer erreichen; denn nach dem ursprünglichen Gesetzentwurf hätten die bei der Kontrolle der Straßennutzung

⁴⁹ Gesetzentwurf der Landesregierung vgl. Drs. 15/7613, S. 1 ff.; das Gesetz wurde vom Landtag in zweiter Lesung am 16. Dezember 2015 verabschiedet.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

erhobenen Daten längerfristig gespeichert werden sollen, um die Berechtigung etwaiger Erstattungsverlangen widerlegen zu können. Stattdessen ist nunmehr die unverzügliche Löschung vorgesehen, sobald feststeht, dass die Infrastrukturabgabe entrichtet worden ist oder das Fahrzeug nicht der Abgabepflicht unterliegt (§ 13 Absatz 2 und 3 InfrAG). Die weitergehenden Bedenken der Datenschutzkonferenz gegen die vorgesehene umfassende Datenverarbeitung zur Beitreibung und Kontrolle der Infrastrukturabgabe – auch durch Private und unter Verwendung optisch-elektronischer Überwachungsmaßnahmen – haben den Gesetzgeber aber leider nicht mehr zu einem Einlenken veranlasst. Nunmehr bleibt abzuwarten, ob es trotz des von der EU-Kommission gegen Deutschland eingeleiteten Vertragsverletzungsverfahrens tatsächlich noch zu einer Einführung der Pkw-Maut kommt.

Im Übrigen fördert freilich die Bundesregierung durch verschiedene Projekte, Runde Tische, Foren und Strategiepapiere die Trends zur Automatisierung des Fahrens und zur Vernetzung der Fahrzeuge. Zwar wurden die in meinem letzten Tätigkeitsbericht erwähnten, für 2015 angekündigten intelligenten Verkehrssysteme „Baustellenwarner“ und „Verkehrslageerfassung“ auf dem „Korridor Rotterdam – Frankfurt a.M. – Wien“ noch nicht umgesetzt. Zu erwähnen sind aber auf der anderen Seite der „Runde Tisch Automatisiertes Fahren“ und das hierauf aufbauende Papier „Strategie automatisiertes und vernetztes Fahren – Leitanbieter bleiben, Leitmarkt werden, Regelbetrieb einleiten“⁵⁰ oder die „Strategie Intelligente Vernetzung“.⁵¹ Teil dieser Strategien ist die Erklärung der Bundesautobahn A 9 zum „Digitalen Testfeld Autobahn“, auf dem Industrie und Forschungseinrichtungen Innovationen zum automatisierten und vernetzten Fahren unter Realbedingungen entwickeln und testen sollen. Die Landesregierung Baden-Württemberg hatte dafür plädiert, eine solche Autobahn-Teststrecke auch in unserem Land auf der A 81 einzurichten. Bei der Bundesregierung hat sie sich bislang nicht durchsetzen können; dennoch hält die Landesregierung an der Idee eines Testfeldes für teil- und vollautomatisiertes Fahren in Baden-Württemberg fest.

Der Text der vom Bundesministerium für Verkehr und Infrastruktur, dem Freistaat Bayern, dem Verband der Automobilindustrie (VDA) und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) für das Testfeld in Bayern unterzeichneten „Innovationscharta Digitales Testfeld Autobahn“⁵² für die A 9 stimmt allerdings aus der Blickrichtung des Datenschutzes bedenklich. Denn dort ist ausschließlich die Rede davon, dass Deutschland weiterhin „Leitanbieter [...] und Leitmarkt“ für die neuen Technologien der Vernetzung und der Automatisierung bleiben soll, um „die Wachstums- und Wohlstandschancen der Mobilität 4.0“ zu nutzen. Deswegen setzten sich die Unterzeichner dafür ein, den „rechtlichen Rahmen für den Regelbetrieb des automatisierten und vernetzten Fahrens zu öffnen“. Von dem Schutz des informationellen Selbstbestimmungsrechts als Teil des Konzepts ist dort nichts zu lesen. Vielmehr heißt es ausdrücklich, auf dem „Digitalen Testfeld Autobahn“ erhobene Mobilitäts- und Geodaten sollten in einer Daten-Cloud gebündelt und zur Verfügung gestellt werden; die Daten der beteiligten Unternehmen und Institutionen blieben deren Eigentum(!). Auch auf einem „Testfeld“ erhobene personenbezogene Daten sind indes „Realdaten“ und unterliegen im Interesse der Grundrechtswahrung dem Datenschutzrecht. Dies gilt insbesondere auch für etwaige im Rahmen der Tests mit Videotechnik erhobene personenbezogene Daten. Besonders fragwürdig ist überdies die begriffliche Anknüpfung an den vorangegangenen Feldversuch, das u. a. vom Bund und dem Land Hessen geförderte Projekt „Sichere Intelligente Mobilität – Testfeld Deutschland (SIM TD)“. Dieses Projekt sollte im Hinblick auf den Umgang mit dem Datenschutz wahrlich nicht als Vorbild genommen werden: Der Feldversuch ist schon seit 2013 abgeschlossen, die Abschlussberichte liegen vor⁵³, aber das zu erstellende Datenschutzkonzept wurde – worauf ich bereits in meinem letzten Tätigkeitsbericht hinwies⁵⁴ – nie bekannt. Forschung und Automobilindustrie nehmen sich durch eine derart den Datenschutz vernachlässigende Weise die Chance, ihre Datenschutz-Konzepte zum vernetzten Fahren der öffentlichen Diskussion zu stellen, ob-

⁵⁰ Abzurufen unter <http://www.bmvi.de/SharedDocs/DE/Publikationen/StB/broschuere-strategie-automatisiertes-vernetztes-fahren.pdf?blob=publicationFile>.

⁵¹ BT-Drucksache 18/6022, S. 1 ff.

⁵² <https://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/innovationscharta-digitales-testfeld-autobahn.pdf?blob=publicationFile>

⁵³ http://www.simtd.de/index.dhtml/deDE/backup_publications/Projektergebnisse.html.

⁵⁴ 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, S. 84.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

wohl gerade die Umfrage unter den Testteilnehmern zeigte, wie wichtig solche Konzeptionen für die Akzeptanz der Technologien wären⁵⁵: Nach den Umfrageergebnissen würden 89 % der Befragten nicht akzeptieren, dass auch nur ein eingeschränkter Kreis von Interessenten (z. B. Automobilhersteller und Zulieferer) auf ihre Daten zugreifen könnten; nur 54 % der Befragten wären mit einer anonymisierten Weiterverwendung ihrer Daten einverstanden, die Hälfte der Befragten erwartete dagegen, dass ihre Daten überhaupt nicht – auch nicht anonymisiert – weiterverwendet würden. In Zeiten des sog. Abgasskandals eines großen niedersächsischen Kfz-Herstellers dürfte Vertrauensbildung auch in Hinsicht auf den Umgang mit personenbezogenen Daten durch die Automobilindustrie noch wichtiger geworden sein.

Die Bedeutung des Datenschutzes im Zusammenhang mit den neuen Technologien rückt auf der anderen Seite stärker in das Blickfeld der öffentlichen Diskussion: Unmittelbar nach Erscheinen meines letzten Tätigkeitsberichts hat sich der Verkehrsgerichtstag Ende Januar 2014 unter der Überschrift „Wem gehören die Fahrzeugdaten?“ des Themas angenommen und richtungsweisende Empfehlungen⁵⁶ verabschiedet. Insbesondere hat er zu Recht gefordert, dass der Austausch von Daten und Informationen aus dem Fahrzeug Regeln unterliegen muss, die das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit der Betroffenen (z. B. Fahrzeughalter und Fahrer) sichern. Im Interesse der Transparenz müssten Fahrzeughersteller und weitere Dienstleister die Kunden bei Vertragsabschluss in dokumentierter Form umfassend und verständlich informieren, welche Daten generiert und verarbeitet werden sowie welche Daten auf welchen Wegen und zu welchen Zwecken übermittelt werden. Änderungen dieser Inhalte seien rechtzeitig anzuzeigen und auch die Fahrer seien auf geeignete Weise im Fahrzeug zu informieren. Zur Erhaltung der Wahlfreiheit müssten bei der freiwilligen oder vertraglich vereinbarten Datenübermittlung an Dritte Fahrzeughalter und Fahrer technisch

und rechtlich in die Lage zu versetzt werden, diese zu kontrollieren und ggf. zu unterbinden. Zu Recht forderte der Verkehrsgerichtstag außerdem, dass das Prinzip der Datensparsamkeit sicherzustellen sei. Die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014 griff mit ihrer EntschlieÙung „Datenschutz im Kraftfahrzeug – Die Automobilindustrie ist gefordert“ (vgl. Anhang 30) – gerichtet an Automobilhersteller, Händler, Werkstätten und Anbieter von Kommunikations- und Telediensten – die Forderungen des Verkehrsgerichtstags inhaltlich auf und forderte ergänzend die Berücksichtigung der Prinzipien von Privacy by Design und Privacy by Default bereits in der Konzeptionsphase.

Der Verkehrsgerichtstag 2015⁵⁷ widmete sich u. a. speziell dem Zukunftsthema des automatisierten Fahrens, bei dem sich das Kraftfahrzeug selbständig – ohne einen verantwortlichen Fahrer – beschleunigt und steuert. Hierzu empfahl der Verkehrsgerichtstag, ab dem hochautomatisierten Fahrbetrieb sei der Fahrer bei bestimmungsgemäÙem Gebrauch der Automatisierung von Sanktionen und der Fahrerhaftung frei zu stellen. Zur Klärung von Haftungsansprüchen nach Schadensfällen in jeglichem automatisierten Fahrbetrieb müssten daher Systemhandlungen und Eingriffe des Fahrers beweissicher dokumentiert werden. Datenschutz und Datensicherheit sowie Transparenz für den Nutzer seien dabei zu gewährleisten. Diese Empfehlung zeigt das Spannungsverhältnis zwischen der technischen Entwicklung und ihren möglichen haftungsrechtlichen Auswirkungen einerseits und dem Datenschutz andererseits deutlich auf: Die Herausforderung wird sein, unter dem Gesichtspunkt der Datensparsamkeit nur die Umstände „beweissicher zu dokumentieren“, an deren Dokumentation tatsächlich berechnigte Interessen bestehen und deren Speicherung keine überwiegenden schutzwürdigen Interessen der Fahrzeugnutzer entgegenstehen. Eine Speicherung auf Vorrat, wann das Fahrzeug gefahren wurde – ob automatisiert oder nicht – hielt ich für eine Verletzung des Grundrechts auf informationelle Selbstbestimmung.

Die Automobilindustrie hat ihrerseits durchaus erkannt, dass die Gewährleistung des Datenschutzes

⁵⁵ Vgl. hierzu www.simtd.de/index.dhtml/object.media/deDE/8127/CS/-/backup_publications/Projektresultate/simTD-TP5_Abschlussbericht_Teil_B-2_Nutzerakzeptanz_V10.pdf.

⁵⁶ Im Wortlaut nachzulesen unter http://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_52_vgt.pdf, S. 7.

⁵⁷ http://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_53_vgt.pdf

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

einen wichtigen Faktor für die Akzeptanz der neuen Technologien bildet. Am 3. November 2014 veröffentlichten die Mitglieder des Verbands der Automobilindustrie (VDA) ihre „Datenschutz-Prinzipien für vernetzte Fahrzeuge“.⁵⁸ Darin werden Transparenz, Selbstbestimmung und Datensicherheit als „VDA-Prinzipien“ benannt. Fast zeitgleich – am 12. November 2014 – gaben die amerikanischen Automobilherstellerverbände Alliance of Automobile Manufacturers und Association of Global Automakers (Auto Alliance) ihre Datenschutzprinzipien für Kraftfahrzeugtechnologien und -dienste (Consumer Privacy Protection Principles)⁵⁹ bekannt. Darin verpflichten sich die Hersteller dazu, zumindest angemessene Maßnahmen zur Einhaltung der Prinzipien der Transparenz, der Wahlfreiheit, der Beachtung des Erhebungszusammenhangs (Respect for Context), der Datensparsamkeit, der Datensicherheit, der Datenrichtigkeit und des Datenzugangs (Integrity & Access) sowie der effektiven Umsetzung (Accountability) zu treffen. Und schließlich veröffentlichte auch der Verband der europäischen Automobilhersteller (European Automobile Manufacturers' Association – ACEA) im September 2015 seine Datenschutzprinzipien im Hinblick auf vernetzte Fahrzeuge und Dienste⁶⁰, die er während der IAA präsentierte. Darin erklären die beteiligten europäischen Hersteller ihre Absicht, in Bezug auf vernetzte Fahrzeuge und Dienste, die für den europäischen Markt bestimmt sind, Prinzipien des Datenschutzes als Mindeststandard zu beachten, nämlich das Gebot der Transparenz, das Prinzip der Wahlfreiheit für den Kunden, die Berücksichtigung des Datenschutzes bei der Entwicklung neuer Produkte, Dienste oder Prozesse, die Datensicherheit und das Gebot eines „angemessenen“ Umganges mit personenbezogenen Daten, das Elemente der Datensparsamkeit umfasst.

Erfreulicherweise geht die deutsche Automobilindustrie überdies offen auf die Datenschutzbehörden zu: Seit Dezember 2014 finden regelmäßige Ge-

spräche zwischen Mitgliedern des Arbeitskreises Verkehr der Datenschutzkonferenz und Vertretern des VDA mit dem Ziel statt, ein möglichst gemeinsames Verständnis der datenschutzrechtlichen Anforderungen an das automatisierte und vernetzte Fahren zu erreichen. Die Verhandlungen finden naturgemäß nicht immer einvernehmlich, aber stets in einer konstruktiven Atmosphäre statt. Ein erstes Arbeitsergebnis wurde inzwischen erreicht: Ende 2015 wurde eine Gemeinsame Erklärung der Datenschutzkonferenz und des Verbandes der Automobilindustrie zu verschiedenen datenschutzrechtlichen Aspekten bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge verabschiedet (vgl. Anhang 32). Darin werden Fragen des Personenbezugs, des Zeitpunkts der Datenerhebung und nach der verantwortlichen Stelle ebenso behandelt wie in Betracht kommende Rechtsgrundlagen, Anforderungen an die Transparenz und Auskunftsrechte von Betroffenen, schließlich auch die Möglichkeit der Disposition über Datenverarbeitungsvorgänge durch den Nutzer. Nicht in Bezug auf alle Fragen konnten vollständig einvernehmliche Lösungen gefunden werden. So wurden insbesondere datenschutzrechtliche Fragestellungen, die sich bei der Besitzüberlassung eines Kraftfahrzeuges z. B. im Rahmen eines Dienst- oder Arbeitsverhältnisses oder einer Vermietung ergeben, ausdrücklich aus dem Anwendungsbereich des Papiers ausgenommen. Auch die Frage, ob die im Fahrzeug verarbeiteten Daten teilweise rein technischer Natur sind und keinen Personenbezug aufweisen, konnte keiner vollständigen Klärung zugeführt werden. Immerhin haben die Mitglieder des VDA aber bekräftigt, dass eine Verbindung zur Fahrzeugidentifikationsnummer (FIN) ausreicht, um von einem Personenbezug auszugehen (vgl. § 45 Satz 2 des Straßenverkehrsgesetzes). Damit ist insbesondere klargestellt, dass auf alle Daten, die mit Bezug zur FIN beispielsweise zu Qualitätssicherungs- oder Produktbeobachtungszwecken bei den Herstellern gespeichert werden, das Datenschutzrecht Anwendung findet. Außerdem begrüße ich, dass die Hersteller – auch soweit sie nicht selbst verantwortliche Stelle im Sinne von § 3 Absatz 7 des Bundesdatenschutzgesetzes sind – die Schutzbedürftigkeit der im Fahrzeug abgelegten Daten im Hinblick auf das Recht auf informationelle Selbstbestimmung anerkannt und ihre eigene Verantwortung aufgrund ihrer Gestaltungsmacht als Hersteller anerkannt haben. Ich hoffe, dass die Gespräche zwischen den Daten-

⁵⁸ Abzurufen unter <https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html>.

⁵⁹ Abzurufen z. B. über den Link „Principles“ auf <http://www.autoalliance.org/automotiveprivacy>.

⁶⁰ Principles of Data Protection in relation to connected Vehicles and Services, abzurufen unter http://www.acea.be/uploads/publications/ACEA_Principles_of_Data_Protection.pdf.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

schutzbehörden und dem VDA weitergeführt und vertieft werden.

Meine Dienststelle hat sich – neben der Bearbeitung von Einzelfällen von Petenten in diesem Themenbereich – in die Verhandlungen mit dem VDA aktiv eingebracht. Außerdem haben sich meine Mitarbeiter und ich an vielen öffentlichen, fachlichen und wissenschaftlichen Diskussions- und Vortragsveranstaltungen beteiligt, zahlreiche Interviewanfragen beantwortet sowie Firmen der Automobilindustrie zu Informations- und Beratungszwecken aufgesucht. Ich bin überzeugt, dass datenschutzkonforme Lösungen im Kfz-Bereich zur Vertrauensbildung beitragen und damit auch ein wichtiges Verkaufsargument für die heimische Automobilindustrie werden können. Schließlich muss man auch im Auge behalten, dass es global agierende Internetfirmen gibt, die in der anbrechenden Ära des Internet der Dinge ihre technischen Plattformen nur allzu gerne in Kraftfahrzeugen verankern und die Automobilindustrie auf die Rolle von Zulieferern für ihre Geschäftsmodelle beschränken möchten.

Bei allen Vorteilen für Flüssigkeit und Sicherheit des Straßenverkehrs, die die Automatisierung und Vernetzung von Kraftfahrzeugen mit sich bringen, sind die datenschutzrechtlichen Anforderungen frühzeitig bei der Entwicklung der neuen Techniken zu berücksichtigen. Trotz der zahlreichen Interessenten an Verkehrsdaten – zu denen z. B. auch der Staat im Rahmen der Abgabenerhebung gehört – muss das Recht auf grundsätzlich unbeobachtete Teilnahme am Straßenverkehr erhalten bleiben.

6.2 Projekt TwoGo

Das Ministerium für Verkehr und Infrastruktur (MVI) ist zu Recht daran interessiert, den Ausstoß von Kohlendioxid durch den Straßenverkehr im Land und weitere negative Umweltauswirkungen des hohen Verkehrsaufkommens zu reduzieren. Das gilt in besonderem Maße für den Verkehr in der hoch belasteten Landeshauptstadt, die ihrerseits selbst an einer Reduktion des Verkehrsaufkommens und der damit verbundenen Luftverschmutzung ein vitales Interesse hat. Ein Großteil des Verkehrs geht auf Berufstätige zurück, die überwiegend die Fahrten zum Arbeitsplatz jeder für sich allein in einem Pkw unternehmen. Da liegt der Gedanke nahe, die in

Stuttgart tätigen Mitarbeiter der Landes- und der Stadtverwaltung im Sinne einer Vorbildfunktion dazu zu animieren, Fahrgemeinschaften zu bilden. Die SAP Deutschland AG SE & Co. KG (im Folgenden: SAP) bietet hierzu eine technische Plattform namens TwoGo by SAP an, die nach den Plänen des MVI und der Stadt Stuttgart den Bediensteten die Bildung von Fahrgemeinschaften erleichtern sollte. Datenschutzrechtlich stellte sich das Projekt, zu dem das MVI meine Beratung einholte, allerdings als durchaus tückisch heraus. Denn die Vermittlung von Mitfahrgelegenheiten unter Bediensteten setzt eine vielfältige Verarbeitung personenbezogener Daten voraus.

Zunächst war zu klären, ob es sich datenschutzrechtlich bei der beabsichtigten Leistungserbringung der Firma SAP um eine Auftragsdatenverarbeitung im Sinne von § 7 LDSG oder um eine Funktionsübertragung handelt. Charakteristisch für eine Auftragsdatenverarbeitung ist, dass sich die datenschutzrechtlich verantwortliche Stelle eines Dritten für die Durchführung bestimmter Datenverarbeitungsvorgänge bedient. Die maßgeblichen Entscheidungen über den Umgang mit den personenbezogenen Daten verbleiben aber bei der beauftragenden Stelle. Der weisungsgebundene Auftragnehmer fungiert gleichsam als ausgelagerte Abteilung des weiterhin datenschutzrechtlich verantwortlichen Auftraggebers, der als „Herr der Daten“ die volle Verfügungsgewalt über die Daten behält und daher den Auftragnehmer wie eigene Mitarbeiter bei der Datenverarbeitung zu beaufsichtigen hat. Bei der sog. Funktionsübertragung wird dagegen eine Stelle für eine andere dergestalt tätig, dass die „eingeschaltete“ Stelle im Rahmen des übernommenen Auftrags selbst alle erforderlichen Entscheidungen trifft. Dem „Beauftragten“ kommt bei der Funktionsübertragung deswegen eine weitgehende Selbständigkeit bei der Wahrnehmung des Auftrages zu, typischerweise auch weil der „Auftraggeber“ aus rechtlichen oder tatsächlichen Gründen gar nicht in der Lage wäre, dem „Beauftragten“ bis ins Einzelne Vorgaben für die Durchführung des „Auftrags“ zu machen. Datenschutzrechtlich bedeutet dies, dass die „beauftragte“ Stelle selbst zur datenverarbeitenden Stelle bei der Erledigung des „Auftrags“ wird und für die Einhaltung der datenschutzrechtlichen Pflichten verantwortlich ist.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

Zum Verständnis des Sachverhalts ist zunächst klarzustellen, dass SAP zwei verschiedene Versionen der Plattform TwoGo zur Verfügung stellt: Zum einen gibt es eine offene Plattform, die nach Einrichtung eines Nutzerkontos unter <https://www.twogo.com/de> jedermann (kostenlos) zur Verfügung steht. Zum anderen hat SAP eine Unternehmensversion der Plattform entwickelt, bei der nur Mitarbeiter des jeweiligen Unternehmens ein Konto einrichten und so an der Vermittlung von Mitfahrgelegenheiten teilnehmen können. Hintergrund für diese Unternehmensversion ist die Annahme, dass die Mitarbeiter eines Unternehmens (bzw. hier Landes- und Stadtbedienstete untereinander) durch den geschlossenen Nutzerkreis ein höheres wechselseitiges Vertrauen hätten und sich daher eher für eine Teilnahme entscheiden würden. Das Geschäftsmodell von SAP sieht deswegen vor, dass der Arbeitgeber, der eine solche – auf seine Mitarbeiter begrenzte – Plattform anbieten möchte, entgeltlich eine für alle den Dienst nutzenden Mitarbeiter hinreichende Anzahl an Lizenzen erwerben muss. Die Zugehörigkeit zum Kreis der Berechtigten soll dabei dadurch sichergestellt werden, dass die Anmeldung zur Plattform – anders als die spätere Nutzung, für die auch eine sonstige E-Mail-Adresse verwendet werden kann, – über die dienstliche E-Mail-Adresse erfolgen muss. Die Fahrtvermittlung soll den Mitarbeitern dann aber – jedenfalls im Fall der Mitarbeiter der Ministerien und der Stadt Stuttgart – sowohl zu dienstlichen als auch zu privaten Zwecken zur Verfügung stehen.

Nach anfänglicher Diskussion konnte zwischen dem MVI und der Firma SAP Einvernehmen hergestellt werden, dass das Verhältnis zwischen beiden eine Funktionsübertragung und keine Auftragsdatenverarbeitung darstellt. Hierfür sprach insbesondere, dass im Wesentlichen ein von der Firma SAP entwickeltes Verfahren übernommen werden sollte, das diese – wenngleich zugeschnitten auf Bedienstete der Ministerien und der Stadt – selbständig betreiben sollte; das MVI und die Stadt sind zudem – mangels Kenntnis des genauen Algorithmus der Fahrtenvermittlung im Einzelnen – nicht in der Lage, konkrete Weisungen zum Datenumgang zu geben.

Aber auch bei der Funktionsübertragung muss der „Auftraggeber“ eine sorgfältige Auswahl der Funktion Übernehmenden vornehmen. Insbesondere muss er sicherstellen, dass die personenbezoge-

nen Daten bei der Stelle, auf die die Verantwortlichkeit für die Verarbeitung im Wege der Funktionsübertragung übergeleitet wird, zu keinem anderen Zweck verarbeitet werden, als dies bei der „beauftragenden“ Stelle zulässig wäre. Ferner muss gewährleistet sein, dass nur in dem Maße personenbezogene Daten eines Dritten durch den „Auftragnehmer“ erhoben und verarbeitet werden, wie dies im Interesse des „Auftraggebers“ angemessen ist. Dazu ist der Verarbeitungszweck – ähnlich wie im Falle der Auftragsdatenverarbeitung nach § BDSG (bzw. hier § 7 LDSG) in einer Vereinbarung zwischen diesen beiden Stellen festzulegen. Auch muss sichergestellt werden, dass bei der Stelle, die die Funktion nunmehr wahrnimmt, eine datenschutzgerechte Organisation der Datenverarbeitung gewährleistet ist. Das gilt insbesondere dann, wenn es sich um sensible Informationen wie Personaldaten handelt. In der Vereinbarung müssen deshalb Regelungen entsprechend § 11 Absatz 2 Satz 2 Nummer 1 bis 6 und 10 BDSG getroffen werden.⁶¹

Zur Umsetzung dieser Verpflichtungen riet ich dem MVI, insoweit zumindest Einblick in das Verzeichnisse der SAP zu nehmen.

Außerdem sollten jedenfalls die folgenden Punkte überprüft und ggf. vertraglich geregelt werden:

- Welche personenbezogenen Daten werden im Einzelnen auf welcher Rechtsgrundlage erhoben, gespeichert und an Dritte übermittelt?
- Hält sich die Datenverarbeitung an das Prinzip der Datensparsamkeit, indem nur die zur jeweiligen Zweckerreichung erforderliche Datenverarbeitung vorgenommen wird?
- Wird eine Einwilligung der Nutzer eingeholt und genügt diese den gesetzlichen Anforderungen hinsichtlich der Form und der Darlegung der Verarbeitungszwecke?
- Werden ansonsten die gesetzlichen Anforderungen an die Transparenz der Datenverarbeitung (vgl. § 4 Absatz 3 BDSG) erfüllt?

⁶¹ Im konkreten Fall wurde wegen der differenzierteren Anforderungen eine entsprechende Anwendung des BDSG für sinnvoll gehalten. Vgl. zur Gesamtheit meiner 30. Tätigkeitsbericht 2010/2011, LT-Drs. 15/955, S. 147 und 156, sowie mein unter <http://www.baden-wuerttemberg.datenschutz.de/auftragsdatenverarbeitung-und-funktionsubertragung/> abrufbares Merkblatt „Auftragsdatenverarbeitung und Funktionsübertragung“, Stand 31. Dezember 2012, S. 5.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

- Welche technischen und organisatorischen Maßnahmen im Sinne des § 9 BDSG sind vorgesehen?

Das MVI (und mittelbar die ebenfalls unserer Aufsicht unterliegende SAP) nahmen in der Folge meine Beratung in Anspruch, die zu einer grundlegenden Überarbeitung der Vertragsunterlagen, der Datenschutzerklärung, des Einwilligungsverfahrens und von Teilen des Fahrtenvermittlungsverfahrens selbst führte. Aus der Vielzahl der Einzelfragen möchte ich nur folgende Punkte hervorheben:

- In den Nutzungsbedingungen und in der Datenschutzerklärung muss klar unterschieden werden zwischen denjenigen Verarbeitungsvorgängen, die auf eine (widerrufliche) Einwilligung des Nutzers gestützt werden sollen und über die vor Einholung der Einwilligung zu informieren ist, und denjenigen Vorgängen, die auf eine Rechtsvorschrift gestützt werden und über die nach § 4 Absatz 3 BDSG, § 13 Absatz 1 des Telemediengesetzes (TMG) zu unterrichten ist. Insbesondere ist zu trennen zwischen den Daten, die für die Durchführung des Mitfahrportals unabdingbar sind (und daher nach § 28 Absatz 1 Nummer 1 BDSG erhoben und verarbeitet werden), und denen, die z. B. für die Erbringung von Zusatzleistungen (im eigenen Interesse oder im Interesse der Betroffenen) benötigt werden und daher nur kraft einer gesonderten Einwilligung verarbeitet werden, von der aber die Teilnahme am Mitfahrportal nicht abhängt.
- Das Transparenzgebot gegenüber dem Nutzer verbietet dabei Bezugnahmen in der Darstellung auf nur dem MVI und SAP vorliegende Vertragsdokumente. Die Darstellung gegenüber den Nutzern muss vielmehr aus sich heraus verständlich sein.
Die den Interessenten an einer Fahrtvermittlung zu übermittelnden Daten waren – soweit nicht eine freiwillige Einwilligung zu weitergehenden Übermittlungen eingeholt wird – auf das erforderliche Maß zu beschränken.
- In Bezug auf solche zusätzlichen Datenverarbeitungen wurden auf meinen Rat hin die Verfahren zur Erhebung der Einwilligung verbessert.
- Die Unterlagen sahen ursprünglich vor, dass SAP seine Nutzungsbedingungen jederzeit nach billigem Ermessen ändern könne. Hierzu wies

ich darauf hin, dass die positive Zustimmung der Betroffenen erforderlich ist, soweit sich die geänderten Nutzungsbedingungen auf die Verarbeitung der personenbezogenen Daten kraft Einwilligung beziehen. Eine konkludente Zustimmung durch Weiternutzung des Mitfahrportals, wie in den Nutzungsbedingungen zunächst vorgesehen, ist datenschutzrechtlich nicht möglich. Vielmehr muss sichergestellt sein, dass – entsprechend dem Verfahren bei der erstmaligen Anmeldung – auch bei Änderungen erneut eine Zustimmung eingeholt wird.

- Das Programm sah ferner vor, über den Nutzer jeweils ein Punktekonto zu führen und darin insbesondere die Anzahl der in vermittelten Fahrgemeinschaften zurückgelegten Kilometer zu erfassen. Diese – zunächst als obligatorisch vorgesehenen – Erfassungen hielt ich nicht für erforderlich zur Durchführung des Mitfahrportals und empfahl daher, auf diese Datenerfassungen und -speicherungen zu verzichten.
- Auch auf die Einbeziehung von sozialen Netzwerken in die Kommunikation mit den Nutzern empfahl ich zu verzichten.

Die Annahme einer Funktionsübertragung hat im Übrigen zur Folge, dass ein Austausch personenbezogener Daten zwischen SAP und dem MVI (bzw. der Stadt Stuttgart) eine Übermittlung darstellt, die einer Rechtsgrundlage bedarf. Daher habe ich durchgreifende Bedenken geäußert, dass der Arbeitgeber von der SAP personenbezogene Rückmeldungen über die Nutzung des Portals erhält. Hierfür sah ich zum einen keine Erforderlichkeit. Auch stehen überwiegend schutzwürdige Interessen des Arbeitnehmers einer solchen Datenübermittlung an den Arbeitgeber entgegen, nicht zuletzt im Hinblick auf die eröffnete Möglichkeit der privaten Nutzung des Portals. Hieraus ergab sich die Notwendigkeit, verschiedene in der Unternehmensversion von TwoGo by SAP zunächst vorgesehene Vertragsbestimmungen abzuändern:

- Die Regelungen sahen an sich vor, dass das MVI zur Unterstützung der Landesbediensteten bei der Nutzung des Portals selbst Betreuer bestellt, die Administratoren-Rechte mit Zugriff auf personenbezogene Daten der Endnutzer erhalten sollten. Diese Konstruktion hielt ich für unzulässig. Denn die Administratoren des MVI hätten ihrerseits entweder einen Auftragsdatenverar-

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

beitungsvertrag mit SAP schließen müssen. Oder die Gewährung eines Zugriffs auf die personenbezogenen Daten der Landesbediensteten hätte eine – wie ausgeführt unzulässige – Datenübermittlung an das MVI bedeutet.

- Die Bestimmungen des Vertragsentwurfs sahen weiter ein Recht des MVI vor, nach einer Vertragskündigung „die Auftraggeberdaten“ exportieren und abrufen zu können. Der Export von Daten der Nutzer wäre aber wiederum eine – unzulässige – Datenübermittlung an das MVI.
- Ähnlich war die Regelung zu beurteilen, dass für das MVI bzw. allgemein für den Arbeitgeber das amtliche Kennzeichen desjenigen Kraftfahrzeuges abrufbar werde, dessen Fahrer in eine Fahrgemeinschaft vermittelt worden sei, damit das MVI/der Arbeitgeber die Parkberechtigung für speziell für die Nutzer von TwoGo reservierte Firmenparkplätze überprüfen könne. Nachdem derartige spezielle TwoGo-Parkplätze von Seiten des MVI ohnehin nicht vorgesehen waren, konnte dieser Passus gestrichen werden.
- Das MVI sollte im Übrigen Statistiken erhalten über die Nutzung des Portals durch Landesbedienstete. Hier war darauf zu achten, dass die übermittelten Daten tatsächlich hinreichend kumuliert sind, um als anonym angesehen zu werden; das ist meiner Ansicht nach nur der Fall, wenn auch bei der Kombination verschiedener Auswahlkriterien der Stichprobenumfang die Zahl fünf nicht unterschreitet.
- Auch das Problem, wie nach Ausscheiden eines Mitarbeiters aus dem Landesdienst das Konto des Mitarbeiters datenschutzkonform beendet werden kann, obwohl das MVI als funktionsübertragende Stelle nicht weiß, welcher Mitarbeiter ein TwoGo-Nutzerkonto unterhält, und daher für eine entsprechende Mitteilung an SAP nicht sorgen kann, war zu lösen. Vorsorglich jedes Ausscheiden eines Mitarbeiters der Firma SAP mitzuteilen, schied datenschutzrechtlich aus. Ich schlug vor, dass in bestimmten Abschnitten eine erneute Legitimation als zur Nutzung berechtigter Landesbediensteter mittels der dienstlichen E-Mail-Anschrift vorgesehen werden sollte.

Insgesamt betrachte ich zwar mit Skepsis, dass eine öffentliche Stelle ein Privatunternehmen dazu „animiert“, ein Verfahren zu betreiben, bei dem personenbezogene Daten von Behördenmitarbeitern, die

gegenüber dem Privatunternehmen als Privatpersonen auftreten, verarbeitet werden. Im konkreten Fall war immerhin erfreulich, dass sowohl das MVI als auch SAP meine beratenden Hinweise in sehr konstruktiver Weise aufgenommen haben.

Bei der Funktionsübertragung verbleiben bestimmte Prüfungs- und Kontrollpflichten bei der übertragenden Stelle, und zwar auch und gerade, wenn eine öffentliche Stelle Funktionen auf eine nicht-öffentliche Stelle überträgt. Das entstehende Dreiecksverhältnis zwischen Betroffenen, funktionsübertragender Stelle und funktionsübernehmender Stelle wirft im Falle der Einrichtung eines Mitfahrerportals für Mitarbeiter der funktionsübertragenden Stelle auf eine privatwirtschaftliche Plattformbetreiberin komplizierte datenschutzrechtliche Fragestellungen auf.

6.3 PolyGo: Eine für alles, alles auf einer?

Alles auf eine Karte setzen, gilt als riskant. Genau dieses Wagnis gingen jedoch – gleichsam als Musketiere moderner Mobilitätsformen – „jede Menge starke Partner“⁶² unter der Konsortialführerschaft der Stuttgarter Straßenbahnen AG (SSB) ein, darunter Anbieter des Öffentlichen Personennahverkehrs (ÖPNV), Car- und Bikesharing-Anbieter, Parkplatzbetreiber, ein Energieversorger, eine Bank und die Stadt Stuttgart, als sie – unterstützt mit Fördergeldern des Bundesministeriums für Wirtschaft und Energie – sich daran machten, im Rahmen des zunächst „Stuttgart Services“ genannten Forschungsprojekts eine gemeinsame Chip-Karte zu entwickeln. Mit dieser Karte sollen ihre Inhaber im Raum Stuttgart nicht nur Busse und Bahnen nutzen, sondern auch andere Mobilitätsformen – insbesondere Car- und Bikesharing sowie die Ladesäuleninfrastruktur des teilnehmenden Energieversorgers – in Anspruch nehmen, kulturelle Angebote der Stadt (z. B. der Stadtbibliothek) wahrnehmen und darüber hinaus auch noch Zahlungen durchführen können. Ergänzt wird das Projekt einer multifunktionalen Chip-Karte durch eine „multi- und intermodale Informations- und Buchungsplattform inklusive Echtzeitinformationen zur Vernetzung von (elektromobilen) Mobilitätsdienstleistungen mit urbanen Angeboten in der Region Stuttgart“.

⁶² So der Slogan auf <https://www.mypolygo.de/>.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

Das dicke Portemonnaie der Stuttgarter soll schlanker werden. Statt vieler verschiedener, den Geldbeutel aufblähender Plastikkarten im Raum Stuttgart soll für die verschiedensten Mobilitätsformen und städtischen Angebote nur noch eine einzige Karte ausreichen. Hinter diesem zunächst vielleicht marginal erscheinenden Gedanken stehen weitreichende umwelt-, verkehrs- und energiepolitische Strategie-Überlegungen: Das als Forschungsprojekt eingestufte Vorhaben „Stuttgart Services“ mit der daraus hervorgegangenen Marke „Polygo“ ist Teil des vom Bundesministerium für Wirtschaft und Energie als „Schaufenster Elektromobilität Baden-Württemberg“ geförderten Projektverbundes des Landes „LivingLab BW⁶³ mobil“ und wird wissenschaftlich durch das Institut für Wirtschaftswissenschaften der Universität Ulm sowie das Fraunhofer Institut für Arbeitswirtschaft und Organisation (IAO) begleitet. Die Fördermittelgeber erhoffen sich, große Teile der Bevölkerung in einem begrenzten regionalen Gebiet an die Elektromobilität heranzuführen. Die elektrischen Angebote im Individualverkehr sollen mit bewährten (Elektro-) Mobilitätsangeboten des ÖPNV (Stadtbahn, S-Bahn usw.) vernetzt werden. Insbesondere durch die Verknüpfung mit dem großen Kundenkreis des ÖPNV sowie mit dem alltäglichen Leben in der städtischen Region soll die für eine wirtschaftliche Umsetzung der Elektromobilität notwendige kritische Kundenmasse erreicht werden. Deswegen soll dem Projekt „eine Karte für alle“ auch ein Auskunft- und Buchungstool zu Seite gestellt werden, um die Nutzer zur Lösung ihrer konkreten Mobilitätswünsche auf alternative Fortbewegungsmittel hinzuweisen.

Im Frühjahr 2013 erfuhr ich aus der Presse von dem Projekt. Unter dem Aspekt des Datenschutzes erschien es mir von besonderem Interesse. Im Hinblick auf das Recht auf informationelle Selbstbestimmung wäre es äußerst problematisch, wenn ein großer Anteil der Bevölkerung im Raum Stuttgart angehalten würde, durch die Verwendung einer solchen „Superkarte“ sämtliche Mobilitätsnutzungen und jede Teilhabe an kulturellen Angeboten der Stadt sowie die vorgenommenen Zahlungsvorgänge zentral erfassen und womöglich

auch speichern zu lassen.⁶³ Daher erkundigte ich mich bei der Konsortialführerin nach dem Vorhaben. In der Folge wurde ich um Beratung gebeten und ein Mitarbeiter meiner Dienststelle nahm – soweit möglich – regelmäßig an den quartalsweise stattfindenden Treffen des sogenannten Arbeitspaktes Datenschutz, eines Kreises der Datenschutzbeauftragten der beteiligten Projektpartner, teil.

Das Verfahren erwies sich als durchaus komplex: Die vielen Konsortialpartner – teilweise verschiedenen Branchen angehörend, teilweise aber auch Konkurrenten auf demselben Markt – mit unterschiedlichen Vorstellungen, Ausgangslagen und Anforderungen an die Datenverarbeitung sollten unter einen Hut gebracht werden. Um nur ein Beispiel aus dem Bereich des Datenschutzes für unterschiedliche rechtliche Anforderungen an die Partner zu nennen, sei darauf verwiesen, dass für die Verarbeitung personenbezogener Daten für städtische Angebote das Landesdatenschutzgesetz, für die Mobilitätsangebote und die Zahlungsfunktion dagegen das Bundesdatenschutzgesetz Anwendung finden. Meine Mitwirkungsmöglichkeiten waren gegenüber der Komplexität des Vorhabens schon unter dem Gesichtspunkt meiner Zuständigkeit und im Hinblick auf die personellen Kapazitäten meiner Dienststelle begrenzt: Anteil konnte ich nur an der Arbeit der Datenschutzgruppe nehmen, einem von ursprünglich acht Arbeitspaketen, das selbst oft von Vorentscheidungen und Informationen durch andere Stellen des Projektes abhängig war. Außerdem beschränkte sich mein Einblick auf punktuelle Einsichtnahmen bei den Quartalsmeetings und die vom Arbeitspaket Datenschutz mir konkret auch außerhalb dieser Treffen zugetragenen Fragestellungen. Dabei war zudem der Informationsfluss leider nicht immer ideal. Auch der Charakter eines Forschungsprojektes erschwerte die datenschutzrechtliche Prüfung und Beratung: Bei solchen Forschungsprojekten steht das Ob und Wie der tatsächlichen Realisierung nicht fest, Planungen werden nicht selten weitreichend verändert; selbst in fortgeschrittenen Phasen eines derartigen Vorhabens ist daher typischerweise noch nicht klar, welche personenbezogenen Daten zu welchem konkreten Zweck verar-

⁶³ Vgl. auch den Bericht des Behördlichen Beauftragten für Datenschutz und IT-Sicherheit der Stadt Stuttgart, abzurufen unter <http://www.domino1.stuttgart.de/web/ksd/KSDredsystem.nsf/AnVoGrSuch/Verwaltungsausschuss9922013?OpenDocument>.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

beitet werden sollen. Diesen Umständen war es z. B. geschuldet, dass über lange Zeit noch nicht einmal das nur in seinen Umrissen skizzierte Datenschutz- und Sicherheitskonzept mit konkreten Inhalten gefüllt wurde.

Bald zu Beginn meiner Beteiligung stellten die Konsortialpartner allerdings klar, dass ein im Prinzip datenschutzfreundlicher Ansatz gewählt werden sollte: Im Grundsatz sollten Kunden- und vor allem Abrechnungs- sowie Buchungsdaten ausschließlich in den Systemen der beteiligten Partner verwaltet werden. Auf dem Chip sollte über unterschiedliche Berechtigungen sichergestellt werden, dass jeder Partner nur auf die Daten zugreifen kann, die die jeweils eigene Geschäftsbeziehung zum Kunden betreffen. Soweit die Partner keine Daten auf der Karte selbst ablegen, sollten sie einen Personenbezug nur über eine User-ID erhalten. Die Befürchtung, dass möglicherweise sämtliche Kartennutzungen der einzelnen Kunden an einer zentralen Stelle erfasst und sogar gespeichert werden sollten, wurde damit entschärft.

Dennoch tauchten in der Folge zahlreiche datenschutzrechtliche Fragen auf, an deren Beratung ich im beschriebenen eingeschränkten Umfang teilnahm. Einige ausgewählte Problemstellungen möchte ich skizzieren:

Hinsichtlich der *Mobilitätskarte* selbst wurde insbesondere erörtert, ob bestimmte Daten auf der Karte im allgemein lesbaren Teil oder nur in den jeweils gesonderten „Fächern“ für einzelne Partner enthalten sein dürften und welche Daten verschlüsselt werden müssen. Wegen der sich während des Prozesses noch zu entwickelnden technischen Architektur des Kartensystems waren freilich aus meiner Sicht endgültige Aussagen zu diesem Punkt schwierig zu treffen. Weiteres Beratungsthema war die mögliche und gebotene technische Absicherung im Hinblick auf die zum Einsatz kommende *Near-Field-Communication*. Einen breiteren Raum nahm in den Erörterungen ferner das *Kartenmanagement* ein: Hier stellte sich zunächst die Frage, in welchem Umfang die Hinterlegung personenbezogener Kundendaten an zentraler Stelle erforderlich ist und wer lesenden bzw. schreibenden Zugriff auf diese zentrale Datei erhält. Als Problemfeld erwies sich hier insbesondere das Anliegen, Karten zentral sperren zu können. Dabei ist zunächst klarzustellen, dass

eine Sperrung der Gesamtkarte wegen Zahlungsrückständen nicht in Betracht kommt: Die Prüfung der Einhaltung von Zahlungsverpflichtungen ist Teil der Beziehung zwischen dem Kunden und dem jeweiligen Anbieter und unterliegt daher der Kontrolle nur des einzelnen Konsortialpartners. Diesem steht es natürlich frei, bei Zahlungsrückständen entsprechend den Bestimmungen seiner Vertragsbeziehung zum Kunden die *Nutzungsberechtigung* der Karte für seinen Bereich zu sperren. An eine Sperrung der Gesamtkarte ist dagegen vorwiegend im Fall des Verlusts oder Diebstahls gedacht; hier hätte man es als misslich empfunden, wenn der Kunde darauf verwiesen worden wäre, die Sperrung bei jedem Konsortialpartner, mit dem er einen Vertrag geschlossen hat, selbst zu beantragen. Wenn man aber eine solche zentrale Sperrung ermöglichen möchte, stellen sich die Fragen, welche Angaben der Kunden bei einem Sperrungswunsch machen muss, damit seine Identität geprüft und die ihm zugeordnete(n) Karte(n) ermittelt werden können, ob die Sperrung initiativ von der zentralen Stelle weitergemeldet („Push“) oder nur von den Partnern abgerufen werden sollen („Pull“), in welchen zeitlichen Abständen ggf. solche Sperrungen mit welchen weiteren Zusatzinformationen an die teilnehmenden Partner übermittelt werden sollen und ob Sperrungen jeweils an alle Konsortialpartner gemeldet werden oder ob nur diejenigen instruiert werden, mit denen der Kunde tatsächlich einen Vertrag geschlossen hat. Die hier vorgesehenen Verfahren haben Einfluss auf den Umfang der Daten, die im zentralen Management vorgehalten werden müssen.

Mit der *Auskunfts- und Buchungsplattform* sollen für den Benutzer, nachdem er seinen Streckenwunsch eingegeben hat, aus den Angeboten der teilnehmenden Mobilitätsprovider, ggf. unter Berücksichtigung seiner Mobilitätspräferenzen, geeignete „Fahrten“ errechnet werden. Wenn sich der Benutzer für eine Fahrt entscheidet, sollen über die Schnittstellen mit den jeweiligen Mobilitäts Providern die jeweiligen Teilstrecken gebucht werden. Im Hinblick auf diese Plattform war zu klären, ob und in welchem Umfang der Nutzer persönliche Daten zur Durchführung von Anfragen eingeben muss bzw. in welchem Umfang ihm zu Zwecken der Nutzungsvereinfachung die Möglichkeit eingeräumt werden soll, in seinem persönlichen Konto Grundeinstellungen zu hinterlegen (z. B. typische Ausgangspunkte und Ziele, aber

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

auch persönliche Mobilitätspräferenzen wie die maximale Fußweglänge, Neigung zur Nutzung von [Elektro-]Fahrrädern, Bevorzugung der schnellsten/kostengünstigsten Verbindung, Auswahl der in Betracht kommenden Mobilitätsanbieter o. ä.). Außerdem ergab sich als konkretes Beratungsthema die Frage, ob und unter welchen Kautelen für jede Anfrage und ggf. Buchung eine Identitätsnummer (Correlation-ID) vergeben und mitprotokolliert werden dürfe, die in den verschiedenen Partner-Systemen eindeutig ist, um auf diese Weise Fehler bei der Auskunftserteilung oder Buchung leichter systemübergreifend analysieren zu können.

Eine der Hauptanwendungen der Mobilitätskarte soll ihr Einsatz als *elektronisches Ticket* für den ÖPNV sein, der in der Region vom Verkehrs- und Tarifverbund Stuttgart (VVS) koordiniert wird. Auch im Hinblick auf diese Komponente wurde ich dankenswerter Weise zur Beratung hinzugezogen. Zwar haben schon andere Verkehrsverbünde eTickets als Ersatz für Papierfahrkarten im Einsatz. Der Verband Deutscher Verkehrsunternehmen (VDV) hat hierfür bereits in den Jahren 2002–2005 einen Rollen-, Daten- und Schnittstellen-Standard entwickelt – die sogenannte Kernapplikation (auch „VDV-KA“) –, der Grundlage für das elektronische Fahrkartensystem „eTicket Deutschland“ ist. Die Technik und deren Anpassung an die örtlichen Gegebenheiten erfordern aber immer wieder weitreichende Änderungen, die datenschutzrechtlich geprüft werden müssen. So soll erstmals bei diesem System eine Komponente zum Einsatz gebracht werden, die eine sichere Missbrauchsprüfung ermöglicht. Da die Fahrberechtigungen auf der PolyGo-Karte gespeichert sind, ist eine rein optische Kontrolle nicht mehr möglich. Die aktuelle Fahrberechtigung muss vielmehr aus der Chip-Karte ausgelesen werden. Das wird sowohl von Prüfungs-Personal durchgeführt als auch dann, wenn die Chip-Karte beispielsweise im Bus an einem Lesegerät vorbeigeführt wird. Dann muss in Hintergrundsystemen geprüft werden, ob die Fahrberechtigung gültig ist, das heißt ob das eTicket vom entsprechenden Verkehrsunternehmen ausgegeben wurde und für die Strecke gültig ist. Daneben ist nun aber außerdem beabsichtigt, weitere Prüfungen durchzuführen, die dazu dienen sollen, Missbrauchsfälle einschließlich der Erstellung von Duplikaten aufzudecken. Dies stellt ein grundsätzlich berechtigtes Interesse dar. Dass eTicket-Systeme über die Fälschungs- und Betrugsmöglichkeiten bei

Papiertickets hinaus weitere Varianten des Missbrauchs eröffnen, dürfte schon deshalb nachvollziehbar sein, weil es sich – vereinfacht ausgedrückt – um ein aus mehreren Rechnern bestehendes System handelt, etwa so wie das Internet im Kleinen. Die Erfahrung lehrt leider beständig, dass solche Systeme auf vielfältige Weise dem Missbrauch ausgesetzt sind. Es besteht daher kein Zweifel, dass gewisse Kontrollen erforderlich sind. Welche Kontrollen erfolgversprechend sind, Missbrauch aufzudecken, ist im Voraus nicht klar, auch nicht, von welcher Seite aus welche Angriffe erfolgen werden. Andererseits muss die Verarbeitung personenbezogener Daten natürlich gesetzmäßig sein. Namentlich müssen überwiegend schutzwürdige Interessen der Nutzer daran, dass über ihr Mobilitätsverhalten keine Profilbildung erfolgt, gewahrt werden. Ich bin derzeit dabei, mit der verantwortlichen Stelle abzuklären, welche Verarbeitungen erforderlich und zielführend sind, um Missbrauchsfälle zu erkennen, und wie lange die personenbezogenen Daten hierfür gespeichert werden müssen. Dieser Zeitraum ist so kurz wie möglich auszulegen, um die Möglichkeit der Profilbildung auszuschließen. Aktuell haben die beteiligten Verkehrsunternehmen eine Speicherdauer von 72 Stunden vorgeschlagen. Die Prüfung der Erforderlichkeit ist noch nicht abgeschlossen.

Die Art und Weise, wie die PolyGo-Karte im Laufe des Jahres 2015 durch die SSB AG für VVS-Abonnenten eingeführt wurde, war übrigens nicht mit mir abgesprochen. Ich würde sie auch als weniger gelungen bezeichnen. Zahlreiche Beschwerden und Nachfragen erreichten mich hierzu. Den zeitlichen Zwängen der Fördervorgaben war es vermutlich geschuldet, dass Daten zur Umstellung der bisherigen Verbundpass-Wertmarken auf PolyGo-Karten erhoben wurden, bevor das Datenschutz- und Sicherheits-Konzept für die polygo-Karte und das eTicket-System des VVS fertiggestellt waren. Unklare Auskünfte erhielten wir daher z. B. auf die uns von Petenten gestellten berechtigten Fragen, welche Kontrollen des elektronischen Tickets beabsichtigt seien. Ein weiterer Schwerpunkt der von den Petenten erhobenen Kritik war, dass von den Fahrkarten-Abonnenten stets ein Lichtbild verlangt wurde. Soweit der Abonnent ein übertragbares Ticket bezieht und nicht beabsichtigt, Angebote von anderen PolyGo-Partnern zu nutzen, ist die Erhebung eines Lichtbildes aber unzweifelhaft nicht erforderlich. Auch wurde von den Petenten kritisiert, dass

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

die Eingabe des üblichen Fahrtweges mit Start- und Zielhaltestelle verlangt werde. Auf meine Nachfrage bestätigte die SSB AG zwar, dass die Einreichung eines Lichtbildes bei übertragbaren Tickets durch Nutzer, die keine Angebote anderer Polygo-Karten zu verwenden beabsichtigen, nicht zwingend verlangt werde. Auch sei die Eingabe der konkreten Start- und Zielhaltestelle des Nutzers, wie sich aus den Einzelerläuterungen auf der Internetseite www.mypolygo.de/faq ergebe, tatsächlich nur eine Alternative für den Kunden. Dieser könne alternativ auch selbst die gewünschten Zonennummern (oder ggf. das gesamte Netz) als Bereich angeben, für den sein Ticket gültig sein soll; bei der Angabe der konkreten Strecke profitiere der Kunde allerdings davon, dass er bei einer künftigen Änderung der Zonenzugehörigkeit automatisch informiert und er auch auf die sogenannte Alternativzonen-Regelung hingewiesen werde, nach der er für bestimmte Fahrbeziehungen kostenfreie Zonen zusätzlich erhalte. In der Außendarstellung sind diese Punkte freilich noch nicht zufriedenstellend gelöst. Schon deswegen bleibe ich mit der SSB AG und dem VVS noch im Gespräch.

Es bleibt zu hoffen, dass das aufwendige Forschungsprojekt „Stuttgart Services“ auch unter dem Gesichtspunkt des Datenschutzes nachhaltig verträgliche Ergebnisse erzielt.

Das Projekt, eine einheitliche Chip-Karte für die Angebote verschiedener Mobilitätsprovider und der Stadt Stuttgart sowie parallel hierzu eine Auskunfts- und Buchungsplattform zu entwickeln, warf technisch und datenschutzrechtlich unterschiedlichste Fragen auf. Ob die gefundenen Lösungen jeweils zutreffend und praxistauglich sind, wird sich noch erweisen müssen.

6.4 Saisonkarten der Bodenseeschifffahrt

Die Fischerin vom Bodensee ist nach dem berühmten Lied von Franz Winkler eine schöne Maid, in deren Netz sich ein junges Fischlein sofort verfängt und ein alter Hecht gerne gefangen wäre. Ein weißer Schwan zieht ihren Kahn auf dem blauen See dahin. Eine derart exquisite Beförderung über das große Schwäbische Meer wird aber nun einmal nicht jedem zuteil. Wer dieses märchenhafte Privileg nicht genießt, kann das Netz der von den Vereinigten Schifffahrtsunternehmen für den Bodensee und

Rhein (VSU) betriebenen „Weißen Flotte“ nutzen. Ein Angebot für Vielfahrer ist dabei die Saisonkarte, mit der man ein Jahr lang „freie Fahrt“ auf allen Kursschiffen der Flotte genießen soll. Umso überraschter waren mehrere Kunden, als sie nach Erwerb der Saisonkarte 2014 einen Strichcode auf der Rückseite des Passes vorfanden und bei jedem Betreten eines Flottenschiffs angehalten wurden, den Strichcode an Lesegeräten einscannen zu lassen.

Nach den Angaben der Petenten wurden sie beim Erwerb der Saisonkarten weder mündlich noch schriftlich auf diese neue Verfahrensweise hingewiesen; vom Schiffspersonal sei Ihnen nur erläutert worden, das Verfahren diene „statistischen Zwecken“. Teilweise soll es zu ernsthaften Auseinandersetzungen hierüber auf den Schiffen zwischen Saisonkarteninhabern und dem Schiffspersonal gekommen sein, wenn ein Kunde die Saisonkarte nicht habe scannen lassen. Der Südkurier vom 19. April 2014 berichtete, das neue Verfahren solle „für Irritationen unter den Stammkunden“. Ein Sprecher der Bodensee-Schiffsbetriebe GmbH (BSB) habe hierzu erklärt, es würden lediglich die Kartennummer, das aktuelle Datum und die Zustiegsstelle erfasst, um die Gültigkeit der Karte prüfen zu können und Missbrauch zu verhindern. Das Verfahren sei im Übrigen „mit dem Datenschutz abgestimmt“. Das hat die Petenten zu Recht nicht überzeugt.

Auf unser Anschreiben an die VSU, einen Zusammenschluss der Bodensee-Schiffsbetriebe GmbH (BSB), der Vorarlberg Lines Walter Klaus Bodenseeschifffahrt GmbH & Co (VLB), der SBS Schifffahrt AG und der Schweizerischen Schifffahrtsgesellschaft Untersee und Rhein (URh), antwortete uns die BSB und bezeichnete sich als für das Verfahren verantwortliche Stelle. Zur Rechtfertigung der Pflicht zum Scannen des Strichcodes verwies sie auf den Bodensee-Personentarif, Punkt 31.5.1, wobei sie zugleich einräumte, dass dort nur die Pflicht zur Vorlage des Fahrausweises und nicht zum Einlesen durch ein elektronisches Lesegerät geregelt war. Zum Beginn des Vorverkaufs der Saisonkarten sei das neue Verfahren noch nicht bekannt gewesen, erläuterte sie. Deswegen sei auf dem Antrag für die Saisonkarte 2014 auch noch kein „Einwilligungsvermerk“ angebracht gewesen. Das wolle man auf dem Antrag für 2015 nachholen. Beim Scannen würden die Kartennummer, die Kartenart,

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

das Tagesdatum und die Zustiegsstelle erfasst. Das Verfahren diene vor allem dazu, durch die erhobenen Nutzungsdaten für eine gerechtere Verteilung der Einnahmen aus dem Verkauf der Saisonkarten unter den beteiligten Schifffahrtsunternehmen zu sorgen. Denn bislang würden die Gelder nach einem vereinbarten Schlüssel verteilt, was ein eher ungenaues Verfahren darstelle. Die Daten würden zum Zweck der Verteilung nur intern und anonym ausgewertet. Eine personenbezogene Auswertung sei zu diesen Zwecken „nicht ohne Umwege möglich“ und würde auch nicht durchgeführt. Durch die elektronische Erfassung und Kontrolle würden sich außerdem auch gefälschte oder gesperrte Karten feststellen lassen. Nur im Betrugsfalle erfolge unter Umständen eine Weitergabe an Strafverfolgungsbehörden. Ausschließlich bei offiziellen Anfragen von Ermittlungsbehörden ließen sich über die Kartennummer Name und Anschrift des Benutzers ermitteln. Es sei beabsichtigt, die Nutzungsdaten nach der finalen statistischen Auswertung am Ende der Saison zu löschen.

Wie man bei dieser Sachlage gegenüber der Presse – wie diese es jedenfalls darstellte – behaupten konnte, das Verfahren sei „mit dem Datenschutz abgestimmt“, ist mir schleierhaft. Datenschutzrechtlich stimmte hier so gut wie nichts. Für mich blieb schon unklar, wer tatsächlich datenschutzrechtlich verantwortliche Stelle für das Verfahren sein sollte und welche Rolle die einzelnen, die Daten erfassenden und an die zentrale Stelle weiterleitenden Schifffahrtsunternehmen – die teilweise ihren Sitz außerhalb Deutschlands haben – spielen sollten. Eine Rechtsgrundlage für die Erhebung und weitere Verarbeitung der personenbezogenen Daten über den jeweiligen Einstieg konnte ich außerdem nicht erkennen. Dabei stellte ich zunächst klar, dass die mit der Kartennummer verbundenen Informationen „personenbezogen“ im Sinne von § 3 Absatz 1 BDSG sind, da die zugehörige Person – der Karteninhaber – zumindest bestimmbar bleibt, auch wenn tatsächlich bei der Auswertung der Daten der Bezug in der Regel nicht hergestellt wird. Dass eine Einwilligung nicht eingeholt wurde, hatte die BSB eingeräumt; diese Möglichkeit, eine Datenerhebung, –verarbeitung oder -nutzung zu rechtfertigen (vgl. § 4 Absatz 1 BDSG), schied daher von vornherein aus. Keinesfalls konnte die Absicht, beim Antrag für das Folgejahr einen „Einwilligungsvermerk“ nachzuholen, diesen Mangel in irgendeiner Form rückwirkend

heilen. Aber auch eine gesetzliche Rechtsgrundlage für die Erhebung und Speicherung der Nutzungsdaten war für mich nicht ersichtlich. Zwar kann eine kurzfristige Erfassung der Kartennummer nach § 28 Absatz 1 Nummer 1 oder 2 BDSG gerechtfertigt sein, wenn sie nur dem sofortigen Abgleich vor Fahrtantritt dient, ob die Kartennummer tatsächlich ausgegeben und auch nicht wieder gesperrt wurde. Für eine darüber hinausgehende Speicherung karten- und damit personenbezogener Nutzungsdaten zum Zweck der Verteilung der Einnahmen unter den Schifffahrtsunternehmen des Verbundes stellen diese Vorschriften indes keine Rechtsgrundlage dar. Denn es ist nicht nachvollziehbar, dass hierfür der konkrete Kartenbezug erhalten werden müsste; die allgemeine (statistische) Feststellung, wie oft Saisonkarten an welchen Einstiegsstellen genutzt wurden, reicht vielmehr für diesen Zweck aus. Die Speicherung und Nutzung der personenbezogenen Daten ist daher zum Zweck der Ermittlung des Verteilungsschlüssels schon nicht erforderlich. Überdies würden einem möglicherweise grundsätzlich berechtigten Interesse der Verbundteilnehmer im Sinne von § 28 Absatz 6 1 Nummer 2 BDSG, einen gerechten Verteilungsschlüssel zu ermitteln, überwiegend schutzwürdige Interessen der Kunden entgegenstehen, nämlich zu verhindern, dass Daten über ihre Nutzung der vorab bezahlten Saisonkarten langfristig gespeichert werden und so u. U. sogar die Erstellung von Bewegungsprofilen ermöglicht wird. Daher forderte ich die BSB auf, die rechtswidrig gespeicherten Daten unverzüglich zu löschen.

Weiterhin wies ich darauf hin, dass die Einholung einer Einwilligung für die Auswertung zwar denkbar wäre, dass aber auch insoweit der Grundsatz der Datensparsamkeit aus § 3a BDSG zu beachten ist. Außerdem würde die Einwilligung gem. § 4a BDSG eine umfassende Aufklärung über den Umfang der beabsichtigten Datenverarbeitung oder Datennutzung und über die Möglichkeit des Widerrufs voraussetzen. Vor allem aber müsste sichergestellt werden, dass die Einwilligung freiwillig erteilt werde. An der Freiwilligkeit würde es jedoch fehlen, wenn ein Kunde ohne sie keine Saisonkarte erwerben könne.

Die BSB versuchte zunächst noch, für die Saisonkarte 2015 in den entsprechenden Vordrucken eine Einwilligung der Kunden für das Scan-Verfahren einzuholen. Sie räumte aber alsbald ein, dass die

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

Einwilligung aufgrund dieses Vordruckes weder informiert noch freiwillig sei und verzichtete daher nach ihren Aussagen in der Saison 2015 auf das Scannen der Saisonkarten. Nachdem sie zunächst noch geltend machte, es könne statt der Löschung der 2014 erhobenen Daten eine nachträgliche Anonymisierung erfolgen, führte sie auf mein Insistieren hin, dass eine nachträgliche Anonymisierung wiederum eine rechtsgrundlose Datenverarbeitung (im Sinne einer Datenveränderung) darstellen würde, im Frühjahr 2015 die überfällige Löschung durch.

Die BSB erbat anschließend meine Beratung gem. § 38 Absatz 1 Satz 2 BDSG für ihr Anliegen, ein datenschutzkonformes Verfahren zur Ermittlung eines gerechteren Verteilungsschlüssels unter ihren Mitgliedsunternehmen einzuführen. Entsprechende Hinweise wurden von meinen Mitarbeitern gegeben; die BSB überlegt noch, wie sie sie umsetzen kann.

Allein das Interesse der Unternehmen eines Verkehrsverbundes an einer gerechten Verteilung der Einnahmen aus Verbundkarten rechtfertigt nicht die Speicherung und Auswertung von personenbezogenen Kartennutzungsdaten.

6.5 Reisezeitermittlung

In meinem 31. Tätigkeitsbericht 2012/2013 (LT-Drs. 15/4600, S. 90) hatte ich über ein Projekt des Verkehrsministeriums berichtet, entlang eines Teilschnitts der B 27 mittels Erhebung von Bluetooth-Adressen Reisezeiten zu messen. Auf der so ermittelten Datenbasis sollte den Verkehrsteilnehmern der Umstieg auf öffentliche Verkehrsmittel schmackhaft gemacht werden, wenn erkennbar ist, dass man mit diesen nach der aktuellen Verkehrssituation schneller ans Ziel kommt. Aufgrund meiner Kritik kam das Verkehrsministerium letztlich zum Ergebnis, von dem Vorhaben Abstand zu nehmen. Der stetig zunehmende Verkehr und die damit verbundenen nachteiligen Auswirkungen zwingen die Straßenbauverwaltung aber geradezu, nach Wegen zu suchen, den Verkehr so zu beeinflussen, dass sich die Belastungen möglichst in Grenzen halten. Sog. Netzbeeinflussungsanlagen haben Konjunktur. Da diese aber immer nur auf der Basis von Daten funktionieren können, stellt sich regelmäßig die Frage, wie solche Konzepte mit dem Datenschutz in Einklang zu bringen sind. Im Berichtszeitraum hatte ich

mich deshalb mit einem weiteren solchen Projekt zu befassen.

Die Landesstelle für Straßentechnik (LST), eine Abteilung des Regierungspräsidiums Tübingen, wandte sich an mich und bat um eine Beratung hinsichtlich der datenschutzrechtlichen Zulässigkeit einer geplanten Verkehrsbeeinflussungsanlage im Bereich der Bundesautobahnen (BAB) 6 und 67 im Rhein-Neckar-Raum (Projekt NBA [Netzbeeinflussungsanlage] Rhein-Neckar). Die LST ist das Fachzentrum der Straßenbauverwaltung des Landes Baden-Württemberg für Forschung, Entwicklung, Information und zentrale Projekte im Straßenbau und der Verkehrstechnik.

Im Rahmen des Projekts sollen an relevanten BAB-Standorten (Anschlussstellen, Autobahnknoten und -dreiecke) sowohl die Kennzeichen der vorbeifahrenden Fahrzeuge als auch die gefahrene Geschwindigkeit erfasst und hieraus die Reisezeiten für einzelne Streckenabschnitte berechnet werden. Die so ermittelten Verkehrszustände sollen zur Schaltung betroffener dWiSta-Anzeigen verwendet werden (als Dynamischer Wegweiser mit integrierten Stauinformationen – dWiSta – wird ein Anzeigesystem bezeichnet, das Verkehrsinformationen an die Verkehrsteilnehmer weitergibt).

Das mir vorgelegte Datenschutz- und Sicherheitskonzept sieht im Wesentlichen Folgendes vor:

- Der Kennzeichenleser an der Strecke erfasst das Fahrzeug samt Kennzeichen und liest mittels einer Erkennungssoftware das Kennzeichen aus. Aus den ausgelesenen Kennzeichendaten wird sofort mit dem Algorithmus SHA-2 ein 256 Bit langer Hashwert gebildet. Das Abbild des Fahrzeugs und das ausgelesene Kennzeichen werden unmittelbar danach automatisch gelöscht.
- Sodann wird durch den Kennzeichenleser der von einem übergeordneten Teilsystem bereitgestellte aktuell gültige geheime Schlüssel (256 Bits) mit dem vorher bestimmten Hashwert zusammengefasst und aus dem so erhaltenen Wert wird mit dem Algorithmus SHA-2 wiederum ein 256 Bit langer Hashwert gebildet.
- Dieser 256 Bit lange Hashwert wird dann verkürzt, d. h. von den 256 Bit werden die niederwertigsten 20 Bits genommen und dieser 20-Bit-

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

lange endgültige Wert zum übergeordneten Teilsystem in der Zentrale zur weiteren Verarbeitung übertragen.

- Alle in der Zentrale übernommenen Hashwerte werden in einem gemeinsamen Hauptspeicherbereich so abgebildet, dass gleiche Werte den gleichen Speicherplatz adressieren (Hash-Verfahren). Wird der gleiche Hash-Wert an einer benachbarten Messstelle wieder erkannt, werden die zugehörigen Wertepaare ohne die zugrundeliegenden Hash-Werte als Daten einer Fahrt zwischen zwei Messstellen an eine Fachapplikation zur Bestimmung von Reisezeit, Reise-Geschwindigkeit, Fahrtrichtung und ggf. eines Störfalls übergeben.
- Alle Datensätze werden nach Erkennen einer zusammenhängenden Fahrt im Überwachungsbereich nach Ablauf einer bestimmten Frist, die nach Angabe der LST maximal 120 Minuten betragen soll, im Hauptspeicher vollständig gelöscht. Sollte der gleiche Hashwert zu einem späteren Zeitpunkt im Detektionsnetz erneut auftreten, werden die zugehörigen Datensätze einer neuen Fahrt zugeordnet.
- Das übergeordnete Teilsystem ermittelt täglich (alle 24 Stunden) einen geheimen, zufälligen Schlüssel, der an alle Kennzeichenleser zur erneuten Verschlüsselung der erfassten und lokal bereits gehashten Kennzeichen übertragen wird.

Prinzipiell lehne ich Videoüberwachungsmaßnahmen (um eine solche handelt es sich bei dem Projekt), die nicht die Voraussetzungen des § 20a des Landesdatenschutzgesetzes (LDSG) erfüllen, ab. Dies entspricht auch der grundsätzlichen Haltung aller Datenschutzaufsichtsbehörden in Deutschland. Gleichwohl sah ich vorliegend Besonderheiten, die mich unter Zurückstellung von Bedenken dazu veranlassen haben, das Vorhaben zu akzeptieren. Rechtlich beurteile ich das so:

Wenn hier mittels der eingesetzten Kamertechnik das Kennzeichen erfasst wird, bedeutet dies zunächst, dass damit personenbezogene Daten i.S. des § 3 Absatz 1 LDSG erhoben werden. Kraftfahrzeugkennzeichen gehören zweifelsfrei zu den personenbeziehenden Daten. Damit wäre grundsätzlich der Anwendungsbereich des § 20a LDSG eröffnet. Das Projekt erfüllt dessen Voraussetzungen nicht, so dass es eigentlich abzulehnen gewesen wäre.

Allerdings war hier zu berücksichtigen, dass aufgrund der technisch-organisatorischen Ausgestaltung nicht von einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung auszugehen war. Das Bundesverfassungsgericht hat in mehreren Entscheidungen (BVerfGE 100, 313–403; 107, 299–339; 115, 320–381; 120, 378–433; auch: BVerwG NVwZ 2015, 906–908) festgestellt, dass es für die Frage, ob eine maschinelle Datenerfassung in das informationelle Selbstbestimmungsrecht eingreife, maßgeblich auf eine Gesamtbetrachtung ankomme. Zu prüfen sei, ob sich mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet habe, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen sei. Soweit die Daten unmittelbar nach der Erfassung technisch wieder spurlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert würden und auch nicht beabsichtigt sei, sie zum Gegenstand weiterer, nachfolgender Maßnahmen zu machen, würden Datenerfassungen keinen für die Annahme eines Grundrechtseingriffs hinreichenden Gefährdungstatbestand bilden.

Vor dem Hintergrund dieser Rechtsprechung sah ich im konkreten Einzelfall das Recht auf informationelle Selbstbestimmung nicht als gefährdet an. Eine Rolle spielte bei dieser Bewertung insbesondere auch, dass das Kennzeichen selbst nicht gespeichert und der aus diesem gebildete Hash-Wert – über die Verwendung als Identifikator für die Errechnung der Reisezeit hinaus – nicht Ausgangspunkt für weitere Maßnahmen sein soll und nicht sein kann. Dies unterscheidet dieses Projekt meines Erachtens beispielsweise von dem sog. Section-Control-Verfahren, bei der jedenfalls die verfremdeten Kennzeichen derjenigen, die eine bestimmte Durchschnittsgeschwindigkeit überschreiten, weiter verwendet werden sollen, um eine Klaraufnahme des Fahrzeugs auszulösen. Überdies dürfte bei realistischer Betrachtung auch die Möglichkeit auszuschließen sein, in der kurzen Zeitspanne, in der die Hash-Werte gespeichert werden (im konkreten Fall maximal zwei Stunden), diese für die Ermittlung von Kfz-Kennzeichen, etwa durch Schaffung eines Vergleichswertes, personenbeziehbar und damit für weitere Zwecke nutzbar zu machen.

32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

Allerdings habe ich der LST noch folgende technische Änderungen des Konzepts zur Auflage gemacht:

- Die parametrierbare Zeit, d. h. die Zeit vom Eintritt in das Netz bis zum Austritt (am Netzausgang oder an einer Anschlussstelle), darf maximal zwei Stunden betragen. Die Daten dieser Fahrt müssen dann, ohne den Hashwert, an die Anwendungssoftware für die Netzbeeinflussung weitergeleitet und alle Daten dieser Fahrt, inkl. des Hashwertes, im Kommunikationsrechner und damit im gesamten System unwiederbringlich gelöscht werden.
- Es dürfen nur Kennzeichen von Fahrzeugen erhoben werden. Dies ist durch geeignete Kameraposition und Kameraobjektiv zu realisieren. Sollte diese Anforderung nicht erfüllt werden können, müssen kameraintern nicht zu erhebende Bildbereiche geschwärzt werden.
- Der Grad der Anonymität der Daten bemisst sich maßgeblich an der Vertraulichkeit des Salt-Wertes, mit dem die Kraftfahrzeugkennzeichen verknüpft werden, um damit einen nichtinjektiven Hashwert zu berechnen. Deshalb darf der Salt-Wert nur auf den Rechnersystemen gespeichert werden, die den Wert für die Berechnung der Hashwerte benötigen. Insbesondere ist eine Speicherung auf dem zentralen Informationssystem, mit dem keine Hash-Werte berechnet, sondern diese lediglich weiterverarbeitet werden, nicht erforderlich. Ich habe empfohlen, den Salt-Wert mit den Kennzeichenlesern zu berechnen und beim Austausch der Hash-Werte secret-sharing-Protokolle anzuwenden.
- Die Generierung des Salt-Werts sollte durch eine Entropie-Quelle erfolgen, die mindestens eine Technik wie HAVEGE (hardware volatile entropy gathering and expansion) verwendet. Aus einem Pseudozufallsgenerator gewonnene (sukzessive) Salt-Werte erfüllen die datenschutzrechtlichen Anforderungen an die Anonymisierung nicht.
- Es sollte ein Hashfunktion gemäß der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 15. Dezember 2014 (oder aktueller) der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen angewandt werden.
- Der Salt-Wert sollte in indeterministischen Zeitabständen (mindestens einmal täglich) generiert werden. Gegebenenfalls müssen parallel zwei Hashwerte mit den Salt-Werten des vorangegangenen und des aktuellen Zeitabschnitts berechnet und auf dem zentralen Informationssystem verarbeitet werden.

Die Antwort der LST steht noch aus.

Bei Verfahren zur Reisezeitermittlung bedarf es hinsichtlich der Frage, ob das Grundrecht auf Datenschutz gefährdet ist, stets einer Einzelfallbetrachtung, bei der der technisch-organisatorischen Ausgestaltung, insbesondere einem hinreichend ausgeprägten Anonymisierungsverfahren, maßgebliche Bedeutung zukommen kann.



32. Tätigkeitsbericht 2014/2015 - 6. Verkehr

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

7. Gesundheit und Soziales

7.1 Das Gesetz über den öffentlichen Gesundheitsdienst (Gesundheitsdienstgesetz)

Anfang Juni 2015 leitete mir das Ministerium für Arbeit und Sozialordnung, Familie, Frauen und Senioren Baden-Württemberg (Sozialministerium) als Entwurf das „Gesetz über den öffentlichen Gesundheitsdienst und zur Änderung anderer Vorschriften“ zu, durch das, kurz gesagt, die Aufgaben und Schwerpunkte des öffentlichen Gesundheitsdienstes neu geordnet werden sollen. Grundlage war der vom Ministerrat im Oktober 2012 beschlossene „Zukunftsplan Gesundheit – Gesundheitsdialog Baden-Württemberg“. Seit Inkrafttreten des bislang geltenden Gesundheitsdienstgesetzes zum 1. Januar 1995 hatte sich das Spektrum der Aufgaben der Gesundheitsämter und des Landesgesundheitsamts nicht unwesentlich verändert; Fragen des Gesundheitsschutzes und der Öffentlichen Gesundheit seien – so der Gesetzentwurf – als Teil der Daseinsvorsorge in den Vordergrund getreten. Zu den wesentlichen Änderungen gehört die Einrichtung von medizinischen Gutachtenstellen für bestimmte amtsärztliche Untersuchungen und Begutachtungen an vier Standorten, die Durchführung von ärztlichen Einstellungsuntersuchungen durch geeignete niedergelassene oder andere approbierte Ärzte, die Erstellung ärztlicher Atteste oder Bescheinigungen auf der Grundlage verschiedener Ausbildungs-, Weiterbildungs- und Prüfungsordnungen durch niedergelassene oder andere approbierte Ärzte und die Neufassung der Aufgabenbeschreibungen auf der Grundlage der Praxiserfahrungen des öffentlichen Gesundheitsdienstes in den vergangenen 20 Jahren.

Angesichts der Komplexität dieses Vorhabens mit seiner Vielzahl datenschutzrechtlicher Aspekte war die vom Sozialministerium für meine Stellungnahme eingeräumte Frist von zwölf Werktagen unangemessen kurz und im Sinne einer sachgerechten Beteiligung im Sinne von § 31 Absatz 4 Satz 2 LDSG ungeeignet. Bereits mehrfach habe ich auf den Missstand unangemessen kurzer Fristen bei meiner Beteiligung hingewiesen, offenbar ohne durchschlagenden Erfolg.

Der Zeitfaktor war hinsichtlich der Beteiligung meines Amtes in diesem Fall aus einem weiteren Grund ein Ärgernis: Dieser Referentenentwurf hatte u. a. Regelungen über amtsärztliche Untersuchungen zum Gegenstand. Anlässlich einer Eingabe zu einer Einstellungsuntersuchung für den Vorbereitungsdienst hatte ich bereits 2010 gegenüber dem Sozialministerium datenschutzrechtliche Bedenken geäußert und daraufhin vom Ministerium die Zusage erhalten, meine Anregungen aufzugreifen und meine Dienststelle bei der Weiterentwicklung und Novellierung des Gesundheitsdienstgesetzes frühzeitig zu beteiligen. Später geriet dieses Versprechen offenbar in Vergessenheit. Wie sich nun herausstellte, hatte das Sozialministerium schon 2014 im Vorfeld der Vorbereitung dieses Referentenentwurfs Gespräche mit einzelnen betroffenen Ministerien geführt, an der meine Dienststelle nicht beteiligt worden war. Daher habe ich das Sozialministerium nachdrücklich gebeten, mich bei anstehenden Gesetzgebungsvorhaben möglichst frühzeitig zu beteiligen, zumindest jedoch ausreichende Fristen zur Stellungnahme einzuräumen.

In der Kürze der gesetzten Frist war mir nur eine cursorische Prüfung möglich. Hinzu kam, dass der Gesetzentwurf an verschiedenen Stellen auf ein geplantes Landesgesundheitsgesetz Bezug nahm, das mir damals noch nicht als Entwurf zugeleitet worden war (das geschah erst Ende Juli 2015). Bereits die cursorische Prüfung ließ gravierende Mängel des Gesetzentwurfs erkennen. Zu den grundlegenden Anforderungen des Datenschutzes gehört, dass Vorschriften über das Verarbeiten personenbezogener Daten (auch für die möglichen Betroffenen) klar erkennen lassen, ob durch sie die Zulässigkeit des Verarbeitens personenbezogener Daten begründet oder erweitert werden soll, ggf. inwieweit (also auch, ob sie konstitutiv oder deklaratorisch sind). Der Wortlaut der Vorschriften muss, wiederum auch für die möglichen Betroffenen, hinreichend deutlich die durch den Zweck sowie die Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit gezogenen Grenzen, etwa in Gestalt der Eingriffsintensität und des konkreten Zwecks der Datenverarbeitung bestimmen, innerhalb derer das Verarbeiten personenbezogener Daten zulässig sein soll. Eine Vielzahl der geplanten Regelungen genügte diesen Anforderungen nicht. Zu den im Einzelnen von mir festgestellten Mängeln gehörte das Versäumnis, eine tragfähige Rechtsgrundlage für die Durchfüh-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

zung der Einschulungsuntersuchung zu schaffen. Dies ist für mich nicht nachvollziehbar, nachdem ich über Jahre hinweg immer wieder Zweifel daran geäußert habe, dass für die umfangreiche Datenerhebung im Rahmen der neuen Einschulungsuntersuchung eine tragfähige Rechtsgrundlage besteht, und dazu eine umfangreiche Korrespondenz mit dem Sozialministerium geführt habe.

Das Sozialministerium griff meine Anmerkungen erfreulicherweise auf und überarbeitete seinen Referentenentwurf. Im Rahmen einer vom Ministerium gewünschten eingehenden Erörterung konnte mein zuständiger Mitarbeiter das Ministerium ausführlich beraten und noch klärungsbedürftige Punkte herausarbeiten. Darauf erhielten wir die Zusage, dass der Gesetzentwurf unter Berücksichtigung dieser mündlichen Beratung in vielen Punkten weiter überarbeitet werden solle, teilweise auch grundlegend, etwa zur Präzisierung der Vorschriften über die Einschulungsuntersuchung.

Im Oktober 2015 ließ mir das Sozialministerium den fortgeschriebenen Gesetzentwurf zukommen; das Gesetz (vgl. LT-Drs. 15/7723) wurde am 16. Dezember 2015 durch den Landtag verabschiedet.

7.2 Das Landesgesundheitsgesetz

Ein weiteres Gesetzgebungsvorhaben, bei dem mich das Sozialministerium im Sommer 2015 beteiligte, läuft unter der Kurzbezeichnung „Landesgesundheitsgesetz“. Erste Anhaltspunkte, worum es dabei, auch in Abgrenzung zu dem vorstehend behandelten Gesundheitsdienstgesetz, konkret geht, ergaben sich aus dem Vorblatt des Gesetzentwurfs: Zur „Schaffung einer tragfähigen Grundlage für die Weiterentwicklung des Gesundheitswesens in Baden-Württemberg“ soll, unter „Abkehr von der sektoralen Betrachtungsweise hin zu einem sektorenübergreifenden und populationsbezogenen Ansatz“, „das Zusammenwirken von Landes- und kommunaler Ebene im Bereich des Gesundheitswesens gestärkt und die sektorenübergreifende Zusammenarbeit intensiviert werden“. Dazu sollen „neue und bewährte Dialog- und Arbeitsformen, nämlich die Gesundheitskonferenzen auf Landes- und Kreisebene sowie der sektorenübergreifende Landesausschuss nach § 90a des Fünften Buches Sozialgesetzbuchs (SGB V) und ein Landesausschuss für Gesundheitsförderung und Prävention etabliert und

auf eine gesetzliche Grundlage gestellt“ werden, wobei es sich bei diesen Konferenzen und Ausschüssen um „Gremien der Politikberatung“ handeln soll.

Dem Gesetzentwurf und weiteren Mitteilungen des Sozialministeriums war aber nicht zu entnehmen, ob das geplante Gesetz überhaupt den Umgang mit personenbezogenen Daten zum Gegenstand hat, ggf. in welcher Weise, und ob die vom Sozialministerium erbetene „Prüfung“ des Gesetzentwurfs durch mich auf der Grundlage des § 31 Absatz 4 Satz 2 LDSG erfolgen sollte. Soweit die vorgesehenen Regelungen ohne datenschutzrechtliche Bedeutung sind, war mein Amt nach § 31 Absatz 4 Satz 2 LDSG ohnehin nicht zu beteiligen und meinerseits grundsätzlich auch nichts anzumerken. Für den Fall, dass es aber, ohne dass ich das bis dato erkennen konnte, doch um datenschutzrechtlich bedeutsame Regelungen geht, zum Beispiel weil sich die Gremien bei ihrer Arbeit auch mit Einzelfällen und dabei angefallenen personenbezogenen Daten, etwa von Patienten, befassen sollen, um ihre Aufgabe der Politikberatung effizient wahrnehmen zu können, habe ich dem Sozialministerium empfohlen, den Entwurf so zu überarbeiten, dass ggf. normenklar zum Ausdruck kommt, welche Verarbeitung welcher Arten personenbezogener Daten und welche damit verbundenen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung zugelassen werden sollen.

Für den Fall, dass die Gremien auch mit personenbezogenen Daten umgehen (sollen), habe ich das Sozialministerium zudem gebeten, in eigener Verantwortung zu klären, wer für solche Datenverarbeitungen verantwortlich sein soll, etwa diese Gremien selbst, sofern man sie als öffentliche Stellen im Sinne des § 2 Absatz 1 Satz 1 LDSG etablieren will, oder die Stelle, die den Vorsitz innehat oder bei der eine Geschäftsstelle eingerichtet ist, oder die jeweils handelnde Person oder Organisation, welche diese Person repräsentiert. Diese Frage ist von grundlegender Bedeutung. Denn hinsichtlich jeder Verarbeitung personenbezogener Daten muss klar sein, wer dafür verantwortlich ist. Insbesondere müssen auch die datenschutzrechtlich Betroffenen klar und unmissverständlich erkennen können, an wen sie sich zur Wahrung ihrer Datenschutzrechte, beispielsweise mit einem Antrag auf Auskunft oder auf Berichtigung oder Löschung ihrer Daten, wenden können.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

7.3 Datenschutz in Krankenhäusern

7.3.1 Dauerpatient Krankenhaus

In Krankenhäusern fallen große Mengen sehr sensibler personenbezogener Daten an. Deshalb muss das Krankenhaus die vom Gesetzgeber und von der Rechtsprechung gezogenen Grenzen sorgfältig beachten. Nur wenn der Patient sicher sein kann, dass die intimen Informationen über ihn mit der größtmöglichen Vertraulichkeit behandelt werden, wird das Krankenhaus den an ein modernes Dienstleistungsunternehmen gestellten Anforderungen gerecht.

Krankenhäuser werden diesem Anspruch in der Praxis oft nicht hinreichend gerecht. Sowohl die im Berichtszeitraum durchgeführten Kontrollen vor Ort als auch die im Rahmen von Beschwerden betroffener Patienten bekannt gewordenen Vorgänge haben leider erneut Mängel ergeben, die in meinen Tätigkeitsberichten schon mehrfach gerügt worden waren und die deshalb eigentlich nicht mehr vorkommen dürften. Folgendes ist in diesem Zusammenhang erwähnenswert:

■ Das anzuwendende Datenschutzrecht

Es kommt immer wieder vor, dass Krankenhäuser beim Umgang mit sensiblen Patientendaten den Überblick verlieren, welche datenschutzrechtlichen Regelungen zu beachten sind. Die Tatsache, dass den Mitarbeitern eines Krankenhauses nicht einmal bekannt war, dass Baden-Württemberg über ein Landeskrankengesetz (LKHG) verfügt und das Krankenhaus dieses auch zu beachten hat, war gleichwohl überraschend. Immerhin existiert dieses wichtige Gesetz bereits seit dem Jahre 1986.

Die 1992 neu eingefügten Vorschriften des 7. Abschnitts „Datenschutz“ enthalten bereichsspezifisches Datenschutzrecht für Krankenhäuser und die ihnen gleichgestellten Einrichtungen. Nach § 43 Absatz 5 LKHG sind auf Patientendaten die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden, soweit sich aus dem LKHG nichts anderes ergibt. Das LKHG regelt nur Teilbereiche, stellt also keine abschließende und ausschließ-

liche Datenschutzregelung dar. Daneben ist noch das allgemeine Datenschutzrecht anzuwenden (BDSG und LDSG).

Grundsätzlich gilt: Die Zulässigkeit der Erhebung, Speicherung, Veränderung, Nutzung und Übermittlung von Patientendaten kraft gesetzlicher Vorschrift richtet sich für das Krankenhaus nach dem LKHG. Für das Sperren und Löschen, für die Art und Weise der Datenverarbeitung, für Pflichten der datenverarbeitenden Stellen, für Rechte der betroffenen Patientinnen und Patienten sowie für die Kontrolle und die Aufsicht sind das BDSG oder das LDSG maßgebend.

■ Die Krankenhauseelsorge

Die Krankenhauseelsorge ist ein altes Thema, das mich immer wieder beschäftigt und das leider in immer wieder neuen Fallgestaltungen auftritt.

Aus Sicht der informationellen Selbstbestimmung steht es dem Patienten frei, von den seelsorgerischen Angeboten im Krankenhaus Gebrauch zu machen. Dies ist so auch in § 45 Absatz 2 LKHG aufgegriffen worden. Danach darf das Krankenhaus die Religionszugehörigkeit des Patienten erheben und speichern, wenn der Patient darauf hingewiesen wurde, dass die Angabe hierüber freiwillig ist und seine Religionszugehörigkeit für Zwecke der Krankenhauseelsorge erhoben werden soll. Dies muss allerdings deutlich, also nicht beiläufig und versteckt geschehen.

Gibt der Patient nach einem entsprechenden Hinweis auf die Freiwilligkeit und den Zweck der Erhebung seine Religionszugehörigkeit an, darf das Krankenhaus dem Krankenhauseelsorger die Konfession und die Patientendaten mitteilen, die erforderlich sind, um die Krankenhauseelsorge aufnehmen zu können, insbesondere Name, Geburtsdatum und Aufnahmedatum des Patienten.

Lehnt es der Patient ab, seine Religionszugehörigkeit anzugeben oder widerspricht er der Mitteilung an den Krankenhauseelsorger ausdrücklich, bleibt es dabei. Sowohl das Kranken-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

haus als auch der Krankenhauseelsorger haben die Entscheidung des Patienten zu respektieren.

Konkret bedeutet dies:

- Das Krankenhaus darf bei der Patientenaufnahme die Konfession nicht routinemäßig erheben, sondern nur dann, wenn der Patient zuvor über Freiwilligkeit und Zweck informiert wurde.
 - Es dürfen nur diejenigen Religionszugehörigkeiten erhoben werden, für die tatsächlich eine Krankenhauseelsorge angeboten werden kann (vgl. 20. Tätigkeitsbericht, LT-Drs. 12/4600 S. 42 ff.).
 - Soweit der Patient hierauf bei der Frage nach der Konfession hingewiesen wird, ist auch die Abfrage der Religionszugehörigkeit zu Zwecken einer konfessionsübergreifenden Seelsorge möglich.
 - Das Krankenhaus darf dem Krankenhauseelsorger nur die zur Aufnahme der Krankenhauseelsorge erforderlichen Patientendaten mitteilen (vgl. 25. Tätigkeitsbericht, LT-Drs. 13/3800 S. 46). Nicht zulässig wäre daher zum Beispiel die Erhebung der Wohnanschrift oder gar medizinischer Diagnosen und Therapien.
 - Gibt der Patient seine Konfession nicht an, bringt er damit zum Ausdruck, dass er keine Kontaktaufnahme durch den Seelsorger wünscht. Gleichwohl erfolgende Besuche in Patientenzimmern durch Seelsorger mit dem Ziel, seelsorgerische Dienste anzubieten und darüber zu informieren, widersprechen der gesetzlichen Regelung – auch wenn die Besuche noch so gut gemeint sind.
- **Übermittlung von Patientendaten an Hausarzt sowie weiterbehandelnde Ärzte**
Die Übermittlung von Befundberichten, Entlassberichten und ähnlichen Angaben durch das Krankenhaus an einen niedergelassenen Arzt, der im Anschluss an eine Krankenhausbehandlung die Behandlung ambulant fortsetzt, stellt eine Verarbeitung von personenbezogenen Daten dar und bedarf deshalb entweder einer gesetzlichen Grundlage oder der Einwilligung des

Patienten. Leider wird dabei das Verhältnis zwischen § 46 Absatz 1 Nr. 3b LKHG und § 73 Absatz 1b des Fünften Sozialgesetzbuchs (SGB V) oftmals nicht beachtet.

- Datenübermittlung zur ambulanten Weiterbehandlung:
Das Krankenhaus kann nach § 46 Absatz 1 Nr. 3b LKHG diejenigen Daten an den ambulant weiterbehandelnden Arzt übermitteln, die zur sachgerechten weiteren Behandlung des Patienten erforderlich sind, sofern der Patient nicht widersprochen hat. Nicht gefordert wird durch Nr. 3b, dass der Patient auf sein Widerspruchsrecht oder auf die beabsichtigte Weitergabe der Patientendaten hingewiesen wird.
 - Datenübermittlung an den Hausarzt:
Nach § 73 Absatz 1b SGB V ist das Krankenhaus bei gesetzlich versicherten Patienten verpflichtet, die Behandlungsdaten und Befunde an den Hausarzt des Versicherten zu übermitteln. Diese Verpflichtung gilt allerdings nur, wenn der Patient hierin schriftlich einwilligt.
 - Handelt es sich bei dem Hausarzt gleichzeitig um den weiterbehandelnden Arzt, ist eine Datenübermittlung also auch ohne ausdrückliche Einwilligung des Patienten möglich.
- **Die Auftragsdatenverarbeitung**
Eine im Auftrag des Krankenhauses erfolgende Datenverarbeitung durch externe Stellen, bei der also Leistungen des Krankenhauses ausgelagert werden, hat in den letzten Jahren zunehmend an Bedeutung gewonnen. In verschiedenen Tätigkeitsberichten habe ich mich zur Verarbeitung von Patientendaten außerhalb des Krankenhauses geäußert (zum Beispiel 31. Tätigkeitsbericht, LT-Drs. 15/4600 S. 101; 22. Tätigkeitsbericht, LT-Drs. 13/520 S. 76 ff., 5. Tätigkeitsbericht des Innenministeriums, LT-Drs. 14/4963 S. 91 ff.). In der Praxis bereitet das sog. Outsourcing aus unterschiedlichen Gründen erhebliche Probleme. Ein Grund liegt nach meiner Erfahrung in der Unkenntnis der maßgeblichen Rechtsgrundlagen.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Eine externe Datenverarbeitung bedingt in der Regel eine Herausgabe bzw. Weiterleitung von Patientenunterlagen an außerhalb des Krankenhauses befindliche externe Stellen. Sofern die Mitarbeiter des externen Dienstleisters Einblick in die personenbezogenen Gesundheitsdaten erhalten können, liegt eine Offenbarung von Patientengeheimnissen vor, zu deren Rechtfertigung es entweder einer gesetzlichen Grundlage oder einer Einwilligung des Patienten bedarf. Sofern weder eine gesetzliche Grundlage die Übermittlung legitimiert oder die Einholung der Einwilligung undurchführbar oder zu aufwendig ist, kann sich das Krankenhaus dadurch behelfen, dass es die Möglichkeit der Kenntnisnahme der Daten ausschließt oder die Daten pseudonymisiert. Einen weiteren Ausweg kann ggf. eine Auftragsdatenverarbeitung darstellen.

Entscheiden sich Krankenhäuser für eine Auftragsdatenverarbeitung, wird diese häufig auf das allgemeine Datenschutzrecht (§ 11 BDSG, § 7 LDSG) gestützt. Dabei wird übersehen, dass die Weitergabe von Daten, die beim Auftraggeber durch Berufsgeheimnisse i.S.v. § 203 des Strafgesetzbuchs (StGB) geschützt sind, zwar keine datenschutzrechtliche Übermittlung, wohl aber eine Offenbarung des Geheimnisses darstellt. Die Verarbeitung besonders geschützter Patientendaten durch externe Dienstleister kann daher in vielen Fällen nur auf die Einwilligung der betroffenen Patienten gestützt werden, es sei denn, eine spezialgesetzliche Regelung enthält hierfür eine ausdrückliche Befugnis. § 48 LKHG stellt eine solche spezialgesetzliche Norm dar. Solange die Vorgaben des § 48 LKHG eingehalten werden, liegt auch kein Verstoß gegen § 203 StGB vor, die ärztliche Schweigepflicht ist gewahrt.

Während das allgemeine Datenschutzrecht die Auftragsdatenverarbeitung durch jede geeignete Person oder Stelle zulässt, schränkt § 48 LKHG dies im Grundsatz ein. Nach Absatz 1 sind Patientendaten in dem Krankenhaus selbst oder im Auftrag eines Krankenhauses durch ein anderes Krankenhaus zu verarbeiten. Unter bestimmten Voraussetzungen dürfen Patientendaten nach

Absatz 2 auch durch ein Rechenzentrum im Auftrag des Krankenhauses automatisiert verarbeitet werden.

Aufgrund der mir vorliegenden Erkenntnisse muss ich davon ausgehen, dass externe Dienstleister häufig ohne tragfähige Rechtsgrundlage Patientendaten für Krankenhäuser verarbeiten. Krankenhäusern empfehle ich, die Beauftragung externer Stellen auf deren Zulässigkeit zu überprüfen und ggf. datenschutzkonforme Verfahren vorzusehen. Hierauf werde ich bei künftigen Kontrollen verstärkt achten.

7.3.2 Umsetzung der Orientierungshilfe Krankenhausinformationssysteme

Im Jahr 2011 beschloss die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe Krankenhausinformationssysteme (OH KIS). Inzwischen ist die Orientierungshilfe überarbeitet und Ende März 2014 in einer zweiten Fassung herausgegeben worden. Sowohl im 30. Tätigkeitsbericht (LT-Drs. 12/5740, S. 96 f.) als auch im 31. Tätigkeitsbericht (LT-Drs. 15/4600, S. 101 ff.) habe ich ausführlich darüber berichtet und die Krankenhausbetreiber aufgefordert, schnellstmöglich die Umsetzung der Orientierungshilfe anzugehen.

Im Berichtszeitraum habe ich in mehreren Krankenhäusern vor Ort die Umsetzung geprüft. Das Ergebnis war ernüchternd. Auch knapp fünf Jahre nach Veröffentlichung der Orientierungshilfe besteht vor allem bei kleineren und mittelgroßen Krankenhäusern nach wie vor großer Handlungsbedarf.

Erfreulich ist, dass alle besuchten Krankenhäuser inzwischen über ein Rollen- und Berechtigungskonzept verfügen. Auch wenn die Konzepte noch überarbeitet und weiterentwickelt werden müssen, so ist damit doch bereits eine deutliche Verbesserung des Patientenschutzes erzielt worden. Denn endlich können Ärzte, medizinisches Personal, Pflegekräfte und Mitarbeiter in administrativen Funktionen nicht mehr uneingeschränkt ohne weiteres auf alle Patientendaten zugreifen.

Die Krankenhäuser protokollieren aber bislang nicht oder in nur sehr eingeschränktem Umfang, wann welche personenbezogenen Daten in welcher

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Weise verarbeitet oder genutzt hat. Eine Überprüfung der Ordnungsmäßigkeit bzw. eines Verstoßes bei der Verarbeitung personenbezogener Daten ist somit nicht oder nur eingeschränkt möglich. Ich gehe allerdings davon aus, dass die Krankenhäuser die Erstellung der notwendigen Protokollierungs- und Auswertungskonzepte, soweit noch nicht geschehen, jetzt in Angriff nehmen.

Eine Sperrung von Patientendaten mit dem Ziel, Zugriffe auf Patientendaten zu beschränken und regelhaft auf begründete Sonderfälle einzugrenzen, konnte ebenfalls nicht festgestellt werden. Begründet wurde dies damit, dass das im Krankenhaus eingesetzte KIS-System diese Möglichkeit nicht oder nur eingeschränkt bietet. Hier müssen die Krankenhäuser schnellstmöglich zusammen mit den KIS-Herstellern Abhilfe schaffen. Bedauerlich ist auch, dass die KIS-Systeme nach wie vor nicht die Möglichkeit bieten, Daten physikalisch zu löschen.

Ich habe immer wieder betont, dass mir durchaus bewusst ist, dass den Krankenhäusern eine sofortige vollständige Umsetzung der Anforderungen der OH nicht möglich ist. Ich war und bin daher bereit, eine angemessene Übergangsfrist zu akzeptieren. Die datenschutzkonforme Ausgestaltung der eingesetzten IT-Verfahren ist jedoch zwingend ein Ziel, das von allen Krankenhäusern möglichst schnell erreicht werden muss. Knapp fünf Jahre (seit Veröffentlichung der Orientierungshilfe) reichen meines Erachtens jedoch aus, um nicht nur den Umsetzungsprozess anzustoßen, sondern auch datenschutzrechtliche Fortschritte vorweisen zu können.

Meine Dienststelle wird den Umsetzungsprozess in den Krankenhäusern auch künftig aufmerksam begleiten. Krankenhäusern, die noch gar nicht aktiv in dem Umsetzungsprozess eingestiegen sind, rate ich, dies nun endlich zu tun. Ich zähle weiterhin auf die Einsicht und Bereitschaft der Krankenhäuser. Sollten allerdings künftig keine wesentlichen Fortschritte in den einzelnen Krankenhäusern erkennbar sein, werde ich aufsichtsrechtliche Maßnahmen ins Auge fassen müssen – auch wenn dies für mich bisher nur eine letzte Option darstellt. Nicht zuletzt darf ich auch an die erheblich verschärften Sanktionsmöglichkeiten meiner Dienststelle ab Inkrafttreten der EU-Datenschutz-Grundverordnung im Jahr 2018 erinnern.

7.3.3 Auskünfte gegenüber Strafverfolgungsbehörden

Auskunftersuchen von Polizei und Staatsanwaltschaft verunsichern in der Regel Krankenhausmitarbeiter. Einerseits dürfen personenbezogene Daten nicht unbefugt herausgegeben werden, andererseits soll die Arbeit der Polizei bzw. Staatsanwaltschaft, zum Beispiel bei der Suche nach einem Unfallopfer, nicht behindert werden.

Eine generelle Verpflichtung zur Auskunftserteilung gegenüber Behörden, Staatsanwaltschaft oder Polizei besteht für Krankenhäuser nicht. Die Anfrage nach den Personalien, der Anschrift oder allgemein nach dem Umstand, ob sich eine Person in Krankenhausbehandlung befindet, rechtfertigt grundsätzlich keine Offenbarung dieser Daten. Die Verpflichtung zur Verschwiegenheit bleibt also bestehen. Von diesem Grundsatz sind Ausnahmen zu beachten.

- Nach § 46 Absatz 1 Nr. 6 des Landeskrankenhausesgesetzes (LKHG) ist es zulässig, Patientendaten weiterzugeben, wenn dies zum Schutz des Patienten oder eines Dritten erforderlich ist.

§ 46

Zulässigkeit der Übermittlung

(1) Patientendaten dürfen an Personen und Stellen außerhalb des Krankenhauses übermittelt werden, soweit dies erforderlich ist

...

6. zur Abwehr einer Gefahr für Leben, Gesundheit oder Freiheit des Patienten oder eines Dritten, wenn die Gefährdung dieser Rechtsgüter das Geheimhaltungsinteresse des Betroffenen überwiegt und die Gefahr in vertretbarer Weise nicht anders beseitigt werden kann.

Voraussetzung ist, dass die genannten Zwecke nicht mit anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Bei § 46 Absatz 1 Nr. 6 LKHG handelt es sich um eine spezialgesetzliche Regelung zum sog. rechtfertigenden Notstand nach § 34 StGB. Die Vorschrift des LKHG ist jedoch enger als § 34 StGB, weil eine Gefahr für Leben, Gesundheit oder Freiheit des Patienten oder eines Dritten vorausgesetzt wird. Eine Datenübermittlung setzt zudem voraus, dass die vom Krankenhaus vorzunehmende Güterabwägung ein Zurücktreten der Interessen des Betroffenen ergibt. Außerdem muss die Übermittlung nicht anonymisierter Daten das einzige Mittel sein, um die Gefahr abzuwehren.

Ein Fall des § 46 Absatz 1 Nr. 6 LKHG kann beispielsweise dann vorliegen, wenn ein Patient als Kraftfahrer im Straßenverkehr teilnimmt, obwohl er wegen einer bestehenden Erkrankung oder infolge von Medikamenten oder Suchtmittelannahme sich und/oder andere gefährdet. Dann kann es zulässig sein, die Straßenverkehrsbehörde zu informieren. Dies gilt ebenso für die Information eines Dritten im Falle einer drohenden Ansteckung mit einer schweren übertragbaren Krankheit.

Selbstverständlich darf das Krankenhaus auch in diesen Fällen nur die Daten weitergeben, die erforderlich sind, um die drohende Gefahr abwenden zu können.

- Das Strafverfolgungsinteresse des Staates kommt als höherwertiges Rechtsgut regelmäßig nicht in Betracht. Es hat hinter dem Geheimhaltungsinteresse des Patienten zurückzustehen und stellt – von schweren Fällen abgesehen – keinen Offenbarungsgrund dar. Sofern es um die Verhinderung drohender Straftaten geht, ist die Aussageverpflichtung des Arztes gem. § 138 StGB bei Kenntniserlangung von geplanten, in dieser Vorschrift aufgeführten Verbrechen zu beachten.
- Eine weitere Ausnahmeregelung findet sich in der seit 1. November 2015 geltenden Vorschrift des § 32 des Bundesmeldegesetzes (BMG).

§ 32

Besondere Meldepflicht in Krankenhäusern, Heimen und ähnlichen Einrichtungen

(1) Wer in Krankenhäusern, Pflegeheimen oder sonstigen Einrichtungen, die der Betreuung pflegebedürftiger oder behinderter Menschen oder der Heimerziehung dienen, aufgenommen wird oder dort einzieht, muss sich nicht anmelden, solange er für eine Wohnung im Inland gemeldet ist. Wer nicht für eine Wohnung im Inland gemeldet ist, hat sich, sobald sein Aufenthalt die Dauer von drei Monaten überschreitet, innerhalb von zwei Wochen anzumelden. Für Personen, die ihrer Meldepflicht nicht persönlich nachkommen können, haben die Leiter der Einrichtungen die Aufnahme innerhalb von zwei Wochen der Meldebehörde mitzuteilen, die für den Sitz der Einrichtung zuständig ist; die betroffenen Personen sind zu unterrichten. § 17 Absatz 3 Satz 3 bleibt unberührt.

(2) Der zuständigen Behörde ist Auskunft aus den Unterlagen der genannten Einrichtungen zu erteilen, wenn dies nach Feststellung der Behörde zur Abwehr einer erheblichen und gegenwärtigen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermissten und Unfallopfern im Einzelfall erforderlich ist. Die Auskunft umfasst folgende Daten:

- 1. Familienname,*
- 2. Vornamen,*
- 3. Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,*
- 4. Staatsangehörigkeiten,*
- 5. Anschriften,*
- 6. Datum der Aufnahme und Datum der Entlassung.*

Mit § 32 BMG wurde die bisherige Verpflichtung der Krankenhäuser aufgegeben, gesonderte Verzeichnisse über die aufgenommenen Personen zu führen, weil diese Einrichtungen ohnehin Unterlagen mit den entsprechenden Daten ihrer Patienten führen. Absatz 2 Satz 1 ermächtigt die zu einer Identitätsfeststellung berechtigten Behörden, die bisher ihre Auskunft über die Identität einzelner Personen aus diesen Verzeichnissen erhalten haben, künftig die Auskunft aus den Unterlagen der Einrichtungen

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

zu erhalten. Dabei handelt es sich um eine Offenbarungsbefugnis im Sinne des § 203 StGB.

Welche Behörden einen Anspruch auf Auskunft haben, regelt das Gesetz nicht ausdrücklich. Dies ergibt sich vielmehr aus der jeweiligen Aufgabenstellung. In Betracht kommen neben den Meldebehörden selbst insbesondere Polizeidienststellen und Staatsanwaltschaften, da diese mit Aufgaben der Gefahrenabwehr oder der Strafverfolgung befasst sind. Kein Auskunftsrecht haben hingegen die Verfassungsschutzbehörden, der Bundesnachrichtendienst und der Militärische Abschirmdienst oder Jugend- und Sozialämter. Die um Auskunft ersuchende Behörde hat ihre Entscheidungsgründe für ein Auskunftersuchen aktenkundig zu machen und trägt die Verantwortung für dessen Zulässigkeit.

Der Leiter des Krankenhauses hat also der zuständigen Behörde Auskunft aus den Krankenunterlagen zu erteilen, wenn dies nach Feststellung der anfragenden Behörde aus nachfolgenden Gründen im Einzelfall erforderlich ist:

- zur Abwehr einer erheblichen oder gegenwärtigen Gefahr,
- zur Verfolgung von Straftaten oder
- zur Aufklärung des Schicksals von Vermissten und Unfallopfern.

Mit diesen Beschränkungen trägt der Gesetzgeber dem Umstand Rechnung, dass ein Krankenhausaufenthalt eine sehr sensible Information sein kann.

Die von der Auskunft umfassten Daten sind in Absatz 2 abschließend aufgezählt. Darüber hinausgehend angefragte Daten, etwa zum Behandlungsverlauf und zu Diagnosen, dürfen nicht weitergegeben werden.

7.4 Der neue Leitfaden zum Datenschutz in medizinischen Forschungsprojekten

Medizinische Forschung dient der Weiterentwicklung diagnostischen und therapeutischen Wissens und nützt den Patienten durch Verbesserung der Behandlungsqualität. Dafür werden viele medizinische Patientendaten, zunehmend auch Biomaterialien (Blut-, Gewebeproben etc.) benötigt. Dadurch greift die Forschung in das grundgesetzlich geschützte allgemeine Persönlichkeitsrecht (Artikel 2

Absatz 1 i. V. mit Artikel 1 Absatz 1 des Grundgesetzes) ein.

Medizinische personenbezogene Daten sind für die Forschung ein wichtiges Gut, weil sie die Grundlage für neue Erkenntnisse bilden. Sie zählen zu den sensibelsten persönlichen Informationen und müssen daher sorgfältig geschützt werden. In der täglichen Arbeit ist jeder, der personenbezogene Daten im Wissenschaftsbereich erhebt, gefordert, den bestmöglichen Ausgleich zwischen dem Persönlichkeitsrecht des Einzelnen und der Freiheit von Wissenschaft, Forschung und Lehre zu finden. Der Rahmen wird durch den Gesetzgeber im Bundesdatenschutzgesetz bzw. dem jeweiligen Landesdatenschutzgesetz gesetzt.

Um zu zeigen, wie medizinische Forschung unter diesen Randbedingungen möglich ist, entwickelte die Technologie- und Methodenplattform für die vernetzte Forschung e.V. (TMF) bereits 2003 zusammen mit den Datenschutzbeauftragten des Bundes und der Länder einen „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten“. Das Datenschutzkonzept enthielt Musterlösungen für verschiedene Arten von medizinischen Forschungsnetzen. 2006 wurde darüber hinaus zwischen der TMF und den Datenschutzbeauftragten des Bundes und der Länder ein generisches Datenschutzkonzept für den Aufbau und Betrieb von Biomaterialbanken abgestimmt. Die Konzepte gewährleisten die Wahrung der Forschungsinteressen bei gleichzeitig angemessenem Schutz der Patientendaten durch bestimmte Verfahrensvorgaben (Patienteninformation und -aufklärung, Anonymisierungs- und Pseudonymisierungsverfahren, Treuhändereinsatz, technisch-organisatorische Maßnahmen).

Die generischen Datenschutzkonzepte der TMF sind in den vergangenen Jahren einer grundlegenden Revision unterzogen worden. Um die Anforderungen verschiedenster Forschungsverbände, -projekte und -einrichtungen abbilden zu können und damit leichter adaptierbar zu sein, wurden sie nun modular und skalierbar aufgebaut. So können entweder Datenschutzkonzepte für einzelne Bereiche (klinisches Modul, Forschungsmodul, Studienmodul oder Biobank-Modul) oder für das Gesamtszenario eines großen Forschungsverbundes abgeleitet werden. Im Zentrum steht das Identitätsmanagement als verbindender Dienst.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Frühjahrstagung 2014 beschlossen, medizinischen Forschungseinrichtungen und Forschungsverbänden zu empfehlen, den von der TMF entwickelten „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF 2.0“ als Basis für die konkrete Ausgestaltung ihrer Datenschutzkonzepte zu nehmen. Der Leitfaden ist bei der TMF (<http://www.tmf-ev.de>) erhältlich.

7.5 Gesundheitsatlas Baden-Württemberg

Die Gesundheitsberichterstattung als Aufgabe des öffentlichen Gesundheitsdienstes beschreibt die gesundheitliche Lage und Versorgung der Bevölkerung. Hierzu gehört auch der Gesundheitsatlas Baden-Württemberg, der landesweite und regionale Gesundheitsinformationen zur Gesundheit und zu gesundheitsrelevanten Themen enthält, beispielsweise Daten zum Auftreten von Krankheiten, zur Ärztedichte oder zur Lebenserwartung. Die Daten sind in Form von Tabellen, Karten und Berichten im Internet veröffentlicht (<http://www.gesundheitsatlas-bw.de>).

Nach Angaben des Sozialministeriums stellen diese Daten eine fundierte Grundlage dar, um geeignete Maßnahmen zur Prävention und Verbesserung der Versorgung gesamtgesellschaftlich bedeutsamer, chronischer Erkrankungen planen und evaluieren zu können. Dazu bedürfe es aussagekräftiger, flächendeckender oder regional abgrenzbarer Daten, u. a. zu häufig auftretenden wichtigen Erkrankungen wie beispielsweise Diabetes mellitus.

Das Sozialministerium und das Landesgesundheitsamt beabsichtigten, die Darstellungen im Gesundheitsatlas um zusätzliche, fachlich relevante Diabetes mellitus Typ 2-Indikatoren zu erweitern. Dazu sollten Daten aus den Statistiken des Statistischen Landesamtes und der Statistik der gesetzlichen Rentenversicherung der Deutschen Rentenversicherung Bund, aber auch Abrechnungsdaten mehrerer gesetzlicher Krankenversicherungen genutzt werden.

Im Zusammenhang mit der Beurteilung der datenschutzrechtlichen Zulässigkeit des Vorhabens musste dabei auch die Frage geklärt werden, ob und ggf. auf welcher Rechtsgrundlage die Krankenkassen

berechtigt sind, Abrechnungsdaten für die entsprechenden Darstellungen im Gesundheitsatlas zu nutzen. Leider hatten weder das Sozialministerium oder das Landesgesundheitsamt noch die beteiligten Krankenkassen diese Frage rechtzeitig geprüft.

§ 284 Absatz 1 des Fünften Sozialgesetzbuchs (SGB V) zählt in Nr. 1 bis 14 *abschließend* auf, für welche Zwecke die Krankenkassen Sozialdaten erheben und speichern dürfen, zum Beispiel zur Feststellung des Versicherungsverhältnisses und der Mitgliedschaft oder zur Abrechnung mit Leistungserbringern und Leistungsträgern. Die Ermächtigung zur Verarbeitung und Nutzung der nach Absatz 1 erhobenen und gespeicherten Daten enthält Absatz 3:

(3) Die rechtmäßig erhobenen und gespeicherten versichertenbezogenen Daten dürfen nur für die Zwecke der Aufgaben nach Absatz 1 in dem jeweils erforderlichen Umfang verarbeitet oder genutzt werden, für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist. Die Daten, die nach § 295 Abs. 1b Satz 1 an die Krankenkasse übermittelt werden, dürfen nur zu Zwecken nach Absatz 1 Satz 1 Nr. 4, 8, 9, 10, 11, 12, 13, 14 und § 305 Abs. 1 versichertenbezogen verarbeitet und genutzt werden und nur, soweit dies für diese Zwecke erforderlich ist; für die Verarbeitung und Nutzung dieser Daten zu anderen Zwecken ist der Versichertenbezug vorher zu löschen.

Da die Erhebung und Speicherung von Abrechnungsdaten zum Zwecke der Darstellung der Diabetes-Indikatoren für den Gesundheitsatlas nicht unter den Katalog des Absatzes 1 fallen, konnte eine Nutzung der Abrechnungsdaten durch die Krankenkassen zu diesem Zweck nicht auf diese Vorschrift gestützt werden.

§ 287 SGB V schafft eine Rechtsgrundlage dafür, dass die Datenbestände nach § 284 SGB V über die enge Zweckbindung in § 284 Absatz 3 SGB V hinaus für Zwecke der internen Forschung bei den Krankenkassen verwendet werden können. Diese Vorschrift schränkt allerdings die Verwendung der Datenbestände ganz erheblich ein. Die Verwendung bedarf der Erlaubnis der Aufsichtsbehörde, das Forschungsvorhaben selbst unterliegt bestimmten Ein-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

schränkungen, eine versichertenbezogene Datenverwendung ist ausgeschlossen und die Sozialdaten sind zu anonymisieren. Da vorliegend ein Forschungsauftrag weder geplant noch erteilt worden war, kamen auch die beteiligten Krankenkassen zu dem Ergebnis, dass sie zur Nutzung ihrer Abrechnungsdaten für die Darstellung der Diabetes mellitus Typ 2-Indikatoren im Gesundheitsatlas nicht berechtigt sind. Das Sozialministerium und das Landesgesundheitsamt stellten daraufhin die beabsichtigte Darstellung dieser zusätzlichen Indikatoren im Gesundheitsatlas bis auf weiteres zurück.

Soweit im Gesundheitsatlas statistische Daten des Statistischen Landesamtes und/oder der Deutschen Rentenversicherung Bund dargestellt werden, begegnet dies keinen datenschutzrechtlichen Bedenken.

Krankenkassen, aber auch Personen und Stellen, die an der Nutzung der von den Krankenkassen zulässigerweise erhobenen und gespeicherten Versichertendaten zu unterschiedlichen Zwecken Interesse haben, müssen sich darüber im Klaren sein, dass die derzeitige Gesetzeslage dies nur sehr eingeschränkt zulässt.

7.6 Datenschutz bei Sozialleistungsträgern

7.6.1 Hausbesuche bei fehlgeleiteten Arbeitsunfähigkeitsbescheinigungen

Werden Arbeitsunfähigkeitsbescheinigungen durch Ärzte versehentlich an eine unzuständige Krankenversicherung weitergeleitet, ist es unzulässig, dass deren Außendienstmitarbeiter den betroffenen Versicherten die Bescheinigungen anlässlich eines Hausbesuchs zurückgeben. Die Versicherung hat andere, datenschutzfreundlichere Möglichkeiten einer Kontaktaufnahme.

Ein Arzt stellt eine sog. Arbeitsunfähigkeitsbescheinigung (AU-Bescheinigung) aus, wenn ein Arbeitnehmer arbeitsunfähig erkrankt ist, und leitet diese an die Krankenkasse des Arbeitnehmers weiter. Dabei kommt es leider immer wieder vor, dass eine AU-Bescheinigung versehentlich an eine unzuständige Krankenkasse gesendet wird.

Auch eine Krankenkasse in Baden-Württemberg erhielt in der Vergangenheit mehrfach solche Irrläu-

fer. Die Krankenkasse nahm dies zum Anlass, den Versicherten einen Hausbesuch abzustatten. Sie gab gegenüber meiner Dienststelle an, die Kontaktaufnahme von Außendienstmitarbeitern diene in derartigen Fällen in erster Linie zur Abklärung, wie mit den einzelnen Bescheinigungen weiter umgegangen werden soll. Es sei im Interesse des Betroffenen, die AU-Bescheinigung persönlich zu übergeben. Die Betroffenen wunderten sich allerdings über die Hausbesuche der Außendienstmitarbeiter, einige fühlten sich massiv bedrängt, da die Besuche auch zur Mitgliederwerbung genutzt wurden.

Krankenkassen haben sicherlich dafür zu sorgen, dass fehlgeleitete AU-Bescheinigungen möglichst schnell zurückgegeben werden. Ich erkenne auch an, dass eine Kontaktaufnahme durchaus im Interesse des Versicherten erfolgt, um abzuklären, an wen die Bescheinigung geschickt werden soll. Eine telefonische Kontaktaufnahme mit dem Betroffenen halte ich daher grundsätzlich für zulässig. Ist die Telefonnummer des Betroffenen nicht bekannt, stehen Vorgehensweisen zur Verfügung, die datenschutzfreundlicher sind als Hausbesuche. In Betracht kommt die postalische Übersendung an den Betroffenen, an die zuständige Krankenkasse oder an den Arzt mit dem Hinweis, dass die nicht zuständige Versicherung irrtümlich die AU-Bescheinigung erhalten hat. Damit kann die Krankenkasse schnell und auf einfache Art und Weise die AU-Bescheinigung auf den richtigen Weg bringen. Ein Hausbesuch ist dazu jedenfalls nicht erforderlich.

Eine Rechtsgrundlage, die es der Krankenkasse erlauben würde, fehlgeleitete AU-Bescheinigungen zum Zwecke eines Hausbesuchs zu nutzen, existiert nicht. Dies gilt erst recht für den Fall, dass die Kontaktaufnahme der Eigenwerbung dienen soll.

7.6.2 Krankengeldfallmanagement der Krankenkassen

Seit Jahren stellen Aufsichtsbehörden einen datenschutzrechtlich bedenklichen Umgang mit Sozialdaten von Versicherten im Rahmen des sog. Krankengeldfallmanagements der gesetzlichen Krankenkassen fest. Es werden z.T. detaillierte Gesundheitsdaten von Versicherten erhoben, die längere Zeit arbeitsunfähig sind oder bereits Krankengeld erhalten. Die gesetzliche Aufgabentrennung zwischen dem Medizinischen Dienst der Krankenversicherung

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

(MDK) und den gesetzlichen Krankenversicherungen wird dabei oft ignoriert.

Mit dem Krankengeldfallmanagement versuchen Krankenkassen dazu beizutragen, dass Versicherte eine Arbeitsunfähigkeit überwinden und wieder in das Arbeitsleben integriert werden. Das Angebot der Versicherung besteht darin, Leistungen medizinischer Dienstleistungsangebote und verschiedener Kostenträger für den Versicherten zu koordinieren. Der sog. Krankengeldfallmanager einer gesetzlichen Krankenkasse wird aktiv, wenn Versicherte über einen gewissen Zeitraum arbeitsunfähig sind. Er lädt den Versicherten zu einem persönlichen Beratungsgespräch ein, ruft ihn an oder schickt ihm einen Fragebogen zur Selbstauskunft. Die Krankenkassenmitarbeiter stellen dem Versicherten Fragen zur Arbeitsplatz- und Krankheitssituation und teilweise auch zu seinem familiären und sozialen Umfeld. Bei diesen Befragungen werden oftmals detaillierte Gesundheitsdaten der Versicherten erhoben und verarbeitet, so dass gesetzliche Krankenkassen sensible Sozialdaten von Versicherten zur Kenntnis nehmen.

Aus datenschutzrechtlicher Sicht ist dies unzulässig. Grund dafür ist die gesetzliche Aufgabentrennung zwischen dem MDK und den gesetzlichen Krankenkassen (§§ 275 ff. SGB V). Auch aus Gründen des Sozialdatenschutzes hat der Gesetzgeber die Prüfung medizinischer Sachverhalte ausdrücklich dem MDK übertragen. In welchen Fällen der MDK einzuschalten ist, legt § 275 SGB V fest. Demnach berät der MDK die Krankenkassen in allgemeinen Fragen, bei denen medizinisches Fachwissen notwendig ist, und gibt in deren Auftrag u. a. gutachtliche Stellungnahmen über die Arbeitsfähigkeit und die Einleitung von Maßnahmen zur Rehabilitation ab. Zur Erfüllung dieser Aufgaben ist der MDK gem. § 276 Absatz 2 Satz 1 SGB V auch befugt, Sozialdaten zu erheben, soweit dies für die Prüfungen, Beratungen und Stellungnahmen nach § 275 SGB V erforderlich ist. Werden hierzu medizinische Informationen von Leistungserbringern benötigt, müssen diese dem MDK unmittelbar übermittelt werden (§ 276 Absatz 2 Satz 2 SGB V). Mit der Festlegung dieser gesetzlichen Aufgaben des MDK hat der Gesetzgeber auch entschieden, dass Krankenkassen von medizinischen Informationen der Versicherten keine Kenntnis nehmen dürfen. Sie sind vielmehr auf ein Tätigwerden des MDK angewiesen.

Beratungen und Kontrollen des Krankengeldfallmanagements

Auch das sog. Umschlagverfahren (siehe Kapitel 7.7.2), bei dem Vertragsärzte Unterlagen über die Krankenkassen in einem verschlossenen Umschlag an den MDK weiterleiten, spielt eine Rolle im Rahmen des Krankengeldfallmanagements. Beauftragt die Krankenkasse den MDK mit der Erstellung eines Gutachtens über die Arbeitsfähigkeit des Versicherten, werden medizinische Unterlagen im verschlossenen Umschlag zur Begutachtung durch den MDK auch direkt an die Krankenkassen übermittelt. Bei einem Kontrollbesuch meiner Mitarbeiter bei einer gesetzlichen Krankenkasse zeigte sich, dass medizinische Behandlungsunterlagen dort zum Bestandteil einer Fall-Akte wurden. Die medizinischen Unterlagen befanden sich zwar ordnungsgemäß im verschlossenen Umschlag, der Umschlag wurde aber dauerhaft zusammen mit den übrigen Fall-Unterlagen aufbewahrt und später zusammen mit der Fall-Akte vernichtet.

Diese Praxis halte ich datenschutzrechtlich für unzulässig. Bei den archivierten Unterlagen im verschlossenen Umschlag handelt es sich um medizinische Dokumente des MDK. Der MDK ist insoweit datenschutzrechtlich verantwortliche Stelle gem. § 67 Absatz 9 des Zehnten Buches des Sozialgesetzbuches (SGB X) i.V. mit § 276 Absatz 2 SGB V und damit auch für die gesetzeskonforme Verarbeitung der Sozialdaten, insbesondere auch für deren Archivierung und Vernichtung verantwortlich. Auch wenn bei der stichprobenartigen Überprüfung nur verschlossene Umschläge vorgefunden wurden, bestand doch für die Mitarbeiter der Krankenkasse jederzeit die Möglichkeit, diese zu öffnen. Weitere Sicherungsmaßnahmen, die eine unbefugte Kenntnisnahme des Inhalts der Umschläge verhindern, waren nicht vorgesehen. Ungeachtet dessen haben Krankenkassen und MDK unterschiedliche Aufbewahrungsfristen zu beachten: Der MDK hat Sozialdaten gem. § 276 Absatz 2 Satz 3 SGB V nach fünf Jahren zu löschen, für gesetzliche Krankenkassen gelten dagegen Aufbewahrungsfristen von bis zu zehn Jahren (§ 304 SGB V i.V. mit § 84 Absatz 2 SGB X). Dass die bei der Krankenkasse aufbewahrten Unterlagen des MDK (durch MDK oder Krankenkasse) rechtzeitig gelöscht werden, konnte nicht festgestellt werden.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Der Gesetzgeber hat mittlerweile klargestellt, dass das bislang praktizierte Umschlagverfahren unzulässig ist (siehe Kapitel 7.7.2.). Medizinische Unterlagen des MDK dürfen demnach nicht mehr über die gesetzlichen Krankenkassen an den MDK weitergeleitet werden, auch nicht im verschlossenen Umschlag.

Anspruch auf Krankengeldfallmanagement

Durch das Gesetz zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) vom 16. Juli 2015 (BGBl. I S. 1211) wurde das SGB V um einen Anspruch der Versicherten auf Krankengeldfallmanagement erweitert. Aufgrund der o. g. datenschutzrechtlichen Probleme habe ich mich zusammen mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 16. Dezember 2014 („Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!“) gegen die Einführung einer solchen Regelung ausgesprochen (siehe Anhang 13). Der Gesetzgeber hat sich aber für die Einführung des Anspruchs entschieden, der nunmehr in § 44 Absatz 4 SGB V geregelt ist. Er erstreckt sich auf individuelle Beratung und Hilfestellung durch die Krankenkasse, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind. Solche Maßnahmen und die dazu erforderliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten dürfen nur mit schriftlicher Einwilligung und nach vorheriger schriftlicher Information des Versicherten erfolgen. Die Einwilligung kann jederzeit schriftlich widerrufen werden.

Trotz der neuen gesetzlichen Aufgabe der Krankenkassen sind deren datenschutzrechtliche Befugnisse m. E. nicht auf die Erhebung medizinischer Unterlagen von Versicherten erweitert worden. Auch bei Vorliegen einer Einwilligungserklärung bleibt dies allein dem MDK vorbehalten. Eine datenschutzrechtliche Befugnis zum Zweck der Auswahl von Versicherten für Maßnahmen nach § 44 Absatz 4 Satz 1 SGB V und zu deren Durchführung (vgl. § 285 Absatz 1 Nr. 16 SGB V) ist – wie bislang auch – durch den gesetzlichen Aufgabenbereich des MDK in Fällen des § 275 SGB V begrenzt. Die im Wortlaut genannte „individuelle Beratung und Hilfestellung“ durch die Krankenkassen endet dort, wo die Krankenkasse den MDK einschalten muss, ins-

besondere bei der Prüfung von Maßnahmen zur Sicherung des Behandlungserfolgs, wie der Einleitung von Maßnahmen der Leistungsträger für die Wiederherstellung der Arbeitsfähigkeit oder wenn Zweifel an der Arbeitsunfähigkeit bestehen (§ 275 Absatz 1 Nummer 3 Buchstaben a und b SGB V). Medizinische Unterlagen sind zur Erfüllung des Anspruchs gem. § 44 Absatz 4 SGB V daher regelmäßig nicht erforderlich. Es ist allein Aufgabe des MDK im Rahmen der ihm zugewiesenen Aufgaben, Zweifel an einer Arbeitsunfähigkeit zu beseitigen und hierbei ggf. Daten zu erheben.

Meine Dienststelle wird die weitere Umsetzung des Anspruchs auf Krankengeldfallmanagement kritisch begleiten und darauf dringen, dass die gesetzlichen Voraussetzungen von den Krankenkassen eingehalten werden.

7.6.3 Bekanntgabe von Reha-Entlassungsberichten an die Deutsche Rentenversicherung

Wenn ein Patient eine Rehabilitationseinrichtung, beispielsweise eine Klinik, verlässt, wird dort regelmäßig ein Entlassungsbericht gefertigt, der in Gestalt eines Arztberichts eine Vielzahl höchst sensibler Daten über den Patienten enthalten kann. Dabei stellt sich u. a. die Frage, ob die Deutsche Rentenversicherung (DRV) zu den Stellen gehört, die einen solchen Bericht in datenschutzrechtlich zulässiger Weise erhalten dürfen.

Bei der Bearbeitung diesbezüglicher Beschwerden wurde meiner Dienststelle entgegengehalten, die Weitergabe des Reha-Entlassungsberichts durch eine private Klinik an die DRV als Rehabilitations-träger sei zulässig, stelle sich in datenschutzrechtlicher Hinsicht aber nicht als Datenübermittlung dar, sondern als Nutzung von Sozialdaten innerhalb der datenschutzrechtlich verantwortlichen Stelle. Dieser Aussage lag wohl der Gedanke zugrunde, dass die DRV hinsichtlich der Rehabilitationsmaßnahmen datenschutzrechtlich verantwortlich sei und bleibe, weil sie sich der privaten Klinik oder sonstigen externen Rehabilitationseinrichtung als Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung bediene. Ein Widerspruchsrecht der betroffenen Patienten nach § 76 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) wurde dabei nicht anerkannt, weil dieses nur in Fällen der Datenübermittlung,

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

nicht aber im damals angenommen Fall der Auftragsdatenerarbeitung bestehe.

Auch die Deutsche Rentenversicherung Bund (DRV Bund) hat früher die Auffassung vertreten, die Weitergabe solcher Entlassungsberichte durch private Rehabilitationseinrichtungen, mit denen sog. Belegungsverträge abgeschlossen wurden, an die DRV sei eine interne Nutzung, ist aber erfreulicherweise davon abgerückt. Die DRV Bund betrachtet die Weitergabe solcher Berichte nur noch in den Fällen als interne Nutzung im Rahmen einer Auftragsdatenverarbeitung, in denen die Leistungen zur medizinischen Rehabilitation in von der Rentenversicherung selbst betriebenen, eigenen Rehabilitationseinrichtungen durchgeführt werden. Denn diese eigenen Rehabilitationseinrichtungen lassen sich zu Recht als Teil des sie betreibenden Rentenversicherungsträgers qualifizieren. Die Weitergabe der Reha-Entlassungsberichte ist damit datenschutzrechtlich eine zulässige Nutzung von Daten nach § 67 Abs. 7 SGB X. Anders verhält es sich, nun auch nach Einschätzung der DRV Bund, hinsichtlich privater Einrichtungen, mit denen Belegungsverträge abgeschlossen wurden. Diese Vertragseinrichtungen sind im Verhältnis zur DRV in datenschutzrechtlicher Hinsicht „Dritte“ im Sinne von § 67 Absatz 10 SGB X. Somit ist die Weitergabe des Berichts an die DRV in diesen Fällen als Übermittlung zu qualifizieren, die nach § 78 SGB X, §§ 28, 39 BDSG zulässig sein kann, ohne dass es der Einwilligung der jeweiligen Patienten bedarf. In den Fällen, in denen die eigene Rehabilitationseinrichtung eines Rentenversicherungsträgers einen Entlassungsbericht an einen anderen, für die medizinische Rehabilitation des betroffenen Patienten zuständigen Rentenversicherungsträger senden will, kann dies auf die Übermittlungsbefugnis nach § 69 Absatz 1 Nummer 1 3. Alternative SGB X gestützt werden, wobei es auch hier der Einwilligung der betroffenen Patienten nicht bedarf.

Die Rechtslage sollte nun auch für die Deutsche Rentenversicherung Baden-Württemberg und für baden-württembergische Rehabilitationseinrichtungen klar sein.

7.7 Datenschutz beim Medizinischen Dienst der Krankenversicherung

7.7.1 Kontrollbesuch beim Medizinischen Dienst der Krankenversicherung

Im Berichtszeitraum führten meine Mitarbeiter einen Kontroll- und Beratungsbesuch beim Medizinischen Dienst der Krankenversicherung Baden-Württemberg (MDK) in dessen Hauptverwaltung durch. Geprüft wurde u. a. der Umgang des MDK mit sozialmedizinischen Gutachten, die im Auftrag der Krankenkassen erstellt werden.

Der MDK berät die gesetzlichen Kassen in allgemeinen Grundsatzfragen und gibt in deren Auftrag gutachtliche Stellungnahmen zu Einzelfällen ab. Die gesetzlichen Aufgaben des MDK sind in § 275 des Fünften Buches des Sozialgesetzbuches (SGB V) beschrieben. Hierzu gehören u. a. Stellungnahmen für die Krankenkassen bei Fragen zur Arbeitsunfähigkeit, Notwendigkeit, Art, Umfang und Dauer von Rehabilitationsleistungen, Verordnung von Arznei-, Verband-, Heil- und Hilfsmitteln, Notwendigkeit und Dauer einer Krankenhausbehandlung sowie Notwendigkeit und Dauer von häuslicher Krankenpflege.

Schwerpunkt der Prüfung war der Umgang des MDK mit sozialmedizinischen Gutachten. Näher überprüft wurden insbesondere Verfahren und Umfang der Übermittlung von Gutachten im Rahmen von Arbeitsunfähigkeitsbescheinigungen, einschließlich der allgemeinen technischen und organisatorischen Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit im Umgang mit Patienten- und Gesundheitsdaten.

§ 277 SGB V regelt die Übermittlungspflichten und die Übermittlungsbefugnisse des MDK gegenüber der Auftrag gebenden Krankenkasse sowie dem an der vertragsärztlichen Versorgung teilnehmenden Arzt bzw. dem sonstigen Leistungserbringer, über dessen Leistung der MDK eine gutachtliche Stellungnahme abgegeben hat.

§ 277 Absatz 1 SGB V

Der Medizinische Dienst hat dem an der vertragsärztlichen Versorgung teilnehmenden Arzt, sonstigen Leistungserbringern, über deren Leistungen er

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

eine gutachtliche Stellungnahme abgegeben hat, und der Krankenkasse das Ergebnis der Begutachtung und der Krankenkasse die erforderlichen Angaben über den Befund mitzuteilen. Er ist befugt, den an der vertragsärztlichen Versorgung teilnehmenden Ärzten und den sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, die erforderlichen Angaben über den Befund mitzuteilen. Der Versicherte kann der Mitteilung über den Befund an die Leistungserbringer widersprechen.

Der Umfang des MDK-Gutachtens richtet sich grundsätzlich nach der Anfrage bzw. dem Auftrag der jeweiligen Krankenkasse. Der MDK darf der gesetzlichen Krankenkassen jedoch nur das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitteilen. Vollständige Gutachten dürfen nicht übermittelt werden. Grund dafür ist die gesetzliche Aufgabentrennung zwischen dem MDK und den Krankenkassen; der Gesetzgeber hat die Prüfung medizinischer Sachverhalte ausdrücklich dem MDK übertragen (siehe Kapitel 7.6.2).

In der Vergangenheit hatte der MDK den Krankenkassen regelmäßig die kompletten von ihm erstellten Gutachten über die betroffenen Versicherten übersendet (vgl. 19. Tätigkeitsbericht, LT-Drs. 12/3480, S. 20 f.). Umso erfreulicher ist es, dass die Prüfung vor Ort nun ergab, dass der MDK sich an die gesetzlichen Vorgaben des § 277 Absatz 1 SGB V hält. Eine stichprobenartige Kontrolle übermittelter MDK-Gutachten ergab keine Hinweise darauf, dass der MDK – neben dem Ergebnis der Begutachtung und den Angaben über den Befund – detaillierte Erläuterungen zum Krankheitsverlauf, zur Vorgeschichte oder zum sozialen Umfeld des Patienten an die Krankenkassen weiterleitet. Zur geänderten Verfahrensweise dürfte dabei vor allem auch eine datenschutzfreundlichere Programmvoreinstellung in der vom MDK verwendeten Software beigetragen haben. In der Grundeinstellung werden der Befund und die medizinische Vorgeschichte des Patienten standardmäßig nicht mehr an die Krankenkassen übermittelt. Hält die begutachtende Person die Angaben für die Leistungsentscheidung der Krankenkasse im Einzelfall für erforderlich, muss sie die Übermittlung aktiv auswählen.

Die Kontrolle des MDK ergab ein durchweg erfreuliches Ergebnis. Das Datenschutzbewusstsein ist dort sehr ausgeprägt.

7.7.2 Ende des Umschlagverfahrens

Das sog. Umschlagverfahren, bei dem Vertragsärzte Unterlagen über die Krankenkassen in einem verschlossenen Umschlag – in der Regel mit der Aufschrift „Ärztliche Unterlagen nur vom MDK zu öffnen“ – an den MDK weiterleiten, ist nicht mehr zulässig. Künftig sind die erforderlichen Unterlagen direkt dem MDK zu übersenden.

Der MDK berät die Krankenkassen in allgemeinen Fragen, bei denen medizinisches Fachwissen notwendig ist, und gibt in deren Auftrag gutachtliche Stellungnahmen, zum Beispiel zur Arbeitsfähigkeit, zur Einleitung von Maßnahmen zur Rehabilitation, zur Notwendigkeit und Dauer einer Krankenhausbehandlung oder sonst zu der Frage ab, ob und in welchem Umfang die Kassen bestimmte Leistungen erbringen müssen (§ 275 Absatz SGB V). Werden hierzu medizinische Informationen von Leistungserbringern benötigt, müssen sie diese dem MDK unmittelbar übermitteln (§ 276 Absatz 2 Satz 1, Halbsatz 2 SGB V).

Bislang habe ich die Anforderung von medizinischen Informationen durch die Krankenkasse akzeptiert, wenn die Leistungserbringer die betreffenden Unterlagen in einem verschlossenen Umschlag zur Weiterleitung an den MDK direkt an die Krankenkasse übersandten. Zum Teil wurde dies auch so gehandhabt, dass dem Arzt oder sonstigem Leistungserbringer ein farbiger, an den MDK adressierter Umschlag gleich mitgeliefert wurde. Die Krankenkasse leitete daraufhin den verschlossenen Umschlag zur Begutachtung an den MDK weiter.

Nicht alle Krankenkassen hielten sich an die Vorgaben des Umschlagverfahrens, mit der Folge, dass Mitarbeiter der Kassen Kenntnis von sensiblen Versichertendaten erhalten haben, die nur für den MDK bestimmt sind. Der Gesetzgeber hat darauf reagiert und mit dem Gesetz zur Reform der Strukturen der Krankenhausversorgung (Krankenhausstrukturgesetz – KHSG) eine Änderung des § 276 Absatz 2 Satz 2 SGB V zum 1. Januar 2016 vorgesehen:

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

§ 276 Absatz 2 Satz 2 SGB V

Haben die Krankenkassen oder der Medizinische Dienst für eine gutachtliche Stellungnahme oder Prüfung nach § 275 Absatz 1 bis 3 erforderliche versichertenbezogene Daten bei den Leistungserbringern angefordert, so sind die Leistungserbringer verpflichtet, diese Daten unmittelbar an den Medizinischen Dienst zu übermitteln.

Mit der Neuregelung des § 276 Absatz 2 Satz 2 SGB V soll laut der Gesetzesbegründung sichergestellt werden, dass Krankenkassen keine Kenntnis von medizinischen Daten erhalten, die nur für die Begutachtung durch den MDK erforderlich und bestimmt sind. Zur Vereinfachung des Verwaltungsablaufes bleibe es zwar weiterhin möglich, dass Krankenkassen personenbezogene Daten für den MDK anfordern, der Rücklauf der medizinischen Unterlagen soll aber nur noch direkt an den MDK erfolgen. Das bislang praktizierte Umschlagverfahren ist damit nicht mehr möglich.

MDK und Krankenkassen müssen schnellstmöglich ein neues und gesetzeskonformes Verwaltungsverfahren implementieren. Ich werde diesen Prozess begleiten und bis zur Ablösung des Umschlagverfahrens verstärkt kontrollieren, dass Krankenkassen medizinische Unterlagen, die für den MDK bestimmt sind, nicht zur Kenntnis nehmen.

7.8 Datenschutz in Pflegeeinrichtungen**7.8.1 Datenerhebung durch Hilfsmittelerbringer in Pflegeeinrichtungen**

Um die Versorgung von Bewohnern stationärer Pflegeeinrichtungen mit Hilfs- und Pflegehilfsmitteln zu gewährleisten, bedienen sich Krankenkassen und Pflegeeinrichtungen sog. Hilfsmittelerbringer. Diese haben im Umgang mit personenbezogenen Gesundheitsdaten von Pflegeheimbewohnern besondere Datenschutzvorschriften zu beachten.

Sind stationäre Pflegeheimbewohner auf individuelle Versorgung angewiesen, erhalten sie bestimmte, einzeln angepasste Hilfsmittel (Hörgeräte, Sehhilfen, Prothesen etc.). Die Hilfsmittel werden vom Arzt verordnet und von der Krankenkasse bezahlt.

Voraussetzung dafür ist, dass die Hilfsmittel medizinisch indiziert und im Einzelfall für die Versorgung erforderlich sind (§ 33 SGB V). In Zusammenarbeit mit den Kassen bieten auch private Hilfsmittelerbringer Leistungen der individuellen Versorgung an.

In einer stationären Pflegeeinrichtung in Baden-Württemberg hatte ein Hilfsmittelerbringer die individuelle Versorgung der Bewohner mittels eines sog. Ernährungs-Managements übernommen. Das Ernährungs-Management zielte darauf ab, eine bedarfsgerechte orale Ernährung von kranken und pflegeabhängigen Menschen sicherzustellen. Zu diesem Zweck führte der Hilfsmittelerbringer Ernährungsvisiten im Pflegeheim durch. Die Mitarbeiter des Hilfsmittelerbringers dokumentierten in einem Visitenblatt neben Patientendaten (Name, Pflegeheim, Krankenkasse, Geburtsdatum, Größe, Hausarzt etc.) auch Daten zum Ernährungszustand und zum Nahrungsbedarf der Bewohner (Gewicht, Body-Mass-Index, tägliche Nahrungsaufnahme, Flüssigkeitsbedarf, individuelle Risikofaktoren etc.). Im Anschluss entschieden die Mitarbeiter des Hilfsmittelerbringers nach eigenen Richtlinien, bei welchem Bewohner sie eine Zusatzernährung für angebracht hielten. Erst nach dieser Entscheidung übergaben die Mitarbeiter den betroffenen Pflegeheimbewohnern eine sog. Wahlrechtsbestätigung. Darin sollten diese schriftlich erklären, dass der Hilfsmittelerbringer sie auf der Grundlage einer Verordnung ihres behandelnden Arztes beliefern darf. Damit der Hilfsmittelerbringer die individuelle Zusatzernährung mit den Sozialkassen abrechnen konnte, musste die Leistung von einem Arzt verordnet werden. Zu diesem Zweck leitete das Unternehmen die selbst erstellten Visitenblätter an die vermeintlich behandelnden Hausärzte der Pflegeheimbewohner weiter. Ein Arzt wandte sich an unsere Dienststelle, nachdem er auf diesem Weg mehrere Visitenblätter von Pflegeheimbewohnern erhalten hatte, die er nur z. T. als Patienten betreute.

In diesem Fall handelte der Hilfsmittelerbringer weder bei der Erhebung noch bei der weiteren Verarbeitung der Gesundheitsdaten auf einer rechtlichen Grundlage. Eine wirksame Einwilligungserklärung der Pflegeheimbewohner in die Datenerhebung und -verarbeitung existierte nicht. Die Bewohner oder deren Vertreter wurden zu keinem Zeitpunkt hinreichend über eine Erhebung oder Verarbeitung ihrer

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Gesundheitsdaten durch einen Hilfsmittelerbringer informiert.

Der Hilfsmittelerbringer war auch nicht im Rahmen eines sog. Versorgungsmanagements nach § 11 Absatz 4 SGB V zur Datenübermittlung oder -erhebung befugt. Um die Versorgung ihrer Versicherten mit Hilfsmitteln sicherzustellen, schließen Krankenkassen Verträge mit privaten Hilfsmittelerbringern ab (vgl. §§ 126 ff. SGB V). Als Vertragspartner der Krankenkassen sind Hilfsmittelerbringer daher auch sog. sonstige oder übrige Leistungserbringer i.S. der Sozialgesetzbücher. Im Rahmen eines Versorgungsmanagements ist es Aufgabe der betroffenen Leistungserbringer, für eine sachgerechte Anschlussversorgung des Versicherten zu sorgen. Zu diesem Zweck sind die Leistungserbringer befugt, sich gegenseitig die erforderlichen Informationen zu übermitteln (vgl. § 11 Absatz 4 Satz 2 SGB V). Zur Erhebung von Daten ist ein Leistungserbringer nach dieser Vorschrift aber nicht befugt und zur Übermittlung von Daten nur dann, wenn der Versicherte vorher informiert wurde und er in die Datenübermittlung eingewilligt hat (vgl. § 11 Absatz 4 Satz 5 SGB V). Die Pflegeheimbewohner wurden aber weder informiert noch willigten sie in die Übermittlung von Daten im Rahmen eines Versorgungsmanagements ein.

Für die Einwilligung in die Erhebung und Verarbeitung von Gesundheitsdaten und die Information der Betroffenen gelten besondere gesetzliche Vorschriften, beispielsweise in § 4a Absatz 3 BDSG, § 67a Absatz 3 SGB X und § 11 Absatz 4 Satz 5 SGB V. Danach hätte sich eine wirksame Einwilligung der Bewohner u. a. ausdrücklich auf die erfassten Gesundheitsdaten, die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung der Daten und die Identität der verantwortlichen Stelle beziehen müssen. Die Wahlrechtsbestätigung, die der Hilfsmittelerbringer nach seiner Datenerhebung ausgegeben hatte, erfüllte keine dieser Voraussetzungen.

Der Hilfsmittelerbringer war auch nicht aufgrund einer vertraglichen Vereinbarung mit dem Pflegeheim oder aufgrund anderer Vorschriften der Sozialgesetzbücher zur Erhebung, Verarbeitung oder Nutzung von Gesundheitsdaten der Pflegeheimbewohner befugt.

Hilfsmittelerbringer sind als sonstige Leistungserbringer gem. § 294 SGB V dazu verpflichtet, die für

die Erfüllung der Aufgaben der Krankenkassen sowie der Kassenärztlichen Vereinigungen notwendigen Angaben, die aus der Erbringung, der Verordnung sowie der Abgabe von Versicherungsleistungen entstehen, aufzuzeichnen und gemäß den nachstehenden Vorschriften den Krankenkassen, den Kassenärztlichen Vereinigungen oder den mit der Datenverarbeitung beauftragten Stellen mitzuteilen. Aus dieser Verpflichtung entsteht für die Leistungserbringer jedoch keine datenschutzrechtliche Befugnis, umfangreich Gesundheitsdaten von Versicherten zu erheben bzw. solche aufzuzeichnen. Der Vorschrift unterfallen nur die für die Erfüllung der Aufgaben der Krankenkassen sowie der Kassenärztlichen Vereinigungen notwendigen Angaben. Der Umfang der Aufzeichnungspflicht des § 294 SGB V richtet sich daher nach den Befugnissen der Krankenkassen sowie der Kassenärztlichen Vereinigungen zum Erheben und Speichern von Sozialdaten (§§ 284, 285 Absatz 2 SGB V). Deren datenschutzrechtliche Befugnisse richten sich wiederum spiegelbildlich nach der gesetzlichen Mitteilungspflicht der sonstigen Leistungserbringer. Ausführliche personenbezogene Gesundheitsdaten dürfen gem. § 302 SGB V aber nicht an Krankenkassen oder Kassenärztliche Vereinigungen übermittelt werden. In der Folge erstreckt sich die Aufzeichnungspflicht des § 294 SGB V gerade nicht auf umfangreiche Gesundheitsdaten der Versicherten. Eine Übermittlungsbefugnis an andere Leistungserbringer (Vertragsärzte, Psychotherapeuten, Krankenhäuser etc.) ist von § 294 SGB V nicht umfasst.

Da auch das Bundesdatenschutzgesetz keine Rechtsgrundlage für die Erhebung der Gesundheitsdaten und deren Weiterleitung an einen Arzt bot, war das Vorgehen des Hilfsmittelerbringers rechtswidrig. Das Pflegeheim hat die Zusammenarbeit mit ihm mittlerweile beendet.

Aufgrund der Sensibilität der betroffenen Gesundheitsdaten und des besonders nachlässigen Umgangs des Hilfsmittelerbringers mit diesen Daten habe ich die Angelegenheit an die zentrale Bußgeldstelle beim Regierungspräsidium Karlsruhe weitergeleitet.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

7.8.2 Fotoaufnahmen von Pflegeheimbewohnern für Notfall- und Evakuierungspläne

Aufgrund einer Beschwerde wurde eine vermutlich gar nicht seltene Praxis in Pflegeheimen bekannt. Wir schildern den Fall auch, um etwaige Nachahmer zu sensibilisieren.

Meine Dienststelle wurde darüber informiert, dass eine Betreiberin von Pflegeheimen Heimbewohner gebeten hatte, sich fotografieren zu lassen, damit bei der Evakuierung der Gebäude in Notfällen Rettungskräfte an Hand stockwerksbezogener Listen mit entsprechenden Fotos die Bewohner sofort erkennen können. Ich wurde gefragt, ob das aus datenschutzrechtlicher Sicht in Ordnung ist.

Auf meine Nachfrage erklärte die Betreiberin, nach einem größeren Brandereignis vor einigen Jahren hätten Rettungsdienste und die Polizei den Wunsch geäußert, im Einsatzfall eine Bilddokumentation nebst Personenbeschreibung zu erhalten, um verwirrte Senioren, die sich nicht in ihrem üblichen Aufenthaltsbereich befinden, identifizieren und ansprechen zu können. Die Betreiberin halte diesen Wunsch für sinnvoll und wolle ihn umsetzen. Dazu sei auch ein Vordruck für die eventuelle schriftliche Einwilligung der Bewohner erstellt worden. Dieser offenbarte bei näherem Hinsehen allerdings gravierende Defizite. Die Firma hat sich offenkundig nicht darum gekümmert, in ihrem Vordruck präzise anzugeben, worin die Heimbewohner konkret einwilligen sollen. Stattdessen wurde das Problem sogar verschärft: Es ging nun nicht mehr nur um Fotos für den Evakuierungsfall, sondern um das „Einverständnis“, dass „Dokumente, Foto- und Videoaufnahmen“ der Bewohner „zeitlich, räumlich und inhaltlich unbegrenzt“ „für Zwecke der Veröffentlichung“ in von den Bewohnern ggf. „speziell freigegebenen Online-Medien, jeweils zum Zwecke der Außendarstellung“ der Betreiberin genutzt werden können. Im Text, unter den die Bewohner ihre Unterschrift setzen konnten, fand sich auch die Aussage „Diese Einwilligung gilt über den Tod hinaus.“. Abgesehen davon, dass nicht nachvollziehbar ist, warum eine Einwilligung in die Verwendung von Daten im Zusammenhang mit Evakuierungsplänen über den Tod eines Bewohners hinaus gelten soll, war dieser erweiterte Umfang der Einwilligung in keiner Weise hilfreich. Man konnte den Eindruck gewinnen, es handele sich um den Versuch, der

wohl durchaus leistbaren, aber evtl. als zu mühevoll empfundenen Arbeit zur Umsetzung datenschutzrechtlicher Anforderungen hinsichtlich der Fotodokumentation durch die „Flucht nach vorne“ zu entgehen. Eine solche Fluchtmöglichkeit eröffnet das Datenschutzrecht aber nicht. Dies habe ich der Betreiberin deutlich zu verstehen gegeben. Darauf teilte diese mit, sie halte Fotoaufnahmen zur Notfall-Evakuierung weiterhin für richtig, werde dieses Vorhaben aber vorerst zurückstellen.

Damit könnte ich dieses Thema formal als abgeschlossen betrachten. Gleichwohl möchte ich, auch zur Vermeidung des Eindrucks, der Datenschutz stehe sinnvollen Maßnahmen zur Evakuierung von Seniorenheimen im Weg, sowie mit Blick auf andere Heimbetreiber im Land, die sich evtl. mit solchen Gedanken tragen, auf Folgendes hinweisen:

Ich kann nicht von vornherein ausschließen, dass eine Fotodokumentation bei der Evakuierung von Gebäuden in Notfällen u.U. nützlich sein könnte. Wenn sich nach einer von Heimbetreibern, evtl. in Zusammenarbeit mit Organisationen des Rettungsdienstes, der Feuerwehr und der Polizei, sorgfältig durchgeführten Prüfung insbesondere die Geeignetheit und Verhältnismäßigkeit dieses Instruments und der damit verbundenen Datenverarbeitung gezeigt hat, können auch die datenschutzrechtlichen Anforderungen bewältigt werden, die eigentlich recht einfach sind: Ein Heimbetreiber, der die datenschutzrechtliche Einwilligung in die Verwendung von Fotos und evtl. auch weiteren Daten einholen will, muss insbesondere über die „Spielregeln“, also die Datenarten, den Zweck und die vorgesehene Datenverwendung klar und verständlich informieren. Nur dann sind die Heimbewohner in der Lage, ihr Grundrecht auf informationelle Selbstbestimmung auszuüben. Die Behauptung, dass Feuerwehr und Rettungskräfte auf verrauchten Fluren die Bewohner mit Hilfe einer Fotodokumentation schneller identifizieren könnten, halte ich dagegen für vorgeschoben; ich gehe davon aus, dass für die Rettungskräfte die schnellstmögliche Rettung von Menschenleben Vorrang hat – und zwar unabhängig davon, um wen es sich im Einzelfall handelt.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

7.9 Datenschutz bei Ärzten**7.9.1 Einsatz von Verrechnungsstellen durch Ärzte**

In meinem 31. Tätigkeitsbericht (LT-Drs. 15/4600, S. 108) habe ich allgemein dargestellt, was ein Arzt u. a. beachten muss, wenn er Daten über einen Patienten an eine Verrechnungsstelle weitergibt, damit diese seine Leistungen abrechnet und ggf. auch geltend macht. Wichtig ist dabei vor allem, dass die Patienten eine hinreichende Vorstellung davon haben, wer welche Daten wozu bekommen soll. Die Verrechnungsstellen stellen dazu den Ärzten Vordrucke zur Verfügung, welche die Ärzte wiederum ihren Patienten vorlegen. Im Berichtszeitraum habe ich mich mit einzelnen Formulierungen in solchen Vordrucken beschäftigt.

Konkret ging es um Formulierungen, die es der Verrechnungsstelle erlauben soll, die Zahlungsfähigkeit der Patienten zu überprüfen, um Forderungsausfälle abzusichern und Forderungen zur Refinanzierung an eine Bank weiter abzutreten.

Der Bundesgerichtshof hat dazu in seinem Urteil vom 10. Oktober 2013, III ZR 325/12, Folgendes entschieden:

„Eine wirksame Einwilligung im Sinne von § 203 Absatz 1 Nummer 1 des Strafgesetzbuchs setzt voraus, dass der Erklärende eine im Wesentlichen zutreffende Vorstellung davon hat, worin er einwilligt, und die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag. Er muss deshalb wissen, aus welchem Anlass und mit welcher Zielsetzung er welche Personen von ihrer Schweigepflicht entbindet; auch muss er über Art und Umfang der Einschaltung Dritter unterrichtet sein.“

In seinem Urteil vom 21. September 2011, 10 C 102/11, befasste sich das Amtsgericht Mannheim mit der Frage, ob sich bei der Abtretung der Forderung aus einer Arztrechnung an ein Abrechnungsunternehmen die Einwilligung des Patienten zu der Weitergabe seiner Daten auch darauf beziehen muss, dass bei einer weiteren Abtretung der Forderung die Patientenunterlagen an eine Bank übermittelt werden:

„Für den Patienten macht es in der Regel einen Unterschied aus, ob externe und durch den Arzt nicht kontrollierbare Dritte eingeschaltet werden. Es muss für ihn eindeutig und zweifelsfrei zu entnehmen sein, dass dem Zessionar (der Verrechnungsstelle) zu diesem Zweck sämtliche zur Erstellung der Abrechnung erforderlichen Behandlungsdaten vom behandelnden Arzt zu überlassen sind, also der Umfang der Datenübermittlung, zu der sich der behandelnde Arzt aufgrund des mit der Verrechnungsstelle geschlossenen Vertrages verpflichtete. Zu einer im Wesentlichen zutreffenden Vorstellung von der Tragweite der Einwilligung hätte hier schließlich gehört, dass dem Patienten die nach dem Abrechnungs- und Vorfinanzierungssystem vorgesehene Weitergabe von Patientendaten durch die Verrechnungsstelle an Finanzierungsinstitute erkennbar gewesen wäre.“

Bei einer Formulierung zum möglichen Einholen einer Information bei einer Auskunft, um die Bonität des Patienten zu prüfen, muss also hinreichend klar sein, welcher verantwortlichen Stelle (etwa dem Arzt oder der Verrechnungsstelle) der Patient unter welchen konkreten Voraussetzungen und hinsichtlich welcher dabei zu übermittelnder Datenarten eine Bonitätsanfrage erlaubt. Eine Erklärung zur Bonitätsanfrage, bei der das nicht hinreichend klar ist, könnte insoweit ins Leere gehen.

Wenn es darum geht, dass die Verrechnungsstelle die an sie abgetretene Forderung zur (für sie dann günstigeren) Refinanzierung an eine namentlich genannte Bank weiter abtritt, kommt es auch darauf an, ob an diese Bank gegebenenfalls Patientendaten weitergegeben werden und ob das für den Patienten erkennbar ist.

Die Verrechnungsstellen sollten ihre Vordrucke, soweit diese unklar sind, ändern – sowohl im eigenen Interesse als auch im Interesse ihrer Vertragspartner, u. a. der Ärzte.

7.9.2 Laborauftrag durch behandelnden Arzt

In meinem 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 100) habe ich mich insbesondere zur ärztlichen Schweigepflicht geäußert sowie eine stillschweigende Bevollmächtigung angesprochen, von der nur ausgegangen werden könne, wenn u. a. der behan-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

delnde Arzt den Patienten über die beabsichtigte Laboruntersuchung unterrichtet habe. Neben der stillschweigenden Bevollmächtigung geht es auch darum, ob bei einer stillschweigenden Bevollmächtigung eine datenschutzrechtliche Einwilligung notwendig ist.

Nach einem Urteil des Bundesgerichtshofs vom 14. Januar 2010 – III ZR 188/09 – handelt der behandelnde Arzt im Regelfall als Stellvertreter des Patienten, wenn er einen externen Laborarzt beauftragt:

„Nach allgemeiner Auffassung wird bei der Inanspruchnahme eines externen Laborarztes durch den behandelnden Arzt letzterer im Regelfall als Stellvertreter des Patienten tätig. Übersendet er Untersuchungsmaterial des Patienten an den Laborarzt, erteilt er den damit verbundenen Auftrag grundsätzlich im Namen des Patienten. Hat dieser ihn dazu bevollmächtigt, wird neben dem Behandlungsverhältnis zwischen dem Patienten und dem Arzt ein weiteres eigenständiges Vertragsverhältnis zwischen dem Patienten und dem Laborarzt begründet. Nur dies entspricht normalerweise dem Willen und Interesse der Beteiligten sowie den Bedürfnissen der Praxis.“

Diese Bevollmächtigung des behandelnden Arztes durch den Patienten kann auch stillschweigend erfolgen, so der Bundesgerichtshof mit Urteil vom 29. Juni 1999 – VI ZR 24/98 –:

„Aus den Umständen muss daher entnommen werden, dass der behandelnde Arzt bei Übersendung des Untersuchungsmaterials als Vertreter des Patienten handelt und für diesen mit dem Arzt für Pathologie einen Vertrag abschließen will, wozu ihn der Patient mit seinem Einverständnis, sich Gewebeprobe zum Zwecke der Untersuchung durch einen Spezialisten entnehmen zu lassen, stillschweigend bevollmächtigt und ihm die Auswahl des Spezialisten überlassen hat. Gerade bei der histologischen Untersuchung hat der Patient im Allgemeinen kein besonderes Interesse daran, den die Untersuchung durchführenden Arzt selbst auszuwählen.“

Das bedeutet datenschutzrechtlich: Hat der Patient den behandelnden Arzt (stillschweigend) bevollmächtigt, für ihn (den Patienten) mit einem Laborarzt einen Vertrag zu schließen, und gibt der behandelnde Arzt gegenüber dem Laborarzt eine entsprechende Erklärung ab, dann wirkt diese Erklärung unmittelbar für und gegen den Patienten. Rechtlich teilt der Patient selbst – vertreten durch den behandelnden Arzt – die personenbezogenen Daten über sich dem Laborarzt mit; weil der behandelnde Arzt dann (als selbst verantwortliche Stelle) keine personenbezogenen Daten über den Patienten übermittelt, ist insoweit kein Raum für eine datenschutzrechtliche Einwilligung des Patienten.

Beauftragt der behandelnde Arzt als Stellvertreter des Patienten einen externen Laborarzt, dann benötigt der behandelnde Arzt für die damit verbundene Weitergabe personenbezogener Daten über den Patienten keine datenschutzrechtliche Einwilligung.

7.10 Informationspflicht bei Datenschutzverstößen

Datenpannen können vorkommen. Sie zu verschweigen, kann teuer werden.

Nichtöffentliche Stellen und ihnen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen müssen gem. § 42 a BDSG gravierende Datenschutzverstöße der zuständigen Aufsichtsbehörde anzeigen sowie die Betroffenen informieren und ihnen Handlungsempfehlungen unterbreiten. § 83 a des Zehnten Buchs des Sozialgesetzbuchs (SGB X) verpflichtet die dem Sozialgeheimnis unterliegenden Stellen, im Falle der unrechtmäßigen Kenntniserlangung von Sozialdaten unverzüglich die Aufsichtsbehörde nach § 90 SGB IV, die zuständige Datenschutzaufsichtsbehörde und die Betroffenen zu informieren. In meinem 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 22 f.) habe ich diese Meldepflichten bereits vorgestellt. Auf meiner Internetseite sind Informationen dazu abrufbar:

<http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/12/Merkblatt-LfD-BW-§-42a-Stand-12.12.14.pdf>.

Auch im Gesundheitsbereich lassen sich Datenpannen nicht völlig ausschließen. Die Zahl der gemeldeten Fälle nimmt zwar stetig zu, allerdings gehe ich davon aus, dass die Dunkelziffer hoch ist. Dies liegt

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

möglicherweise daran, dass den verantwortlichen Stellen bzw. deren Mitarbeitern die ihnen obliegende Meldepflicht gar nicht bekannt und/oder die Versuchung groß ist, eine Meldung zu unterlassen, um Versäumnisse nicht preiszugeben und Imageverluste durch die Bekanntgabe der Datenpanne zu vermeiden.

Verantwortliche Stellen müssen daher interne Regelungen treffen, die sicherstellen, dass Mitarbeiter datenschutzrelevante Vorgänge an zu benennende interne Stellen oder Personen melden. Die intern verantwortlichen Personen haben unter Beteiligung des betrieblichen Datenschutzbeauftragten zu prüfen, ob eine Meldepflicht besteht und ggf. die entstehenden Handlungspflichten festzulegen und umzusetzen.

Die ordnungsgemäße Mitteilung nach § 42 a BDSG ist bußgeldbewehrt (§ 43 Absatz 2 Nr. 7 BDSG), ebenso der Verstoß gegen die Informationspflicht nach § 83 a SGB X (§ 85 Absatz 2 Nr. 6 SGB X). Bei Missachtung der Informationspflichten drohen Bußgelder bis zu 300.000 Euro, wenn dies vorsätzlich oder fahrlässig geschieht.

Ich halte es im Interesse aller Beteiligten für sinnvoll, wenn Datenpannen so früh wie möglich offenbart werden, damit gemeinsam nach Lösungen gesucht werden kann, um solche Pannen künftig zu vermeiden.

7.10.1 Datenlecks in Krankenhäusern

Die im Berichtszeitraum von Krankenhäusern angezeigten Fälle betrafen überwiegend den Verlust von Speichermedien und mobilen Datenträgern, aber auch Pannen im Zusammenhang mit der medizinischen Behandlung. Glücklicherweise waren jeweils nur wenige Patienten betroffen, die vom jeweiligen Krankenhaus auch informiert wurden. Beispielhaft erwähne ich nachfolgend Datenschutzverstöße, die sich so oder ähnlich leider immer wieder zutragen.

- Ein Arzt einer Klinik hatte Unterlagen einer Patientin – Patientenfragebogen, Notizen des Aufnahmegesprächs, neuropsychologisches Gutachten für ein laufendes Gerichtsverfahren, Untersuchungs- und Entlassberichte früherer Klinikaufenthalte, Zuweisungsschein der Rentenversicherung, verschiedene medizinische

Unterlagen – zur Dokumentation eines Aufnahmegesprächs über das Wochenende mit nach Hause genommen. Unterwegs legte er mehrere Zwischenhalte ein. Am darauffolgenden Montag konnte der Arzt die Tasche, in der sich die Patientenunterlagen befanden, nicht mehr auffinden. Trotz intensiver Nachforschungen konnte nicht nachvollzogen werden, wann und auf welche Art und Weise Tasche und Patientenunterlagen abhandengekommen waren. Das Krankenhaus hatte den Mitarbeitern untersagt, Patientenakten mit nach Hause zu nehmen. Möglicherweise war dem Arzt diese Regelung nicht bekannt oder aber er hatte sie ignoriert. Der Vorfall wurde jedenfalls zum Anlass genommen, die Mitarbeiter nochmals schriftlich und im Rahmen einer Datenschutzschulung darüber in Kenntnis zu setzen, dass die Mitnahme von Patientenakten nicht gestattet ist. Ungeachtet dessen haben Krankenhäuser bzw. deren Mitarbeiter Patientenakten und sonstige schriftliche Aufzeichnungen von Patientendaten unter Wahrung des Grundsatzes der Datensicherheit und der ärztlichen Schweigepflicht und damit geschützt vor dem Zugriff Unbefugter aufzubewahren. Dazu bedarf es klarer schriftlicher Hinweise bzw. Dienst-/Arbeitsanweisungen zum Umgang mit personenbezogenen Daten.

- Ein weiterer meldepflichtiger Vorfall ereignete sich während der Zugreise eines Arztes eines Krankenhauses. Dieser hatte ein Notebook, auf dem sich Videosequenzen von Patienteninterviews befanden, mit auf die Reise genommen. Das Notebook wurde während der Fahrt entwendet. Die Festplatte des Notebooks war nicht verschlüsselt, aber immerhin mit einem Kennwort gesichert. Eine vom Hersteller angebotene Sperrung bzw. Fernlöschung war wegen fehlender Konnektivität leider nicht möglich. Das Krankenhaus ergriff nach Meldung des Vorfalls umgehend technische und organisatorische Maßnahmen zur Vermeidung einer Wiederholung. Es wurde mir mitgeteilt, dass ein gruppenweites Datenschutz-Projekt durchgeführt werde, das auch die Erstellung von Richtlinien, u. a. zur Nutzung von mobilen Geräten, beinhalte. Geplant sei, dass für die geschäftliche Nutzung keine privaten Endgeräte oder Datenträger (z. B. externe Festplatten oder USB-Sticks) ein-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

gesetzt werden dürften. Ferner befinde sich unternehmensweit ein Projekt in der Umsetzung, in deren Verlauf die Festplatten aller Laptops verschlüsselt würden. Geplant werde außerdem die Einführung von Passwort-Policies und Bildschirmschoner mit Passwortsperrung sowie von Blickschutz-Filtern für alle Desktoparbeitsplätze mit Patientenkontakt und für alle Notebooks.

Ich empfehle bei mobilen Geräten grundsätzlich, die systemeigene Laufwerks-/Geräteverschlüsselung (Device Encryption) zu aktivieren bzw. die Dateien selbst nur verschlüsselt abzulegen. Sollte ein Computer oder Speichermedium verloren gehen oder gestohlen werden, verhindert diese Verschlüsselung, dass Unbefugte auf die Daten zugreifen können, indem sie das Laufwerk oder Medium beispielsweise ausbauen und einfach an einen anderen Rechner anschließen.

- Ein Klinikum fertigt im Rahmen gefäßchirurgischer Operationen regelmäßig Röntgenfilme an, die zwar keine Personen abbilden, jedoch mit Namen und Geburtsdatum der Patienten gekennzeichnet sind. Nachdem der Speicherplatz des Röntgengerätes ausgeschöpft war, wurde der interne Datenspeicher geleert und die Daten wurden auf einem USB-Stick (zwischen)gespeichert, um weitere Untersuchungen vornehmen zu können. Der USB-Stick wurde von einem Klinik-Mitarbeiter auf einem Schreibtisch im Büro des Zentralen Operationsbereichs abgelegt und dort vergessen. Der Stick konnte trotz umfangreicher Recherchen nicht gefunden werden. Der USB-Stick war nicht verschlüsselt.

Das Klinikum hat in der Folge die regelmäßige Sicherung der Bilddateien über eine Netzanbindung der Modalität an die Archivsysteme realisiert, was den Gebrauch von USB-Medien obsolet macht. Außerdem wurden die Regelungen zur Handhabung mobiler Datenträger angepasst.

Grundsätzlich haben Krankenhäuser Regelungen für alle mobilen Datenträger vor deren Einsatz zu treffen. Diese müssen neben dem Da-

tentransport auch die Datenlöschung sowie die Aufbewahrung und Vernichtung des Datenträgers umfassen. Verschlüsselung ist auch hier das geeignete Mittel, um im Verlustfall den Schaden zu minimieren.

- Einmal mehr wurde ich durch eine Patientin über einen „klassischen“ Datenschutzverstoß in Kenntnis gesetzt. Die Patientin wurde in einem Krankenhaus in der Notfallaufnahme behandelt. Während sie dort längere Zeit in einem Behandlungsraum warteten musste, konnte sie auf dem Bildschirm des dort vorhandenen Computers die vollständigen Namen und den jeweiligen Grund der Behandlung anderer Patienten lesen (beispielsweise „auf die Badewannenkante gestürzt“ oder „Pille danach“). Eine einfache Maßnahme wie beispielsweise ein aktivierter Bildschirmschoner oder alternativ Sichtschutzblenden oder Blickschutzfilter, hätte hier schon ausgereicht, um die Patientendaten vor dem Einblick durch Unbefugte zu schützen. Ein Blickschutzfilter besteht aus parallel ausgerichteten Lamellen (vergleichbar mit einer offenen Jalousie, nur senkrecht dazu). Eine Person, die nicht exakt vor dem Blickschutzfilter steht, kann daher nicht sehen, was auf dem Bildschirm dargestellt wird. Die Abmessungen der heutigen Lamellen bewegen sich im Submillimeterbereich und sind somit auch als Displayfolien erhältlich.

7.10.2 Diebstahl eines Praxiscomputers

Im Sommer 2015 teilte ein Psychotherapeut mit, dass ihm im Verlauf einer Urlaubsreise neben anderen Dingen sein Praxiscomputer (Laptop) mit darauf befindlichen Patientendaten aus einem verschlossenen ausländischen Hotelzimmer gestohlen worden sei. Der Therapeut hatte sich zunächst an die Polizei am Urlaubsort gewandt, die ihm erklärte, es bestünden geringe Chancen, das Gerät wieder zu erlangen. Auf die Frage des Therapeuten nach seinen weitergehenden Pflichten habe ich ihn auf seine Informationspflichten nach § 42a BDSG gegenüber meiner Dienststelle hingewiesen.

Die weiteren Informationen, die wir darauf umgehend erhielten, ließen erkennen, dass es um unverschlüsselt gespeicherte Daten (Adressen, Ver-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

sichertheitsnummern, Krankenkassen sowie Daten zur jeweiligen gesundheitlichen Vorgeschichte in Anträgen) von ca. 100 Patienten ging. Immerhin war das Programm auf dem Laptop durch ein Passwort geschützt. Die Tür des Hotelzimmers hatte zwar eine elektronische Verriegelung, allerdings ohne Blende über dem Türspalt, so dass der Riegel von außen sichtbar war und dadurch ein unbefugtes Öffnen erleichtert wurde. Der Therapeut hatte die betroffenen Patienten bereits schriftlich über den Vorfall informiert.

In unserem abschließenden Schreiben habe ich dem Therapeuten empfohlen, seinen Patienten eine erhöhte Wachsamkeit hinsichtlich eventueller Unregelmäßigkeiten bei Abrechnungen und Schriftverkehr mit ihren Krankenkassen ans Herz zu legen, da mit den Versichertendaten, insbesondere der lebenslang gültigen Versichertennummer, beispielsweise über Online-Formulare, Namens- und Adressänderungen beantragt werden könnten. Zudem habe ich ihm geraten, bei einem evtl. beschafften Ersatzgerät und ggf. bei anderen derart genutzten elektronischen Geräten, soweit noch nicht geschehen, die systemeigene Laufwerks-/Geräteverschlüsselung (Device Encryption) zu aktivieren. Denn diese Verschlüsselung verhindert im Fall des Diebstahls oder sonstigen Verlusts, dass Unbefugte auf die Daten zugreifen können, indem sie das gesperrte Laufwerk einfach an einen anderen PC anschließen.

Eine naheliegende Konsequenz hat der umsichtige Therapeut selbst gezogen, ohne dass es eines Hinweises meinerseits bedurfte: Er will künftig keine Arbeitsmaterialien mehr in den Urlaub mitnehmen.

7.10.3 Medizinischer Dienst der Krankenversicherung (MDK)

Im Berichtszeitraum wurden meiner Dienststelle mehrere Datenpannen gem. § 83a des Zehnten Buches des Sozialgesetzbuches (SGB X) mitgeteilt.

- So versandte der MDK ein medizinisches Gutachten irrtümlich an eine unbeteiligte Klinik. Zur Prüfung, ob die Leistungsvoraussetzungen einer vollstationären Krankenhausbehandlung vorliegen, fertigten Mitarbeiter des MDK ein sozialmedizinisches Gutachten eines Patienten an. Nachdem das Gutachten fertiggestellt war,

übermittelte der Gutachter die Dokumente per Post an die zuständige Krankenkasse und irrtümlich auch an eine völlig unbeteiligte Klinik. Der Betroffene erhielt daraufhin von der angeschriebenen Klinik unaufgefordert Anmelde- und Informationsunterlagen zugesandt.

Das Gutachten enthielt neben den allgemeinen Daten zur Person des Betroffenen auch sensible Gesundheitsdaten, z.T. mit ärztlichen Diagnosen, der medizinischen Vorgeschichte des Betroffenen und dem Ergebnis des Gutachtens. Der MDK gab dazu an, dass das Gutachten aufgrund der Eilbedürftigkeit der Versendung fehlerhaft adressiert worden sei.

Der Betroffene wurde vom MDK benachrichtigt und die Klinik zur Löschung des Gutachtens und ggf. weiterer gespeicherter personenbezogener Daten aufgefordert. Den MDK habe ich veranlasst zu prüfen, mit Hilfe welcher zusätzlicher Maßnahmen künftig ein Fehlversand vermieden werden kann, beispielsweise durch eine Plausibilitätsprüfung hinsichtlich der eingegebenen Adresse – vor dem eigentlichen Versand eines Gutachtens.

- Auf dem Postweg sind auch in zwei weiteren Fällen eine Vielzahl persönlicher Gesundheitsdaten verloren gegangen. So erreichten einige medizinische Unterlagen, die zum Zweck der Erstellung eines Pflegegutachtens zusammengestellt wurden, und drei vollständige Pflegegutachten nicht den richtigen Empfänger. Bei den verlorengegangenen Dokumenten handelte es sich u. a. um ein älteres Pflegegutachten, einen Hilfebedarfsbogen, einen Krankenhausbericht und zwei aktuelle Klinikberichte. Die ausgefüllten Formulargutachten dienten der Feststellung der Pflegebedürftigkeit.

Auch in diesen Fällen gingen sensible Gesundheitsdaten der Betroffenen auf dem Postweg verloren, beispielsweise ärztliche Diagnosen mit pflegerelevanter Vorgeschichte und Befunden, Angaben zur Heil- und Hilfsmittelnutzung, Angaben zur aktuellen medikamentösen Versorgung und weiteren detaillierte Feststellungen zur Alltagskompetenz und Pflegebedürftigkeit

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

der Betroffenen (Körperpflege, Ernährung, Mobilität etc.).

Die Betroffenen wurden vom MDK auch hier über den Datenverlust informiert. Ein Fehler- sand von Dokumenten auf dem Postweg kann sicherlich nicht vollständig ausgeschlossen werden. Die verantwortliche Stelle hat jedoch geeignete Maßnahmen vorzusehen, die sicherstellen, dass dies soweit wie möglich vermieden wird. Ich habe daher den MDK aufgefordert, entsprechende Gegenmaßnahmen zu ergreifen und Maßnahmen zur Vermeidung von weiteren Datenverlusten vorzunehmen. Der MDK hat die Prüfung ergänzender Maßnahmen zur Absicherung des Postversands eingeleitet.

7.11 Datenschutz im Jobcenter

7.11.1 Bei Jobcentern vor Ort

Meine Dienststelle hat im Berichtszeitraum vier Jobcenter vor Ort kontrolliert. Erfreulicherweise konnten wir insbesondere bei Themen, die in der Vergangenheit zu zahlreichen Eingaben geführt haben, deutliche Verbesserungen erreichen bzw. feststellen.

Zur Unzulässigkeit der *Aufbewahrung (ungeschwärtzter) Kopien des Personalausweises* von Leistungsbeziehern hatte ich in meinem 31. Tätigkeitsbericht (LT-Drs. 15/4600, S. 111) Stellung genommen: Danach dürfte regelmäßig ein Vermerk darüber genügen, dass sich der Antragsteller durch Personalausweis oder sonstige Ausweispapiere ausgewiesen hat. Ggf. kann außerdem vermerkt werden, dass die im Antrag angegebenen Angaben mit denen auf dem Personalausweis übereinstimmen. Alle vier von meiner Dienststelle besuchten Jobcenter nehmen keine Kopien von Personalausweisen (mehr) zur Akte.

Zur Vorlage einer vom Vermieter auszufüllenden und zu unterzeichnenden *Mietbescheinigung* hatte ich mich bereits im 29. Tätigkeitsbericht (LT-Drs. 14/5500, S. 101) geäußert: Eine solche darf nur unter engen Voraussetzungen verlangt werden.

Keines der besuchten Jobcenter besteht inzwischen noch auf der Vorlage einer Mietbescheinigung: An-

tragsteller, die keine Mietbescheinigung vorlegen wollen, brauchen dies auch nicht zu tun. Ich habe diejenigen Jobcenter, die überhaupt noch Mietbescheinigungen anfordern, aufgefordert, die Antragsteller auch darauf *hinzuweisen*, dass sie die zur Antragsbearbeitung erforderlichen Angaben statt mit einer Mietbescheinigung auch in anderer Weise (z. B. mit Mietvertrag, Kontoauszug, Nebenkostenabrechnung) belegen können.

Bereits wiederholt hatte ich mich mit der Thematik der Anforderung von *Kontoauszügen* befasst (29. und 31. Tätigkeitsbericht). Hier ist insbesondere zu beachten, dass Antragsteller auf der *Ausgabenseite* der Kontoauszüge, soweit *besondere Arten personenbezogener Daten* (Angaben über die rassistische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) betroffen sind, den Verwendungszweck bzw. den Empfänger der Überweisung regelmäßig schwärzen können. Auf diese Möglichkeit der Schwärzung der Adressaten auf der Ausgabenseite hat das Jobcenter bei der Anforderung der Kontoauszüge *hinzuweisen*.

Alle besuchten Jobcenter haben mitgeteilt, dass sie inzwischen solche Hinweise erteilen.

7.11.2 Formulare

Im Berichtszeitraum hat meine Dienststelle Antragsformulare für das Arbeitslosengeld II geprüft und teilweise erheblichen Verbesserungsbedarf festgestellt.

Auf einem Formular wurden die Antragsteller aufgefordert, den Antrag auf Arbeitslosengeld II *über ihr Bürgermeisteramt* beim Jobcenter (eines Landkreises) einzureichen. Am Ende des Formulars wurde die *Wohnsitzgemeinde* aufgefordert mitzuteilen, ob die vorstehenden Angaben der Wahrheit entsprechen, ob die Notlage anerkannt wird und seit wann die Notlage der Gemeinde bekannt ist.

Es ist nicht ersichtlich, weshalb die Antragsteller den Antrag auf Arbeitslosengeld II über ihr Bürgermeisteramt einreichen sollen. § 16 des Ersten Buchs des Sozialgesetzbuchs (SGB I) begründet lediglich die *Möglichkeit*, Anträge auf Sozialleistungen auch vor Ort bei der Gemeinde (und nicht beim zuständigen Jobcenter) zu stellen.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Zweck dieser Regelung ist es, den Bürgern die Antragstellung zu erleichtern und ihnen größeren Aufwand und längere Anreisewege zu ersparen. Ob ein Antragsteller von dieser Möglichkeit Gebrauch macht, ist seiner eigenen Entscheidung überlassen.

Auch haben Wohnsitzgemeinden keine eigene Prüfzuständigkeit hinsichtlich der Antragsvoraussetzungen beim Arbeitslosengeld II. Daher dürfte es nicht zulässig sein, die Gemeinde aufzufordern, dem Jobcenter mitzuteilen, ob die Angaben des Antragstellers der Wahrheit entsprechen, die Notlage anerkannt wird und seit wann diese bekannt ist. Hierauf wurde bereits im 19. Tätigkeitsbericht (LT-Drs. 12/3480, S. 19) und 23. Tätigkeitsbericht (LT-Drs. 13/1500, S. 49 ff.) meiner Dienststelle im Zusammenhang mit der Beantragung von Sozialhilfe hingewiesen.

Des Weiteren wurde bei der Prüfung der Formulare festgestellt, dass der *Personenkreis*, zu dem Einkommen und Vermögen und weitere, teils sensible Angaben (z. B. den Umstand, ob eine Behinderung vorliegt) verlangt wurden, viel zu weit gefasst war: Die Formulare sahen Angaben von „allen im Haushalt lebenden Personen“ bzw. „aller Familien- und Haushaltsangehörigen“ vor. Das Gesetz spricht jedoch von *Bedarfsgemeinschaft*. Diese ist wesentlich enger gefasst und in § 7 Absatz 3 des Zweiten Buchs des Sozialgesetzbuchs, SGB II) wie folgt definiert:

Zur Bedarfsgemeinschaft gehören

1. die *erwerbsfähigen Leistungsberechtigten*,
2. die *im Haushalt lebenden Eltern oder der im Haushalt lebende Elternteil eines unverheirateten erwerbsfähigen Kindes, welches das 25. Lebensjahr noch nicht vollendet hat, und die im Haushalt lebende Partnerin oder der im Haushalt lebende Partner dieses Elternteils*,
3. *als Partnerin oder Partner der erwerbsfähigen Leistungsberechtigten*
 - a) die *nicht dauernd getrennt lebende Ehegattin oder der nicht dauernd getrennt lebende Ehegatte*,
 - b) die *nicht dauernd getrennt lebende Lebenspartnerin oder der nicht dauernd getrennt lebende Lebenspartner*,
 - c) eine *Person, die mit der erwerbsfähigen leistungsberechtigten Person in einem gemeinsamen Haushalt so zusammenlebt, dass nach verständiger*

Würdigung der wechselseitige Wille anzunehmen ist, Verantwortung füreinander zu tragen und füreinander einzustehen.

4. die dem Haushalt angehörenden unverheirateten Kinder der in den Nummern 1 bis 3 genannten Personen, wenn sie das 25. Lebensjahr noch nicht vollendet haben, soweit sie die Leistungen zur Sicherung ihres Lebensunterhalts nicht aus eigenem Einkommen oder Vermögen beschaffen können.

Ich habe die betroffenen Jobcenter aufgefordert, ihre Formulare zu ändern. Während eines der Jobcenter die Formulare zügig überarbeitet hat, verzichtete ein anderes Jobcenter trotz entsprechender Ankündigung bislang darauf. Ich gehe davon aus, dass dies nun zeitnah nachgebessert wird.

7.11.3 Auskunft an das Hauptzollamt?

Nicht nur zahlreiche Bürger wenden sich mit Fragestellungen zum Datenschutz in Jobcentern an meine Dienststelle; zuweilen erbitten auch die Jobcenter selbst Beratung in datenschutzrechtlichen Fragen.

In einem von einem Jobcenter an meine Dienststelle herangetragenen Fall hatte sich ein Hauptzollamt an dieses Jobcenter gewandt und Auskunft u. a. dazu verlangt, wie viel Geld ein namentlich benannter Hilfebedürftiger von dem Jobcenter erhalte. Die Anfrage hatte anscheinend folgenden Hintergrund: Der Zoll realisiert als „Inkassoorganisation des Bundes“ neben eigenen auch fremde öffentlich-rechtliche Forderungen von Sozialleistungsträgern wie den Agenturen für Arbeit, Krankenkassen und Berufsgenossenschaften. Soweit der Zoll dabei Forderungen von Sozialleistungsträgern (nach § 66 SGB X) vollstreckt, „gilt“ er (nach § 35 Absatz 1 Satz 4 SGB) selbst als Sozialleistungsträger. Dies hat zur Folge, dass andere Sozialleistungsträger (wie das Jobcenter) ihm bei Vorliegen bestimmter Voraussetzungen zur Erfüllung seiner Aufgaben erforderliche Angaben gem. § 69 SGB X mitteilen dürfen.

Hierbei muss das Hauptzollamt allerdings ausreichende Darlegungen machen, damit das Jobcenter prüfen kann, ob es eine solche Übermittlungsbezugnis hat: Denn die Verantwortung für die Zulässigkeit der Übermittlung trägt im Bereich des Sozialgesetzbuchs die *übermittelnde* Stelle – auch wenn die

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

Übermittlung auf Ersuchen, d. h. auf Anforderung einer anderen öffentlichen Stelle erfolgt.

Die Darlegungen des Hauptzollamts waren vorliegend zur Feststellung einer Übermittlungsbefugnis nicht ausreichend, so dass das Jobcenter meines Erachtens zu Recht keine Daten weitergegeben hat.

7.12 Wohn-, Teilhabe- und Pflegegesetz

7.12.1 Das neue Gesetz

Im Berichtszeitraum ist in Baden-Württemberg das (Landes-)Gesetz für unterstützende Wohnformen, Teilhabe und Pflege (WTPG) in Kraft getreten. Das Gesetz löst das bisherige Landesheimgesetz ab. Schwerpunkte des neuen Gesetzes sind die Aufnahme von ambulant betreuten Wohngemeinschaften (als neue Wohnform) in den heimrechtlichen Schutz und die Verbesserung der den Bewohnern zu gewährenden Informationsrechte.

Der Verbesserung der Information der (Heim-) Bewohner dient insbesondere das in § 8 des Gesetzes geregelte *Transparenzgebot*. Nach dieser Vorschrift ist der Träger einer stationären Einrichtung verpflichtet, den jeweils aktuellen Prüfbericht der Heimaufsichtsbehörde an gut sichtbarer Stelle in seinen Büro- oder Geschäftsräumen auszuhängen oder auszulegen. Hierdurch sollen die Bewohner eines Pflegeheims und auch künftige Bewohner einen Einblick in die personelle und räumliche Ausstattung des Heims, die hygienischen Verhältnisse, die Pflegefachlichkeit, die medizinische und medikamentöse Versorgung, freiheitsbeschränkende Maßnahmen und Mitwirkungsmöglichkeiten erhalten; immerhin betreffe dies – der Gesetzesbegründung zufolge – ihre eigene Lebenssituation und Lebensumstände unmittelbar.

Dieser Anspruch auf Informationen hat auch einen datenschutzrechtlichen Aspekt. Bestandteil der Prüfung der Heimaufsicht kann nämlich auch eine Wohnervisite sein. Deswegen kann der Prüfbericht auch konkrete Informationen über Heimbewohner enthalten, die sehr sensibel sind, da sie die pflegerische Situation einzelner Personen beschreiben und Angaben über deren Gesundheit enthalten können. Somit besteht ein grundlegendes Dilemma zwischen dem Informationsinteresse der (potenziel-

len) Bewohner und dem Recht auf informationelle Selbstbestimmung derjenigen Bewohner, die in dem Bericht erwähnt werden.

Der Gesetzgeber hat diesen Konflikt erkannt und im WTPG vorausschauend und in klarer Weise festgeschrieben, dass die Heimaufsichtsbehörde sicherzustellen hat, dass der zum Aushang bestimmte Prüfbericht mit Ausnahme des Namens und der Anschrift des Trägers und der Leitung der stationären Einrichtung *keine* personenbezogenen Daten enthält. Dies bedeutet, dass die Heimaufsichtsbehörde die insoweit zugänglichen Prüfberichte anonymisieren muss. Damit hat der Gesetzgeber eine einheitliche datenschutzkonforme Vorgehensweise beim Umgang mit den Prüfberichten sichergestellt und Konflikte von vornherein vermieden.

Wie im Folgenden zu lesen ist, hatte meine Dienststelle mit der Vorschrift nicht nur im Gesetzgebungsverfahren – bei dem meine Dienststelle stets zu beteiligen ist, wenn die Verarbeitung personenbezogener Daten betroffen ist – zu tun, sondern auch noch nach Inkrafttreten des Gesetzes: Denn es hat sich gezeigt, dass die Umsetzung der Regelung in der Praxis Probleme mit sich gebracht hat.

7.12.2 Prüfberichte der Heimaufsicht

Meiner Dienststelle wurden von dritter Seite Prüfberichte von Heimaufsichtsbehörden vorgelegt. Vorwurf war, dass diese personenbezogene Daten von Bewohnern der stationären Einrichtung enthalten. Wie im vorangehenden Kapitel ausgeführt, wäre dies ein Verstoß gegen das Wohn-, Teilhabe- und Pflegegesetz (WTPG).

Eine Durchsicht der Prüfberichte bestätigte die vorgetragene Kritik. Einem der Prüfberichte konnte ich Folgendes über einen Bewohner entnehmen: Der Bewohner ist männlich und hat Pflegestufe 3. Ich erfuhr sein Geburtsjahr, bei welcher Krankenkasse er versichert ist, seit welchem Tag er Bewohner in der Einrichtung ist, seine Größe und sein Gewicht. Weiter entnahm ich den Ausführungen der Heimaufsichtsbehörde, dass er in einem Einzelzimmer wohnt und in welcher Etage des Heims sich dieses Zimmer befindet. Beim weiteren Lesen erhielt ich über den Bewohner teils sensibelste Informationen zu den Themen „Essen und Trinken“, „Ausscheiden“, „Sexualität“, „Kommunikation“, „Sich bewegen“ und „Wunden/Wundversorgung“. In diesem Zu-

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

sammenhang ist zu erwähnen, dass es in der fraglichen Einrichtung zum Zeitpunkt der Prüfung weniger als 20 Bewohner mit Pflegestufe 3 gab.

Bei einer solchen Vielzahl von Angaben und weniger als 20 in Betracht kommenden Personen (von denen wahrscheinlich noch ein Teil weiblich ist) habe ich es mit personenbezogenen Daten zu tun, auch wenn Name und Vorname und das Geburtsdatum des Bewohners in dem Bericht geschwärzt waren. Denn auch Daten, die auf eine konkrete Person schließen lassen (ohne sie namentlich zu benennen), zählen zu den personenbezogenen Daten im Sinne des Datenschutzrechts.

Hier sollte man sich auch einmal die Situation vor Augen führen, dass der beschriebene Prüfbericht an gut sichtbarer Stelle in den Büro- oder Geschäftsräumen der stationären Einrichtung ausgehängt oder ausgelegt wird und sowohl andere Bewohner als auch deren Angehörige die recht schonungslosen Ausführungen lesen und ggf. dem Mitbewohner zuordnen können.

Ich habe mich in der Angelegenheit an das Ministerium für Arbeit und Soziales, Familie, Frauen und Senioren Baden-Württemberg als oberste Heimaufsichtsbehörde gewandt. Das Sozialministerium hat sich meiner Auffassung angeschlossen, dass die Prüfberichte personenbezogene Daten enthalten. Außerdem hat das Sozialministerium mein Einschreiten zum Anlass genommen, die Heimaufsichtsbehörden nochmals verstärkt auf die Kriterien zur Anonymisierung personenbezogener Daten hinzuweisen und somit auf eine datenschutzkonforme Umsetzung des WTPG zu drängen.

Seitdem habe ich zu der Thematik keine Beschwerden mehr erhalten. Ich hoffe, dass Prüfberichte wie der beschriebene der Vergangenheit angehören.

7.12.3 Zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen

Um Anreize zur Pflege in ambulant betreuten Wohngruppen zu geben und damit neue Wohn- und Betreuungsformen zu fördern, gewähren Pflegekassen einen pauschalen Zuschlag zum Pflegegeld nach § 38a SGB XI. Im Zusammenhang mit der Anspruchsprüfung fragen Pflegekassen häufig mehr personenbezogene Daten ab, als zur Erfüllung ihrer

gesetzlichen Aufgaben erforderlich ist. So geschehen in einem Antragsformular für zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen.

Pflegebedürftige erhalten zusätzliche finanzielle Unterstützung von ihrer Pflegekasse, wenn sie gemeinschaftlich in einer ambulant betreuten Wohngruppe leben. Ein Anspruch auf den sog. Wohngruppenzuschlag entsteht dann, wenn die Voraussetzungen des § 38a SGB XI erfüllt sind. Eine Pflegekasse in Baden-Württemberg verwendete zur Abfrage dieser gesetzlichen Anspruchsvoraussetzungen ein ausführliches Antragsformular. Darin sollten die Pflegebedürftigen personenbezogene Angaben machen, die deutlich über das gesetzlich Verlangte hinausgingen.

Die Pflegebedürftigen mussten dazu nachweisen, dass mindestens zwei weitere Mitbewohner der betreuten Wohngemeinschaft Leistungen der Pflegestufe 1 beziehen (§ 38a Absatz 1 Nr. 1 SGB XI). Die Pflegekasse hatte ihr Formular so gestaltet, dass nicht nur zwei, sondern alle Mitbewohner des Antragstellers mit Pflegestufe 1 angegeben werden sollten. Das Formular sah dementsprechend bis zu elf zusätzliche Eingabefelder vor. Nach der Vorstellung der Pflegekasse sollten die Mitbewohner des Antragstellers dabei nicht nur ihren vollen Namen, ihr Geburtsdatum und ihre Pflegekasse angeben, sondern ihre Angaben auch mit der eigenen Unterschrift bestätigen. § 38a SGB XI verlangt allerdings nur den Nachweis über die Pflegestufe von zwei weiteren Mitbewohnern. Die Datenerfassung der übrigen Mitbewohner war von der Rechtsvorschrift nicht gedeckt und damit nicht zulässig. Auch konnte die Pflegekasse die Mitbewohner des Antragstellers nicht dazu verpflichten, eigene Angaben im Formular zu machen, da eine Mitwirkungspflicht Dritter nur in Ausnahmefällen vorgesehen ist. Ein solcher Ausnahmefall lag hier nicht vor. Ein Hinweis, dass die Angaben der Mitbewohner freiwillig erfolgen, fand sich im Formular ebenfalls nicht.

Zwischenzeitlich hat der Gesetzgeber § 38a SGB XI mit dem Ersten Gesetz zur pflegerischen Versorgung und zur Änderung weiterer Vorschriften (Erstes Pflegestärkungsgesetz – PSG I, BGBl. I 2014 S. 2222) zum 1. Januar 2015 geändert. Der Gesetzgeber hat nunmehr klargestellt, welche Daten zur Feststellung der Anspruchsvoraussetzungen bei dem Antragsteller erhoben werden dürfen.

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

§ 38a

*Zusätzliche Leistungen für Pflegebedürftige
in ambulant betreuten Wohngruppen*

(1) Pflegebedürftige haben Anspruch auf einen pauschalen Zuschlag in Höhe von 205 Euro monatlich, wenn

1. sie mit mindestens zwei und höchstens elf weiteren Personen in einer ambulant betreuten Wohngruppe in einer gemeinsamen Wohnung zum Zweck der gemeinschaftlich organisierten pflegerischen Versorgung leben und davon mindestens zwei weitere Personen pflegebedürftig im Sinne der §§ 14, 15 sind oder eine erhebliche Einschränkung der Alltagskompetenz nach § 45a bei ihnen festgestellt wurde,

2. sie Leistungen nach den §§ 36, 37, 38, 45b oder § 123 beziehen,

3. eine Person von den Mitgliedern der Wohngruppe gemeinschaftlich beauftragt ist, unabhängig von der individuellen pflegerischen Versorgung allgemeine organisatorische, verwaltende, betreuende oder das Gemeinschaftsleben fördernde Tätigkeiten zu verrichten oder hauswirtschaftliche Unterstützung zu leisten, und

4. keine Versorgungsform vorliegt, in der der Anbieter der Wohngruppe oder ein Dritter den Pflegebedürftigen Leistungen anbietet oder gewährleistet, die dem im jeweiligen Rahmenvertrag nach § 75 Absatz 1 für vollstationäre Pflege vereinbarten Leistungsumfang weitgehend entsprechen; der Anbieter einer ambulant betreuten Wohngruppe hat die Pflegebedürftigen vor deren Einzug in die Wohngruppe in geeigneter Weise darauf hinzuweisen, dass dieser Leistungsumfang von ihm oder einem Dritten in der Wohngruppe nicht erbracht wird, sondern die Versorgung auch durch die aktive Einbindung ihrer eigenen Ressourcen und ihres sozialen Umfeldes sichergestellt werden kann.

(2) Die Pflegekassen sind berechtigt, zur Feststellung der Anspruchsvoraussetzungen bei dem Antragsteller folgende Daten zu erheben, zu verarbeiten und zu nutzen und folgende Unterlagen anzufordern:

1. eine formlose Bestätigung des Antragstellers, dass die Voraussetzungen nach Absatz 1 Nummer 1 erfüllt sind,

2. die Adresse und das Gründungsdatum der Wohngruppe,

3. den Mietvertrag einschließlich eines Grundrisses der Wohnung und den Pflegevertrag nach § 120,

4. Vorname, Name, Anschrift und Telefonnummer sowie Unterschrift der Person nach Absatz 1 Nummer 3 und

5. die vereinbarten Aufgaben der Person nach Absatz 1 Nummer 3.

Für den Nachweis, dass mindestens zwei weitere Mitbewohner der betreuten Wohngemeinschaft pflegebedürftig sind oder eine erhebliche Einschränkung der Alltagskompetenz bei ihnen festgestellt wurde, ist somit eine formlose Bestätigung des Antragstellers ausreichend. Personenbezogene Daten von pflegebedürftigen Mitbewohnern dürfen zu diesem Zweck nicht erhoben werden.

Gesetzliche Pflegekassen dürfen nur diejenigen personenbezogenen Daten erheben, die zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind. Mit eindeutigen gesetzlichen Regelungen kann der Gesetzgeber den Umfang der Datenerhebung von Anfang an auf das Erforderliche beschränken.

7.13 Wohngeld: Das Formular

Wohngeld ist ein Zuschuss zu den Kosten für selbst genutzten Wohnraum und soll einkommensschwachen Menschen helfen, ihre Wohnkosten zu tragen. Es wird auf Antrag geleistet. Für die Bearbeitung des Antrags ist die Wohngeldbehörde – datenschutzrechtlich betrachtet – berechtigt, diejenigen personenbezogenen Daten zu erheben, die zur Entscheidung über die Gewährung von Wohngeld erforderlich sind.

Ein Bürger, der Wohngeld beantragt hatte, wandte sich an meine Dienststelle und legte ein Formular der Wohngeldbehörde vor, welches er ausfüllen sollte: Das Formular sah Angaben dazu vor, welche durchschnittlichen monatlichen Ausgaben er jeweils

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

für die Bereiche Ernährung, Unterkunft, Neuanschaffung von Bekleidung, Reinigung und Reparatur von Kleidung, Haushaltsgegenstände und Möbel, persönliche Dinge des täglichen Lebens (Kosmetik, Körperpflege, Bücher, Zeitschriften, Vereine usw.), Telefon/Rundfunk/Fernsehen, Versicherungen (Hausrat-, Haftpflicht-, Lebensversicherung) und Kraftfahrzeug (hier sollte einzeln aufgelistet werden, welche monatlichen Beträge für Versicherung, Kfz-Steuer, Treibstoff, Wartung, Reparatur und Garagenmiete ausgegeben werden) hatte.

Der Bürger war der Auffassung, dass es niemanden etwas angehe, wofür er seine Einkünfte im Detail ausgeben.

Die Wohngeldbehörde hat die Datenerhebungen mir gegenüber damit begründet, dass bei dem Antragsteller nicht nachvollziehbar sei, wie er mit den wenigen, von ihm angegebenen Einnahmen bislang in der Lage gewesen sei, seinen Lebensunterhalt zu bestreiten.

Ich konnte mich der Auffassung der Wohngeldbehörde, dass ihre umfangreichen Datenerhebungen zulässig seien, nicht anschließen. Hinzu kam im konkreten Fall, dass der Antragsteller – in für mich nachvollziehbarer Weise – vortrug, seine Ausgaben bislang z. T. durch den Verbrauch seines Vermögens getragen zu haben.

Deswegen habe ich mich in der Angelegenheit an das Ministerium für Finanzen und Wirtschaft Baden-Württemberg, welches die Fachaufsicht beim Wohngeld ausübt, gewandt und diesem meine Auffassung dargelegt. Das Ministerium hat mir zugestimmt und Folgendes mitgeteilt: Wenn berechtigte Zweifel an der Glaubhaftigkeit und Vollständigkeit der Angaben des Antragstellers bestehen – weil die angegebenen Einnahmen unter dem tatsächlichen oder sozialhilferechtlichen Bedarf liegen –, könne die Wohngeldbehörde den Antragsteller auffordern, weitere Angaben zur Glaubhaftmachung der Einkommenssituation zu tätigen. Für diese Glaubhaftmachung könne aber nicht zwingend das Ausfüllen des beschriebenen Formulars gefordert werden – dem Antragsteller sei vielmehr die Möglichkeit zu eröffnen, einen Nachweis der Plausibilität der Einkommenssituation auch in anderer Weise zu führen.

Das Finanz- und Wirtschaftsministerium hat in seinem Schreiben angekündigt, die Wohngeldbehörden über diese Rechtsauffassung zu unterrichten.

Ich habe daher die Erwartung, dass alle Wohngeldbehörden in Baden-Württemberg den Vordruck – wenn überhaupt – nur noch in der Form verwenden, dass sie den Antragsteller darauf hinweisen, dass er den Nachweis der Plausibilität der Einnahmen auch in anderer Weise führen kann.

7.14 Datenverarbeitung im Auftrag

Behörden müssen sich nicht um alles selbst kümmern, sondern können manche Tätigkeit – z. B. aus Kostengründen – auch an Dritte auslagern. Werden im Rahmen einer solchen Auslagerung personenbezogene Daten verarbeitet, hat man es häufig mit einer *Datenverarbeitung im Auftrag* zu tun. Ein typisches Beispiel hierfür ist die Entsorgung von Schriftgut mit personenbezogenen Daten durch eine entsprechend spezialisierte Firma. Eine solche Beauftragung Dritter ist – wenn auch in engeren Grenzen als sonst – auch im Bereich der *Sozialleistungsträger* möglich. Geregelt ist diese Datenverarbeitung im Auftrag in § 80 des Zehnten Buchs des Sozialgesetzbuchs (SGB X).

Zur Sicherstellung des Schutzes der personenbezogenen Daten der Betroffenen – dies können beispielsweise Mitglieder einer Krankenkasse oder Bezieher von Elterngeld sein – hat die Behörde bei der Beauftragung Dritter bestimmte Anforderungen zu beachten. So ist z. B. dem Dienstleister ein *schriftlicher Auftrag* zu erteilen, der im Gesetz näher beschriebene Festlegungen zu enthalten hat. Des Weiteren muss der Sozialleistungsträger seiner *Aufsichtsbehörde* rechtzeitig vor der Auftragserteilung die geplante Auftragsdatenverarbeitung *schriftlich anzeigen* (vgl. § 80 Absatz 3 Satz 1 SGB X). Sinn dieser Regelung ist es der Gesetzesbegründung zufolge, der Aufsichtsbehörde Gelegenheit zu geben, noch vor der Auftragserteilung durch Beratung und ggf. mit den ihr sonst zur Verfügung stehenden Aufsichtsmitteln tätig zu werden.

Im Berichtszeitraum hat sich eine (Rechtsaufsichts-) Behörde mit der Frage an meine Dienststelle gewandt, wer denn überhaupt diese „Aufsichtsbehörde“ sei: Ist dies die *Rechts- bzw. Fachaufsichtsbehörde* (also z. B. das Bundesversicherungsamt in Berlin bei einer bundesunmittelbaren Krankenkasse, das jeweilige Regierungspräsidium bei Sozialhilfeträgern in Baden-Württemberg) oder ist dies der

32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

jeweilige *Datenschutzbeauftragte des Bundes oder der Länder*?

Ich konnte der anfragenden Stelle mitteilen, dass es sich hierbei um die Rechts- bzw. Fachaufsichtsbehörden handelt. Hierfür spricht schon der Wortlaut bzw. die Systematik der Vorschrift: In einem anderen Absatz derselben Vorschrift wird von dem *Bundesbeauftragten für den Datenschutz* und den *Landesbeauftragten für den Datenschutz* gesprochen (vgl. § 80 Absatz 6 SGB X). Es ist davon auszugehen, dass der Gesetzgeber, wenn er in beiden Absätzen den Bundesbeauftragten für den Datenschutz und die Landesbeauftragten für den Datenschutz gemeint hätte, keine unterschiedlichen Begriffe verwendet hätte. Auch Kommentarliteratur und andere Datenschutzbeauftragte teilen diese Auffassung



32. Tätigkeitsbericht 2014/2015 - 7. Gesundheit und Soziales

32. Tätigkeitsbericht 2014/2015 - 8. Datenschutz an Schulen und Hochschulen

8. Datenschutz an Schulen und Hochschulen

8.1 Verwaltungsvorschrift Datenschutz an öffentlichen Schulen

Am 1. Januar 2015 ist die aktualisierte Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ des Ministeriums für Kultus, Jugend und Sport Baden-Württemberg (Kultusministerium) in Kraft getreten (veröffentlicht in „Kultus und Unterricht“, 2015, S. 15 f.). Verschiedene von mir bemängelte Punkte der vorherigen Fassung wurden erfreulicherweise verbessert.

Die überarbeitete Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ stellt nunmehr klar, dass Schulen vor der Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet/ Intranet oder in Printmedien (z. B. Jahrbuch der Schule), auf denen minderjährige Schülerinnen und Schüler abgebildet sind, nicht nur eine schriftliche oder elektronische Einwilligung der Erziehungsberechtigten einzuholen haben, sondern nach Vollendung des 14. Lebensjahres auch zusätzlich von den betroffenen Schülerinnen und Schülern. Dies gilt auch, wenn Fotos, Filme und andere digitale Medien, auf denen minderjährige Schülerinnen und Schüler abgebildet sind, an andere Personen weitergegeben oder ausgetauscht werden sollen (Abschnitt II. 1.4). Diese Einwilligung gilt bis zum Ende des Schulbesuches und kann jederzeit ohne Angabe von Gründen widerrufen werden (Abschnitt II. 4.1).

Auch die Videoüberwachung während des Schulbetriebs auf dem Schulhof und in den sonstigen für den Schulbetrieb genutzten Räumlichkeiten ist nun klar geregelt. Nach Abschnitt I. 10 entscheidet bei öffentlichen Schulen grundsätzlich der Schulträger für öffentlich zugängliche Bereiche und die Außenhaut des Gebäudes samt Stellflächen für PKW und Fahrräder, ob bei Vorliegen der gesetzlichen Voraussetzungen von der Videoüberwachung Gebrauch gemacht werden soll. Klargestellt wird auch, dass der Schulträger datenschutzrechtlich verantwortlich für die Videoüberwachung ist. Während des Schulbetriebs ist eine Videoüberwachung auf dem Schulhof sowie in den sonstigen für den Schulbetrieb genutzten Räumlichkeiten grundsätzlich nicht zulässig.

Hilfreich für die Schulen sind ferner die in Abschnitt II. 5.2 konkret benannten Löschfristen personenbezogener Daten in den unterschiedlichen Bereichen wie zum Beispiel Klassen- und Kurstagebüchern, Abschlusszeugnissen oder Prüfungsunterlagen.

Erstmals wird in Abschnitt II. 3.2 auch die Thematik E-Mail-Verkehr zwischen Lehrkräften und Erziehungsberechtigten sowie Dritten (beispielsweise Ausbildungsbetriebe im Berufsschulbereich) geregelt. Aus Rückmeldungen von Teilnehmern verschiedener Fortbildungsveranstaltungen zum Datenschutz für Schulleiter, Datenschutzbeauftragte und Lehrkräfte ist mir bekannt, dass hier Unsicherheit und Unzufriedenheit bestehen. Häufig fühlen sich die Lehrkräfte mit den vorgegebenen strikten Regelungen (verschlüsselte Kommunikation mit Dritten außerhalb des Landesverwaltungsnetzes) und den unterschiedlichen Voraussetzungen an den Schulen (vom E-Mail-Account beim Privatanbieter, E-Mail-Hosting bei BelWü [Landeshochschulnetz] bis hin zum eigenen E-Mail-Server an der Schule) im Stich gelassen. Das Kultusministerium beabsichtigt, bereits ab dem Jahr 2016 allen Lehrern in Baden-Württemberg für ihre Arbeit künftig eine persönliche dienstliche E-Mail-Adresse bereitzustellen. Dies ist Teil der „Digitalen Bildungsplattform“, die – neben der persönlichen E-Mail-Adresse – die Möglichkeit vorsehen soll, Dateien auf der Plattform abzulegen, auf die dann alle Lehrer im Land und später einmal auch Schüler zugreifen können.

Zu begrüßen ist der explizite Hinweis zur Erstellung eines Verfahrensverzeichnis für automatisierte Verfahren, beispielsweise das Schulverwaltungsprogramm SVP (Abschnitt I. 7) und zur notwendigen Erteilung eines Auftrages zur Datenverarbeitung, sofern personenbezogene Daten im Auftrag der Schule durch andere Personen oder Stellen verarbeitet werden (Abschnitt I. 12).

Dies trägt hoffentlich dazu bei, den Schulen bewusst zu machen, dass sie sich verstärkt auch um diese Themen kümmern müssen. Das Kultusministerium hat den Schulen dazu umfangreiche Hilfestellungen zur Verfügung gestellt. Mittlerweile steht ein Portfolio aus Onlineverfahren, Vordrucken, Handreichungen und Fortbildungsmaßnahmen bereit, die die Schulen und ihre Datenschutzbeauftragten (soweit vorhanden) nutzen können.

32. Tätigkeitsbericht 2014/2015 - 8. Datenschutz an Schulen und Hochschulen

Das Kultusministerium hat seine Anstrengungen zur Verbesserung des Datenschutzes an Schulen in den letzten Jahren erfreulich verstärkt. Nun ist die konsequente Umsetzung, vor allem aber die Inanspruchnahme der bereitgestellten Verfahren und Hinweise durch die Schulen selbst erforderlich. Die verpflichtende Bestellung von behördlichen Datenschutzbeauftragten nach der neuen EU-Datenschutz-Grundverordnung wird ab 2018 hoffentlich dazu beitragen.

8.2 Medienbildung im Bildungsplan 2016

Medienbildung ist eine der sechs Leitperspektiven des neuen Bildungsplans und soll u. a. in einem Basiskurs Medienbildung in der fünften Jahrgangsstufe vermittelt werden. Nach der Erprobung von Arbeitsfassungen und dem Abschluss der Anhörungsphase im Herbst 2015 wird der neue Bildungsplan zum Schuljahr 2016/17 zur Umsetzung kommen.

Seit meiner Berichterstattung im letzten Tätigkeitsbericht (31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, S. 125) hat sich im Zuge der Bildungsplanreform 2016 zwar einiges an Neuerungen ergeben, allerdings wurden meine Vorschläge in den wesentlichen Punkten nicht aufgegriffen.

Der Bildungsplan sieht nunmehr zusätzlich zu den ursprünglich fünf etablierten Leitperspektiven seit dem Jahre 2014 eine weitere, in der Öffentlichkeit viel diskutierte allgemeine Leitperspektive „Bildung von Toleranz und Akzeptanz“ vor. Im Hinblick auf die themenspezifische Leitperspektive „Medienbildung“ und deren Verankerung im Bildungsplan fand meine Anregung, Medienkompetenz als ein eigenständiges Fach zu vermitteln, leider kein Gehör. Zwar wurde ein Basiskurs Medienbildung in Klasse 5 installiert. Mit nur 35 Unterrichtsstunden ist dieser jedoch sehr knapp bemessen und wird überdies in den höheren Klassen nicht fortgeführt. Nach meiner Auffassung kann der Basiskurs in seiner jetzigen Konzeption lediglich einen ersten Beitrag zur Verbreitung dieser wichtigen Kompetenz im Schulalltag leisten.

Der Basiskurs soll anschließend in den höheren Klassen bis zum Schulabschluss eine spiralcurriculare und fächerübergreifende Medienbildung ermöglichen. Bislang finden sich – mit Ausnahme des

Faches Deutsch – in den einzelnen Fächerplänen aber nur phasenweise Themenfelder der Medienbildung, vorrangig „Information und Wissen“ zur typischen Internet-Recherche im Unterricht.

Die von mir vorgeschlagene unterrichtliche Auseinandersetzung mit datenschutzrechtlichen Risiken und den damit verbundenen möglichen Auswirkungen auf unsere Gesellschaft ist im Kern durch den Bildungsplan erfasst. Die von mir ebenfalls angeregten und darauf aufbauenden Kenntnisse über die Funktionsweise und die Rahmenbedingungen des Internets (zum Beispiel: wie funktionieren Cookies und wozu dienen sie; Zählpixel und Like-it-Button als Möglichkeit, zentrale Datensammlungen anzulegen) lassen sich in den Bildungsplanentwürfen hingegen nicht erkennen. Gerade diese erachte ich aber für eine differenzierte Meinungsbildung und den Kompetenzerwerb der Schüler für ebenso erforderlich, zumal es dabei ganz konkret um das Verhalten und den Selbstschutz der Schüler in ihrem Internet-Alltag geht.

Erfreulich ist deswegen die kurz vor Redaktionsschluss dieses Berichts bekannt gewordene Meldung aus dem Kultusministerium, dass ein neuer „Aufbaukurs Informatik“ für Schülerinnen und Schüler aller allgemeinbildenden Schulen in der Klassenstufe 7 angeboten werden soll, dessen Inhalte in den Klassenstufen 8 bis 10 weiter vertieft werden; parallel dazu werde ein darauf abgestimmtes Fortbildungskonzept für Lehrerinnen und Lehrer aufgelegt. Der verbindliche „Aufbaukurs Informatik“ solle im Umfang von einer Wochenstunde ab Schuljahresbeginn 2017/2018 unterrichtet werden; hierfür würden zusätzliche Deputate geschaffen. Als Vertiefungsmöglichkeit in den Klassenstufen 8 bis 10 soll in den Gymnasien und Gemeinschaftsschulen ein neues Profulfach namens „Informatik, Mathematik, Physik“ eingeführt werden, das von den Schulen alternativ zum bereits bestehenden Profulfach „Naturwissenschaft und Technik“ angeboten werden kann. In den Realschulen soll in den gleichen Jahrgangsstufen ein neues Wahlfach „Informatik“ für alltagsrelevante Themen mit Praxisbezug eingeführt werden. Es bleibt zu hoffen, dass die neuen Angebote nicht zu spät für eine wertorientierte und umfassende Medienbildung der Schülerinnen und Schüler aufsetzen.

32. Tätigkeitsbericht 2014/2015 - 8. Datenschutz an Schulen und Hochschulen

Sehr positiv verlief in meinen Augen die Entwicklung der Mediacurricula des Landesmedienzentrums (LMZ). Wie schon im letzten Tätigkeitsbericht erwähnt, wurde meiner Dienststelle Gelegenheit gegeben, die bis dato entwickelten Entwürfe um einige datenschutzrechtliche Aspekte zu ergänzen. In den Curricula finden sich nun klare Formulierungen zum Kompetenzerwerb des Schülers wieder. Zur konkreten Umsetzung und Vermittlung im Unterricht stehen – schulstufendifferenziert – Vorschläge und zusätzliche Informationen, in Form von Unterrichtsmodulen und -materialien sowie Linklisten zum Thema, zur Verfügung.

Ergänzend erarbeitet derzeit das Landesinstitut für Schulentwicklung (LS) in Kooperation mit den Landesakademien eine elektronische Form der „Kompetenzraster“ auf der Lernplattform Moodle und schafft so ein weiteres pädagogisches und modernes Instrument zur Dokumentation des Lernprozesses für Lehrkräfte.

Zur Medien- und Datenschutzkompetenz sind neben entsprechenden Haltungen und Werten auch technische Grundlagen wichtig, um die Zusammenhänge einordnen zu können. Ob die verstärkten Anstrengungen im Bereich Informatik dem hinreichend und rechtzeitig Rechnung tragen, wird sich zeigen.

8.3 Toiletten-Schließanlagen an Schulen

Elektronische Schließanlagen für Schultoiletten gelten zunehmend als adäquates Mittel, Verunreinigungen und Vandalismus entgegenzuwirken. Datenschutzrechtlich ist dies problematisch.

Durch eine Eingabe wurde ich darauf aufmerksam, dass an einer Schule der Zugang zu den Schülertoiletten mit einer Chipkarten-basierten Schließanlage versehen werden sollte. Ziel war es, Verunreinigungen und Vandalismus in den Toilettenräumen durch die Erfassung der Schüler, die die Toilette nutzen, zu verhindern.

Durch die Erfassung der Schüler und der Uhrzeit der Toilettennutzung werden allerdings personenbezogene Daten der Schüler erhoben, gespeichert und genutzt. Eine derartige Verarbeitung personenbezogener Daten ist nach § 4 Absatz 1 LDSG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat.

Der Schulträger als datenschutzrechtlich verantwortliche Stelle stützte das Vorhaben auf die Einwilligung der betroffenen Schüler bzw. deren Erziehungsberechtigte. Soll eine Einwilligung Grundlage für die Datenverarbeitung sein, ist jedoch zu beachten, dass die Einwilligung tatsächlich freiwillig sein muss. Vorliegend habe ich insoweit Bedenken geäußert. Der Schulträger wollte zwar nicht alle Toiletten mit einer Schließanlage ausstatten, so dass den Schülern, die mit der Erfassung ihrer Daten nicht einverstanden gewesen wären, andere Toiletten zur Verfügung gestanden hätten. Allerdings hätte sich die Anzahl der frei nutzbaren Toiletten deutlich reduziert und die Entfernung zu den Toiletten für einzelne Schüler zugenommen, was vor allem in den Pausen zu „Engpässen“ hätte führen können.

Der Schulträger konnte auch nicht nachvollziehbar belegen, dass die geplante Maßnahme geeignet ist, Sachbeschädigungen zu verhindern und ggf. den Täter zu ermitteln. Jedenfalls wäre es ohne weiteres möglich gewesen, die Toilettenanlagen auch ohne Chipkarte zu betreten, solange die Zugangstüren noch geöffnet gewesen wären. Und da die Ermittlung des exakten Zeitpunktes einer Sachbeschädigung häufig gar nicht möglich ist, war zu befürchten, dass dann u.U. eine Vielzahl von Schülern (grundlos) in Verdacht geraten.

Ich habe daher dem Schulträger empfohlen, weniger in die Persönlichkeit der Schüler eingreifende Maßnahmen zu prüfen, beispielsweise eine verstärkte Aufsicht während der Pausen. Das Kultusministerium hat sich meiner Auffassung angeschlossen.

8.4 Das neue Internetportal youngdata.de

Kindern und Jugendlichen stehen heute zahlreiche Möglichkeiten der Mediennutzung offen. Häufig sind sie jedoch noch nicht in der Lage, die Vorteile und die Risiken, die sich daraus ergeben, richtig einzuschätzen und danach zu handeln. Das neue gemeinsame Portal der Bundes- und Landesbeauftragten für den Datenschutz www.youngdata.de, das beim LfD Rheinland-Pfalz gehostet wird, bietet ein umfangreiches Informationsangebot.

Mit Young Data wollen die Datenschutzbeauftragten die Themen Datenschutz und Privatsphäre für die Jugend zielgruppengerecht, pädagogisch und didak-

32. Tätigkeitsbericht 2014/2015 - 8. Datenschutz an Schulen und Hochschulen

tisch geschickt aufbereiten. Die Webseite will junge Leute für den sorgsamsten Umgang mit den eigenen Daten und Daten anderer sensibilisieren. Hier finden sie Informationen zum Datenschutz, Tipps für ein kluges Verhalten im Internet und Berichte über die digitale Zukunft unserer Gesellschaft. Young Data enthält Informationen zum Selbstschutz bei der Nutzung von Facebook, WhatsApp, Skype & Co., YouTube, Spielekonsolen, Smartphones und anderen Anwendungen, klärt über die Gefahren von Cybermobbing auf und bietet Hintergrundinformationen zum Datenschutz im Allgemeinen. Die Rubrik „Digitale Selbstverteidigung“ gibt praktische Tipps, um private Informationen zu schützen. Die Artikel werden von Bildern und Videos begleitet und auf Seiten mit weiterführenden Informationen verlinkt. Daher eignet sich das Portal m.E. auch hervorragend zum Einsatz im Unterricht.

8.5 Erst Verzeichnis, dann Betrieb

Wann müssen öffentliche Stellen ein Verzeichnis erstellen und meiner Dienststelle den Einsatz und die wesentliche Veränderung eines automatisierten Verfahrens melden?

Jede öffentliche Stelle führt nach § 11 Absatz 1 Satz 1 LDSG „ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden“ – das sog. Verzeichnis. In dieses sind die in § 11 Absatz 2 LDSG genannten Angaben einzutragen, etwa die Bezeichnung des Verfahrens, die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung und die technischen und organisatorischen Maßnahmen nach § 9 LDSG. Nach dem Wortlaut müssen die Angaben spätestens dann im Verzeichnis eingetragen sein, wenn mit dem Verfahren erstmals personenbezogene Daten verarbeitet werden. Ist ein Datenschutzbeauftragter nach § 10 LDSG bestellt, dann hat er das Verzeichnis zu führen.

Die öffentlichen Stellen, die keinen Datenschutzbeauftragten nach § 10 LDSG bestellt haben, müssen zudem meiner Dienststelle nach § 32 Absatz 1 LDSG den Einsatz und die wesentliche Veränderung eines automatisierten Verfahrens melden (ausgenommen die in § 11 Absatz 3 und 4 Satz 2 LDSG genannten Verfahren). Außerdem haben sie nach § 32 Absatz 2 LDSG spätestens gleichzeitig mit der ersten Einspeicherung die in das Ver-

zeichnis einzutragenden Angaben mitzuteilen.

Am 10. Dezember 2014 erhielt meine Dienststelle ein Schreiben einer Universität, die keinen Datenschutzbeauftragten nach § 10 LDSG bestellt hatte, wonach ein automatisiertes Verfahren, mit dem personenbezogene Daten verarbeitet werden, am 15. Dezember 2014 starten sollte; die meiner Dienststelle mitzuteilenden Angaben fehlten jedoch. Das habe ich gegenüber der Universität beanstandet und sie um Stellungnahme gebeten. Die Universität gestand daraufhin u. a. ein, auch sie sehe in der inhaltlich nicht ausreichenden Meldung einen Verstoß gegen § 32 LDSG; die für das Verzeichnis bedeutsamen Fragen des Datenschutzes und der IT-Sicherheit seien damals berücksichtigt, allerdings noch nicht (in einer Anlage zum Verzeichnis) dokumentiert gewesen.

Spätestens dann, wenn mit einem automatisierten Verfahren erstmals personenbezogene Daten verarbeitet werden, müssen die vorgeschriebenen Angaben im Verzeichnis eingetragen sein. Die öffentlichen Stellen, die keinen behördlichen Datenschutzbeauftragten bestellt haben, müssen zudem meiner Dienststelle den Einsatz und die wesentliche Veränderung eines meldepflichtigen automatisierten Verfahrens melden und spätestens gleichzeitig mit der ersten Einspeicherung die in das Verzeichnis einzutragenden Angaben mitteilen.

32. Tätigkeitsbericht 2014/2015 - 9. Datenschutz in der Arbeitswelt

9. Datenschutz in der Arbeitswelt

9.1 Mindestlohngesetz und Datenschutz

Zum 1. Januar 2015 ist das Mindestlohngesetz in Kraft getreten, das nicht zuletzt durch den Streit über die damit verbundenen Dokumentationspflichten für Arbeitgeber immer wieder im Fokus der politischen und medialen Aufmerksamkeit stand. Das Bundesgesetz wirft auch eine Reihe von datenschutzrechtlichen Problemen auf.

Nach § 13 des Mindestlohngesetzes (MiLoG) i. V. mit § 14 des Arbeitnehmerentendegesetzes haftet ein auftraggebendes Unternehmen wie ein Bürge dafür, wenn der Auftragnehmer seinen Beschäftigten nicht den gesetzlichen Mindestlohn zahlt; diese Haftung erstreckt sich ggf. auch auf weitere Subunternehmer und deren Arbeitnehmer, wobei sich der Betroffene aussuchen kann, gegen welchen übergeordneten Auftraggeber er vorgehen will. Weiterhin steht ein Bußgeld im Raum, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass der Subunternehmer nicht den Mindestlohn zahlt (§§ 20, 21 Absatz 2 MiLoG). Wie die Überprüfung, ob ein Auftragnehmer den Mindestlohn tatsächlich zahlt, konkret zu erfolgen hat, wird im Mindestlohngesetz jedoch nicht näher bestimmt. Die Industrie- und Handelskammern berichten von einer erheblichen Versäumnis bei Unternehmen, die mittlerweile versuchen würden, sich durch entsprechende Verpflichtungserklärungen ihrer Subunternehmer abzusichern. Dabei würden z.T. auch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf Beschäftigtendaten beim Auftragnehmer (Lohnlisten, Verdienstbescheinigungen usw.) eingefordert.

Aus Sicht des Datenschutzes geht es angesichts dieser Problemlage darum, Wege aufzuzeigen, wie Unternehmen ihren gesetzlich vorgeschriebenen Prüfpflichten bezüglich der Einhaltung der Mindestlohnvorgaben durch ihre Subunternehmer nachkommen können, ohne – oder zumindest nur so wenig wie möglich – personenbezogene Daten der Beschäftigten ihrer Subunternehmer erheben zu müssen. Grundsätzlich muss der Auftraggeber zunächst eine gewisse Sorgfalt bei der Auswahl seiner Geschäftspartner walten lassen, beispielsweise also unrealistisch billige Angebote von Subunternehmen eingehend prüfen. Im Übrigen ist er nicht daran gehindert, das mit dem Mindestlohn- bzw. Arbeitneh-

merentendegesetz verbundene Haftungsrisiko auf den neuen Vertragspartner abzuwälzen. Hierzu bieten sich vorrangig zivilrechtliche Vereinbarungen zwischen dem Unternehmen und seinen Subunternehmern an, in denen die Subunternehmer versichern, die Voraussetzungen des Mindestlohngesetzes einzuhalten, und für den Fall von Zuwiderhandlungen Vertragsstrafen vereinbart werden; ergänzend sollten Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer vorgesehen werden. Darüber hinaus kann ggf. die Überlassung anonymisierter Lohnabrechnungsdaten vereinbart werden. Schließlich können sich Unternehmen die Bestätigung eines vom Subunternehmer eingeschalteten Steuerberaters oder Wirtschaftsprüfers vorlegen lassen, wonach der Subunternehmer die Mindestlohnvorgaben beachtet („Testatlösung“). Lediglich dann, wenn eine solche Bestätigung nicht vorgelegt werden kann und im Einzelfall konkrete Anhaltspunkte dafür bestehen, dass ein Subunternehmer seinen Arbeitnehmern nicht den gesetzlichen Mindestlohn auszahlt, kann es zulässig sein, dass ein vom Unternehmen beauftragter Wirtschaftsprüfer oder Steuerberater Einblick in die Lohnabrechnungsdaten des Subunternehmers nimmt. Darüber hinaus ist die Erhebung personenbezogener Beschäftigtendaten durch Unternehmen zur Kontrolle der Einhaltung der Mindestlohnvorgaben durch ihre Subunternehmer weder geboten noch erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung vom 18./19. März 2015 in diesem Sinne zu der Thematik geäußert (vgl. Anhang 20); etwaige Beratungen meiner Dienststelle erfolgen auf dieser Grundlage.

Zur Kontrolle der Einhaltung der Vorgaben des Mindestlohngesetzes bei Subunternehmern durch ihre Auftraggeber ist im Regelfall keine Übermittlung personenbezogener Daten der Beschäftigten des Subunternehmers an seinen Auftraggeber erforderlich. Solche Übermittlungen sind daher grundsätzlich unzulässig. Daran ändern auch entsprechende vertragliche Vereinbarungen zwischen Auftraggeber und Subunternehmer nichts.

32. Tätigkeitsbericht 2014/2015 - 9. Datenschutz in der Arbeitswelt

9.2 Abgleich von Beschäftigendaten mit Sanktionslisten der EU sowie sonstiger Drittstaaten

Durch Presseberichte wurde ich zu Beginn des Jahres 2015 darauf aufmerksam, dass ein großes Industrieunternehmen mit Sitz in Baden-Württemberg auf der Grundlage einer Konzernbetriebsvereinbarung alle drei Monate die Daten seiner Mitarbeiter und von Bewerbern – bevor an diese Geld ausbezahlt wird – sowie von Kunden und Lieferanten anhand von Vor- und Nachnamen, Geburtsdatum und Adresse automatisch mit sogenannten Sanktionslisten abgleicht. Dabei handelt es sich um Anhänge zu zwei europäischen Rechtsverordnungen zur Terrorbekämpfung, in denen terrorverdächtige Personen und Organisationen gelistet sind. Die Listen werden laufend im Abstand weniger Wochen aktualisiert. Die Antiterror-Verordnungen verbieten es, den gelisteten Personen unmittelbar oder mittelbar Gelder oder sonstige wirtschaftliche Ressourcen zur Verfügung zu stellen, regeln allerdings nicht, was Unternehmen tun müssen oder dürfen, um sicherzustellen, dass sie nicht gegen das Verbot verstoßen. Solche Abgleiche werden auch von anderen Unternehmen durchgeführt, wobei die Handhabung sehr unterschiedlich ist; z.T. erfolgt der Abgleich vor jeder Gehaltsauszahlung, andere beschränken den Abgleich auf Mitarbeiter in sensiblen Bereichen oder auf neue Mitarbeiter. Manche Unternehmen überlassen den Abgleich auch den Banken.

Von den Datenschutzaufsichtsbehörden werden diese massenhaften Datenabgleiche schon länger kritisch gesehen. Da die Antiterror-Verordnungen der EU die Vornahme von Namensabgleichen nicht ausdrücklich regeln, scheiden sie als Rechtsgrundlage hierfür aus. Allerdings berufen sich die Unternehmen darauf, dass sie die Abgleiche vornehmen müssten, um das Risiko auszuschließen, selbst bestraft zu werden. Die vorsätzliche Finanzierung der gelisteten Personen stellt einen Straftatbestand dar; bei Fahrlässigkeit handelt es sich um eine Ordnungswidrigkeit, für die eine Geldbuße bis zu 500.000 € verhängt werden kann. Der Vorwurf der Fahrlässigkeit setzt jedoch einen Sorgfaltspflichtverstoß voraus, d. h. das Unterlassen angemessener und zumutbarer Vorkehrungen. Ob und unter welchen Voraussetzungen dazu regelmäßige anlassunabhängige und systematische Abgleich aller Beschäftigten und sonstiger Zahlungsempfänger mit

den Sanktionslisten zählen, ist allerdings ungeklärt. Die Bundesregierung hat die Unternehmen bislang darauf verwiesen, dass sie einen Abgleich nur nach Maßgabe von Sorgfaltspflichten, d. h. differenzierend nach verschiedenen Verkehrskreisen und Risikolagen vornehmen müssten. Diese sehr unbestimmte Aussage lässt die Unternehmen im Grunde mit der Frage allein, in welchen Fällen ein Abgleich vorgeschrieben oder erlaubt ist.

Ich habe deshalb die Bundesfinanzverwaltung um Auskunft gebeten, ob und unter welchen Voraussetzungen Unternehmen zu anlassunabhängigen Abgleichen mit Sanktionslisten verpflichtet sind, ob eine etwaige Verpflichtung auf Beschäftigte in sicherheitsrelevanten Bereichen beschränkt ist und ob nicht die von den Banken ohnehin vorgenommenen Abgleiche zusätzliche Abgleiche durch die Unternehmen entbehrlich machen. Leider war die erst nach etlichen Wochen eingegangene Antwort der Bundesfinanzdirektion Südost alles andere als erhellend. Es wurde lediglich darauf hingewiesen, dass sich die zu fordernde Sorgfaltspflicht an den jeweiligen Umständen des Einzelfalls und den Fähigkeiten des Pflichtigen zu orientieren habe und pauschale Aussagen zu den Sorgfaltspflichten im Hinblick auf die Prüfung der Personenlisten nach den EU-Sanktionsverordnungen daher nicht möglich seien. Die Anforderungen seien umso höher, je größer die wirtschaftlichen Verflechtungen eines Unternehmens, je höher die allgemeine Risikolage aufgrund der Handelspartnerländer sei und je häufiger der Kreis der Zahlungsempfänger wechsele. Die Bundeszollverwaltung stellte außerdem klar, dass Abgleiche nicht auf Mitarbeiter in sicherheitsrelevanten Bereichen beschränkt werden könnten und es problematisch wäre, wenn die Unternehmen im Hinblick auf die Vornahme von Abgleichen durch Banken von eigenen Abgleichen absähen, weil sie sich etwaige Versäumnisse der Banken in vollem Umfang zurechnen lassen müssten.

Die Antiterror-Verordnungen stammen aus den Jahren 2001 und 2002. Bis 2010 wurden nach Aussage der Bundesregierung in ganz Deutschland trotz der massenhaft durch alle Banken durchgeführten Abgleiche Zahlungen an gelistete Personen und Organisationen nur in Höhe von insgesamt ca. 200,00 €

32. Tätigkeitsbericht 2014/2015 - 9. Datenschutz in der Arbeitswelt

entdeckt⁶⁴. Das spricht dafür, dass sich gelistete Personen im genannten Zeitraum nur in ganz wenigen Fällen unter ihrem echten Namen Gelder auf Konten bei Banken in Deutschland haben überweisen lassen. Damit ist unterm Strich fraglich, ob sich der große Aufwand, den die Banken mit den Abgleichen betreiben müssen, wirklich lohnt, umso mehr, ob ein zusätzlicher Abgleich durch Arbeitgeber erforderlich ist.

Solange sich aber die für den Vollzug des Außenwirtschaftsgesetzes zuständige Bundeszollverwaltung nicht zu einer klaren Aussage dazu durchringen kann, ob und unter welchen Voraussetzungen deutsche Unternehmen zu anlassunabhängigen Abgleichen mit Sanktionslisten des EU-Rechts verpflichtet sind, und Unternehmen, die solche Abgleiche unterlassen, daher die Verhängung von Bußgeldern befürchten müssen, halte ich die Vornahme solcher Abgleiche zumindest für vertretbar. Dabei müssen die Betroffenen allerdings vorab über den Umfang der Abgleiche informiert werden. Positiv zu bewerten ist auch, wenn der Arbeitgeber seine Beschäftigten im Fall eines Treffers bei der Durchführung von Entlistungsverfahren unterstützt und Betriebsrat und betrieblicher Datenschutzbeauftragter in das Verfahren einbezogen werden.

Bei Abgleichen mit Sanktionslisten ausländischer Rechtsordnungen, z. B. solchen des US-Rechts, kommt es auf eine Abwägung im Einzelfall an. Die Nachteile, die dem Unternehmen und seinen Mitarbeitern im Fall einer Zuwiderhandlung im Ausland drohen, sind mit den Interessen der Betroffenen abzuwägen. Insoweit ist etwa zu berücksichtigen, ob es individuelle Rechtsschutzmöglichkeiten gegen eine Aufnahme in die Liste in dem Drittstaat gibt.

Bei der Auslegung der Bußgeldtatbestände des Außenwirtschaftsgesetzes zieht die Bundeszollverwaltung nicht an einem Strang mit der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder. Anlasslose und systematische Abgleiche von Beschäftigtendaten mit den Sanktionslisten des EU-Rechts durch Arbeitgeber müssen daher bis auf weiteres hingenommen werden. Der Europäi-

sche Gesetzgeber ist aufgerufen, in dieser Frage für Klarheit zu sorgen

9.3 Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern: Die Ausnahme muss wieder zur Regel werden

Diesen Text aus der automatisierten Begrüßungsansprache eines Call-Centers kennen wir alle: „Aus Gründen der Qualitätssicherung und für Schulungszwecke werden einzelne Gespräche aufgezeichnet.“ Das Aufzeichnen und Abhören von Telefongesprächen ist aber strafbar, soweit dies unbefugt im Sinne des § 201 Absatz 1 StGB erfolgt. Danach wird das unbefugte Aufnehmen des nicht-öffentlich gesprochenen Wortes eines anderen auf einem Tonträger mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe geahndet. Die Betreiber von Call-Centern müssen daher rechtlich Einiges beachten, damit diese Form der Datenverarbeitung auch rechtmäßig durchgeführt werden kann.

Man gewinnt fast den Eindruck, dass das Aufzeichnen und Mithören von Telefongesprächen in Call-Centern inzwischen die Regel ist. Auch der Grundsatz der Datensparsamkeit scheint hier bedauerlicherweise keine Rolle zu spielen. Den Betreibern der Call-Center scheinen dabei die rechtlichen Grenzen des Aufzeichnens und Mithörens oft nicht bewusst zu sein.

Die als Begründung genannten Schulungs- und Qualitätssicherungsmaßnahmen werden in der Regel in folgenden Varianten durchgeführt:

- das vom Beschäftigten und vom Kunden gesprochene Wort wird durch eine Kontrollperson direkt am Arbeitsplatz im Call-Center unter Nutzung eines Kopfhörers offen mitgehört,
- das vom Beschäftigten und vom Kunden gesprochene Wort wird ohne direkte Anwesenheit einer Kontrollperson am Arbeitsplatz durch Aufschalten mitgehört oder
- das Gespräch wird aufgezeichnet und später ausgewertet.

Datenschutzrechtlich ist zwischen den Rechten des Kunden und denen der Beschäftigten zu unterscheiden.

⁶⁴ vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Ulla Jelpke u. a. Fraktion Die Linke, EU-Terroristen und Außenwirtschaftsgesetz, vom 4. Januar 2010, BT-Drs. 17/388 (Antwort auf Frage 8 b auf Seite 5), <http://dipbt.bundestag.de/dip21/btd/17/003/1700388.pdf>

32. Tätigkeitsbericht 2014/2015 - 9. Datenschutz in der Arbeitswelt

9.3.1 Aufzeichnung oder Mithören von Telefongesprächen in Call-Centern aus Sicht des Kunden

Jedem Kunden steht das Recht am gesprochenen Wort als Ausfluss des grundrechtlich geschützten allgemeinen Persönlichkeitsrechts des Artikels 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes zu. Jedermann soll – sowohl im privaten als auch im geschäftlichen Bereich – grundsätzlich selbst entscheiden können, ob seine Worte allein dem Gesprächspartner oder auch Dritten zugänglich sein sollen oder ob diese gar auf Tonträger aufgenommen werden dürfen.

Gem. § 4 Absatz 1 BDSG ist die Erhebung und Verarbeitung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Als mögliche Rechtsgrundlagen für das Mithören und Aufzeichnen von Telefongesprächen könnten § 28 Absatz 1 Satz Nr. 1 und Nr. 2 BDSG in Betracht kommen. Diese sind aber im Regelfall im Rahmen der Abwägung zwischen den berechtigten Geschäftsinteressen des Unternehmens und den schutzwürdigen Interessen der Kunden und Mitarbeiter *abzulehnen*, weil

- das Recht am gesprochenen Wort wirtschaftlichen oder geschäftlichen Interessen grundsätzlich vorgeht und
- die Gespräche umfangreicher sein können, als es für die Erfüllung des Geschäftszwecks erforderlich ist.

Daraus folgt, dass die heimliche Aufzeichnung bzw. das Abhören von Telefongesprächen grundsätzlich verboten ist und gem. § 201 StGB sogar mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden kann.

Ein solches Aufzeichnen oder Mithören ist demnach nur zulässig, wenn der Kunde

- vor Beginn des Aufzeichnens oder Mithörens hierüber informiert wird und
- nach seiner ausdrücklichen Einwilligung im Sinne von § 4a BDSG gefragt wird.

Ebenso müssen die Kunden über die Identität der verantwortlichen Stelle und den Zweck der Erhe-

bung und Verarbeitung aufgeklärt werden, § 4 Abs. 3 Satz. 1 BDSG.

Nur wenn der Kunde anschließend ausdrücklich mit einem „Ja“ in das Aufzeichnen oder Mithören einwilligt, ist dies zulässig und erlaubt. Ein Schweigen des Kunden genügt hierfür nicht. Erst nach dieser Entscheidung des Kunden darf die Aufzeichnung oder das Mithören beginnen.

Eine reine Widerspruchslösung („Wenn Sie mit einer Gesprächsaufzeichnung nicht einverstanden sind, geben Sie bitte zu Beginn des Gesprächs unserem Kundenberater Bescheid.“) reicht keinesfalls aus, da diese eine konkludente Einwilligung unterstellt, die aber keine Einwilligung im Sinne der §§ 4 Absatz 1 und 4a Absatz 1 BDSG darstellt. Erforderlich ist vielmehr die Erkundigung zu Beginn des Gesprächs, ob der betroffene Kunde einverstanden ist oder nicht.

Der Kunde kann seine erteilte Einwilligung natürlich auch während des Telefongesprächs jederzeit ohne Angabe von Gründen widerrufen. Die bisherige Aufzeichnung muss dann gelöscht bzw. das Mithören umgehend beendet werden. Sowohl die Einwilligung als auch der Widerruf der Einwilligung sind vom Unternehmen zu dokumentieren.

Auch die Aufzeichnung von Telefongesprächen im *Arbeitsspeicher* der Rechner ist ein Speichern im Sinne von § 3 Absatz 4 Nr. 1 BDSG und somit eine automatisierte Datenverarbeitung, die das vorherige Erheben der Daten nach § 3 Absatz 3 BDSG voraussetzt. Selbst wenn die Gespräche nur für Sekunden oder Minuten im (flüchtigen) Arbeitsspeicher gespeichert werden, liegt tatbestandlich ein Erheben und physikalisches Speichern vor. Die Aufzeichnungen sind erst dann gelöscht im Sinne von § 35 Absatz 2 BDSG, wenn die entsprechenden Bereiche des Arbeitsspeichers überschrieben werden. Es kommt auch nicht darauf an, ob ein Zugriff auf diese Daten erfolgt.

Ein Aufzeichnen von Telefongesprächen kann schließlich auch gegen den Grundsatz der Datenvermeidung und Datensparsamkeit aus § 3a BDSG verstoßen. Soweit andere Möglichkeiten vorhanden sind, um eine Aufnahme von Telefonaten zu vermeiden, sollten diese auch wahrgenommen werden.

32. Tätigkeitsbericht 2014/2015 - 9. Datenschutz in der Arbeitswelt

9.3.2 Aufzeichnung von Telefongesprächen in Call-Centern aus Sicht der Mitarbeiter

Auch im Hinblick auf die Rechte der Beschäftigten in den Call-Centern bestehen für das Aufzeichnen und Mithören von Telefongesprächen klare Grenzen.

§ 32i des Gesetzentwurfs der Bundesregierung zu einem Gesetz zur Regelung des Beschäftigtendatenschutzes vom Dezember 2010 (BT-Drs. 17/4230) sah in diesem Zusammenhang Folgendes vor:

§ 32i

Nutzung von Telekommunikationsdiensten

(1) Soweit dem Beschäftigten die Nutzung von Telekommunikationsdiensten ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubt ist, darf der Arbeitgeber bei dieser Nutzung anfallende Daten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist zur Gewährleistung des ordnungsgemäßen Betriebs von Telekommunikationsnetzen oder Telekommunikationsdiensten, einschließlich der Datensicherheit, zu Abrechnungszwecken oder zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskontrolle und soweit keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Beschäftigten an einem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegen. Werden nach Satz 1 Nummer 3 erhobene Daten einem bestimmten Beschäftigten zugeordnet, ist dieser über eine Verarbeitung und Nutzung zu unterrichten, sobald der Zweck der Verarbeitung oder Nutzung durch die Unterrichtung nicht mehr gefährdet wird.

(2) Inhalte einer ausschließlich zu beruflichen oder dienstlichen Zwecken erlaubten Nutzung von Telefondiensten darf der Arbeitgeber nur erheben, verarbeiten und nutzen, soweit dies zur Wahrung seiner berechtigten Interessen erforderlich ist und der Beschäftigte und seine Kommunikationspartner im Einzelfall vorher darüber informiert worden sind und darin eingewilligt haben. Ist die ausschließlich zu beruflichen oder dienstlichen Zwecken erbrachte telefonische Dienstleistung wesentlicher Inhalt der geschuldeten Arbeitsleistung, darf der Arbeitgeber Inhalte dieser Nutzung ohne Kenntnis des Beschäftigten im Einzelfall zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskon-

trolle erheben, verarbeiten und nutzen, wenn der Beschäftigte in geeigneter Weise vorab darüber informiert worden ist, dass er in einem eingegrenzten Zeitraum mit einer Kontrolle zu rechnen hat, und die Kommunikationspartner des Beschäftigten über die Möglichkeit der Erhebung, Verarbeitung und Nutzung informiert worden sind und darin eingewilligt haben.

Der Arbeitgeber hat den Beschäftigten unverzüglich über die Erhebung, Verarbeitung und Nutzung der Inhaltsdaten nach Satz 2 zu unterrichten.

Diese Vorschrift ist zwar nicht in Kraft getreten⁶⁵; sie gibt jedoch den aktuellen Stand der arbeits- und datenschutzrechtlichen Rechtsprechung und Literatur zur Auslegung des § 32 BDSG im Zusammenhang mit der Aufzeichnung dienstlicher Telefongespräche wieder.

Das bedeutet, dass ein Aufzeichnen und eine spätere Auswertung bzw. ein Abhören der aufgezeichneten Gespräche zum Zweck einer Verhaltens- und Leistungskontrolle zum einen zulässig ist

- während der Anlernphase von Mitarbeitern und danach
- nur stichprobenartig oder anlassbezogen, d. h. im Fall konkreter Kundenbeschwerden oder bei Anhaltspunkten für offensichtliche Qualitätsmängel bei einzelnen Mitarbeitern in einem eingegrenzten Zeitraum. Im Fall stichprobenartiger Kontrollen sind von der verantwortlichen Stelle konkrete Zahlenobergrenzen hierfür festzulegen (z. B. 3 % aller geführten Gespräche oder 30 Gespräche im Monat).

Darüber hinaus ist ein berechtigtes Interesse des Arbeitgebers anzuerkennen, Telefongespräche zum Zwecke der Gewinnung von Schulungsmaterial aufzuzeichnen oder auszuwerten. Aufzeichnungen zu diesem Zweck sind jedoch nur so lange zulässig, bis der Arbeitgeber genügend Schulungsmaterial zusammengestellt hat und können daher keine unbegrenzte und unbefristete Aufzeichnung von Telefongesprächen rechtfertigen. Die Aufzeichnung von Telefongesprächen muss zudem offen geschehen, d. h. die Arbeitnehmer sind grundsätzlich im Einzel-

⁶⁵ vgl. hierzu 30. Tätigkeitsbericht 2010/2011, LT-Drs. 15/955, S. 24 f.

32. Tätigkeitsbericht 2014/2015 - 9. Datenschutz in der Arbeitswelt

fall vor jeder Aufzeichnung hierüber zu informieren. Ausnahmsweise kann (entsprechend der Regelung in § 32i Absatz 2 Satz 2 des o. g. Entwurfs) eine Vorabinformation des Arbeitgebers, dass der Arbeitnehmer in einem eingegrenzten Zeitraum mit Kontrollen zu rechnen hat, genügen. Auch dies gilt jedoch nur im Fall stichprobenartiger oder anlassbezogener Leistungs- oder Verhaltenskontrollen.

Ausnahmsweise können *Beweisinteressen* der verantwortlichen Stelle ein dauerhaftes Aufzeichnen von Telefongesprächen rechtfertigen. Dies setzt jedoch voraus, dass ein *überwiegendes Beweisinteresse des Arbeitgebers* besteht, welches nur dann anzuerkennen ist, wenn telefonisch etwa ausschließlich oder weit überwiegend zivilrechtliche Verträge von nicht unerheblicher finanzieller Bedeutung abgeschlossen werden, über die es nachträglich erfahrungsgemäß häufig zu Streit kommt (etwa Telefonbanking).

Die Vereinbarung von Terminen mit Kunden, deren Beratung oder sonstiger telefonischer Kundenservice begründet grundsätzlich *kein* entsprechendes überwiegendes Beweisinteresse des Arbeitgebers. Außerdem besteht in solchen (Ausnahme-)Fällen grundsätzlich eine Zweckbindung, d.h. die Gespräche dürfen nur soweit abgehört und ausgewertet werden, wie das Beweisinteresse des Arbeitgebers – etwa zur Geltendmachung zivilrechtlicher Ansprüche gegenüber Kunden – dies *unabweisbar* erfordert. Nutzungen der Aufzeichnungen zu anderen Zwecken – etwa dem einer Verhaltens- und Leistungskontrolle der Mitarbeiter – sind nur unter den oben dargelegten Voraussetzungen, d.h. insbesondere nur stichprobenartig oder anlassbezogen, d. h. im Fall konkreter Beschwerden im Einzelfall, zulässig.

Der Umfang der Aufzeichnung und Auswertung von Telefongesprächen sowie der oder die damit verfolgte(n) Zweck(e) und die Speicher- und Lösungsfristen für Aufzeichnungen sind stets vorab schriftlich festzulegen.

Einwilligungen der betroffenen Arbeitnehmer in das Mithören oder Aufzeichnen in einem darüber hinausgehenden Umfang können eine entsprechende Datenerhebung *nicht* rechtfertigen. Dies folgt bereits aus der zumeist fehlenden Freiwilligkeit von Einwilligungen, die Arbeitnehmer im Arbeitsverhältnis abgeben.

Das Aufzeichnen und Mithören von Telefongesprächen in Call-Centern nimmt leider überhand – auf Kosten der Kunden und Beschäftigten der Call-Center. Ich werde daher die Kontrollen in diesem Bereich ausweiten. Denn es wäre meines Erachtens eher ein Ausdruck des Service- und Qualitätsgedankens eines Unternehmens, das Aufzeichnen und Mithören von Telefongesprächen auf ein datenschutzrechtlich gebotenes Mindestmaß zu reduzieren.

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

10. Datenschutz in der Wirtschaft**10.1 Datenschutzrechtliche Anforderungen an E-Mail-Werbung: Eine konkrete Anleitung mit Formulierungsvorschlägen für die Praxis**

Regelmäßig wenden sich Beschwerdeführer wegen unerwünschter E-Mail-Werbung an mich. Zwar scheint es sich inzwischen allgemein herumgesprochen zu haben, dass bei der Anmeldung zum Beispiel für einen Newsletter eine gesonderte Einwilligung einzuholen und darüber hinaus das sogenannte „Double-Opt-in-Verfahren“ dringend zu empfehlen ist (siehe 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Kapitel 10.2, S. 131 f.). Dennoch fällt auf, dass seitens der Unternehmen häufig durch Pflichtfelder zum Ankreuzen sowie durch eine unzulässige Vermischung von Allgemeinen Geschäftsbedingungen und Datenschutzerklärung eine – vermeintliche – Zulässigkeit von E-Mail-Marketing konstruiert wird. Dem will ich mit diesem Überblick und einigen konkreten Hilfestellungen begegnen.

Für E-Mail-Werbung sind aus datenschutzrechtlicher Sicht im Wesentlichen die folgenden drei Gesetze heranzuziehen:

- **Telemediengesetz (TMG)**

Werbe-E-Mails, Newsletter und ähnliche elektronische Informationsdienste sind nach § 1 Absatz 1 Satz 1 TMG Telemedien.

- **Bundesdatenschutzgesetz (BDSG)**

Das Bundesdatenschutzgesetz ist auf die sogenannten Inhaltsdaten anzuwenden, z. B. auf Bestellhistorien oder Anschriftendaten, die in die Auswahl oder die Gestaltung der Werbung einfließen. Zudem ist § 28 Absatz 3 bis 3b BDSG als Spezialvorschrift für werblichen Umgang mit personenbezogenen Daten zumindest überall dort anzuwenden, wo das Telemediengesetz nichts regelt. Da E-Mail-Adressen (ebenso wie die Telefonnummer) nicht zu den sogenannten Listendaten zählen, fällt E-Mail-Werbung allerdings nicht unter das Listenprivileg nach § 28 Absatz 3 Satz 2 BDSG.

- **Gesetz gegen den unlauteren Wettbewerb (UWG)**

Werbung ist Teil des Wettbewerbs und hat im Fall von E-Mail-Marketing direkte Auswirkungen auf die Verbraucher und ihre Rechte; zudem hat der deutsche Gesetzgeber einige Vorgaben aus dem europäischen Datenschutzrecht statt im deutschen Datenschutzrecht im deutschen Wettbewerbsrecht umgesetzt (siehe Kapitel 10.1.1). Auch der Grundsatz des Einwilligungsvorbehalts mit nur einem sehr eingeschränkten Privileg für Eigenwerbung ist hier verankert.

Zugegebenermaßen ist das gesetzliche Regelwerk für E-Mail-Marketing nicht ganz übersichtlich gelungen. Das ist, wie schon aus den anzuwendenden Gesetzen hervorgeht, vor allem der Tatsache geschuldet, dass dieser Bereich an einer Schnittstelle zwischen Wettbewerbsrecht (Potential zur Belästigung) und Datenschutzrecht (Gebrauch von personenbezogenen Daten) liegt.

Entsprechend vielfältig, aber auch uneinheitlich sind die möglichen Rechtsfolgen für datenschutzwidriges E-Mail-Marketing. Sie reichen von Bußgeldtatbeständen nach § 16 TMG und § 43 BDSG für verschiedene Einzelaspekte bis zu zivilrechtlichen Unterlassungsansprüchen nach § 8 UWG (in der Praxis vor allem per Abmahnung durchgesetzt).

10.1.1 Grundsatz für E-Mail-Marketing: Nur mit vorheriger, informierter und ausdrücklicher Einwilligung der betroffenen Person zulässig

Werbung per E-Mail, SMS oder MMS – wettbewerbsrechtlich unter dem Begriff „elektronische Post“ zusammengefasst – hat immer auch das Potential zur unzumutbaren Belästigung. Entsprechend ist sie in § 7 Absatz 1 Satz 1, Absatz 2 Nummer 3 UWG streng geregelt und – abgesehen von einer Ausnahme – nur mit ausdrücklicher und vorheriger Einwilligung des Betroffenen erlaubt (sog. „Opt-in“).

§ 7 UWG – Unzumutbare Belästigungen

(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. ...

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

(2) Eine unzumutbare Belästigung ist stets anzunehmen

...

3. bei Werbung unter Verwendung einer automatischen Anrufmaschine, eines Faxgerätes oder elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt

...

Dieses wettbewerbsrechtliche Verbot schlägt auch auf die datenschutzrechtliche Bewertung durch. Bei Werbe-E-Mails, Newslettern u. Ä. handelt es sich um – nicht vertraglich vereinbarte – Telemediendienste, für die folglich die Vorgaben von §§ 12 und 15 TMG gelten; mangelt es schon an der wettbewerbsrechtlichen Zulässigkeit der Werbemaßnahme an sich, kann weder von einer Einwilligung (§ 12 TMG) noch von einer gewollten „Inanspruchnahme“ dieses Informationsdienstes durch die angesprochene Person (§ 15 TMG) die Rede sein, so dass auch für die zugehörige Verwendung personenbezogener Daten keine Erlaubnis besteht. Übrigens: Auch Kundenzufriedenheitsabfragen sind Werbung. Entsprechende E-Mails sind daher ohne vorherige Einwilligung unzulässig.

10.1.2 Formale Anforderungen an die Einwilligung:
Abbestellbarkeit, Protokollierung und Abrufbarkeit

Schriftliche oder elektronische Erklärung

Die Einwilligung kann insbesondere schriftlich erfolgen (z. B. im Bestellformular, das einem Katalog beiliegt, oder in Anträgen für die Kundenkarte, die im Ladengeschäft ausliegen) oder auch elektronisch. Im letzteren Fall müssen die formalen Anforderungen von § 13 Absatz 2 und 3 TMG (fast gleichlautend § 28 Absatz 3a Satz 1 BDSG) eingehalten werden, damit die Einwilligung wirksam ist:

§ 13 TMG – Pflichten des Diensteanbieters

...

(2) Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

- 1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,*

...

- 4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.*

(3) Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. ...

Das bewusste und eindeutige Erteilen der Einwilligung ist beim gesonderten Opt-in mit sauberem Einwilligungstext automatisch sichergestellt.

Widerrufsmöglichkeit

Die Möglichkeit zum jederzeitigen Widerruf der Einwilligung (§ 13 Absatz 2 Nummer 4 TMG) wird sinnvollerweise durch einfache technische Optionen zum jederzeitigen Beenden der Nutzung geschaffen (§ 13 Absatz 4 Nummer 1 TMG, siehe Unterabschnitt 10.1.2). Aber auch „formlose“, also etwa per E-Mail oder Brief an den Kundenservice gerichtete Widersprüche, müssen in jedem Fall beachtet werden.

Protokollierung und Abrufbarkeit

Eine elektronische Einwilligung nach § 13 Absatz 2 TMG (ebenso auch nach § 28 Absatz 3a BDSG) wird in Onlineshops der Regelfall sein. Damit sie wirksam ist, muss sie von der verantwortlichen Stelle in jedem einzelnen Fall protokolliert und so aufbereitet werden, dass ihr genauer Inhalt jederzeit abrufbar ist.

§ 13 TMG

Pflichten des Diensteanbieters (Fortsetzung)

(1) ... Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

(2) Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

...

- 2. die Einwilligung protokolliert wird,*

- 3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann ...*

...

- (3) Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. Absatz 1 Satz 3 gilt entsprechend.*

- (4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass*

- 1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,*

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

...

(8) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

Beim gängigen und datenschutzrechtlich gebotenen **Double-Opt-in-Verfahren**⁶⁶ sind diese Voraussetzungen leicht erfüllt.

Die Protokollierung nach Nummer 2 gehört bereits zu einem sauberen Double-Opt-in-Verfahren. Entscheidend ist hier, dass in der zweiten, der „Bestätigungsmail“, der vollständige Einwilligungstext und die Widerrufsbelehrung enthalten sind. Dann stehen dem Nutzer der Inhalt der Einwilligung und die Widerrufsbelehrung in seinem E-Mail-Postfach (und von dort aus problemlos an jedem Speicherort seiner Wahl) rund um die Uhr zur Verfügung, sind also jederzeit abrufbar im Sinne von § 13 Absatz 2 Nummer 3 TMG.

Eine andere Möglichkeit, die jederzeitige Abrufbarkeit zu gewährleisten, sind Einwilligungen samt Widerrufsbelehrung innerhalb eines **Kundenkontos**. Dort können dann bei jedem Login die individuell erteilten Einwilligungen angezeigt und Widerruf direkt entgegengenommen werden.

Die Möglichkeit zum jederzeitigen Beenden der Nutzung (§ 13 Absatz 4 Nummer 1 TMG) wird technisch am einfachsten und sichersten durch einen Abbestelllink in jeder Werbe-E-Mail bzw. die Möglichkeit zur Abwahl der entsprechenden Einwilligungen im Kundenkonto eröffnet.

Neben den Inhalten müssen auch die (z. B. aus Nachweisgründen) hinzugespeicherten Daten wie der Zeitpunkt der Erklärung und ggf. seine zugehörige IP-Adresse dem Nutzer auf Verlangen zumindest auf dem Weg der Auskunft nach § 13 Absatz 8 TMG bzw. § 34 Absatz 1 BDSG mitgeteilt werden können. Das fällt aber unter die allgemeine datenschutzrechtliche Auskunftspflicht und gehört nicht

⁶⁶ siehe 31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Abschnitt 10.2, S. 131 f.

mehr zu den Wirksamkeitsvoraussetzungen der elektronisch erklärten Einwilligung.

10.1.3 Inhaltliche Anforderungen an die Einwilligung

Die folgenden Musterformulierungen und -gestaltungen habe ich im Rahmen meiner Beratungstätigkeit aus dem offensichtlichen Bedarf im Onlinebereich heraus entwickelt. Der Vollständigkeit halber habe ich die wettbewerbsrechtlichen Formulierungen für die ebenfalls streng geregelte Werbung per Telefonanruf gleich mit aufgenommen.

Die Muster sind natürlich auch für schriftliche Einwilligungserklärungen (z. B. vor Ort im Geschäft) anwendbar.

- Einfaches Musterformular für das Unternehmen XY, das auf allen „klassischen“ Kanälen **allgemeine Eigenwerbung** schalten möchte

[] Ja, ich möchte vom Unternehmen XY unter meiner oben angegebenen
[] E-Mail-Adresse
[] Telefonnummer per SMS
[] Telefonnummer per Anruf durch eine/n Servicemitarbeiter/in
über Neuigkeiten und interessante Angebote informiert werden.

Ich habe zur Kenntnis genommen, dass ich jede Einwilligung in die Verwendung meiner Daten für Werbung jederzeit widerrufen kann, z. B. [soweit jeweils angeboten] in meinem Kundenkonto unter „Meine Einwilligungen“, schriftlich an <Anschrift der X GmbH>, per E-Mail an <E-Mail-Adresse>, durch Anklicken des Abmeldelinks am Ende jeder Werbe-E-Mail oder telefonisch unter <Telefonnummer>.

Einwilligungen in Weitergaben für Werbezwecke an dritte Unternehmen müssen ebenso konkret und ausdrücklich eingeholt werden. Diese Dritten und die jeweiligen Kanäle, die diese für ihre Werbung nutzen werden, sind dabei möglichst genau zu benennen.

- Differenziertes Musterformular für das Unternehmen XY, das seine Kunden und Interessenten auf allen „klassischen“ Kanälen zu verschiede-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

denen Produktbereichen möglichst gezielt ansprechen möchte

Ja, ich möchte, dass mich das Unternehmen XY künftig unter meiner oben angegebenen

- E-Mail-Adresse
- Telefonnummer per SMS
- Telefonnummer per Anruf durch eine/n Servicemitarbeiter/in kontaktiert, um mich

über ihr gesamtes Angebot zu informieren

über ihre Angebote aus dem Bereich / den Bereichen (bitte auswählen)

- Gartenbedarf
- Spielwaren
- Bücher

zu informieren.

zu meiner Zufriedenheit mit seinem Service zu befragen.

Ich habe zur Kenntnis genommen, dass ich jede Einwilligung in die Verwendung meiner Daten für Werbung jederzeit widerrufen kann, z. B. [soweit jeweils angeboten] in meinem Kundenkonto unter „Meine Einwilligungen“, schriftlich an <Anschrift des Unternehmens XY GmbH>, per E-Mail an <E-Mail-Adresse>, durch Anklicken des Abmeldelinks am Ende jeder Werbe-E-Mail oder telefonisch unter <Telefonnummer>.

Auch hier müssen Einwilligungen in die Weitergabe für Werbezwecke an dritte Unternehmen ebenso konkret und ausdrücklich eingeholt werden. Diese Dritten, die jeweiligen Kanäle, die diese für ihre Werbung nutzen werden, und die jeweils übermittelten Datenarten sind dabei möglichst genau zu benennen.

Ergänzende Hinweise

Wenn für E-Mail-Werbung das Double-Opt-in-Verfahren angewandt wird⁶⁷, sollte dies wie folgt ergänzt werden (für SMS-Werbung ggf. entsprechend):

⁶⁷ Für Telefonwerbung wäre das Double-Opt-in-Verfahren denkbar ungeeignet (so auch BGH, Urteil „Double-opt-in-Verfahren“ vom 10. Februar 2011, Az. I ZR 164/09)

Um Ihre E-Mail-Adresse und diese Einwilligung zu bestätigen, wird Ihnen zunächst eine gesonderte E-Mail zugehen. Wir werden Ihre Einwilligung erst registrieren, wenn Sie den in dieser E-Mail enthaltenen Bestätigungslink angeklickt haben.

Exkurs: Für postalische Werbung gilt: Die in den Mustern abgedruckten Einwilligungsoptionen sind die datenschutz- und nutzerfreundlichere Variante und würden im zweiten Muster zudem erlauben, sich die Erlaubnis für fast alle gewünschten Datenarten zu holen, soweit diese dort konkret benannt sind. Wenn für postalische Werbung stattdessen auf das Listenprivileg nach § 28 Absatz 3 Satz 2 ff. BDSG zurückgegriffen werden soll, sollte ein Hinweis wie der folgende angefügt werden und ein zusätzliches (verwirrendes und rechtsunsicheres) Abfragen einer Einwilligung ohne triftigen Grund unbedingt unterbleiben:

Wir weisen Sie darauf hin, dass wir <verwendete Datenarten, z. B. „Ihren Namen samt Anrede und Ihre Anschrift“> für postalische Werbung (z. B. das Zusenden von unseren Prospekten) im Rahmen der gesetzlichen Erlaubnisse auch ohne Ihre ausdrückliche Zustimmung <beabsichtigte Verwendungen, z. B. „speichern, nutzen und an die Konzernzentrale übermitteln“>.

*Einer solchen Verwendung Ihrer Daten zu Werbezwecken können Sie jederzeit unter den oben angegebenen Kontaktdaten widersprechen.*⁶⁸

10.1.4 Eine Einwilligung in E-Mail-Werbung durch das pauschale Akzeptieren von „Kleingedrucktem“ ist unwirksam

Zwischenzeitlich ist unstrittig, dass eine (wettbewerbsrechtliche) Einwilligung in E-Mail-Werbung auch durch das Ankreuzen einer entsprechend konkret vorformulierten Erklärung wirksam erteilt wer-

⁶⁸ Diese Hinweise nach § 4 Absatz 3 und § 28 Absatz 4 Satz 2 BDSG würden theoretisch auch in der Datenschutzerklärung des Onlineshops genügen. Um Irritationen und Beschwerden vorzubeugen, empfehlen sie sich aber an dieser Stelle, damit der Nutzer auf einen Blick alles erfassen kann, was ggf. an Werbung auf ihn zukommt.

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

den kann.⁶⁹ Diese Einwilligung muss in jedem Fall separat von allen anderen Erklärungen abgegeben (oder eben verweigert) werden können, um wirksam zu sein.

Zwar sieht der Wortlaut von § 7 Absatz 2 Nummer 3 UWG nicht ausdrücklich vor, dass für die Erteilung der Einwilligung eine gesonderte Erklärung erforderlich ist. Dies ergibt sich aber – so der Bundesgerichtshof in ständiger Rechtsprechung⁷⁰ – aus der Datenschutzrichtlinie für elektronische Kommunikation⁷¹. Dieser zufolge kann „die Einwilligung in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website“ (Erwägungsgrund 17).

Die Formulierung „spezifische Angabe“ mache dabei deutlich, dass eine gesonderte, nur auf die Einwilligung in die Zusendung von Werbung mittels elektronischer Post bezogene Zustimmungserklärung des Betroffenen erforderlich sei. Folglich sei für die Einwilligung in die Zusendung von Werbung mittels elektronischer Post eine Zustimmungserklärung erforderlich, die durch eine spezifische Angabe und eine gesonderte Erklärung durch zusätzliche Unterschrift oder individuelles Markieren eines entsprechenden Feldes zum Ausdruck kommen muss.

Die Einwilligung zusammen mit der Akzeptanz der übrigen Allgemeinen Geschäftsbedingungen (AGB) oder der übrigen Datenschutzbestimmungen wirksam einzuholen, ist demnach nicht möglich; die Entscheidung wäre dann nicht hinreichend frei. Zudem bedeutet eine Einfügung der Einwilligungserklärung in die pauschalen AGB in aller Regel ohnehin faktisch eine „Pflichteinwilligung“, da das Unternehmen die Bestellung wohl erst gar nicht annehmen würde, wenn die AGB nicht akzeptiert wurden.

Auch eine Ausgestaltung als „Streichklausel“ (etwa: „Wenn Sie diese Einwilligung in E-Mail-Werbung nicht erteilen möchten, streichen Sie bitte diese Klausel.“ oder „... setzen Sie bitte hier ein Häkchen.“) oder als nicht verpflichtende, aber vorkreuzte Einwilligung hilft nicht weiter; solche (Opt-out-)Einwilligungen sind wettbewerbsrechtlich und in der Folge datenschutzrechtlich ebenfalls unwirksam.⁷²

Übrigens wäre es auch nicht ausreichend, Einwilligungen in mehrere oder alle der in § 7 Absatz 2 UWG aufgezählten Werbeformen zwar freiwillig und separat vom Rest des Vertrages, aber untereinander zusammengefasst abzufragen. Die verschiedenen Kanäle müssen einzeln angewählt werden können⁷³, siehe hierzu auch die Muster in Kapitel 10.1.3.

10.1.5 Eine Einwilligung in Werbung per E-Mail durch erzwungenes Opt-in (Einwilligung als separates Pflichtfeld) ist unwirksam

Oft ist die Einwilligung in E-Mail-Werbung zwar als separates Ankreuzfeld ausgestaltet, aber so, dass ohne das Setzen dieses Häkchens der Bestellvorgang nicht fortgesetzt werden kann. Auch auf diese Weise wird keine wirksame Einwilligung eingeholt.

In E-Mail-Werbung einzuwilligen, um überhaupt den Vertrag abschließen zu können, ist generell kein Ausdruck einer hinreichend freien Entscheidung. Wenn der Betroffene diese „Einwilligung“ gesondert widerrufen müsste, würde die Initiative zur Wiederherstellung der ungestörten Privatsphäre vielmehr in unangemessener Weise einseitig auf ihn verlagert.⁷⁴

In dieser Ausgestaltung handelt es sich im Wesentlichen um eine spezielle Form der Zustimmung zu AGB, so dass das in Kapitel 10.1.4 zur Einwilligung im „Kleingedruckten“ Dargelegte auch hier gilt; die Entscheidung des Kunden ist nicht hinreichend frei.

⁶⁹ z. B. BGH, Urteil „Einwilligung in Werbeanrufe II“ vom 25. Oktober 2012, Az. I ZR 169/10, Rn. 21

⁷⁰ vgl. insbesondere das „Payback-Urteil“ vom 16. Juli 2008, Az. VIII ZR 348/06, Rn. 28

⁷¹ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

⁷² BGH, Urteil vom 16. Juli 2008, Az. VIII ZR 348/06, Rn. 27 („Payback“)

⁷³ BGH, Beschluss vom 14. April 2011, Az. I ZR 38/10, Rn. 9

⁷⁴ BGH, Urteil vom 24. März 1999, Az. IV ZR 90/98, Rn. 59

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

10.1.6 Eine formal korrekte, aber zu wenig konkrete Einwilligung in E-Mail-Werbung ist unwirksam

Soweit der Kunde aufgrund der Unbestimmtheit der Beschreibungen nicht nachvollziehen kann, welchen Umfang seine Einwilligung hat, ist diese wegen unangemessener Benachteiligung des Verbrauchers gem. § 307 Abs. 1 BGB unwirksam.

Um wettbewerbs- und datenschutzrechtlich überhaupt wirksam sein zu können, muss eine Einwilligung für den konkreten Fall und in Kenntnis der Sachlage erfolgen. Der Verbraucher muss wissen, dass seine Erklärung ein Einverständnis darstellt und worauf sie sich bezieht. Die Einwilligung erfolgt dann für den konkreten Fall, wenn klar wird, welche Produkte oder Dienstleistungen welcher Unternehmen sie konkret erfasst.⁷⁵

Drei häufig zu beobachtende Wendungen, die jede für sich in aller Regel schon zur Unwirksamkeit führen, beschreiben die Weitergabe „Ihrer [nicht näher bezeichneten] Daten“ „für Zwecke der Werbung [über nicht näher bezeichnete Kanäle]“ „an [nicht näher bezeichnete] befreundete oder Partner-Unternehmen“.⁷⁶ Ausreichend informiert ist der Betroffene nur, wenn konkret dargelegt wird, welche Daten an welches Unternehmen weitergegeben werden.

10.1.7 Ausnahme vom Einwilligungserfordernis: Privileg des § 7 Absatz 3 UWG – aber nicht ohne Opt-out-Möglichkeit

Die einzige Ausnahme vom Einwilligungserfordernis ist in § 7 Absatz 3 UWG beschrieben:

§ 7 UWG – Unzumutbare Belästigungen

...

(3) Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn

1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem

Kunden dessen elektronische Postadresse erhalten hat,

2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,

3. der Kunde der Verwendung nicht widersprochen hat und

4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Dieses Privileg habe ich anlässlich eines Einzelfalles bereits früher behandelt (31. Tätigkeitsbericht 2012/2013, LT-Drs. 15/4600, Kapitel 10.4, S. 138 ff.) und verweise daher für Einzelheiten auf die dortigen Ausführungen.

Auch hier gilt also zunächst die Grundregel, dass für jeden Kanal, der von Gesetzes wegen privilegiert (d. h. ohne Einwilligung) für Werbung genutzt werden darf und soll, eine Widerspruchsbelehrung nötig ist.

Zu ergänzen ist an dieser Stelle allerdings noch, wie das **Opt-out** nach § 7 Absatz 3 Nummer 4 UWG ausgestaltet werden muss. Da der Kunde beim Bestellvorgang im Internet seine E-Mail-Adresse meist im Rahmen eines Pflichtfelds angeben muss, um überhaupt bestellen zu können (z. B. als Adresse für die Bestellbestätigung), führt dies oft dazu, dass ein Unternehmen ohne jede Wahlfreiheit des Kunden ihn zunächst per E-Mail bewirbt, bis sein Widerspruch (z. B. per Abmeldelink in der ersten Werbe-E-Mail) angekommen und „aus technischen Gründen innerhalb von bis zu zwei Wochen“ umgesetzt ist. Dies ist jedoch **datenschutzwidrig**.

Der Kunde muss die Möglichkeit haben, dieser werblichen Nutzung seiner E-Mail-Adresse bereits zum Zeitpunkt der Erhebung seiner E-Mail-Adresse, also noch während des Bestellvorgangs im Online-shop, zu widersprechen. Dies gebietet Artikel 13 Absatz 2 der Datenschutzrichtlinie für elektronische Kommunikation; dieser sieht vor, dass der Kunde bereits bei der Erhebung der Daten die Möglichkeit haben muss, die Nutzung zum Zwecke der Werbung **von vornherein abzulehnen**. Entsprechend

⁷⁵ BGH, Urteil „Einwilligung in Werbeanrufe II“ vom 25. Oktober 2012, Az. I ZR 169/10, Rn. 24

⁷⁶ sehr instruktiv z. B. LG Berlin, Urteil vom 30. April 2015, Az. 15 O 92/12, zu einigen AGB von Apple

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

muss nicht nur die Möglichkeit zum Widerspruch nach § 7 Absatz 3 Nr. 4 UWG bereits bei der Erhebung der elektronischen Kontaktdaten technisch angeboten werden, sondern auch dessen sofortige Umsetzung noch vor dem Versand der ersten elektronischen Werbung technisch gewährleistet sein. Auf die Bestellung an sich darf diese Option keinen Einfluss haben.

Beispielsweise könnte folgende Formulierung in das Onlineformular an der Stelle, wo die E-Mail-Adresse eingetragen werden muss, aufgenommen werden:

** [] Ich habe zur Kenntnis genommen, dass es gesetzlich zulässig ist, dass mich das Unternehmen XY künftig auch ohne meine ausdrückliche Einwilligung per E-Mail über ähnliche eigene Angebote informieren darf wie die, die ich dort bereits bestellt habe. Ich weiß, dass ich dieser Verwendung meiner E-Mail-Adresse und meines Bestellverlaufs jederzeit widersprechen kann (z. B. unter oben genannten Kontaktdaten oder durch Ankreuzen gleich [] hier), ohne dass mir dafür mehr Kosten entstehen dürfen, als nach den Basis-Übermittlungstarifen ohnehin für die Kontaktaufnahme anfallen (z. B. für die Übermittlung meiner Widerspruchs-E-Mail).*

Damit die Unterrichtung sichergestellt ist, muss das mit dem Stern markierte Ankreuzfeld hier ein Pflichtfeld sein, d. h. ohne dass es angekreuzt wurde, darf der Bestellvorgang nicht fortgesetzt werden können. Es darf dann natürlich auch nicht vorangekreuzt sein.

Auch wenn die Gesetzeslage z. T. etwas unübersichtlich und unklar geraten sein mag, existieren mittlerweile aufgrund der Rechtsprechung des Bundesgerichtshofs doch erfreulich klare Vorgaben für E-Mail-Marketing. Da diese allerdings über mehrere Einzelfallurteile und deren umfangreiche Begründungstexte verstreut sind und zudem noch nicht alle Fragen restlos beantworten, halte ich – neben der aufsichtsrechtlichen Kontrolle und der „Selbstregulierung“ durch zivilrechtliche Abmahnungen – den Ansatz, Positivbeispiele vorzugeben, für einen geeigneten Weg, um möglichst allen interessierten Unternehmen Orientierung und Rechtssicherheit beim Marketing zu bieten.

10.2 Übermittlung der E-Mail-Adresse eines Kunden durch einen Online-Versandhändler an ein Logistik- oder Postunternehmen nur mit vorheriger Einwilligung zulässig

Zu Servicezwecken geben immer häufiger Online-Versandhandelsunternehmen neben Namen und Anschrift auch die E-Mail-Adresse des Kunden an die beauftragten Logistik- und Postunternehmen weiter, ohne ihn darüber zu informieren oder gar zuvor seine Einwilligung hierfür einzuholen. Für die datenschutzrechtliche Zulässigkeit ist es jedoch wichtig, dass die Versandhändler ihren Informationspflichten nachkommen und den Betroffenen selbst die Wahl lassen, ob sie vom Serviceangebot des Logistik- oder Postunternehmens, insbesondere der Möglichkeit der Sendungsverfolgung, Gebrauch machen wollen – oder eben nicht.

Im Berichtszeitraum erreichten meine Dienststelle mehrere Beschwerden bezüglich der Weitergabe auch der E-Mail-Adresse des Kunden durch Online-Versandhandelsunternehmen an Logistik- und Postunternehmen. Die Weitergabe erfolgte, so die Versandhändler, um die Servicequalität zu erhöhen und es den Kunden auf diese Weise zu erleichtern, sich über den Verbleib ihrer bestellten Ware und den stundengenauen Auslieferungszeitpunkt laufend informieren zu können. Bei der sogenannten Sendungsverfolgung und Paketankündigung werden – neben dem Namen und der Anschrift – auch die E-Mail-Adressen der Kunden durch den Online-Versandhändler automatisch an das jeweils beauftragte Logistik- oder Postunternehmen übermittelt. Die Kunden erhalten anschließend eine E-Mail des Logistik- oder Postunternehmens mit einem Link, durch den sie den aktuellen Versandstatus nachverfolgen können. Oft werden auch alternative Paketabgabemöglichkeiten angeboten, wenn man zum anvisierten Zustellzeitpunkt nicht zuhause sein sollte.

Die Übermittlung des Namens und der Anschrift des Kunden an das beauftragte Unternehmen, das das Warenpaket zum Kunden bringen wird, ist unstrittig nach § 28 Absatz 1 Satz 1 Nr. 1 BDSG ohne vorherige Einwilligung des Kunden zulässig, da der korrekte Versand des Pakets an den richtigen Empfänger erforderlich ist, damit der Online-Versandhändler den Kaufvertrag erfüllen kann.

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

Anders verhält es sich aber bei der Weitergabe der E-Mail-Adresse des Kunden an das Logistik- oder Postunternehmen: § 28 Absatz 1 Satz 1 Nr. 1 BDSG greift hier nicht, da die Übermittlung der E-Mail-Adresse nicht erforderlich ist, damit die Ware ihren Weg zum Kunden findet.

Die Regelung des § 28 Absatz 1 Satz 1 Nummer 2 BDSG regelt die Zulässigkeit u. a. der Datenübermittlung als Mittel für die Erfüllung eigener Geschäftszwecke, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Da die Datenweitergabe in den vorliegenden Fällen nicht zwangsläufig für die Erfüllung eigener Geschäftszwecke der Online-Versandhändler erforderlich ist, kann aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG keine Erlaubnisnorm abgeleitet werden, zumal das schutzwürdige Interesse des Kunden, selbst über die Weitergabe seiner E-Mail-Adresse entscheiden zu können, überwiegt.

Da also eine gesetzliche Datenübermittlungsbefugnis ausscheidet, muss der Online-Versandhändler zuvor eine Einwilligung des Kunden nach § 4a BDSG einholen, da er sonst eine datenschutzwidrige Datenübermittlung begehen und den Bußgeldtatbestand des § 43 Absatz 2 Nr. 1 BDSG verwirklichen würde.

Erforderlich ist im Ergebnis ein informiertes Opt-in, also eine Checkbox, die der Kunde ankreuzen kann, wenn er in die Übermittlung seiner E-Mail-Adresse an das konkret genannte Logistik- oder Postunternehmen einwilligen möchte. Eine solche Einwilligungsoption kann problemlos in den Online-Bestellprozess eingebunden werden.

Die von meiner Dienststelle angeschriebenen Unternehmen haben ihren Bestellprozess inzwischen entsprechend umgestellt bzw. um eine datenschutzkonforme Einwilligungsmöglichkeit ergänzt.

Sicherlich kann es praktisch sein, den Versand des bestellten Pakets in Echtzeit online verfolgen zu können. Dies ändert aber nichts daran, dass es allein in der Entscheidung des Kunden liegt, ob der Online-Versandhändler seine E-Mail-Adresse an das Logistik- oder Postunternehmen übermitteln

darf. Für eine datenschutzrechtliche Zulässigkeit führt in diesen Fällen kein Weg an der vorherigen Einholung einer informierten und freiwilligen Einwilligung vorbei.

10.3 Kein finanzielles Risiko? Dann keine Bonitätsabfrage – auch nicht mit Einwilligung!

Seinen potentiellen Vertragspartner einzuschätzen, ist nie leicht. Und natürlich verlangt das Datenschutzrecht von keinem Online-Unternehmer, unnötige (Zahlungsausfall-)Risiken einzugehen, wenn wertvolle Ware auf die Reise geschickt wird. Aber nicht jede verkaufstaktisch motivierte Datenverarbeitung ist im Sinne des Datenschutzrechts.

In Onlineshops ist es mittlerweile die Regel, dass sich der Händler eine Bonitätsabfrage über den Kunden vorbehält, bevor er die Bestellung annimmt. Das ist gesetzlich, d. h. ohne Einwilligung des Kunden, in all den Fällen grundsätzlich erlaubt, in denen der Händler in Vorleistung geht, d. h. zuerst die Ware abschickt und dann hoffen muss, dass der Kunde auch zahlen kann. Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Kunden ist in diesem Fall nach § 28 Absatz 1 Satz 1 Nummer 2 BDSG durch das berechtigte Interesse des Händlers an einer Minimierung des Zahlungsausfallrisikos gedeckt. Das setzt allerdings voraus, dass für den Händler überhaupt ein Risiko eintritt, d. h. dass der Kunde bereits eine für den Händler riskante Zahlungsart, z. B. „Kauf auf Rechnung“ oder „Kauf auf Raten“, ausgewählt hat. Umgekehrt ist ein Risiko für den Händler nicht erkennbar, wenn der Kunde die Zahlungsart „Vorkasse“ oder „Sofortüberweisung“ wählen sollte.

Eine vorsorgliche Bonitätsabfrage über ausnahmslos jeden Kunden, noch bevor er sich für eine unsichere Zahlungsart entschieden hat, also unabhängig von der Zahlungsart, findet dagegen keine gesetzliche Erlaubnis. Denn hier geht es nicht mehr um konkrete Risiken, die Ware wird dem Käufer schließlich erst nach erfolgter Zahlung übergeben. Will ein Händler aus irgendeinem Grund und unabhängig von der Zahlungsart über jeden potentiellen Vertragspartner eine Bonitätsauskunft einholen, könnte er daher auf die Idee kommen, eine ausdrückliche Einwilligung hierfür abzufragen, ohne die der Bestellvorgang nicht fortgesetzt werden kann:

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

§ 4 BDSG
*Zulässigkeit der Datenerhebung,
-verarbeitung und -nutzung*

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

...

Um allen Anforderungen an eine wirksame Einwilligung nachzukommen, verfasst er einen ausführlichen Einwilligungstext, der alle nach § 4a Absatz 1 Satz 2 BDSG erforderlichen Informationen enthält, und richtet im Formular ein eigenes Ankreuzfeld ein:

§ 4a BDSG
Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. ...

Auf die Frage nach der Freiwilligkeit (§ 4a Absatz 1 Satz 1 BDSG) antwortet der Händler, dass ja niemand gezwungen sei, ausgerechnet bei ihm zu bestellen; seine Waren seien alltägliche Produkte und könnten zudem auch in seinen Ladengeschäften gekauft werden. Zudem seien Bestellungen ohne Bonitätsabfrage telefonisch möglich. Und aus der Freiwilligkeit der (Online-)Bestellung folge natürlich die Freiwilligkeit dieser Einwilligung in die Bonitätsabfrage.

Auch bei einem baden-württembergischen Unternehmen war im Berichtszeitraum ein derartiges Verfahren zu finden. Als an sich plausible Motivation habe ich dabei kennengelernt, dass man dem Kunden eine möglichst große Palette an Zahlungsmöglichkeiten anbieten will, aber jeweils nur die, die der Händler ihm aufgrund seiner Bonität auch wirklich zugestehen wird. Daher erfolgt die Bonitätsabfrage vor Auswahl der Zahlungsart; so soll vermieden werden, dass Kunden eine unsichere Zahlungsart

auswählen, diese ihnen nach der anschließenden – zulässigen – Bonitätsprüfung ggf. wegen negativer Bonitätsauskunft wieder „weggenommen“ wird und sie verärgert den Kauf abbrechen.

Trotz dieser nachvollziehbaren Sorge ist aber hier, wo an die Stelle der Eindämmung konkreter Risiken Verkaufsstrategie und -psychologie treten, für eine Einwilligung über den o. g. gesetzlichen Rahmen hinaus kein Raum. Insbesondere folgende Erwägungen stehen aus meiner Sicht einer wirksamen Einwilligung entgegen:

■ **Wirtschaftliches Ungleichgewicht der Beteiligten – Frage nach der Freiwilligkeit**

Ein (Groß-)Unternehmen kann leicht auf den einzelnen Vertragsschluss verzichten, während die betroffene Person ihre möglicherweise zwingenden Gründe für diesen Weg des Kaufs schlicht nicht geltend machen kann.

■ **Umkehrung des gesetzgeberischen Willens – Frage nach Treu und Glauben**

Die Bonitätsabfrage würde vom gesetzlich erlaubten Zweck – der Minimierung des kreditrisikoreichen Risikos im Einzelfall – losgelöst und zum Instrument für massenhafte Datenerhebung und -verwertung – auch und gerade durch die angeschlossenen Auskunftsteile, die durch die zusätzlichen Abfragen vermutlich doppelt so viele personenbezogene Daten geliefert bekommen⁷⁷ und für ihre Zwecke weiterverwerten dürften. Der Kunde würde also keineswegs nur in eine rein passive Abfrage einwilligen, sondern zugleich vertragsfremde Auswirkungen etwa in Form von Score(neu)berechnungen in Kauf nehmen müssen, die wiederum seine künftige Teilhabe am Wirtschaftsleben beeinflussen werden.

■ **Offensichtliche Verfehlung des Zwecks – Frage nach der Eignung des Verfahrens**

Eine eventuelle Ablehnung der gewünschten Zahlungsart kann ohnehin schon deshalb nicht überraschend kommen, weil der Kunde bei der

⁷⁷ Nach einer Studie der IFH Institut für Handelsforschung GmbH (abrufbar unter <http://www.ifhkoeln.de/News-Press/Konsolidierung-im-Payment-Markt-Online-Haendler-bieten-im-S>) soll im deutschen Onlinehandel etwa jeder zweite Onlinekauf mit einer sicheren Zahlungsart einhergehen.

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

vorgezogenen Bonitätsabfrage nach § 6a Absatz 2 Nummer 2 BDSG vom Onlinehändler sogar ausdrücklich darüber informiert werden muss, dass ihm Zahlungsarten vorenthalten werden:

§ 6a BDSG
Automatisierte Einzelentscheidung

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

...

Auf diese Weise werden alle Kunden, deren Bonität dem Onlinehändler nicht für einen Vertrauensvorschuss genügt, mit einer unschönen Meldung konfrontiert, während beim gesetzlich erlaubten Verfahren nur diejenigen unter ihnen auf ihre „Defizite“ gestoßen werden, die auch tatsächlich eine unsichere Zahlungsart wählen.

Vor diesem Hintergrund habe ich ein aufsichtsrechtliches Verfahren eröffnet, das bis zur Erstellung dieses Berichtes noch nicht abgeschlossen war. Ich gehe aber davon aus, dass am Ende dieses Verfahrens eine datenschutzkonforme Lösung stehen wird.

Bonitätsabfragen und Scoreberechnungen sind für die Minimierung des konkreten kreditorischen Risikos gedacht und grundsätzlich vom Gesetz gedeckt. Darüber hinausgehende Anwendungen, etwa aus verkaufpsychologischen Motiven heraus, sind damit nicht vereinbar. Hier stößt auch das Instrument der Einwilligung an seine datenschutzrechtlichen Grenzen.

10.4 Die Suche nach dem Schuldner

Die Tätigkeit von Wirtschaftsauskunfteien beschäftigt die Datenschutzaufsichtsbehörden in immer neuen Fallkonstellationen.

Die Geschäftsidee von Wirtschaftsauskunfteien beruht darauf, dass Unternehmen bonitätsrelevante Informationen ihrer Geschäftspartner einmelden und andere Auskünfte zu der betreffenden Person einholen, dass also Wirtschaftsunternehmen von den Erfahrungen, die andere gemacht haben, profitieren können. Dementsprechend wurden wir auch im Berichtszeitraum mit Fällen befasst, in denen sich Unternehmen bei einer bestimmten Wirtschaftsauskunftei danach erkundigten, ob zu einer bestimmten Person eine negative Information zu deren Zahlungsverhalten bekannt ist. Nun war bei dieser Auskunftei zwar ein Datensatz vorhanden, dessen Identifizierungsdaten mit Ausnahme der Wohnanschrift den von der anfragenden Stelle angegebenen Grundpersonalien entsprachen. Völlig korrekt prüfte die Auskunftei, ob der Betroffene umgezogen ist und ob er früher an der von der anfragenden Stelle genannten Adresse wohnhaft war. Nachdem diese Ermittlungen positiv verlaufen waren, die Auskunftei sich also davon überzeugt hatte, dass es nicht um verschiedene Personen ging, beantwortete sie die Anfrage im Hinblick auf die finanzielle Bonität des Betroffenen. Doch nahm die Auskunftei ihre Ermittlungen zum Anlass, in ihrer Datei, aus der sie ihre Bonitätsauskünfte erteilt, den Hinweis aufzunehmen, dass der Betroffene „wohnsitzlos“ gewesen sei. In anderen Fällen wurde die anfragende Stelle ohne weitere Recherchen von der Auskunftei kurzerhand dahingehend beschieden, der Betroffene sei an der angegebenen Adresse „postalisch nicht erreichbar“.

Richtig ist, dass Wohnsitzlosigkeit oder generelle Nichterreichbarkeit einer Person ein sog. persönliches Bonitätsnegativmerkmal darstellen kann, das von den Wirtschaftsauskunfteien genauso wie nega-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

tive Angaben zur Zahlungsfähigkeit gespeichert und beaskunftet werden darf. Wer will schon mit einem Partner Geschäfte abschließen, dessen Aufenthaltsort unbekannt ist oder der vielleicht absichtlich untergetaucht ist, um sich Vollstreckungsmaßnahmen zu entziehen. Jedoch darf eine entsprechende Einmeldung bei einer Wirtschaftsauskunftei nur erfolgen, wenn die übermittelnde Stelle sicher ist, dass diese Voraussetzungen vorliegen. Der bloße Wohnungswechsel rechtfertigt ein solches Vorgehen, das den Betroffenen in Misskredit bringen kann, nicht. Vergleichbares gilt für die Auskunftei. Zwar darf diese sich grundsätzlich auf die Richtigkeit der von Dritten eingemeldeten Angaben verlassen. Dieses von der Rechtsprechung entwickelte Privileg greift aber dann nicht, wenn sich der Auskunftei Zweifel an der Richtigkeit der ihr übermittelten Angaben aufdrängen müssen, so dass sie vor einer Speicherung bzw. Beaskunftung eigene Recherchen vorzunehmen hat. Das ist insbesondere dann der Fall, wenn die von der anfragenden Stelle genannten Grundpersonalien und die bei der Auskunftei vorhandenen Daten nicht uneingeschränkt identisch sind. Stellt sich dabei heraus, dass der Betroffene, wenn auch inzwischen unter einer anderen Adresse, ohne weiteres erreichbar ist und nicht etwa seine Erreichbarkeit verschleiern wollte, darf die Auskunftei nicht gegenüber Dritten den Eindruck erwecken, dass das Gegenteil der Fall sei. Vermag die Auskunftei besagte Diskrepanz nicht aufzuklären, muss sie dem sich nach der Bonität erkundigenden Unternehmen mitteilen, dass zu der angefragten Person keine Angaben vorliegen.

Auskunfteien haben bei ihrer Geschäftstätigkeit aufgrund der ihnen eingeräumten Privilegien besondere Sorgfalt walten zu lassen, damit Betroffene nicht unnötig in Misskredit geraten.

10.5 Neues von der Rechtsprechung zum Scoring

Nach einer Entscheidung des Europäischen Gerichtshofs (EuGH NJW 2014, S. 1941) haben aufgrund der Europäischen Verbraucherkreditrichtlinie (RL 2008/48/EG Art. 8, 23) die Mitgliedsstaaten sicherzustellen, dass vor Abschluss eines Kreditvertrages die Kreditwürdigkeit des Verbrauchers anhand ausreichender Informationen zu seinem Schutz bewertet wird. Ob allerdings das in § 28b BDSG vorgesehene Scoringverfahren dafür geeig-

net ist, wird von den Datenschutzaufsichtsbehörden nach wie vor kritisch gesehen. Tatsache ist jedoch, dass die Regierungsparteien im Deutschen Bundestag eine Scoring-Reform derzeit ablehnen⁷⁸.

Allerdings hat die Rechtsprechung in den letzten Jahren wichtige Klarstellungen vorgenommen:

In seinem Urteil vom 28. Januar 2014 (BGH NJW 2014, S. 1235) hat der Bundesgerichtshof zwar entschieden, dass der Betroffene keinen Anspruch gegen eine Auskunftei auf Offenlegung der bei der Berechnung seines Scorewertes verwendeten Scoreformel, die herangezogenen statistischen Werte, die Gewichtung einzelner Bewertungselemente und die Bildung etwaiger Vergleichsgruppen habe. Damit sind auch Kreditgeber mangels Transparenz nicht in der Lage zu entscheiden, inwieweit sie den Berechnungsmethoden einer Auskunftei vertrauen können. Doch hat das Gericht die Rechte der Betroffenen insoweit gestärkt, als dass sie Auskunft darüber verlangen können, „welche personenbezogenen, insbesondere kreditrelevanten Daten in die ermittelten Wahrscheinlichkeitswerte eingeflossen sind“. Dadurch soll der Betroffene die Möglichkeit haben, auf die Korrektur fehlerhafter Daten zu drängen und infolge unzutreffenden Datenmaterials fehlerhaft errechnete Wahrscheinlichkeitswerte zu widerlegen. Daraus folgt, dass ein Scorewert nur rechtmäßig berechnet worden ist, wenn ausreichend viele Angaben zu den finanziellen Verhältnissen des Betroffenen und zu seinem Zahlungsverhalten im Verhältnis zu sonstigen Daten Berücksichtigung gefunden haben, dass keine Schätzdaten, die nicht auf ihre Richtigkeit hin überprüfbar sind, verwendet werden dürfen und dass die Mitteilung an den Betroffenen sich nicht lediglich auf die genutzten Datenarten (vgl. § 34 Absatz 4 Satz 1 Nr. 3 BDSG) beschränken darf. Das gilt auch für die Anschriftendaten i. S. des § 28b Nr. 3 BDSG.

Konsequenterweise hat das OLG Frankfurt/M. (ZD 2015, 335) entschieden, dass eine Scorewertberechnung jeglicher sachlicher Basis entbehre, wenn nur *ein* zutreffendes tatsächliches Merkmal der Berechnung zugrunde gelegt wird, daneben aber un-

⁷⁸ Es ist davon auszugehen, dass sich hieran auch durch den von der Bundestagsfraktion Bündnis 90/Die Grünen aktuell eingebrachten „Entwurf eines Zweiten Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Verbesserung der Transparenz und der Bedingungen beim Scoring“ (Scoringänderungsgesetz), BT-Drs. 18/4864, nichts ändern wird. Auf die Stellungnahmen der Sachverständigen bei der Anhörung vor dem Bundestagsninnenausschuss am 30. November 2015 wird verwiesen.

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

richtige Parameter miteinbezogen werden und wichtige relevante Tatsachen außen vor bleiben. Allerdings kommt das OLG München in einer anderen Entscheidung (ZD 2014, 570) zu der Auffassung, dass der Betroffene nicht verlangen könne, dass neben Daten, die nicht unmittelbar etwas über seine finanziellen Verhältnisse (z. B. Einkommens- und Vermögensverhältnisse) aussagen, solche zwingend in seine Scorewertberechnung Eingang finden müssen, wenn ein wissenschaftlich anerkanntes mathematisch-statistisches Gutachten bestätigt, dass die anderweitigen verwendeten Angaben die Berechnung eines korrekten Wahrscheinlichkeitswertes ermöglichen.

Insgesamt bleibt es bei der seit längerer Zeit gefestigten Rechtsprechung, dass eine unzutreffende Bonitätsauskunft einen Eingriff in das Persönlichkeitsrecht darstellt, dessen Unterlassung der Betroffene verlangen kann (LG München, ZD 2013, 135), doch muss er einen „schlechten“ Scorewert hinnehmen, wenn in seiner Person Bonitätsnegativmerkmale (z. B. nicht rechtzeitig beglichene Forderungen) vorliegen (vgl. BGH, Urt. v. 22.11.2011 – VI ZR 120/10 –; LG Oldenburg, Urt. v. 23.12.2009 – 5 O 1672/09 –).

10.6 Datenverarbeitung aufgrund einer Einwilligung

Das deutsche Datenschutzrecht wird durch das sog. Verbot mit Erlaubnisvorbehalt geprägt. Nach § 4 Absatz 1 BDSG ist danach die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, wenn es dafür eine gesetzliche Ermächtigung gibt oder der Betroffene in beachtlicher Weise eingewilligt hat. Letzteres resultiert aus dem verfassungsrechtlich geschützten Recht auf informationelle Selbstbestimmung. Jeder soll danach eigenverantwortlich entscheiden können, gegenüber wem er persönliche Angaben offenbaren will. Allerdings sehen das Gesetz und die von den Gerichten entwickelte Rechtsprechung zum Schutze des Betroffenen bestimmte Voraussetzungen vor, die erfüllt sein müssen, damit die Einwilligung wirksam ist. Danach gilt Folgendes:

- Einwilligen kann nur, wer ausreichend darüber **informiert** ist, was mit seinen Daten geschehen soll. Deshalb müssen die Betroffenen vor der Abgabe ihrer Einwilligungserklärung über die zu

verarbeitenden Daten, den Verarbeitungszweck bzw. die beabsichtigten Zweckänderungen und den Anlass für die weitere Datenverarbeitung unterrichtet werden. Ggf. muss auch klar sein, ob bzw. unter welchen Voraussetzungen der Erklärungsempfänger die erhaltenen Daten weitergeben darf. Darauf aufmerksam gemacht werden muss außerdem, dass beabsichtigt ist, die Daten im sog. Drittland, in dem kein dem europäischen Niveau entsprechender Datenschutz besteht, zu verarbeiten. Auch ist auf die Nachteile hinzuweisen, die dem Betroffenen im Falle einer Zustimmungsverweigerung drohen, dass etwa ein Erstattungsantrag bei einer Krankenkasse nicht bearbeitet werden kann, wenn der Betroffene nicht in die Verarbeitung seiner Gesundheitsdaten einwilligt. Der Hinweis auf Allgemeine Geschäftsbedingungen, Datenschutzerklärungen, Merkblätter oder Aushänge genügt nur dann dem Unterrichtungserfordernis, wenn diese von dem Betroffenen zum Zeitpunkt der Abgabe seiner Erklärung ohne weiteres eingesehen werden können. Wie dezidiert die Hinweise sein müssen, hängt vom jeweiligen Einzelfall ab.

- Die datenschutzrechtliche Einwilligung ist zu Beweis Zwecken und zum Schutze des Betroffenen vor vorschnellen Erklärungen grundsätzlich **schriftlich** abzufassen und eigenhändig zu unterschreiben. Dabei muss sich die Einwilligungserklärung deutlich von anderen Erklärungen abheben. Auch darf die Einwilligungserklärung nicht mit dem irreführenden Wort „Datenschutz“ überschrieben werden. Vielmehr muss sich bereits in der Überschrift das Wort „Einwilligung“ finden. Eine elektronisch erklärte Einwilligung ist nur wirksam, wenn sie nachweisbar vom Betroffenen vorgenommen worden ist und den Anforderungen des Signaturgesetzes entspricht. Doch ist die Einwilligung nach § 13 Abs. 2 des Telemediengesetzes (TMG) und § 94 des Telekommunikationsgesetzes (TKG) in die Nutzung von Verkehrs- und Bestandsdaten auch mittels Web-Formular, E-Mail oder Telefax möglich, wenn sichergestellt ist, dass der Betroffene seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Betroffene den Inhalt der Einwilligung jederzeit abrufen kann und in der Lage ist, seine Erklärung stets mit Wirkung für die Zukunft zu widerrufen. Ausnahmsweise ist auch eine mündliche

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

oder per nicht signierter E-Mail erklärte Einwilligung ausreichend, wenn wegen besonderer Eilbedürftigkeit oder bei einmaligem Kontakt, etwa bei telefonischen Befragungen, die allerdings nicht der Werbung dienen dürfen, in der Praxis eine schriftliche Datenerhebung nicht in Frage kommt. Dagegen scheidet eine konkludente, stillschweigende oder mutmaßliche Einwilligung grundsätzlich aus.

- Die Einwilligung muss **freiwillig**, also ohne Zwang erfolgen. Unfrei kann eine Einwilligungserklärung abgesehen von physischem oder psychischem Zwang insbesondere sein, wenn sich der Betroffene angesichts des wirtschaftlichen Machtgefälles zwischen ihm und seinem Vertragspartner zur Abgabe der Einwilligungserklärung gezwungen sieht bzw. wenn der Vertragspartner die Vertragskonditionen einseitig bestimmen kann, oder wenn der Betroffene keine zumutbaren Alternativen hat. Auch wird die Freiwilligkeit bei einer Monopolstellung des Erklärungsempfängers bzw. bei einem informationellen Ungleichgewicht in Frage gestellt. Die Rechtsprechung stellt die Ausnutzung der geschäftlichen Unerfahrenheit und das Verleiten zur Abgabe der Erklärung durch übermäßige finanzielle Anreize der mangelnden Freiwilligkeit der Einwilligung gleich.
- Besonderheiten gelten für die Einwilligung bei der **Werbung**. Werbung in diesem Sinne sind auch die telefonische Kundenbefragung, die telefonische Frage an Kunden, ob sie künftig mit der Zusendung von Werbung einverstanden sind und u. U. auch sog. Zufriedenheitserkundigungen beim Kunden. Unabhängig von der datenschutzrechtlichen Bewertung der Einwilligung müssen sich Werbeeinwilligungen auch am Gesetz über den unlauteren Wettbewerb messen lassen. Danach stellt die Missachtung datenschutzrechtlicher Bestimmungen in der Regel auch einen Verstoß gegen wettbewerbsrechtliche Vorschriften dar. Hier gilt:
 - Dem Einwilligenden muss über die Vorgaben des § 4a BDSG hinaus genau mitgeteilt werden, welcher Art die beabsichtigte Werbung ist (Brief, E-Mail, SMS, Telefon, Fax), wer die werbenden Unternehmen sein werden und welche Produktgattungen und Dienstleistungen beworben werden sollen.

- Soll die Einwilligung zur Werbung im Rahmen von Allgemeinen Geschäftsbedingungen oder in einer Datenschutzerklärung eingeholt werden, muss die Hervorhebung gegenüber diesen Texten drucktechnisch in besonderer Weise erfolgen.
- Werbung gegenüber dem Verbraucher per Telefon ist nur gestattet, wenn der Werben- de vorher eine ausdrückliche Einwilligung beim Adressaten eingeholt hat. Wird die Einwilligung telefonisch oder mündlich eingeholt, muss dem Betroffenen der Inhalt seiner Einwilligung schriftlich bestätigt werden.
- Wird die Einwilligung elektronisch (E-Mail, Fax, SMS) eingeholt, muss die verantwortliche Stelle sicherstellen, dass die Einwilligung protokolliert wird, dass der Betroffene jederzeit ihren Inhalt abrufen kann und dass er die Einwilligung stets mit Wirkung für die Zukunft widerrufen kann. Der Betroffene muss eine positive Einwilligungserklärung (Opt-in) abgeben. Die Opt-out-Lösung (Widerspruchslösung) ist nach herrschender Auffassung nicht ausreichend.
- Der Abschluss eines Vertrages darf grundsätzlich nicht von der Einwilligung der Verarbeitung der Daten des Betroffenen für eine Werbeansprache abhängig gemacht werden.

Die Einwilligung kann auf unbegrenzte Dauer erklärt werden, kann sich aber auch auf einen bestimmten Zeitraum beschränken. Ob eine Einwilligung jederzeit mit Wirkung für die Zukunft **widerrufen** werden kann, hängt abgesehen von den Fällen, in denen das gesetzlich – wie beispielsweise für elektronisch erklärte Einwilligungen im Telemedien- und Telekommunikationsrecht – ausdrücklich vorgeschrieben ist, von den jeweiligen Interessen der Beteiligten im Einzelfall ab. Nach der Rechtsprechung kann der Betroffene seine Einwilligung für die Zukunft grundsätzlich nur widerrufen, wenn er dafür ein berechtigtes Interesse hat, etwa wenn sich die Umstände so verändert haben, dass ihm nicht mehr zumutbar ist, an der einmal abgegebenen Einwilligungserklärung festgehalten zu werden. Zwar überwiegt bei dieser Abwägung im Zweifelsfall das Recht auf informationelle Selbstbestimmung des Betroffenen. Diesem darf jedoch kein höherrangiges Interesse seines Geschäftspartners entgegenstehen, etwa wenn der

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

Betroffene für eine Abbildung eine Vergütung erhalten hat oder wenn die Datenverarbeitung ausdrücklich Vertragsgegenstand ist. Andererseits entfällt ein berechtigtes Interesse der datenverarbeitenden Stelle für gewöhnlich, wenn sie das maßgebliche Datum nicht mehr benötigt.

10.7 Auswirkung von Datenschutzverstößen auf gerichtliche Entscheidungen

Nach einer Entscheidung des Bundesverfassungsgerichts gibt es kein grundsätzliches Verbot, rechtsfehlerhaft erhobene personenbezogene Daten zu verarbeiten oder zu nutzen. Vielmehr sei im Einzelfall unter Abwägung der widerstreitenden Interessen zu entscheiden (vgl. BVerfG, RDV 2011, S. 233). Die Entscheidung lässt erkennen, dass von einem Verarbeitungsverbot auszugehen ist bei bewussten, schwerwiegenden oder willkürlichen Datenschutzverstößen oder wenn der absolute Kernbereich privater Lebensgestaltung berührt ist.

Die Zivilgerichte sind, was ein Beweisverwertungsverbot von unter Datenschutzverstößen erlangten Beweismitteln angeht, sehr streng. So dürfen rechtswidrig erlangte Erkenntnisse allenfalls in notwöhnlichen Situationen bei Angriffen auf die Person des Beweispflichtigen im Urteil verwertet werden. Konsequentermaßen haben gleich mehrere Gerichte Dashcam-Aufnahmen wegen eines Verstoßes gegen das allgemeine Persönlichkeitsrecht, gegen das Bundesdatenschutzgesetz und gegen das Kunst- und Urheberrecht nicht als Beweismittel zum Hergang des Unfalls gewertet. Beim Einsatz solcher Überwachungskameras handele es sich um eine unzulässige, anlasslose Überwachung des Straßenverkehrs (LG Heilbronn, NJW-RR 2015, S. 1019; AG München, ZD 2014, S. 530; siehe Kapitel 11.1.5). Dagegen machen die Arbeitsgerichte die Verwertbarkeit eines datenschutzrechtlich zumindest bedenklichen Beweises von der Interessenlage der Parteien im Einzelfall unter Beachtung des Grundsatzes der Verhältnismäßigkeit abhängig. Beobachtet ein Vorgesetzter einen angeblich arbeitsunfähigen Mitarbeiter bei der Freizeitgestaltung, darf er von diesem ein Foto fertigen (LAG Rheinland-Pfalz RDV 2014, S. 44). Dagegen ist es selbst bei einem hinreichenden Verdacht, dass der Mitarbeiter eine Straftat begangen hat, nicht zulässig, dessen Schrank heimlich zu durchsuchen (BAG, Urt. v. 20.06.2013 – 2 AZR 546/12 –). Eine heimliche Vi-

deoüberwachung ist nur zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, es keine andere weniger einschneidende Ermittlungsmethode gibt und die Videoüberwachung insgesamt nicht unverhältnismäßig ist (LAG Köln ZD 2011, S. 47; BAG RDV 2012, S. 297). Ein vom Arbeitgeber rechtswidrig erlangtes Chatprotokoll eines Arbeitsplatzrechners darf verwertet werden, wenn dem Arbeitnehmer lediglich die gelegentliche private Nutzung des Geräts gestattet war und der Arbeitgeber sich Kontrollen vorbehalten hat (LAG Hamm RDV 2012, S. 54).

Im Strafrecht stellt ein Beweisverwertungsverbot eine begründungsbedürftige Ausnahme dar. Es ist grundsätzlich nur angezeigt, wenn die Beweiserhebung gesetzlich oder angesichts der Rechtsprechung des Bundesgerichtshofes unzulässig ist (BVerfG, ZD 2012, S. 375). Danach unterliegen akustische Überwachungsmaßnahmen nicht unbedingt einem Beweisverwertungsverbot (BVerfG, DANA 2012, S. 44), während ein in einem Kraftfahrzeug aufgezeichnetes Selbstgespräch eines sich unbeobachtet fühlenden Betroffenen im Strafprozess nicht verwertet werden darf (BGH RDV 2012, S. 190). Interessant ist, dass die Strafgerichte Dashcam-Aufzeichnungen zum Nachteil des Angeklagten grundsätzlich akzeptieren (AG Nienburg, RDV 2015, S. 211; siehe Kapitel 11.1.5).

Nicht unumstritten ist die Frage, ob die Verwaltung personenbezogene Daten, die sie unter Verstoß gegen das Datenschutzrecht erlangt hat, oder die inzwischen wieder hätten gelöscht werden müssen, bei Bedarf noch verwerten darf. So hat das Verwaltungsgericht Wiesbaden entschieden, dass die in einer ohne Rechtsgrundlage errichteten Datei gespeicherten Daten von der Polizei bzw. Ordnungsverwaltung nicht genutzt werden dürfen (VG Wiesbaden, DANA 2013, S. 84), während der Verwaltungsgerichtshof Baden-Württemberg in einem weithin bekannt gewordenen Beschluss die Auffassung vertritt, zwar dürften Daten, die die Behörde löschen musste, die aber noch in einer Protokolldatei zum Zwecke der Datensicherung gespeichert sind, grundsätzlich zu keinem anderen Zweck mehr verwendet werden. Eine Nutzung dieser Daten käme aber ausnahmsweise etwa in einem dienstrechtlichen Verfahren noch infrage, wenn der Betroffene offenkundig und schwerwiegend gegen beamten-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

rechtlichen Pflicht verstoßen hat (VGH BW, Beschl. v. 30. 07. 2015 – 1 S 1352/13 –).

10.8 Externe Datenschutzbeauftragte bei Stadtwerken

Im Rahmen meiner Beratungstätigkeit wurde ich gefragt, ob kommunale Versorgungsunternehmen einen externen Datenschutzbeauftragten bestellen können. Die breit angelegte Tätigkeit mancher Stadtwerke in einer Vielzahl von Geschäftsfeldern erfordert eine differenzierte Betrachtungsweise.

Die Zulässigkeit der Bestellung eines externen Datenschutzbeauftragten ist im Landesdatenschutzgesetz (LDSG) und im Bundesdatenschutzgesetz (BDSG) unterschiedlich geregelt. Maßgeblich ist daher zunächst, welches Rechtsregime überhaupt anwendbar ist. Das Landesdatenschutzgesetz gilt nach seinem § 2 Absatz 1 Satz 1 für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Als öffentliche Stellen gelten gem. § 2 Absatz 2 Satz 1 LDSG auch juristische Personen des Privatrechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der vorgenannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder der Stimmen beteiligt sind. Zu den Aufgaben der öffentlichen Verwaltung gehören auch Aufgaben der Daseinsvorsorge, beispielsweise die Versorgung mit Strom, Gas und Wasser. Stadtwerke, die diese Leistungen erbringen, sind daher bei entsprechender Mehrheitsbeteiligung der öffentlichen Hand ebenfalls öffentliche Stellen im Sinne des § 2 Absatz 1 LDSG.

Nach § 2 Absatz 4 Satz 1 LDSG finden die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes auf öffentliche Stellen Anwendung, soweit diese als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen. Für Stadtwerke in Form eines Unternehmens mit eigener Rechtspersönlichkeit – also nicht Eigenbetriebe – gilt daher bei Betätigung in Geschäftsbereichen, in denen Wettbewerb besteht, wie zum Beispiel bei der Versorgung mit Strom und Gas, das Bundesdatenschutzgesetz. Hingegen sind im Bereich der Wasser- und Wärmeversorgung in der

Regel mangels Wettbewerbs die Vorschriften des Landesdatenschutzgesetzes anwendbar.

Betätigen sich Stadtwerke mit eigener Rechtspersönlichkeit sowohl in Geschäftsbereichen, in denen sie am Wettbewerb teilnehmen, als auch in solchen, in denen sie eine Monopolstellung inne haben, so bestimmt sich das anwendbare Datenschutzgesetz nach der jeweiligen Tätigkeit im vorgenannten Sinne. Daher können in den Stadtwerken durchaus unterschiedliche Rechtsregime Geltung beanspruchen.

Nach § 4f Absatz 2 Satz 3 Halbsatz 1 BDSG kann zum Beauftragten für den Datenschutz auch eine Person außerhalb der verantwortlichen Stelle bestellt werden. § 10 Absatz 2 Satz 2 LDSG sieht hingegen als Alternative zur Bestellung eines eigenen Mitarbeiters der jeweiligen öffentlichen Stelle nur die Bestellung eines Bediensteten von deren Aufsichtsbehörde vor. Auch können mehrere öffentliche Stellen nach § 10 Absatz 2 Satz 3 LDSG einen ihrer Mitarbeiter zum gemeinsamen Datenschutzbeauftragten bestellen. Darüber hinaus wird die Bestellung eines externen Datenschutzbeauftragten, obwohl nach dem Gesetzeswortlaut nicht ausgeschlossen, im Anwendungsbereich des LDSG als unzulässig angesehen.

Damit ist es nicht zulässig, dass ein externer Datenschutzbeauftragter, der die „Wettbewerbsbereiche“ von Stadtwerken betreut, zugleich die Aufgabe des (fakultativ zu bestellenden) behördlichen Datenschutzbeauftragten für die „Monopolbereiche“ übernimmt. In solchen Fällen bleibt es dem externen Datenschutzbeauftragten aber unbenommen, die Geschäftsleitung datenschutzrechtlich in allgemeiner Form zu beraten, ohne die typischen Befugnisse eines behördlichen Datenschutzbeauftragten auszuüben.

Die rechtliche Differenzierung zwischen Geschäftsfeldern mit und ohne Wettbewerb erschwert die Synergieeffekte, die sich durch die Bestellung eines einheitlichen externen Datenschutzbeauftragten ergeben könnten. Es wäre daher wünschenswert, dass der Landesgesetzgeber insoweit eine Lockerung der gesetzlichen Regeln ins Auge fasst. Anlass hierzu könnte die neue Datenschutz-Grundverordnung der Europäischen Union bieten, denn diese sieht in der konsentierten Fassung vom 15. Dezember 2015 in Artikel 35 vor, dass betriebliche oder

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

behördliche Datenschutzbeauftragte entweder zum eigenen Personal gehören oder auf der Grundlage eines Dienstleistungsvertrages tätig werden können.

10.9 Die rechtlichen Grenzen bei der Beendigung der Bestellung eines betrieblichen Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte nimmt nach den §§ 4ff. BDSG neben den Datenschutzaufsichtsbehörden eine zentrale Rolle im Kontroll- und Beratungssystem des Datenschutzes ein. Daher sind auch bei der Beendigung der Tätigkeit als Datenschutzbeauftragten die jeweils einschlägigen Tatbestände genauestens zu unterscheiden und die jeweiligen Voraussetzungen einzuhalten.

Die betrieblichen Datenschutzbeauftragten haben, so die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit⁷⁹, eine unverzichtbare Funktion bei der Verwirklichung des Datenschutzes, weil ihnen der Gesetzgeber wichtige Aufgaben beim Schutz personenbezogener Daten im Interesse der Bürgerinnen und Bürger, aber auch der Beschäftigten in Behörden und Betrieben übertragen hat. Ihre kontinuierliche Tätigkeit ist ein besonders wichtiger Beitrag zur Umsetzung der datenschutzrechtlichen Bestimmungen und Grundsätze.

Der Gesetzgeber hat den betrieblichen Datenschutzbeauftragten daher sowohl hinsichtlich seiner Funktion als Auftraggeber als auch im Hinblick auf das zugrundeliegende Arbeits- oder Angestelltenverhältnis mit einem besonders hohen Schutz ausgestattet, um seine Arbeitsfähigkeit und Unabhängigkeit zu gewährleisten.

Dies zeigt sich insbesondere auch bei der Beendigung der Bestellung zum betrieblichen Datenschutzbeauftragten. Es liegt gerade nicht im Belieben der verantwortlichen Stelle, einen einmal bestellten Datenschutzbeauftragten „einfach so“ auszutauschen bzw. gegen seinen Willen abzuberufen. Aus meiner täglichen aufsichtsrechtlichen Arbeit ist mir bekannt, wie schwer es nicht wenige betrieb-

liche Datenschutzbeauftragte haben, ihre Tätigkeit vollumfänglich ausüben zu können. Die Datenschutzbeauftragten sind zumeist Einzelkämpfer, sollen den Betriebsablauf so wenig wie möglich stören und sitzen oft – auch im Hinblick auf ihr Grundarbeitsverhältnis – zwischen den Stühlen (siehe hierzu auch Simitis, Kommentar zum BDSG, 8. Auflage, Rn. 177 zu § 4f).

Gerade deshalb ist es ein wichtiges Ziel der Tätigkeit der Datenschutzaufsichtsbehörde, die betrieblichen und behördlichen Datenschutzbeauftragten zu beraten, in der Wahrnehmung ihrer Rechte und Pflichten zu unterstützen – und aufsichtsrechtlich einzuschreiten, wenn wieder einmal ein Auftraggeber unliebsam geworden ist.

Eine Abberufung – gegen den Willen des Betroffenen – ist überhaupt nur möglich, wenn objektive und schwerwiegende Gründe dies rechtfertigen. Eine weitere Tätigkeit als Auftraggeber für den Datenschutz muss der nicht-öffentlichen Stelle unzumutbar sein (Bundesarbeitsgericht, Urteil v. 23. März 2011, Az. 10 AZR 562/0).

Die Funktion als betrieblicher Datenschutzbeauftragter kann nach dem Bundesdatenschutzgesetz **nur in folgenden Fällen** beendet werden:

- (1) Die **Pflicht** zur Bestellung für die verantwortliche Stelle **entfällt** zum Beispiel durch das Absinken der Anzahl von ständig in der Datenverarbeitung tätigen Beschäftigten i.S.v. § 4f Absatz 1 BDSG unter zehn Beschäftigte.
- (2) Der betriebliche Datenschutzbeauftragte **legt sein Amt freiwillig und einseitig nieder**, tritt also von dieser Funktion zurück. Dieser Rücktritt muss schriftlich gegenüber der Leitung der verantwortlichen Stelle erfolgen.
- (3) Die verantwortliche Stelle und der betriebliche Datenschutzbeauftragte **verständigen sich ausdrücklich und einvernehmlich auf eine Beendigung** der Beauftragten-Tätigkeit. Da die Bestellung gem. § 4f Absatz 1 Satz 1 BDSG schriftlich zu erfolgen hat, ist nach herrschender und zutreffender Meinung daher auch für die Beendigung die Schriftform erforderlich (siehe nur Simitis, Kommentar zum BDSG, 8. Auflage, Rn. 178 zu § 4f; Taeger/Gabel, Kommentar zum

⁷⁹ im Vorwort ihres Merkblatts Info 4: „Die Datenschutzbeauftragten in Behörde und Betrieb“ (10. Auflage, Juni 2014); im Internet abrufbar als PDF-Dokument unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO4.pdf?__blob=publicationFile

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

BDSG u. a., 2. Auflage, Rn. 49 zu § 4f). Die beiden Parteien müssen ihr Einverständnis in einer gemeinsamen, ausdrücklich auf die Beendigung der Bestellung bezogenen Vereinbarung schriftlich festhalten. Eine reine Aktenübergabe ersetzt natürlich nicht die Schriftform. Die Aufgaben, Rechte und Pflichten eines Datenschutzbeauftragten sind derart weitgehend und wichtig, dass die Beendigung dieser Aufgabe nicht mündlich, also quasi per Zuruf, vorgenommen werden kann. Nur die Schriftform schafft die unerlässliche Rechtssicherheit vor allem zu Dokumentations- und Beweis Zwecken.

Da dies ein großes Unternehmen mit Sitz in Baden-Württemberg anders sieht, musste ich im Wege einer Verfügung nach § 38 Absatz 5 BDSG anordnen, dass der bisherige betriebliche Datenschutzbeauftragte weiterhin im Amt und in seiner Funktion von der Geschäftsleitung zu unterstützen ist und der neue Beauftragte wieder abberufen werden muss. Da gegen die Verfügung Klage erhoben worden ist, wird nun vor dem Verwaltungsgericht Stuttgart in dieser Sache verhandelt.

- (4) Die verantwortliche Stelle **widerruft** einseitig die Bestellung ihres betrieblichen Datenschutzbeauftragten in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs aus wichtigem Grund (§ 4f Absatz 3 Satz 4 BDSG) innerhalb von zwei Wochen seit Kenntnis des wichtigen Grundes.

Aufgrund der Verweisung in § 4f Absatz 3 Satz 4 BDSG muss für die Abberufung ein wichtiger Grund vorliegen, der es der verantwortlichen Stelle aufgrund von Tatsachen und unter Berücksichtigung der Gegebenheiten des Einzelfalls sowie unter Abwägung der Interessen beider Vertragsteile unzumutbar macht, den Beauftragten weiterhin einzusetzen. Als wichtige Gründe kommen solche in Betracht, die mit der Funktion und Tätigkeit des Datenschutzbeauftragten zusammenhängen und eine weitere Ausübung dieser Tätigkeit unmöglich machen oder sie zumindest erheblich gefährden. Beim Widerruf ist zu beachten, dass hierbei auch das (Vor-)Verhalten der verantwortlichen

Stelle zu berücksichtigen ist (Bergmann/Möhrle/Herb, Kommentar zum Datenschutzrecht, Stand: Januar 2012, Rn. 145 zu § 4f BDSG). Außerdem sollte einvernehmlich zunächst immer nach weniger eingreifenden Maßnahmen gesucht werden (z. B. Änderung des Zuständigkeitsbereichs im Hinblick auf das zugrunde liegende Arbeitsverhältnis).

- (5) Die Datenschutzaufsichtsbehörde **ordnet** gegenüber der verantwortlichen Stelle – bei entsprechender Kenntniserlangung – **die Abberufung** des betrieblichen Datenschutzbeauftragten wegen fehlender Fachkunde und/oder fehlender Unabhängigkeit (§ 4f Absatz 3 Satz 4 2. Halbsatz, § 38 Absatz 5 Satz 3 BDSG) an.
- (6) Unternehmen mit jeweils einem betrieblichen Datenschutzbeauftragten **fusionieren oder verschmelzen** (siehe hierzu: Bundesarbeitsgericht, Urteil v. 29. September 2010, Az.: 10 AZR 588/09⁸⁰).

Um eine wirksame betriebsinterne Datenschutzkontrolle sicherzustellen, wird die Datenschutzaufsichtsbehörde die betrieblichen und behördlichen Datenschutzbeauftragten auch weiterhin in der Wahrnehmung ihrer Rechte und Pflichten unterstützen und ggf. auch aufsichtsrechtlich einschreiten, wenn ein Unternehmen sich einen gewissenhaften Beauftragten „vom Hals schaffen“ will.

10.10 Datenschutz im Hotel

Wo viele Menschen verkehren, gibt es auch viele personenbezogene Daten und mitunter komplizierte Interessenlagen. In Hotels und anderen Beherbergungsstätten gilt dies ganz besonders, speziell auch infolge der besonderen melderechtlichen Pflichten.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hat vor diesem Hintergrund bereits eine Orientierungshilfe „Daten-

⁸⁰ Fundstelle im Internet:
<http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=14831>

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

schutz im Hotelgewerbe“ erstellt.⁸¹ Im aktuellen Berichtszeitraum haben sich im Rahmen meiner Aufsichtstätigkeit insbesondere folgende Einzelfragen aufgetan.

10.10.1 Dauerbrenner Personalausweiskopien – mehr Sicherheit bei „Stundengästen“?

Die Frage nach dem Kopieren von Bundespersonalausweisen und Reisepässen kommt immer wieder auf den Tisch, weil sich die verantwortlichen Stellen von ihnen offenbar größere Sicherheit, eine bessere Dokumentation oder auch einfach nur eine abschreckende Wirkung versprechen. Oft genug gibt es aber auch weniger eingriffsintensive Möglichkeiten – und für manche Zwecke eignen sich diese Kopien schlicht nicht.

Ein ehemaliger Hotelgast hat sich an mich gewandt. Anlässlich einer einzelnen Übernachtung sei bei seiner Anmeldung eine Fotokopie seines Bundespersonalausweises angefertigt worden, ohne dass er darin eingewilligt habe. Auf Nachfrage an Ort und Stelle habe er die – leider noch immer allzu gängige und ebenso unzureichende (siehe hierzu auch Kapitel 10.12) – Auskunft erhalten, dies geschehe auf Anweisung der Geschäftsleitung.

Das bestätigte mir das Management der Hotelgruppe. Bei Übernachtungen ohne Reservierung, die nicht per Vorkasse bezahlt werden, werde für die Dauer des Aufenthalts regelmäßig eine Kopie eines Ausweisdokumentes angefertigt. Damit sollten die Meldedaten überprüft und ggf. Schadensfälle leichter polizeilich verfolgt werden können. Zudem sollten potentielle Zechpreller im Idealfall von vornherein abgeschreckt werden. Dies sei eine Sonderregelung für ein Hotel der Gruppe, das sich in einer unsicheren Bahnhofsgegend befinde. Dort würden sich oft „Stundengäste“ einmieten, die die Zimmer gelegentlich in einem verwüsteten Zustand oder ohne zu bezahlen hinterließen. Nach der – schadensfreien – Abreise würden die Kopien unverzüglich vernichtet.

Mangels einer gesetzlichen Erlaubnis war dieses Anfertigen von Kopien von Personalausweisen oder auch Reisepässen nicht zulässig. Dabei kommt es

nicht darauf an, ob eine Einwilligung des Gastes angenommen werden kann. Kurz gesagt reicht in diesem Zusammenhang eine Einwilligung der betroffenen Person grundsätzlich nicht aus, weil der Personalausweis ebenso wie der Reisepass Bundes Eigentum ist und die Bundesrepublik Deutschland über deren Verwendung (mit-)entscheidet. Nach Ansicht des zuständigen Bundesministeriums des Innern bestehe zwar kein generelles rechtliches Kopierverbot. Allerdings werden hohe Anforderungen an die Zulässigkeit des Kopierens von Personalausweisen gestellt:

- Die Erstellung einer Kopie muss erforderlich sein.
- Dabei ist insbesondere zu prüfen, ob nicht die Vorlage des Personalausweises und ggf. die Anfertigung eines entsprechenden Vermerks (z. B.: „Personalausweis hat vorgelegen.“) ausreichend ist.
- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden.
- Die Kopie muss als solche erkennbar sein.
- Daten, die nicht zur Identifizierung benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden.
- Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.
- Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.
- Eine automatisierte Speicherung der Ausweisdaten ist nach dem Personalausweisgesetz stets unzulässig.

Für deutsche Reisepässe gilt Entsprechendes.

Dass ein Hotelier, der öfter auf unbezahlten Rechnungen oder auf verwüsteten Zimmern sitzenbleibt, diese Folgen vermeiden will, kann ich nachvollziehen. Die Mittel, die er einsetzt, um sich größere Sicherheit zu verschaffen, sollten sich dann aber auch dafür eignen und den Rahmen des Erforderlichen nicht völlig sprengen. Kopien von Personalausweisen kamen für die im vorliegenden Fall angeführten Zwecke aufgrund folgender Erwägungen nicht in Frage:

⁸¹ online unter http://www.datenschutz.rlp.de/downloads/oh/Datenschutz_Hotel.pdf

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

■ **Abschreckung von Zechprellern**

Zur Abschreckung mag sich das Androhen und Anfertigen von Ausweiskopien zwar faktisch eignen. Aus datenschutzrechtlicher Sicht ist diese Verwendung personenbezogener Daten aber nicht erforderlich, um die vertrauenswürdigen Gäste „auszusieben“; beispielsweise könnte auch ein Pfand oder eine Kautions verlangt werden. Zudem ist diese Verwendung insoweit nicht hinnehmbar, als hier die personenbezogenen Daten nicht ihres Inhalts wegen, sondern nur für eine Drohkulisse erhoben und (nichtautomatisiert) gespeichert werden.

■ **Verfolgung von Zechprellern**

Für die Verfolgung von Zechprellern durch die Polizei bringen die Kopien im Vergleich zu Personalien, die beim Einchecken – gerne auch unter Vorlage des Personalausweises (Sichtausweis) – aufgezeichnet werden, nach meiner Kenntnis keinen zusätzlichen Nutzen. Auch die Hotelgruppe blieb mir eine Erläuterung des vermeintlichen Mehrwertes schuldig. Für die erhoffte Verbesserung der Ausgangsposition eignen sich die Kopien daher schlicht nicht.

■ **Überprüfung der Meldedaten**

Das ebenfalls angeführte Überprüfen der Meldedaten ist nicht die Aufgabe von Beherbergungsstätten und kann somit ebenfalls keine Grundlage für das Anfertigen von Ausweiskopien sein – soweit diese dafür überhaupt nötig wären.

Die mir bisher bekannt gewordenen Zwecke, für die an der Hotelrezeption Kopien von Personalausweisen oder Reisepässen angefertigt wurden, hatten alle eines gemeinsam: Mit ihnen ließ sich das Kopieren nicht rechtfertigen und war daher datenschutzwidrig.

10.10.2 Geschwätzige Reservierungsbestätigungen:

Mit einer E-Mail reißen manche Hotels ein
...

... was sie zuvor mit einer verschlüsselten Übertragung von Formulardaten sorgfältig aufgebaut haben.

Im Berichtszeitraum erreichten mich zwei Beschwerden, weil Kreditkartendaten im Rahmen der

Reservierungsbestätigung per E-Mail versandt oder abgefragt wurden. Im ersten Fall umfassten die Daten, die dem Gast in spe in Form einer Reservierungsbestätigung zugemailt wurden, die volle Kreditkartennummer, den Namen des Karteninhabers und das Gültigkeitsdatum. Im zweiten Fall wurde in der Reservierungsbestätigungs-E-Mail um das Nachreichen der zuvor bei der Buchung nicht angegebenen Kreditkartendetails gebeten, um bequem die Antwortfunktion des E-Mail-Programms zu nutzen statt sich erst noch einen sichereren Übertragungsweg zu suchen.

Zu den Online-Buchungsformularen bestand in beiden Fällen eine TLS-verschlüsselte Verbindung (<https://...>). Die anschließende E-Mail-Korrespondenz dagegen beschränkte sich auf ganz „gewöhnliche“ Mails, die eben nicht (inhalts- bzw. Ende-zu-Ende-)verschlüsselt waren.

Dadurch entstand eine datenschutzwidrige Sicherheitslücke. Nach § 9 BDSG müssen nicht-öffentliche Stellen, die mit personenbezogenen Daten umgehen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Ausdrücklich verwiesen wird dabei auf die Anlage zu § 9 BDSG, in der in Satz 3 „insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren“ als Maßnahme genannt wird, um das unbefugte Mitlesen personenbezogener Daten zu verhindern. Insbesondere die Ende-zu-Ende-Verschlüsselung von E-Mails ist heutzutage genau ein solches Verfahren.

Sollte es tatsächlich nötig sein, dem Gast in spe seine eigenen Kreditkartendaten vorzulegen (etwa um sie nochmals bestätigen zu lassen), könnte etwa eine Ende-zu-Ende-Verschlüsselung angeboten, der Postweg gewählt, ein entsprechend gesichertes Kundenkonto angelegt oder eine nochmalige Eingabe in das sichere Online-Formular erbeten werden. Für eine Übertragung in einer Standard-, d. h. lediglich transportverschlüsselten E-Mail sind die Kreditkartendaten entschieden zu heikel.

Dies ist auch der Standpunkt der großen Kreditkartendienstleister, die in ihrem Payment Card Industry

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

Data Security Standard für Hotels⁸² die Übertragung von Kreditkartendaten per einfacher E-Mail kategorisch ausschließen.

Sensible personenbezogene Daten wie Kreditkartendaten sollten heutzutage in keinem Zusammenhang mehr per unverschlüsselter E-Mail übertragen werden. Zumutbare Alternativen gibt es schließlich genug.

10.10.3 Zweckänderung bei Meldedaten – dein Hotelier weiß, wo du wohnst

Unabhängig von Buchungs- und Rechnungsschrift muss auf den Meldescheinen in Hotels und anderen Beherbergungsstätten immer die private Anschrift des Gastes eingetragen werden. Eine Fundgrube, wenn ein Hotel möglichst persönliche Werbung schalten will?

Der ehemalige Gast eines Hotels wandte sich an mich, weil er von einem Hotel Briefwerbung an seine Privatanschrift erhalten hatte, obwohl er bei dem Hotel bereits Jahre zuvor einen Verbewiderspruch eingelegt und um Löschung seiner Daten gebeten habe. Da er kürzlich zwar wieder dort übernachtet hatte, die Buchung aber ausschließlich auf seine Arbeitgeberin lief, vermutete er, das Hotel habe seine Daten aus dem Meldeschein zweckentfremdet.

Auf meine Nachfrage trug das Hotel vor, seine Meldedaten nicht verwendet zu haben. Vielmehr sei auf seinen damaligen Widerspruch hin seine Adresse versehentlich nicht aus der Liste gelöscht worden, die für Werbung an Gäste verwendet werde, die Interesse an einem jährlichen Newsletter bekundet hätten. Wie sie auf diese Liste gelangt war und warum sie trotz mehrfacher Bitte des Beschwerdeführers Jahr für Jahr offenbar *nicht* gelöscht worden war, könne leider nicht mehr nachvollzogen werden. Man entschuldige sich und habe die Adresse nun definitiv aus der Liste gelöscht.

Sofern das Hotel persönlich adressierte Werbung nur auf Einwilligungsbasis schaltet, war bereits die Eintragung in der Werbeliste, spätestens aber die Weiterspeicherung nach dem ersten Protest unzulässig;

die weitere jährliche Nutzung war schließlich sowohl datenschutzwidrig als auch nach § 7 Absatz 1 Satz 1 und 2 UWG unlauter und somit abmahnfähig. Das ist gewissermaßen eine klassische Fallgestaltung im Werbebereich und kommt in der Praxis immer wieder vor. Da in diesem Fall aber der genaue Hergang unklar geblieben war, nahm ich die Befürchtung des Beschwerdeführers ernst und den etwas unbefriedigenden Vortrag des Hotels zum Anlass, das Hotel vorsorglich auch auf die Rechtslage hinsichtlich der Meldedaten hinzuweisen.

Nach § 26 des baden-württembergischen Meldegesetzes (MG) durften Daten aus ausgefüllten Meldescheinen, insbesondere personenbezogene Daten wie Adressen, von den Beherbergungsstätten nicht für eigene Zwecke verwendet werden. Der Umgang der Beherbergungsstätten war vielmehr in §§ 23, 24 MG abschließend geregelt – und eine Zweckänderung, um Werbeadressen zu generieren, war darin nicht vorgesehen.

Seit dem 1. November 2015 ist das baden-württembergische Meldegesetz infolge der Ablösung der Landesmeldegesetze durch das neue Bundesmeldegesetz (BMG) zwar außer Kraft. Die vorstehenden Ausführungen gelten aber genauso für die nun einschlägigen §§ 29 bis 31 BMG.

Für Hotels wie für alle weiteren nach Melderecht verpflichteten Beherbergungsstätten gilt nach wie vor: Als Quelle ansonsten unzugänglicher personenbezogener Daten sind Meldescheine tabu.

10.11 Landesweite schriftliche Datenschutzkontrolle bei Adresshandelsunternehmen sowie Markt- und Meinungsforschungsinstituten zeigt deutlich mehr Licht als Schatten

Vertrauen ist gut – Kontrolle ist besser. Nach diesem Motto hat meine Dienststelle eine landesweite schriftliche Datenschutzkontrolle bei allen Adresshandelsunternehmen sowie Markt- und Meinungsforschungsinstituten mit Sitz in Baden-Württemberg durchgeführt. Insgesamt konnte ein erfreulich hohes Datenschutzniveau in den betroffenen Unternehmen festgestellt werden. Allerdings waren bei einigen (wenigen) Unternehmen auch ein paar Anmerkungen oder Hilfestellungen erforderlich. Leider gibt es auch in diesen beiden Branchen „schwarze Schafe“,

⁸² online abrufbar unter <https://www.usd.de/kreditkartensicherheit-3-0-pci-dss-in-der-deutschen-hotelbranche>

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

die meinen, dass datenschutzrechtliche Vorgaben für sie nicht gelten.

10.11.1 Landes- und branchenweite schriftliche Datenschutzkontrollen – ein Instrument mit mehrfacher Wirkung

Neben den anlassbezogenen Kontrollen (etwa ausgelöst durch mehrere Beschwerden von Betroffenen über dasselbe Unternehmen) kann die Datenschutzaufsichtsbehörde auch anlasslose Kontrollen nach § 38 Absätze 1 und 3 des Bundesdatenschutzgesetzes (BDSG) vornehmen. Diese datenschutzrechtlichen Kontrollen können im Rahmen eines Kontrollbesuchs vor Ort (§ 38 Absatz 4 BDSG), also direkt bei der datenverarbeitenden Stelle, aber auch im Wege eines schriftlichen Kontrollverfahrens durchgeführt werden.

Besonders wirkungsvoll sind solche schriftlichen Kontrollverfahren, wenn sie eine ganze Branche betreffen:

- Für die Datenschutzaufsichtsbehörde ergibt sich so ein vertiefter, vergleichender Einblick in das Datenschutzniveau der verantwortlichen Stellen, die denselben Geschäftszweck verfolgen.
- Die Sensibilität und das nötige Bewusstsein für die besonderen Anforderungen der Unternehmen im Hinblick auf den betrieblichen Datenschutz werden auch über die Branche hinaus geschärft, manche datenschutzrechtliche Anforderung wird gerade (erst) durch die Kontrolle umgesetzt.
- Eine branchenweite Datenschutzkontrolle spricht sich auch über die Landesgrenzen hinaus bis in die jeweiligen Berufsverbände schnell herum.
- Die Erkenntnis verbreitet sich, vielleicht doch schneller als gedacht Gegenstand einer datenschutzrechtlichen Kontrolle zu werden.

Vor diesem Hintergrund hat meine Dienststelle in den Jahren 2014 und 2015 eine landesweite schriftliche Datenschutzkontrolle anhand eines umfangreichen Fragenkatalogs (vgl. Anhang 33) bei

- 19 Adresshandelsunternehmen (durch die Prüfung stellte sich heraus, dass davon 11 Unternehmen Adresshändler im Sinne des BDSG sind, die also tatsächlich personenbezogene Adressen speichern und übermitteln und nicht

nur z. B. die lediglich vermittelnde Funktion von sog. Listbrokern einnehmen) sowie

- 59 Markt- und Meinungsforschungsinstituten (durch die Prüfung stellte sich heraus, dass davon 37 Unternehmen Markt- und Meinungsforschungsinstitute im engeren Sinne von § 30a BDSG sind)

mit Sitz in Baden-Württemberg durchgeführt.

Begriffserläuterungen:

Adresshandelsunternehmen im Sinne von § 29 BDSG sind Unternehmen, die geschäftsmäßig Adresssammlungen zum Zwecke der Überlassung an Dritte generieren. Die Verwendungszwecke der Dritten, die diese Adressen nutzen, können sehr verschieden sein: z. B. Werbung, Datenbereinigung, Scoring, Markt- und Meinungsforschung, Spendenwerbung.

Markt- und Meinungsforschung im Sinne von § 30a BDSG liegt in Anlehnung an die Erläuterung in BT-Drs. 16/12011, S. 43, vor, wenn eine verantwortliche Stelle systematisch und geschäftsmäßig mittels anerkannter wissenschaftlicher Methoden und Techniken unter Verwendung personenbezogener Daten Informationen als empirische Grundlage und zur Unterstützung wirtschaftlicher, gesellschaftlicher und politischer Entscheidungen bereitstellt und diese an öffentliche oder private Auftraggeber übermittelt. Dabei hat die Markt- und Meinungsforschung nicht Aussagen über konkrete Einzelpersonen zum Gegenstand, sondern zieht personenbezogene Daten lediglich heran, um daraus von der Einzelperson unabhängige, verallgemeinerungsfähige Aussagen zu gewinnen. Die von der Markt- und Meinungsforschung erhobenen Daten werden dem Auftraggeber dementsprechend nur in anonymisierter Form übermittelt.

Warum gerade diese beiden Branchen ausgewählt wurden?

Neben den Wirtschaftsauskunfteien sind es im Regelfall die Adresshandelsunternehmen sowie die Markt- und Meinungsforschungsinstitute, die *geschäftsmäßig mit personenbezogenen Daten handeln* und diese Daten an ihre Geschäftspartner übermitteln bzw. aus diesen entsprechende Er-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

kennnisse gewinnen, die sie dann an ihre Auftraggeber übermitteln. Für diese Unternehmen sieht das Bundesdatenschutzgesetz spezielle und strengere Regeln vor, da die personenbezogenen Daten als Ware einem höheren Risiko ausgesetzt sind:

- Jedes Datenverarbeitungsverfahren muss vor der Anwendung an die Datenschutzaufsichtsbehörde *gemeldet* werden (§ 4d Absätze 1 und 4 Nr. 1 bzw. 3 BDSG). Bestandteil der Meldung sind die Angabe der verantwortlichen Stelle und der verantwortlichen Personen sowie eine Beschreibung des Datenverarbeitungsverfahrens sowie der technischen und organisatorischen Sicherungsmaßnahmen. Ebenso ist der Aufsichtsbehörde jede Veränderung der ursprünglichen Meldung (z. B. neues Datenverarbeitungsverfahren, Wechsel in der Geschäftsführung, andere Datensicherungsmaßnahmen) unaufgefordert mitzuteilen. Diese Meldungen werden im sogenannten *Verfahrensregister* nach §§ 38 Absatz 2, 4d Absatz 1 BDSG bei den Aufsichtsbehörden geführt und sind auch – bis auf den Bereich der Datensicherheit nach § 9 BDSG – für jedermann einsehbar.
- Unabhängig von der Anzahl der mit der automatisierten Datenverarbeitung betrauten Beschäftigten muss in diesen Unternehmen gem. § 4f Absatz 1 Satz 6 BDSG *immer ein betrieblicher Datenschutzbeauftragter* bestellt werden, soweit personenbezogene Daten geschäftsmäßig übermittelt werden.

Die befragten Unternehmen haben wir aus den in der Dienststelle vorhandenen Meldungen nach § 4d BDSG sowie anhand einer Internetrecherche zusammengestellt.

10.11.2 Wie sind die Unternehmen mit dem Fragenkatalog umgegangen?

Bei den Adresshandelsunternehmen antworteten sieben Unternehmen (63,6 %) auf mein Kontrollschreiben fristgerecht, drei Unternehmen (27,3 %) hielten die gewährte Fristverlängerung ein, ein Unternehmen musste wegen Fristverletzung angemahnt werden. Bei den Markt- und Meinungsforschungsinstituten zeigt sich ein ähnliches Bild: 23 Unternehmen (62,2 %) antworteten fristgerecht, 11 Unternehmen (29,7 %) haben die gewährte

Fristverlängerung eingehalten, drei Unternehmen (8,1 %) mussten angemahnt werden.

Unterschiedlich fiel die *Vollständigkeit der Beantwortung des Fragenkatalogs* aus. Sieben Adresshandelsunternehmen (63,6 %) haben den Fragenkatalog vollständig abgearbeitet, die restlichen vier Unternehmen (36,4 %) sind Antworten schuldig geblieben. Bei den Markt- und Meinungsforschungsinstituten haben nur 21 Unternehmen (56,8 %) alle Fragen beantwortet, die übrigen 16 Institute (43,2 %) mussten angemahnt werden.

Sehr unterschiedlich fiel auch das Vorhandensein des sogenannten „Jedermann-Verzeichnisses“ nach § 4f Absatz 2 Satz 2 BDSG aus: Während bei 81,8 % der Adresshändler dieses Verzeichnis vorlag, war dies bei den Markt- und Meinungsforschungsinstituten nur bei 48,6 % der Fall.

Die Auswertung der Prüfkation hat sich wegen der rechtlichen Komplexität der Datenverarbeitungsprozesse als langwierig erwiesen, einige Kontrollverfahren waren bei Redaktionsschluss noch im Gange.

10.11.3 Kontrollergebnisse bei den Adresshandelsunternehmen

Bei den Adresshandelsunternehmen sind folgende Kontrollergebnisse zu verzeichnen:

a) Gesamtergebnis

Nur bei einem der elf Adresshandelsunternehmen (9,1 %) wurden keinerlei Auffälligkeiten entdeckt. Bei sieben Unternehmen (63,6 %) mussten lediglich geringe Unregelmäßigkeiten moniert werden. Damit kann 72,7 % der Adresshandelsunternehmen ein gutes bzw. ordentliches Datenschutzniveau attestiert werden.

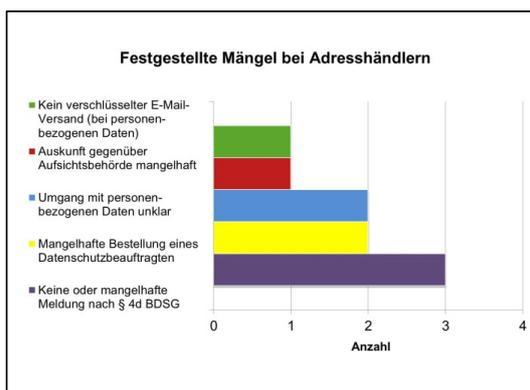
Bei drei Adresshändlern (27,3 %) hingegen wurden erhebliche Mängel festgestellt.



32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

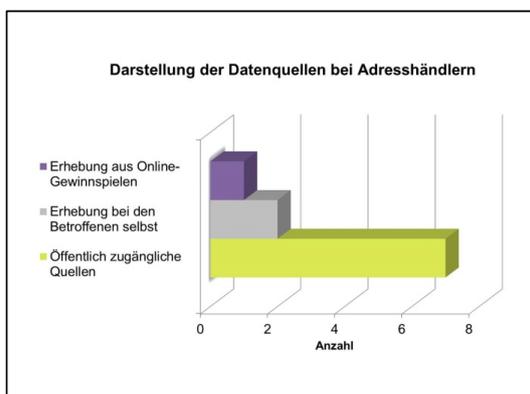
b) Welche datenschutzrechtlichen Mängel wurden konkret festgestellt?

Die sechs häufigsten Mängel ergeben sich aus der nachfolgenden Übersicht:

**c) Datenquellen**

Sieben von 11 Adresshändlern generieren ihre Adressdaten aus allgemein zugänglichen Quellen nach § 29 Absatz 1 Nr. 1 BDSG wie Telefon-, Adress- und Branchenbüchern, Internet oder Pressepublikationen. Ein durchaus großer Adresshändler gewinnt seine Adressbestände fast ausschließlich aus Online-Gewinnspielen. Das ist zwar rechtlich zulässig. Uns liegen aber Hinweise vor, dass gerade Online-Gewinnspiel-Veranstalter, die ihren Sitz im Ausland haben, oft unseriös arbeiten und auch vor Fälschungen nicht zurückschrecken. Hier werden weitere Ermittlungen stattfinden.

Im Übrigen wird auf die nachfolgende Grafik verwiesen:

**d) Datenlöschkonzept**

27,3 % der Adresshändler konnten ein vollständiges und nachvollziehbares Datenlöschkonzept vorlegen. 54,5 % der Unternehmen haben zwar ein solches Konzept, doch es war unvollständig oder teilweise unrichtig. Bei zwei Adresshändlern (18,2 %) musste ein fehlendes Löschkonzept beanstandet werden.

e) Sonstige Erkenntnisse

Bei den meisten Adresshändlern bilden Adressen und weitere Daten für die sog. Business-to-Business-Werbung (B2B) einen Schwerpunkt ihres Angebots. Zwar sind Daten, die sich nur auf ein Unternehmen als juristische Person beziehen, in der Regel nicht personenbezogen. Sobald aber natürliche Personen (z. B. Vertretungsberechtigte/r aus dem Online-Impressum, Ansprechpartner/innen, Geschäftsführer/innen) Teil des Datensatzes werden, greifen die Bestimmungen des Datenschutzrechts. Gleiches gilt natürlich für Selbständige (z. B. Ärzte/Ärztinnen, Rechtsanwälte/Rechtsanwältinnen u. a.), da hier stets der Berufsträger als Person angesprochen wird. Dieser Personenbezug wird leider von nicht wenigen Adresshändlern, anders als bei Business-to-Consumer-Werbung (B2C), nicht beachtet oder für irrelevant gehalten, so dass diese bisher bestenfalls nur die Meldepflicht, schlimmstenfalls aber wesentliche Datenschutzvorschriften vernachlässigt haben.

10.11.4 Kontrollergebnisse bei den Markt- und Meinungsforschungsinstituten

Die Überprüfung der Markt- und Meinungsforschungsinstitute kam zu folgenden Ergebnissen:

a) Gesamtergebnis

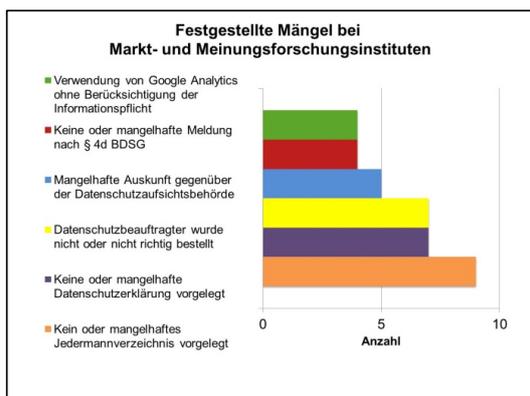
Bei 13 Instituten (35,1 %) konnte ich ein tadelloses Datenschutzniveau feststellen. Neun Institute (24,3 %) fielen lediglich durch kleinere, leicht behebbare datenschutzrechtliche Mängel auf. Somit ist der Datenschutz lediglich bei 59,4 % der Institute gut bzw. ordentlich verankert und organisiert.

Erhebliche Mängel wiesen leider 15 der 37 Institute auf (40,6 %). Hier haben wir entsprechende Veränderungen verlangt.

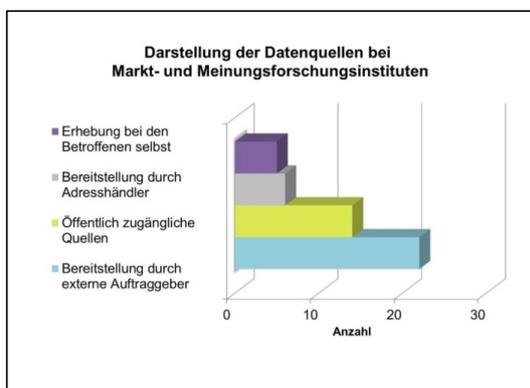
32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

**b) Welche datenschutzrechtlichen Mängel wurden konkret festgestellt?**

Die am häufigsten festgestellten Mängel können Sie der nachfolgenden Zusammenstellung entnehmen:

**c) Datenquellen**

Welche Datenquellen die Institute vorwiegend nutzen, können Sie auf dieser Darstellung erkennen:

**d) Datenlöschkonzept**

Ein vollständiges und rechtlich beanstandungsfreies Datenlöschkonzept konnten 18 Institute (48,6 %) vorweisen. Sieben weitere Institute (18,9 %) besaßen zwar ein solches Konzept. Doch war dieses teilweise unrichtig und musste daher nachgebessert werden. 12 Institute (32,4 %) konnten indes kein ausreichendes bzw. schlüssiges Datenlöschkonzept vorlegen.

e) Sonstige Erkenntnisse

Eine für mich überraschende Erkenntnis dieser Kontrolle war, dass nicht wenige Markt- und Meinungsforschungsinstitute „nur“ mit bereits anonymisierten Datensätzen arbeiten, die sie wiederum von Feldforschung-Dienstleistern erhalten bzw. ankaufen.

Diese Dienstleister erheben die gewünschten personenbezogenen Daten und übermitteln anschließend anonymisierte Datenbestände in aggregierter Form u. a. an Markt- und Meinungsforschungsinstitute (siehe auch Bergmann/Möhrle/Herb, Datenschutzrecht, Rn. 3 zu § 30 BDSG), die daraus dann die entsprechenden Erkenntnisse gewinnen. Teilweise stellen diese Feldforschung-Dienstleister auch Interview- und Diskussionsräume zur Verfügung und rekrutieren die zu befragenden Personen nach den gewünschten Kriterien bzw. Merkmalen. Markt- und Meinungsforschungsinstitute mieten dann diese Räume an und führen die Gespräche, Diskussionen oder Interviews durch. Von den zu befragenden Personen kennen sie in der Regel nur den Vornamen und einige Merkmale (zum Beispiel männlich, Alter zwischen 25 und 30 Jahre, Familienvater, Tennisspieler).

Liegen aber den Instituten lediglich anonymisierte Datenbestände vor, kommt die Anwendung der Vorschriften des BDSG allein wegen der Geschäftstätigkeit nicht in Betracht, da diese die Verarbeitung personenbezogener Daten voraussetzt (§ 1 Absätze 1 und 2 BDSG).

Viele der überprüften Unternehmen legen ein großes Bewusstsein für Datenschutz an den Tag, erfüllen die organisatorischen und rechtlichen Anforderungen an den Datenschutz, erstatten rechtzeitig die fälligen Meldungen und dokumentieren ihre Verfahren sorgfältig. Viele der Unternehmen mit gewissen Defiziten in Sachen Datenschutz zeigten sich durchaus interessiert und kooperativ. Das Instrument der

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

branchenweiten schriftlichen Datenschutzkontrolle hat sich damit bewährt. Ich plane daher, künftig weitere branchenweite Prüfkaktionen durchzuführen. Aber auch bei diesen Kontrollen geht es mir in erster Linie darum, durch Information und Beratung zu einem datenschutzkonformen Umgang mit personenbezogenen Daten in den verantwortlichen Stellen zu kommen und dadurch auch die Gefahr von Datenpannen und die Anzahl der Beschwerden an meine Dienststelle zu reduzieren.

10.12 Datensparsame Fototaschen

Wenn Unternehmen über Sinn und Zweck ihrer Verarbeitung personenbezogener Daten nicht gerade deshalb informieren müssen, weil sie etwas haben wollen, das sie nur mit informierter Einwilligung bekommen, oder weil die betroffene Person selbst um Auskunft gebeten hat, lässt die Transparenz gelegentlich etwas zu wünschen übrig. Insbesondere bei der Direkterhebung personenbezogener Daten werden wichtige Informationen oft „eingespart“ – die betroffene Person könnte ja einfach nachfragen, wenn etwas unklar ist. Sich deshalb zurückzulehnen und auf eventuelle Nachfragen zu warten, führt allerdings zu einer datenschutzwidrigen Intransparenz.

Manchmal bringen an sich datenschutzfreundliche, weil von der Konzeption her datensparsame Verfahren den betroffenen Personen nicht nur Vorteile. So geschehen bei der Entwicklung von Urlaubsfotos, die eine Beschwerdeführerin bei einem Drogeriemarkt in Auftrag gegeben hatte, indem sie die verwendete Einwegkamera in einer sogenannten Fototasche in den dafür vorgesehenen Behälter im Selbstbedienungsbereich des Marktes warf.

Solche Selbstbedienungsservices sind vor allem aus Drogeriemärkten längst nicht mehr wegzudenken. Dabei scheint das Verfahren überall im Wesentlichen das gleiche zu sein: Auf den von den Märkten dafür bereitgehaltenen Fototaschen, in die verpackt das Speichermedium in den zugehörigen Kasten eingeworfen werden soll, sind dabei in der Regel Eintragungen für Name, Anschrift, Telefonnummer und Datum vorgesehen. Die Zwecke dieser Abfrage und ggf. einer weiteren Verarbeitung waren zum damaligen Zeitpunkt nirgends angegeben. Ersichtlich war lediglich, dass diese Daten am Ende – für alle Interessierten gut ablesbar – in den Fächern

prangen würden, in die die Fototaschen mit den entwickelten Bildern zur Selbstabholung gestellt werden.

Leider tauchten die Urlaubsfotos der Beschwerdeführerin dort nie auf. Der Dienstleister, der für den eigentlichen Entwicklungsvorgang zuständig war, konnte auf ihre Reklamation hin den Weg der Negative offenbar auch nicht nachverfolgen, obwohl sie sämtliche Felder ausgefüllt hatte.

Aus Sorge, was denn nun mit ihren Bildern geschehen könne und ob das Verfahren möglicherweise nicht sicher sei, wandte sie sich an mich. Bei meiner Prüfung fand ich keine Hinweise darauf, dass die angewandte Verfahrensweise nicht datenschutzkonform oder unsicher sein könnte. Die nötige Datensparsamkeit und streckenweise Anonymisierung haben allerdings auch – in diesem Fall eben zum Leidwesen der betroffenen Person – zur Folge, dass zur Entwicklung abgegebene Filme nur sehr eingeschränkt nachverfolgt werden können.

Damit musste sich die Beschwerdeführerin wohl oder übel zufriedengeben. Allerdings war nun endgültig unklar, welchen Sinn und Zweck die Datenabfrage auf den Fototaschen eigentlich hatte.

Auf meine Nachfrage trug der Drogeriemarkt vor, dass es für die Vertragserfüllung nicht erforderlich sei, eine dieser Angaben zu machen. Während der Entwicklung würden sie nicht verwendet, und bei der Abholung durch die Kunden genüge es, dass die vorgedruckte Seriennummer auf dem Abholausweis mit der entsprechenden Seriennummer auf der Fototasche übereinstimmt. Der einzige Unterschied bestehe darin, dass eine „adressierte“ Fototasche auch ohne Abholausweis abgeholt werden könne, wenn der Personalausweis vorgezeigt wird sowie Name und Anschrift übereinstimmen. Nur in diesem Zusammenhang würden die auf der Fototasche eingetragenen Daten unternehmensseitig überhaupt zur Kenntnis genommen.

Da es sich sämtlich um freiwillige Angaben handelte, die jedenfalls nicht völlig zweckfrei bei der betroffenen Person direkt erhoben werden sollten, war materiellrechtlich, d. h. hinsichtlich der Zulässigkeit dieser Datenverarbeitung an sich, nichts dagegen einzuwenden. Nichtsdestoweniger wurde die daten-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

schutzrechtliche Grundpflicht zur Transparenz nicht eingehalten, denn es fehlten

- die aktive Information über die Zwecke dieser Erhebung und der anschließenden Verwendung (§ 4 Absatz 3 Satz 1 Nummer 2 BDSG) und
- der Hinweis auf die Freiwilligkeit der Angaben und ggf. den „Preis“ ihrer Verweigerung (§ 4 Absatz 3 Satz 2 BDSG):

§ 4 BDSG
*Zulässigkeit der Datenerhebung,
-verarbeitung und -nutzung*

...

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über die Identität der verantwortlichen Stelle, die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Zwar haben diese sogenannten Unterrichtungspflichten – anders als es die Überschrift des Paragraphen ankündigt – nach herrschender Ansicht oft keinen unmittelbaren Einfluss darauf, ob der anschließende Umgang mit personenbezogenen Daten zulässig ist. Diese vermeintliche rechtliche Unverbindlichkeit endet aber spätestens da, wo die Unterrichtung – bewusst oder versehentlich – lückenhaft war und die betroffene Person die Angaben nicht gemacht hätte, wäre sie korrekt und umfassend über deren weitere Verwendung informiert worden.

Nebenbei bemerkt besteht auch ein wesentlicher Bestandteil der Datensparsamkeit – zu der bekannt-

lich § 3a BDSG allgemein verpflichtet – darin, dass die betroffene Person selbst weiß, welche Angaben sie sich von vornherein (er)sparen kann.

Da sich in diesem Fall keine unerwartete Datenverarbeitung anschloss, bestand auch die Gefahr ihrer Unzulässigkeit hier nicht. Das änderte aber selbstverständlich nichts an der gesetzlichen Pflicht zur Unterrichtung.

Auf mein Einwirken hin wurden die Datenfelder auf den Fototaschen durch einen kurzen Text ergänzt, in dem auf die Freiwilligkeit der Angaben und die komfortablere Auftragsabwicklung als deren Verwendungszweck und zugleich äußersten Rahmen hingewiesen wird. Ein Hinweis auf die Folge der Verweigerung dieser Angaben – dass die Bilder bei Verlust des Abholscheins dann nicht mehr abgeholt werden können – ist hier nicht erforderlich; diese Folge ist leicht abzusehen, zumal dies das von Theatergarderoben und Textilreinigungen altbekannte Standardverfahren ist.

Im Nachhinein finde ich es allerdings bemerkenswert zu beobachten, wie viele Leute offenbar anstandslos Angaben über sich selbst machen (und erst damit den Personenbezug ihrer Fotos für jeden sicherstellen, der an den Abholfächern vorbeikommt und bei Interesse nur hineinzugreifen braucht), nur weil ihnen vom Anbieter ein Formular hingehalten wird – möglicherweise im vollsten Vertrauen darauf, dass das alles schon seine Richtigkeit haben wird.

Die datenschutzrechtlichen Transparenzpflichten rund um die Direkterhebung werden noch allzu oft vernachlässigt, zumal sie nicht unmittelbar mit der Zulässigkeit der sich ggf. anschließenden Datenverarbeitung zusammenhängen. Andererseits sollten die (potentiell) betroffenen Personen nicht gleich jede Angabe über sich machen, nur weil ihnen ein entsprechendes Formular die Gelegenheit hierzu bietet. Warum sollten sie sich überall persönlich „outen“, wo es auch eine Garderobenmarke oder ein Abholschein täte?

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

10.13 Mehr Rechte für Verbraucherschutzorganisationen: Erweiterung des Unterlassungsklagegesetzes um datenschutzrechtliche Vorschriften

Mit dem „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“ (vgl. Entwurf vom 13. Februar 2015, BR-Drs. 55/15) verfolgt die Bundesregierung insbesondere das Ziel, datenschutzrechtliche Vorschriften (Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zu kommerziellen Zwecken) in den Katalog unterlassungsklagefähiger Verbraucherschutzgesetze aufzunehmen.

Neben den Datenschutzaufsichtsbehörden und der Bundesnetzagentur haben schon heute auch Verbraucherschutzorganisationen die Möglichkeit, Verbraucherinteressen in Datenschutzangelegenheiten wahrzunehmen. Insbesondere steht ihnen ein Verbandsklagerecht zu,

- wenn der Datenschutzfall im direkten Zusammenhang mit der Verwendung Allgemeiner Geschäftsbedingungen steht (§ 1 des Unterlassungsklagegesetzes, UKlaG) oder
- wenn die gerügte Bestimmung zugleich einen Verstoß gegen ein Verbraucherschutzgesetz im Sinne von § 2 UKlaG darstellt.

Datenschutzverstöße durch Unternehmen können von den Verbraucherorganisationen somit zum einen nur dann verfolgt werden, wenn die von einem Unternehmen verwendete Datenschutzbestimmung eine Regelung in Allgemeinen Geschäftsbedingungen (AGB) im Sinne des § 305 BGB ist und diese den Verbraucher unangemessen benachteiligt, also gegen datenschutzrechtliche Vorschriften wie zum Beispiel BDSG oder TMG verstößt. In diesem Fall kann der Verbraucherverband ein Unternehmen abmahnen, das heißt, auf Unterlassung in Anspruch nehmen.

Gehört die beanstandete Datenschutzbestimmung nicht zu den Allgemeinen Geschäftsbedingungen des Unternehmens, scheidet ein Einschreiten der Verbraucherschutzorganisation grundsätzlich aus. Gleiches gilt, wenn eine Datenschutzregelung nicht inhaltlich, sondern formal beanstandet werden soll – etwa, wenn eine Regelung drucktechnisch hervor-

gehoben werden müsste (z. B. nach § 28 Absatz 3a Satz 2 BDSG), da § 1 UKlaG nur die AGB-rechtliche Inhaltskontrolle einer Bestimmung vorsieht.

§ 2 UKlaG wiederum fordert, dass es sich um einen Verstoß gegen ein Verbraucherschutzgesetz handeln muss, die streitgegenständliche Norm muss also in erster Linie dem Schutz des Verbrauchers dienen. Die Rechtsprechung kommt hier regelmäßig zum Ergebnis, dass es sich bei datenschutzrechtlichen Vorschriften wie etwa dem BDSG nicht in erster Linie um ein Verbraucherschutzgesetz handle. Das BDSG diene vielmehr dem Schutz des allgemeinen Persönlichkeitsrechts, zudem seien Adressat alle natürlichen Personen, nicht jedoch speziell die Verbraucher (vgl. nur OLG Frankfurt/Main, Urteil v. 30. Juni 2005, Az.: 6U 168/04).

Der bisherige Rechtsrahmen gibt den Verbraucherschutzorganisationen somit im Ergebnis derzeit nur eingeschränkte Möglichkeiten der Verfolgung von Datenschutzverstößen.

Dies möchte die Bundesregierung künftig ändern: Zentrales Element ihres Gesetzentwurfs ist die in Artikel 3 des Entwurfs eines „Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“ vorgesehene Erweiterung der in § 2 UKlaG vorgesehenen Ansprüche der Verbraucherschutzorganisationen und der sonstigen nach § 3 UKlaG anspruchsberechtigten Stellen auf alle „Vorschriften, die für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Verbrauchers durch einen Unternehmer gelten“ (§ 2 Absatz 2 Nr. 11 UKlaG-Entwurf).

Die Neuregelung in § 2 Absatz 2 UKlaG soll folgenden Wortlaut erhalten:

*„11. die Vorschriften, welche die Zulässigkeit regeln
a) der Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer oder
b) der Verarbeitung oder der Nutzung personenbezogener Daten, die über einen Verbraucher erhoben wurden, durch einen Unternehmer,*

wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betriebes einer Auskunft, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden.

Eine Datenerhebung, Datenverarbeitung oder Datennutzung zu einem vergleichbaren kommerziellen Zweck im Sinne des Satzes 1 Nummer 11 liegt insbesondere nicht vor, wenn personenbezogene Daten eines Verbrauchers von einem Unternehmer ausschließlich für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Verbraucher erhoben, verarbeitet oder genutzt werden.“

Die oben dargestellten Lücken sollen auf diese Weise geschlossen werden.

Neu ist auch, dass den Verbraucherschutzorganisationen neben dem bisherigen Unterlassungsanspruch ein Anspruch auf Beseitigung zugestanden wird (§ 2 Absatz 1 Satz 1 UKlaG-E), der etwa das Löschen oder Sperren unzulässig gespeicherter Verbraucherdaten ermöglichen soll.

Um künftig eine abgestimmte und einheitliche Anwendungspraxis des Datenschutzrechts zu gewährleisten, ist – insbesondere auch auf Druck der Datenschutzaufsichtsbehörden – im Gesetzentwurf in Anlehnung an die bestehende Regelung des § 8 Absatz 2 UKlaG in einem neuen § 12a des Gesetzentwurfs eine Verpflichtung für die Gerichte vorgesehen, in datenschutzrechtlichen Verbandsklageverfahren von Verbraucherschutzorganisationen die Datenschutzaufsichtsbehörde zu beteiligen und anzuhören, wenn auch leider nicht in den Eilverfahren.

Der Deutsche Bundestag hat den Gesetzentwurf am 17. Dezember 2015 weitgehend unverändert angenommen (vgl. BR-Drs. 4/16 vom 8. Januar 2016). In Artikel 3 § 17 wurde eine Übergangsfrist für die erweiterte Klagebefugnis von Verbänden bis zum 30. September 2016 für Datenübermittlungen, die vor dem 6. Oktober 2015 auf die Entscheidung 2000/520/EG der Kommission (sog. „Safe Harbor-Entscheidung“) gestützt wurden, aufgenommen. Da der Europäische Gerichtshof diese Entscheidung mit Urteil vom 6. Oktober 2015 aufgehoben hatte (vgl. Kapitel 1.4.3), soll den Unternehmen auf diese Weise mehr Zeit gegeben werden, ihre Datenüber-

mittlung auf eine andere rechtssichere Grundlage zu stützen.

Projekt „Marktwächter Digitale Welt“

In diesem Zusammenhang ist auch das neue Projekt „Marktwächter Digitale Welt“ der Verbraucherzentralen zu nennen. Seit Jahresbeginn 2015 werden diese Marktwächter aufgebaut. Sie sollen den Markt als eine Art „Frühwarnsystem“ beobachten und nach der Devise „Erkennen – Informieren – Handeln“ die Interessen der Verbraucher durchsetzen helfen. Die Marktwächter – neben der digitalen Welt geht es um den Finanzmarkt – sind ein gemeinsames Vorhaben des Bundesverbands der Verbraucherzentralen (vzbv) und der 16 Landesverbraucherzentralen.

Im Marktwächter Digitale Welt wirken fünf Schwerpunktverbraucherzentralen mit, die jeweils ein Handlungsfeld des digitalen Marktes näher untersuchen: Bayern (Digitale Dienstleistungen), Brandenburg (Digitaler Wareneinkauf), Nordrhein-Westfalen (Nutzergenerierte Inhalte), Rheinland-Pfalz (Digitale Güter) und Schleswig-Holstein (Telekommunikationsdienstleistungen). Die zentrale Koordination liegt auch hier beim vzbv. Die Verbraucherzentrale Baden-Württemberg hat ihren Schwerpunkt im Bereich des Finanzmarkts gesetzt, für den ein anderer Marktwächter etabliert wird.

Untersuchungsbedarf im Bereich des Marktwächters Digitale Welt besteht aus Sicht des Verbraucherzentralen neben den klassischen Telekommunikationsdienstleistungen u. a. beim eCommerce und mCommerce, bei digitalen Gütern und Dienstleistungen (wie Vergleichsportalen) sowie bei nutzergenerierten Inhalten.

Die Datenschutzaufsichtsbehörden sind im Beirat des Marktwächters Digitale Welt durch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg vertreten.

Der Marktwächter Digitale Welt wird bis Ende 2017 mit rund 4,5 Mio. Euro durch das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) gefördert.

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

Ich begrüße grundsätzlich die in dem Gesetzentwurf vorgesehene Stärkung und Erweiterung des Verbandsklagerechts der Verbraucherschutzorganisationen, die künftig umfassender Datenschutzverstöße abmahnen und auf deren Unterlassung klagen können. Zwar kann ich vereinzelte Kritik am Gesetzentwurf aus gesetzes- und aufgabensystematischer Hinsicht durchaus nachvollziehen. Jedoch überwiegt das wichtige Ziel, Verbündete – hier die Verbraucherschutzorganisationen – im Einsatz für mehr Datenschutz und damit mehr informationelle Selbstbestimmung des Einzelnen zu stärken und die Schlagkraft des Datenschutzes insgesamt zu erhöhen.

10.14 Orientierungshilfe zur Mieterelbstauskunft

Wer eine Wohnung vermietet, will den Mieter verständlicherweise sorgfältig auswählen. Das Fragerecht des Vermieters darf jedoch nicht zum gläsernen Mietinteressenten führen.

Wohnraum ist besonders in Großstädten ein knappes Gut. Da überrascht es nicht, wenn Vermieter angesichts der großen Auswahl an Mietinteressenten darauf bedacht sind, von diesen peinlichst genau Auskunft über ihre persönlichen und wirtschaftlichen Verhältnisse zu erhalten. Diese Neugier muss jedoch ihre Grenzen haben. Der Vermieter darf den Mietinteressenten vor Abschluss eines Mietvertrags grundsätzlich nach allem fragen, was er wissen muss, um zu beurteilen, ob der Mietinteressent voraussichtlich seine Pflichten aus dem Mietverhältnis erfüllen wird. Zu den hierfür erforderlichen Angaben gehören beispielsweise nicht Mitgliedschaften in Parteien oder Mietervereinen. Auch Fragen nach der persönlichen Lebensplanung, wie Heiratsabsichten, Schwangerschaft oder Kinderwunsch sind unzulässig. Darüber hinaus darf der Vermieter den Mietinteressenten nicht nach dessen bisherigen Vermietern fragen, etwa um bei diesen – entgegen dem datenschutzrechtlichen Direkterhebungsgrundsatz – weitere Erkundigungen über den Mietinteressenten einzuholen. Generell kann hinsichtlich der gebotenen Interessenabwägung zwischen (bis zu) drei Phasen unterschieden werden: a) dem Besichtigungstermin, b) der vorvertraglichen Phase, in der der Mietinteressent dem Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen, und c) der Entscheidung des Vermieters für einen bestimmten

Mietinteressenten. Als Faustformel kann man sagen, dass das Fragerecht des Vermieters in dem Maße zunimmt, wie das Mietverhältnis konkret wird. Beispielsweise ist es im Besichtigungstermin noch nicht erforderlich, sich nach den wirtschaftlichen Verhältnissen des Mietinteressenten zu erkundigen; hingegen darf sich der Vermieter Angaben zur Identität des Interessenten geben lassen und diese ggf. durch einen Blick in den Personalausweis überprüfen (ohne sich davon allerdings eine Kopie machen zu dürfen). Rückt der Abschluss des Mietvertrages in greifbare Nähe, sind wiederum Fragen des Vermieters nach den wirtschaftlichen Verhältnissen des Interessenten statthaft; wenn es zur Unterschrift durch einen bestimmten Mietinteressenten kommt, darf sich der Vermieter auch dessen Verdienstbescheinigungen vorlegen lassen. Der künftige Mieter hat dabei das Recht, die für das Mietverhältnis nicht relevanten Informationen zu schwärzen (beispielsweise hinsichtlich der aus dem Einkommenssteuerbescheid ersichtlichen Religionszugehörigkeit).

Um den Umfang des vermietenseitigen Fragerechts klarzustellen, haben die Datenschutzaufsichtsbehörden des Bundes und der Länder im Jahr 2014 eine Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten erarbeitet. Diese ist auf der Webseite meiner Dienststelle unter <http://www.baden-wuerttemberg.datenschutz.de/dokumente-des-duesseldorfer-kreises> abrufbar.

Die Orientierungshilfe der Datenschutzaufsichtsbehörden zeigt Leitlinien für einen sachgerechten Ausgleich zwischen dem Eigentumsinteresse des Vermieters und dem Grundrecht auf informationelle Selbstbestimmung des Mietinteressenten auf.

10.15 Geldwäschebekämpfung mit Personalausweiskopien

Um Geldwäsche zu bekämpfen, sollen Banken bei Aufnahme der Geschäftsbeziehung ihre Kunden identifizieren. Zu deren Unmut darf dabei auch der Personalausweis kopiert werden.

Immer wieder erreichen mich Anfragen von Bürgern, die verunsichert sind, weil ihr Kreditinstitut eine Kopie ihres Personalausweises angefertigt und zu seinen Unterlagen genommen hat. Diese Praxis ist aus datenschutzrechtlicher Sicht im Ergebnis nicht zu beanstanden. Die Bank ist nämlich nach § 3 Ab-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

satz 1 Nr. 1 und Absatz 2 Satz 1 Nr. 1 des Geldwäschegesetzes (GwG) verpflichtet, den Kunden bei Begründung der Geschäftsbeziehung zu identifizieren. Zu diesem Zweck hat sie gem. § 4 Absatz 3 Nr. 1 GwG den Namen, den Geburtsort, das Geburtsdatum, die Staatsangehörigkeit und die Anschrift des betroffenen Kunden zu erheben. Diese Angaben sind nach § 4 Absatz 4 Satz 1 Nr. 1 GwG anhand eines amtlichen Ausweises, wie zum Beispiel des Personalausweises, zu überprüfen.

Die Bank unterliegt aber nicht nur einer Identifizierungs-, sondern auch einer Aufzeichnungspflicht. Sie hat daher nach § 8 Absatz 1 Satz 1 GwG die im Rahmen der Kundenidentifizierung erhobenen Daten aufzuzeichnen. Dies gilt gem. § 8 Absatz 1 Satz 2 GwG auch für die Art und die Nummer des vorgelegten Ausweisdokuments und die Angabe der ausstellenden Behörde. Um diese Aufzeichnungspflichten zu erfüllen, wäre es grundsätzlich ausreichend, die Identitätsdaten des Kunden aus dem von ihm vorgelegten Personalausweis in ein Kundenformular zu übernehmen und schriftlich zu vermerken, dass der Personalausweis vorgelegen hat. § 8 Absatz 1 Satz 3 GwG sieht aber für die aufzeichnungspflichtige Stelle folgende Verfahrenserleichterung vor: „Die Anfertigung einer Kopie des zur Überprüfung der Identität vorgelegten Dokuments (gilt) als Aufzeichnung der darin enthaltenen Angaben.“ Die Bank ist daher berechtigt, eine Kopie des Personalausweises zu fertigen (und fünf Jahre lang aufzubewahren), obwohl nicht alle darin enthaltenen Daten der Aufzeichnungspflicht unterliegen (Verwaltungsgericht Hannover, Urteil vom 28. November 2013, Az. 10 A 5342/11). Dies gilt beispielsweise für die Augenfarbe, die Körpergröße und die für das Auslesen des im Ausweis enthaltenen Chips benötigte Zugangsnummer.

Dieses Ergebnis ist aus datenschutzrechtlicher Sicht wenig erfreulich, zumal nicht ausgeschlossen werden kann, dass Ausweiskopien abhandenkommen und Dritten unberechtigt zur Kenntnis gelangen. Im Interesse der informationellen Selbstbestimmung der Kunden sollten die Banken und sonstige nach dem Geldwäschegesetz verpflichtete Stellen daher die vorgenannten Daten in den Personalausweiskopien schwärzen. Dies könnte auch durch die Nutzung einer Schablone geschehen, die sicherstellt, dass die nicht aufzeichnungspflichtigen Daten gar nicht erst mitkopiert werden.

Banken und andere Stellen, die aufgrund des Geldwäschegesetzes die Personalausweise ihrer Kunden kopieren, sollten alle nicht benötigten Daten in den Kopien schwärzen.

10.16 In der Post verschollen: Meldepflicht bei Datenverlust

Die meisten Unternehmen kennen erfreulicherweise ihre Informationspflichten, wenn Dritte unrechtmäßig von personenbezogenen Daten Kenntnis genommen haben. Wie aber ist zu verfahren, wenn mit der Post versandte Daten über längere Zeit nicht wieder auftauchen und ihr Schicksal ungewiss bleibt?

Eine Bank wandte sich an mich, nachdem sie eine größere Anzahl personenbezogener Bankkontodaten ihrer Kunden auf dem Postdienst versandt hatte und die Sendungen offenbar nicht angekommen waren. Da die Sendungen mehrere Tage lang weder die Empfänger erreichten noch zum Absender zurückkamen, wollte die Bank wissen, ob sie den Vorfall als „Datenpanne“ nach § 42a des Bundesdatenschutzgesetzes (BDSG) den Betroffenen und meiner Dienststelle zu melden habe. Eine solche Informationspflicht ist grundsätzlich zu bejahen. Zwar stellt der Wortlaut der Vorschrift darauf ab, dass die verantwortliche Stelle eine unrechtmäßige Kenntniserlangung der Daten positiv feststellt. Wollte man aber bei ungewissem Schicksal der versendeten Daten eine Informationspflicht ablehnen, so liefe dies dem Schutzzweck des § 42a BDSG zuwider. Die Meldepflicht soll beim Verlust sensibler personenbezogener Daten, deren unberechtigte Kenntniserlangung leicht zu einer schwerwiegenden Beeinträchtigung des Betroffenen führen kann, den Betroffenen und die Datenschutzaufsichtsbehörde in die Lage versetzen, negative Konsequenzen eines solchen Vorfalls abzuwenden. Dies ist nur möglich, wenn die verantwortliche Stelle mit der Meldung nicht zuwartet, bis ein endgültiger Datenverlust oder eine unberechtigte Kenntniserlangung Dritter sicher feststeht, sondern bereits die längere Nichtauffindbarkeit der Daten meldet.

Für verschollene Postsendungen gilt daher Folgendes: Erfährt die verantwortliche Stelle, dass eine Sendung mit Daten im Sinne des § 42a BDSG nach fünf Tagen, gerechnet ab dem Tag, der dem Tag der Absendung folgt, nicht beim Empfänger eingegangen ist, so hat sie die Aufsichtsbehörde und die

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

Betroffenen nach § 42a BDSG zu informieren, wenn die Sendung nicht umgehend ausfindig gemacht werden kann. Dies gilt nicht, wenn das Ende der Frist auf einen Sonntag fällt.

Der Verlust personenbezogener Daten ist auch dann zu melden, wenn eine Kenntnisnahme Dritter nicht feststeht.

10.17 Hinweisinformationssystem der Versicherungswirtschaft (HIS)

Im Berichtszeitraum hat meine Dienststelle einen Kontrollbesuch bei der informa Insurance Risk and Fraud Prevention GmbH in Baden-Baden, der Betreiberin des HIS, durchgeführt. Dort können die Versicherungen Personen und Sachen einmelden, von denen für die Versicherungswirtschaft ein besonderes Risiko ausgeht. Umgekehrt fragen die Versicherungsunternehmen dort an, wenn sie einen Versicherungsvertrag abschließen oder einen Schadensantrag bearbeiten, ob sie es mit einem potentiellen Betrüger oder jedenfalls mit einer Person zu tun haben, von der ein besonderes Risiko ausgeht. Insgesamt sind im HIS derzeit 1,7 Millionen Datensätze zu Personen und 2,5 Millionen Kraftfahrzeuge gespeichert.

Die § 28 Absatz 2 Nr. 1 und § 29 Absatz 1 Satz 1 Nr. 1 BDSG lassen eine Einmeldung in das HIS bzw. eine Speicherung in diesem System nur zu, wenn dafür ein berechtigtes Interesse besteht und ein schutzwürdigeres Interesse des Betroffenen am Unterbleiben einer solchen Datenverarbeitung nicht überwiegt. Vergleichbare Regelungen finden sich sowohl im Code of Conduct der Versicherungswirtschaft wie auch in den Verträgen der informa Insurance Risk and Fraud Prevention GmbH mit den zur Einmeldung berechtigten Versicherungen. Das bedeutet, dass diese Versicherungen jeweils im Einzelfall eine Abwägung vorzunehmen haben, ob in der Person des Betroffenen ein besonderes Risiko vorliegt, von dem andere Versicherer für den Fall, dass der Betroffene mit ihnen ein Versicherungsverhältnis begründen oder ihnen gegenüber einen Schaden geltend machen will, informiert werden sollten, oder ob das Recht des Betroffenen, bei Dritten nicht in Misskredit gebracht zu werden, vorgeht.

Von einem berechtigten Interesse der Versicherungswirtschaft, andere Versicherer zu warnen, kann in der Regel in folgenden Fällen ausgegangen werden:

- Jede Art von betrügerischem Verhalten, wobei ein solches bereits angenommen werden kann, wenn der Betroffene beim Abschluss eines Versicherungsvertrages oder bei der Geltendmachung eines Schadensersatzanspruchs erst auf hartnäckiges Nachfragen von Seiten der Versicherung den wahren Sachverhalt einräumt.
- Wenn ein Versicherungsnehmer seine Versicherung mehrfach in Anspruch nimmt und erwiesen ist, dass er mit der versicherten Sache sorglos umgegangen ist. Letzteres wird er bei einem Versicherungsverwechsel sicher nicht zugeben.
- Die Identifizierungsdaten von Kraftfahrzeugen, die abhandengekommen oder die bei einem Unfall beschädigt worden sind. Das gilt nicht nur in den Fällen, bei denen der Unfallschaden „auf Gutachterbasis“ abgerechnet worden ist (es sei denn, das Fahrzeug ist endgültig verschrottet worden, weil dann keine Wiederholungsgefahr mehr besteht). Es gilt auch in den Fällen, in denen das beschädigte Fahrzeug repariert worden ist. Zwar drängt sich hier die Frage auf, ob es nicht eine gewisse Bagatelldgrenze geben sollte, also beispielsweise die Daten eines bestimmten Fahrzeugs erst ab dem dritten Unfall registriert werden. Das würde aber voraussetzen, dass die beiden ersten Unfälle bekannt sind, denn sonst wüsste man ja nicht, dass es sich bereits um den dritten Unfall mit diesem Fahrzeug handelt. Die Polizei hat dementsprechend bestätigt, dass generell bereits der erste Versicherungsfall und dann alle folgenden registriert werden sollten, weil nur so dem systematischen Versicherungsbetrug auf die Spur zu kommen ist, insbesondere wenn der Täter jedes Mal eine andere Versicherung in Anspruch nimmt bzw. jeweils ein anderes Fahrzeug benutzt. Unerheblich ist dabei, dass den meisten Unfallverursachern bzw. Unfallgeschädigten eine derartige Absicht nicht unterstellt werden darf. Diese haben aber keinen Einfluss auf eine möglicherweise rechtswidrige Nutzung des Fahrzeugs, wenn sie es veräußert haben bzw. wenn es ihnen abhandengekommen ist.

Dagegen überwiegt das Interesse des Betroffenen, von einer Einmeldung im HIS verschont zu bleiben, für gewöhnlich, wenn

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

- er – auch wiederholt – Ansprüche gegen eine Versicherung geltend macht, von denen er berechtigerweise annimmt, dass sie ihm aufgrund von Gesetz oder Vertrag zustehen,
- er einen Antrag bei einer Versicherung zurücknimmt, es sei denn es gibt Anhaltspunkte, dass er bei einer weiteren Antragstellung unzutreffende Angaben machen oder der Versicherung maßgebliche Informationen bewusst vorenthalten wird,
- er seiner Bürgerpflicht als Zeuge nachgekommen ist, es sei denn, es besteht der begründete Verdacht, dass er falsche Angaben macht bzw. mit dem Anspruchsteller kollusiv zusammenwirkt oder
- er Fahrer oder Halter eines Fahrzeuges ist, das auf Rechnung eines Dritten versichert ist.

Auch dürfen im HIS keine Informationen gespeichert sein, die einen unzutreffenden oder irreführenden Eindruck von dem Betroffenen beim Empfänger vermitteln (vgl. OLG Karlsruhe MDR 2009, S. 156; ZD 2014, S. 474; Specht/Müller/Riemenschneider, NJW 2015, S. 727; Simitis, BDSG, 7. Aufl., § 28 RN 33 f.). Das ist insbesondere der Fall bei Angaben, die darauf schließen lassen, bei dem Betroffenen liege ein Risiko vor, obwohl das nicht zutrifft, bzw. deren Aussagegehalt so unbestimmt ist, dass sie nicht auf ihre Richtigkeit überprüft werden können (z. B. „Einmeldung gemäß Checkliste“ oder „Erschweris“).

Es sei jedem empfohlen, gelegentlich eine Selbstauskunft beim HIS einzuholen, was dort über ihn gespeichert ist, um rechtzeitig auf Löschung bzw. Klarstellung zu drängen.

10.18 Was man als Mieter über sich und alle anderen erfahren kann

Momentan sind Mietinteressenten wegen der großen Nachfrage nach bezahlbarem Wohnraum in einer schwachen Position. Aber müssen sie sich deswegen datenschutzrechtlich alles gefallen lassen?

Eine Wirtschaftsauskunftei bot auf ihrer Internet-Webseite Mietinteressenten an, eine Selbstauskunft zu ihrer Bonität anhand der bei der Auskunftei vorhandenen Informationen anzufordern, um damit ihrem künftigen Vermieter ihre Zahlungsfähigkeit

nachzuweisen. Dazu sollte der Mietinteressent auf einer Maske im Internet Anrede, Vor- und Nachname, E-Mail-Adresse, Mobilfunknummer, Geburtstag und Wohnanschrift eingeben und daraufhin per SMS einen Verifizierungscode erhalten, mit dem er auf der Webseite der Auskunftei sein Auskunftsersuchen bestätigen sollte. Nach Bezahlung einer Gebühr mittels Kreditkarte oder PayPal wurde dem Mietinteressenten die erbetene Selbstauskunft online angezeigt. Der datenschutzrechtliche Haken dabei war jedoch: Da bei der Auskunftei keine Prüfung erfolgte, ob der Anfragende sich nicht mit den Daten einer ganz anderen Person anmeldet, war es möglich, sensible Bonitätsdaten von fremden Menschen in Erfahrung zu bringen, indem man eine Anfrage mit dessen Personalangaben vornimmt.

Als dieser Missstand in der Öffentlichkeit bekannt wurde, stellte die Auskunftei das Portal ein. Wir kritisierten den unzulässigen Umgang mit den Bonitätsdaten und wiesen die Auskunftei darauf hin, dass eine datenverarbeitende Stelle einem nicht persönlich vorsprechenden Betroffenen nur Auskunft über die zu seiner Person gespeicherten Angaben (Selbstauskunft nach § 34 BDSG) geben darf, wenn dieser seine Identität in ausreichendem Maße nachweist. Vergleichbares gilt für die Übersendung einer PIN, mit der der Empfänger im Rahmen einer Mieterselbstauskunft einen Dritten, etwa den Vermieter, ermächtigen kann, bei der Auskunftei Bonitätsauskünfte einzuholen. Dazu geeignet ist jede Kopie eines amtlichen Ausweises, soweit sich aus diesem der Name, der Vorname, die Wohnanschrift, an die die Auskunft begehrt wird, und ggf. das Geburtsdatum ergeben. Weitere Möglichkeiten sind die Vorlage einer Meldebescheinigung, aus der hervorgeht, dass der Betroffene dort wohnt, wohin die Auskunft bzw. der PIN gesendet werden soll, sowie das PostIdent-Verfahren. Je heikler die Daten sind, desto höhere Anforderungen sind nach der neueren Rechtsprechung an den Identitätsnachweis zu stellen (VG Köln, Ur. v. 13.03.2014 – 13 K 7883/13 –, juris).

Inzwischen ist das Portal wieder online, ohne dass die erforderlichen Sicherheitsvorkehrungen gegen missbräuchliche Abfragen getroffen wurden. Die Auskunftei hat nicht einmal die von uns angeforderte Verfahrensbeschreibung und die für eine Vorabkontrolle erforderlichen Unterlagen i. S. des § 4d BDSG vorgelegt. Sollten wir feststellen, dass sich

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

die Auskunft auch weiterhin rechtswidrig verhält, werden wir den Betrieb dieses Portals untersagen.

10.19 Intelligente Stromzähler – Energiewende zu Lasten des Datenschutzes?

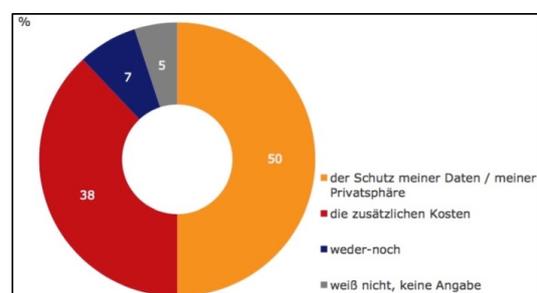
Intelligente Stromzähler, sog. Smart Meter, werden aller Voraussicht nach schon in naher Zukunft zum Einsatz kommen. Die Nutzung von Informationstechnik im Interesse eines effizienten Einsatzes der Energieressourcen darf jedoch nicht einseitig zulasten der informationellen Selbstbestimmung der Stromkunden gehen.

Die Bundesregierung hat am 4. November 2015 den „Entwurf eines Gesetzes zur Digitalisierung der Energiewende“ beschlossen und dem Bundesrat zugeleitet (BR-Drs. 543/15). Der Entwurf sieht ein Artikelgesetz vor, das zunächst in seinem Artikel 1 ein Messstellenbetriebsgesetz (MsbG) einführt und in weiteren Artikeln bestehende Vorschriften abändert. Im Mittelpunkt des Gesetzgebungsvorhabens steht die verpflichtende Einführung von intelligenten Stromzählern bei Haushalten mit einem jährlichen Stromverbrauch von über 6.000 Kilowattstunden. Mithilfe dieser Geräte soll der Messstellenbetreiber gem. § 60 MsbG die Verbrauchswerte im Abstand von 15 Minuten auslesen.

Die zeitgenaue Verbrauchserfassung mittels intelligenter Stromzähler soll eine Optimierung der Netzlaststeuerung sowie die Einführung zeitvariabler Stromtarife ermöglichen. Auf diese Weise sollen der Energieverbrauch gesenkt und natürliche Ressourcen geschützt werden. Dieses zweifellos unterstützenswerte Ziel darf aber nicht zur Aushöhlung der informationellen Selbstbestimmung der Endverbraucher führen.

Die Risiken, die für die informationelle Selbstbestimmung mit dem Einsatz intelligenter Stromzähler verbunden sind, wurden ebenso wie die datenschutzrechtlichen Anforderungen an die technisch-organisatorische Ausgestaltung bereits im 30. Tätigkeitsbericht meiner Dienststelle (LT-Drs. 15/955, 1. Teil, Kapitel 4.4) ausführlich dargestellt. Festzuhalten ist insbesondere, dass bei einer regelmäßigen Erhebung der Stromverbrauchswerte detaillierte Verhaltensprofile zum Endverbraucher erstellt werden können. Zudem können die Verbrauchswerte darüber Auskunft geben, wann die Wohnung des

Endverbrauchers leer steht und als Einbruchsubjekt in Frage käme. Daher überrascht es nicht, dass nach einer Umfrage im Auftrag des Verbraucherzentrale Bundesverband e.V. vom Oktober 2015 (siehe Abbildung) die Hälfte der befragten Verbraucher aufgrund von intelligenten Stromzählern Einbußen beim Schutz ihrer personenbezogenen Daten und eine Beeinträchtigung ihrer Privatsphäre befürchten.



Quelle:

<http://www.heise.de/newsticker/meldung/Verbraucherschuetzer-untermauern-ihre-Kritik-an-intelligenten-Stromzaehlern-2923413.html>

Angesichts der vorgenannten Risiken erscheint es nicht unbedenklich, dass intelligente Stromzähler nach dem Messstellenbetriebsgesetz viertelstündliche Energieverbrauchswerte erheben sollen. Hier sollten sich die verwendeten Systeme vielmehr auf Ausleseintervalle beschränken, die dem entsprechen, was für den jeweiligen Erhebungszweck erforderlich ist. Soweit die Erhebung der Laststeuerung dient, mögen Ausleseintervalle von 15 Minuten zwar erforderlich sein. Hier dürfte aber die Weitergabe an die Versorgungsunternehmen in aggregierter Form, also bezogen auf größere räumliche Einheiten mit mehreren Haushalten genügen. Da auf diese Weise kein Rückschluss auf den einzelnen Verbraucher möglich ist, wäre ein solches Verfahren aus datenschutzrechtlicher Sicht sinnvoll. Soweit hingegen die Verbrauchswerte zu Abrechnungszwecken erhoben werden, bedarf es zwar der Verbrauchswerte der einzelnen Haushalte. Die Verwendung viertelstündlich erhobener Werte ist jedoch nur erforderlich, wenn der Endverbraucher sich bewusst für einen Stromtarif entschieden hat, der je nach Tageszeit und in entsprechender Taktung einen unterschiedlichen Strompreis vorsieht. Solange solche zeitvariablen Tarife sich am Markt nicht durchgesetzt haben, sind für die Rechnungsstellung zeitlich ag-

32. Tätigkeitsbericht 2014/2015 - 10. Datenschutz in der Wirtschaft

regierte Verbrauchswerte, beispielsweise bezogen auf einen Monat oder ein Jahr, ausreichend. Zudem wäre selbst bei zeitvariablen Stromtarifen zu prüfen, inwieweit die Berechnung der Stromkosten lokal beim Verbraucher erfolgen kann, was ebenfalls eine Übermittlung detaillierter Verbrauchswerte an die Energieversorger entbehrlich machen würde.

Der Bundesverband der Verbraucherzentralen hat sich gegen das Gesetz zur Digitalisierung der Energiewende vor allem mit dem Argument einer „Zwangsdigitalisierung“ gewandt, weil auch Privathaushalten mit durchschnittlichem Stromverbrauch die neue Technik aufgezwungen werde, wenn der Messstellenbetreiber den Anschluss wünscht. Zudem sei das Kosten-Nutzen-Verhältnis für diesen Kundenkreis ungünstig. Diese Bedenken scheinen beim Bundesrat inzwischen auf fruchtbaren Boden gefallen zu sein, denn dieser hat am 18. Dezember 2015 u. a. eine „Ausstiegsklausel“ in § 36 Abs. 4 MsbG gefordert, die sich allerdings nicht auf den Einbau von intelligenten Messsystemen generell, sondern auf deren Einbindung in ein Kommunikationsnetz bezieht. Dabei haben auch die Sorgen der Verbraucher vor datenschutzrechtlichen Risiken eine Rolle gespielt.

Beim Einsatz intelligenter Stromzähler sollte von den Möglichkeiten der Aggregation im größtmöglichen Umfang Gebrauch gemacht werden. Meine Dienststelle wird den künftigen Einsatz intelligenter Stromzähler kritisch begleiten.

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

11. Technik und Medien

11.1 Videoüberwachung in allen Varianten

11.1.1 Einleitung

In meinem letzten Tätigkeitsbericht hatte ich über die Zunahme der Zahl der Anfragen und Beschwerden zum Thema Videoüberwachung und die Einrichtung einer Ad-hoc-Arbeitsgemeinschaft „Videoüberwachung“ der Aufsichtsbehörden des Bundes und der Länder berichtet (vgl. 31. TB 2012/2013, LT-Drs. 15/4600, Kapitel 11.1.1). Der Düsseldorfer Kreis hat die zunehmende Bedeutung des Themas erkannt und die Ad-hoc-Arbeitsgemeinschaft im Jahr 2014 verstetigt. Seither findet unter der Federführung meiner Dienststelle ein regelmäßiger Erfahrungs- und Meinungsaustausch der deutschen Datenschutzbehörden zu Fragen der Videoüberwachung statt. Als eines der ersten Arbeitsergebnisse wurde im Februar 2014 eine gemeinsame Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ veröffentlicht. Das Merkblatt klärt über die rechtlichen Voraussetzungen eines zulässigen Einsatzes von Videotechnik auf und enthält u. a. eine Checkliste für Betreiber von Videoüberwachungsanlagen. Die Orientierungshilfe ist auf meiner Internetseite in der Rubrik Service – Orientierungshilfen / Merkblätter unter dem Stichwort „Datenschutz beim Einsatz von Videokameras“ abrufbar.⁸³

Die AG Videoüberwachung hat außerdem als Zusatz zu dieser allgemeinen Orientierungshilfe Hinweise zur Videoüberwachung in Schwimmbädern (vgl. Kapitel 11.1.2) sowie zur Videoüberwachung in öffentlichen Verkehrsmitteln erarbeitet (vgl. Kapitel 11.1.3). Ferner wurden Beschlüsse des Düsseldorfer Kreises zu den Themen „Dashcams“ (vgl. Kapitel 11.1.5) und „Drohnen“ (vgl. Kapitel 11.1.6) initiiert.

11.1.2 Videoüberwachung in Schwimmbädern

Meine Dienststelle erreichen immer wieder Anfragen und Beschwerden zur Videoüberwachung in Schwimmbädern. Rutschen, Schwimmbecken, Mineralbäder, Babybecken, Liegewiesen, Umkleieräume und sogar Saunabereiche werden mitunter über-

wacht. Muss man es wirklich hinnehmen, in Badekleidung oder sogar entkleidet gefilmt zu werden?

Schwimmbäder in privater Trägerschaft, aber auch Bäder in öffentlicher Trägerschaft, welche als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, unterfallen dem Bundesdatenschutzgesetz (BDSG). Die Voraussetzungen für eine Überwachung öffentlich zugänglicher Bereiche ergeben sich damit aus § 6b BDSG. Hiernach ist eine Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Argumente der Schwimmbadbetreiber für eine Videoüberwachung sind so vielfältig wie die Standorte der Kameras: In Badebereichen wird häufig vorgetragen, der Aufenthalt im Wasser sei per se gefährlich und erfordere eine Beobachtung durch das Aufsichtspersonal. Da dieses nicht immer vor Ort sein kann, sei eine Monitorbeobachtung notwendig. Ferner könne man durch Videoaufnahmen die Wahrnehmung von Verkehrssicherungspflichten nachweisen und so das Haftungsrisiko gegenüber Ansprüchen von Badegästen verringern oder sogar ausschließen. Umkleidebereiche müssten aufgrund von Spindaufbrüchen überwacht werden. Kameras am Drehkreuz zur Sauna könnten verhindern, dass sich jemand unberechtigt Zutritt verschafft, und etwaige Verstöße gleichzeitig dokumentieren. Kameras in Saunabereichen würden der Sicherheit der Gäste dienen, da Notfälle schneller erkannt werden könnten.

Da sich die Schwimmbadbesucher im Schwimmbad oder in der Sauna zum Zweck der Freizeitgestaltung aufhalten und häufig nur wenig bekleidet sind, genießen sie besonderen Schutz; es muss daher besonders sorgfältig geprüft werden, ob die genannten gesetzlichen Voraussetzungen einer Videoüberwachung vorliegen. Um dem aus unserer Sicht vorhandenen „Wildwuchs“ der Überwachungstechnik in den Schwimmbädern zu begegnen und um über die rechtlichen Voraussetzungen gerade in diesem Bereich aufzuklären, haben die Aufsichtsbehörden ein Merkblatt veröffentlicht, das die allgemeine Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ (vgl. Kapitel 11.1.1) ergänzt und die

⁸³ <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/03/OH-VÜ-durch-nicht-öffentliche-Stellen.pdf>

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Besonderheiten bei der Videoüberwachung in Schwimmbädern herausstellt.

Die Orientierungshilfe betont, dass insbesondere die Erforderlichkeit einer Videoüberwachung kritisch zu hinterfragen ist. So kann der unberechtigte Zugang zu Bereichen, für die ein zusätzliches Entgelt zu entrichten ist, z. B. zum Saunabereich, durch andere geeignete Maßnahmen wie hohe Drehkreuze oder Schranken ohne unverhältnismäßigen Aufwand verhindert werden. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser berechtigt nicht zu einer personenscharfen Videoüberwachung und schon gar nicht zu einer Aufzeichnung. Der Einsatz von Videoüberwachungstechnik darf kein Ersatz für Aufsicht durch Personal sein! Im Ausnahmefall kann eine reine Beobachtung zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aber aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder statistisch belegbare Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen oder Kinderbecken) sprechen.

Da die Rechtsprechung mehrfach bestätigt hat, dass im Falle eines Unfalls die hinreichende Wahrnehmung der Verkehrssicherungspflicht nicht mit Videoaufzeichnungen nachgewiesen werden muss und der Geschädigte beweispflichtig ist, kann auch der Ausschluss des Haftungsrisikos den erheblichen Eingriff in das Persönlichkeitsrecht der Badegäste nicht rechtfertigen.

Schließlich ist hervorzuheben, dass die schutzwürdigen Interessen der Badegäste immer überwiegen, wenn die Intimsphäre berührt ist. Eine Videoüberwachung von Personen in Sanitärräumen, Umkleekabinen oder Umkleebereichen und in der Sauna ist daher generell unzulässig. Sofern es um die Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen geht, kann eine Videoüberwachung im Einzelfall zulässig sein. Wichtig ist in diesem Zusammenhang, dass nicht gleichzeitig Umkleidebereiche erfasst werden, den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Be-

reich sie sich begeben, und die überwachten Bereiche klar erkennbar sind.

Die Orientierungshilfe „Videoüberwachung in Schwimmbädern“ ist auf meiner Internetseite in der Rubrik Service – Orientierungshilfen / Merkblätter unter dem Stichwort „Datenschutz beim Einsatz von Videokameras“ abrufbar.⁸⁴

Videoüberwachung in Schwimmbädern ist ein sensibles Thema. Insbesondere aufgrund der Tatsache, dass Badegäste einer Freizeitbeschäftigung nachgehen und sich überwiegend in Badekleidung bewegen, ist besondere Sorgfalt geboten. Schwimmbadbetreiber sollten sich daher mit den Voraussetzungen einer Videoüberwachung gründlich auseinandersetzen.

11.1.3 Videoüberwachung in öffentlichen Verkehrsmitteln

Videoüberwachung in öffentlichen Verkehrsmitteln ist ein weiteres Thema, welches die Dienststelle im Berichtszeitraum beschäftigte. Regionalbahnen, U-Bahnen, S-Bahnen, Busse: Kaum ein öffentliches Verkehrsmittel lässt sich heutzutage unbeobachtet nutzen. Die stetig wachsende Zahl von Videoüberwachungsanlagen macht auch vor den öffentlichen Verkehrsmitteln nicht halt. In meiner aufsichtsbehördlichen Praxis konnte ich beobachten, dass Kameras in den Fahrzeugen immer häufiger zur Standardausstattung gehören. Das hängt nicht zuletzt auch mit den Forderungen in den Ausschreibungen der öffentlichen Auftraggeber zusammen.

Videoüberwachung ist unbestritten ein wichtiges Instrument zur Verfolgung von Straftaten im öffentlichen Personennahverkehr (ÖPNV) und im Schienenpersonennahverkehr (SPNV). Gleichzeitig wird jedoch durch eine undifferenzierte und flächendeckende Videoüberwachung erheblich in das Persönlichkeitsrecht des Einzelnen eingegriffen. Die berechtigten Interessen der Verkehrsunternehmen müssen daher in der Praxis mit dem informationellen Selbstbestimmungsrecht der Fahrgäste in einen fairen Ausgleich gebracht werden. Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben ein Merkblatt veröffentlicht, welches

⁸⁴ <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/11/OH-VUE-Schwimmbad.pdf>

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

den Verkehrsunternehmen, aber auch den öffentlichen Aufgabenträgern eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln bieten soll.

Zentrale Kernaussage des Papiers ist, dass vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln stets zu prüfen ist, ob sie für den verfolgten Zweck tatsächlich geeignet und erforderlich ist. Eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste ist unter dem Gesichtspunkt der Erforderlichkeit nicht geboten. Im Rahmen einer abwägenden Einzelfallprüfung ist nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und die Überwachung gemäß § 6b BDSG entsprechend zu beschränken. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist in aller Regel unverhältnismäßig und somit unzulässig. Die ausführliche Orientierungshilfe ist auf meiner Internetseite in der Rubrik Service – Orientierungshilfen / Merkblätter unter dem Stichwort „Datenschutz beim Einsatz von Videokameras“ abrufbar.⁸⁵

Mein Appell richtet sich insbesondere an die Aufgabenträger für den schienengebundenen Personennahverkehr, die Grundsätze der Orientierungshilfe zu beachten. In einem Muster des Fahrzeuglastenhefts ist aktuell für Ausschreibungen in Baden-Württemberg folgende Passage enthalten:

„Für die Überwachung des Fahrgastinnenraumes sind mit Ausnahme der Toilette Videokameras zu installieren. Die Anzahl ist dabei so zu bemessen, dass möglichst der gesamte, mindestens aber 90% des Fahrgastraums erfasst wird und eine Gesichtserkennung zu Ermittlungszwecken möglich ist.“

Diese pauschale und undifferenzierte Forderung nach einer möglichst umfassenden Videoüberwachung kann im Ergebnis zu Überwachungsmaßnahmen führen, die nicht mit § 6b BDSG zu vereinbaren sind. Die Verkehrsunternehmen befinden sich allerdings in einer Zwickmühle: Wenn sie die in den Ausschreibungen verlangte Fahrzeugausstattung liefern, können sie als verantwortliche Stellen in Konflikt mit dem Datenschutzrecht geraten. Halten sie sich an die datenschutzrechtlichen Prämissen,

laufen sie Gefahr, den Auftrag nicht zu bekommen. Ich beabsichtige daher, mit dem Ministerium für Verkehr und Infrastruktur Baden-Württemberg sowie der für die Ausschreibung zuständigen Nahverkehrsgesellschaft Baden-Württemberg Gespräche über eine datenschutzkonforme Modifizierung der Anforderungen zu führen.

Der zielgerichtete und effektive Einsatz von Videotechnik ist ein wichtiges Mittel zur Verfolgung von Straftaten in öffentlichen Verkehrsmitteln. Dabei gilt es jedoch auch die Persönlichkeitsrechte der Fahrgäste zu wahren und das Datenschutzrecht zu beachten. Meine Dienststelle wird sich auch künftig für den Schutz des informationellen Selbstbestimmungsrechts in ÖPNV und SPNV einsetzen.

11.1.4 Videoüberwachung durch Privatpersonen: Was sagt der EuGH?

Im Berichtszeitraum erging eine beachtenswerte Entscheidung des Europäischen Gerichtshofs (EuGH) zu der Frage, ob eine Videoüberwachung, die von einer Privatperson an einem Einfamilienhaus zum Schutz des Eigentums, der Gesundheit und des Lebens der Hausbewohner betrieben wird, aber auch öffentlichen Straßenraum erfasst, dem europäischen Datenschutzrecht unterfällt (Urteil vom 11. Dezember 2014, Rs. C-212/13 – Ryneš).

Die Europäische 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) findet gem. Artikel 3 Absatz 2 keine Anwendung auf die Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (sog. „Haushaltsprivileg“). Der EuGH betont in seinem Urteil vom 11. Dezember 2014, dass diese Ausnahme eng auszulegen ist. Eine Verarbeitung personenbezogener Daten sei nur dann vom Anwendungsbereich der Richtlinie ausgenommen, wenn sie in der ausschließlich persönlichen oder familiären Sphäre desjenigen vorgenommen wird, der die Daten verarbeitet. Das sei nicht der Fall, soweit sich eine Videoüberwachung auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten

⁸⁵ <http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/OH-VUE-OEPNV.pdf>

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet.

Das Urteil des EuGH ist von grundlegender Bedeutung auch für das deutsche Datenschutzrecht, das in § 1 Absatz 2 Nr. 3 BDSG eine entsprechende Ausnahme für ausschließlich persönliche oder familiäre Tätigkeiten enthält. Im Bereich der nachbarschaftlichen Videoüberwachung, die häufig Gegenstand von Beschwerden ist, wurde meine aufsichtsbehördliche Praxis durch das Urteil bestätigt. Privatpersonen, welche Videoüberwachungskameras an ihren Einfamilienhäusern installieren, haben zumindest dann, wenn öffentlicher Straßenraum mitüberwacht wird, die Vorgaben des Bundesdatenschutzgesetzes zu beachten.

Offen bleibt, ob für die Anwendung des Datenschutzrechts jeglicher Öffentlichkeitsbezug bei dem Einsatz von Videotechnik ausreichend ist. Da der EuGH in dem zu entscheidenden Fall objektiv auf den Erfassungsbereich und nicht auf die subjektive Zwecksetzung der Videoüberwachung, z. B. zur Schadensdokumentation, zur Beweissicherung, zur Weitergabe an Strafverfolgungsbehörden oder Versicherungen etc., abgestellt hat, könnte man bei einer engen Auslegung der knappen Entscheidungsgründe aus dem EuGH-Urteil folgern, dass jede Videoaufnahme mit Öffentlichkeitsbezug den datenschutzrechtlichen Vorschriften entsprechen muss. Dies wäre allerdings im Hinblick auf den zunehmenden Einsatz von Videotechnik im Bereich privater Freizeitgestaltung, etwa von Helmkameras durch Skifahrer oder Mountainbiker sowie von Spielzeugdrohnen, nicht unproblematisch, weswegen ich weiterhin, ungeachtet der persönlichkeitsrechtlichen Relevanz, dazu tendiere, von einer persönlichen oder familiären Tätigkeit auszugehen und das Bundesdatenschutzgesetz nicht anzuwenden, sofern die Aufnahmen nicht weitergegeben oder veröffentlicht werden. Das bedeutet selbstverständlich nicht, dass sich die Verwendung solcher Kameras in einem rechtsfreien Raum bewegt. Auch in diesen Fällen ist das Recht am Bild als besondere Ausprägung des Persönlichkeitsrechts zu beachten. Zum Thema „Drohnen“ verweise ich auf Kapitel 11.1.6 in diesem Tätigkeitsbericht.

Im Zusammenhang mit Videoüberwachungsanlagen in der Nachbarschaft ist darauf hinzuweisen, dass der EuGH zwar keine Aussage darüber getroffen

hat, in welchen Fällen eine Überwachung des öffentlichen Straßenraums zulässig ist, jedoch der Grundsatz gilt, dass eine Überwachung außerhalb des eigenen Grundstücks nur in absoluten Ausnahmefällen zulässig ist. Die Beobachtungsbefugnis des Hausrechtsinhabers endet grundsätzlich an den Grenzen seines Grundstücks. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, haben in diesen Fällen in der Regel hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, zurückzustehen. Der Bundesgerichtshof (BGH) hat bereits 1995 festgestellt, dass ein derartiger Eingriff in das allgemeine Persönlichkeitsrecht höchstens dann zulässig sein kann, wenn schwerwiegenden Beeinträchtigungen der Rechte des Betreibers der Videoüberwachungsanlage, etwa Angriffen auf seine Person oder seine unmittelbare Wohnsphäre, nicht in anderer Weise zumutbar begegnet werden kann (vgl. Urteil vom 25. April 1995, Az. VI ZR 272/94). Dies dürfte nur selten der Fall sein. An dieser Stelle möchte ich auch auf einen Beitrag in meinem 30. Tätigkeitsbericht 2010/2011 (LT-Drs. 15/955, 9. Teil, Kapitel 1.1) hinweisen.

Auch Privatpersonen, die zum Schutz ihres Eigentums Kameras an ihrem Einfamilienhaus anbringen und neben ihrem eigenen Grundstück öffentlichen Straßenraum überwachen, unterliegen dem Bundesdatenschutzgesetz. Eine Überwachung außerhalb des eigenen Grundstücks ist nur in Ausnahmefällen zulässig.

11.1.5 Dashcams

Die Videotechnik hat einen weiteren Lebensbereich erobert: den Straßenverkehr. Sog. Dashcams, kleine Kameras, die wie Navigationsgeräte an der Windschutzscheibe oder auf dem Armaturenbrett eines Fahrzeugs befestigt werden und während der Fahrt das Verkehrsgeschehen filmen, finden immer mehr Verbreitung. Die Werbeaussagen der Hersteller versprechen einen zuverlässigen Augenzeugen, um zum Beispiel im Fall eines Unfalls den Geschehensablauf rekonstruieren zu können und ein Beweismittel zur Hand zu haben.

In Deutschland ist der Einsatz solcher Kameras in der Regel datenschutzrechtlich unzulässig. Darauf haben die Aufsichtsbehörden des Bundes und der

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Länder für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) in einem Beschluss vom 25./26. Februar 2014 (vgl. Anhang 27) aufmerksam gemacht.

Der Betrieb von Dashcams ist – wie eine herkömmliche Videoüberwachung – an § 6b Absatz 1 Nr. 3 und Absatz 3 BDSG zu messen. Danach 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. Diese Voraussetzungen sind nach Ansicht der Datenschutzaufsichtsbehörden in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der anderen Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst auch das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Ein permanentes Aufnehmen des vor dem Fahrzeug befindlichen Verkehrsraumes beeinträchtigt deshalb das informationelle Selbstbestimmungsrecht der anderen Verkehrsteilnehmer in unzulässiger Weise, zumal diese sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Die Auffassung der Datenschutzaufsichtsbehörden wurde mittlerweile in mehreren Gerichtsverfahren bestätigt. So hat das Landgericht Heilbronn mit Urteil vom 17. Februar 2015 (Az. I 3 S 19/14) entschieden, dass Aufnahmen von Dashcams im Zivilprozess regelmäßig nicht als Beweismittel zum Hergang eines Unfalls verwertet werden können. Die Aufzeichnung von Personen mittels Dashcam stelle eine Verletzung des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung dar, die auch nicht durch das Interesse an einer Beweissicherung gerechtfertigt sei. Das Gericht führte u. a. hierzu aus:

„Wollte man dies anders sehen und der bloßen Möglichkeit, dass eine Beweisführung erforderlich werden könnte, den Vorrang vor dem Recht auf informationelle Selbstbestimmung einräumen, würde dies bedeuten, dass innerhalb kürzester Zeit jeder Bürger Kameras ohne jeden Anlass nicht nur in seinem Pkw, sondern auch an seiner Kleidung befestigen würde, um damit zur Dokumentation und als Beweismittel zur Durchsetzung von möglichen Schadensersatzansprüchen jedermann permanent zu filmen und zu überwachen. Damit aber würde das Recht auf informationelle Selbstbestimmung praktisch aufgegeben.“

Das Urteil ist aus meiner Sicht uneingeschränkt zu begrüßen.

Ähnlich wie das Landgericht Heilbronn hatte im vergangenen Jahr auch das Amtsgericht München in einem Zivilprozess entschieden (Beschluss vom 13. August 2014, 345 C 5551/14). Zuvor hatte bereits das Verwaltungsgericht Ansbach die Zulässigkeit einer Dashcam verneint (Urteil vom 12. August 2014, 4 K 13.0164). Allerdings ist mittlerweile auch eine strafgerichtliche Entscheidung bekannt geworden, in der die Verwertbarkeit von Dashcam-Aufnahmen (zumindest wenn diese aus aktuellem und konkretem Anlass gefertigt wurden) bejaht wurde (AG Nienburg, Urteil vom 20. Januar 2015, 4 DS 155/14). Zu betonen ist jedoch, dass diese Entscheidung bezogen auf einen Einzelfall erging und in einem Strafprozess die Frage eines Beweisverwertungsverbots anders zu bewerten ist.

Ob Privatfahrzeug, Speditionsfahrzeug, Reisebus oder Taxi: Fahrer bzw. Fuhrunternehmen sollten von dem Einsatz von Dashcams Abstand nehmen. Das unzulässige Filmen mit einer Dashcam kann mit einem hohen Bußgeld geahndet werden.

11.1.6 Drohnen: Harmloses Spielzeug oder eine Gefahr für das Persönlichkeitsrecht?

Auch dieses Mal dürften sie wieder zahlreich unter dem Weihnachtsbaum gelegen haben: Tricopter, Quadrocopter, Hexacocter, Octocopter – Flugdrohnen in allen Variationen. Steuerung über das Smartphone, schwenkbare, hochwertige Kameras an Bord, die Einblicke in sonst unzugängliche Orte gewähren, Aufnahme unverwackelter Videos und Fo-

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

tos aus luftigen Höhen in HD-Auflösung, die an das Smartphone gesendet oder gleich ins Internet übertragen werden: Was das Herz jedes Modellfliegers höher schlagen lässt, löst bei Datenschützern Beklemmung aus. Wo sonst gerade im Wohnumfeld Mauern, Hecken, Zäune oder sonstige Abtrennungen Dritten das Betreten geschützter Bereiche erschweren oder vor Einblicken von außen schützen, können mit Videokameras ausgerüstete Drohnen ohne Weiteres Einblick erhalten und Aufnahmen machen. Der Betroffene kann – wenn er das Gerät überhaupt bemerkt – regelmäßig nicht erkennen, wer die Drohne steuert und gegen wen er ggf. mit dem Ziel der Unterlassung vorgehen kann. Aus diesen Gründen kann der Einsatz von Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben in einem Beschluss vom 15./16. September 2015 (Anhang 31) darauf aufmerksam gemacht, dass, auch wenn Drohnen von Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung betrieben werden, unter Umständen das Bundesdatenschutzgesetz zu beachten ist. Insbesondere wenn die Aufnahmen zum Zweck einer Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt, ist davon auszugehen, dass es sich nicht um eine persönliche oder familiäre Tätigkeit handelt, welche vom Anwendungsbereich des Bundesdatenschutzgesetzes ausgenommen wäre. In solchen Fällen sind Drohnen vielmehr nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle nicht gegeben sind, weil die Interessen der Betroffenen regelmäßig überwiegen. Werden unbefugt Daten erhoben oder verarbeitet, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Die Aufsichtsbehörden betonen, dass in jedem Fall das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren ist. Der Betroffene kann sich gegen den mit einem Drohneneinsatz unter Um-

ständen verbunden Eingriff in das allgemeine Persönlichkeitsrecht zivilrechtlich wehren. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und vor Einblicken von außen geschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet, kann ein Abwehrensanspruch aus § 823 i. V. mit § 1004 Absatz 1 des Bürgerlichen Gesetzbuches (BGB) analog bestehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Schließlich besteht die Möglichkeit, die Strafverfolgungsbehörden einzuschalten, wenn durch den Drohneneinsatz Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches [StGB]) oder Aufzeichnungen des nichtöffentlich gesprochenen Wortes (§ 201 StGB) angefertigt werden. Wer also beispielsweise die umbaute Terrasse eines Atriumhauses oder einen mit Sichtschutz versehenen Balkon mit einer kamerabestückten Drohne überfliegt, um die hübsche Nachbarin beim Sonnenbaden zu filmen, läuft Gefahr sich strafbar zu machen.

Nicht zuletzt aufgrund der Vielzahl der rechtlichen Probleme, die ein Drohneneinsatz nicht nur aus datenschutzrechtlicher Sicht mit sich bringt, z. B. Flugsicherheits- und Haftungsfragen, hat sich auch die Politik des Themas angenommen. Ich würde es begrüßen, wenn den Auswirkungen des Einsatzes von Drohnen für das Persönlichkeitsrecht auch auf gesetzgeberischer Ebene begegnet würde. Das Europäische Parlament hat in einer Entschließung vom 29. Oktober 2015 zum sicheren Einsatz ferngesteuerter Flugsysteme (RPAS) im Bereich der zivilen Luftfahrt⁸⁶ die Kommission und die Mitgliedstaaten u. a. aufgefordert, dafür zu sorgen, dass bei der Ausarbeitung politischer Maßnahmen der EU Garantien für den Schutz der Privatsphäre und den Datenschutz eingefügt werden. Dieser Aufforderung kann ich mich nur anschließen. Anfang November 2015 schlug der Bundesverkehrsminister neue Re-

⁸⁶ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2015-0390+0+DOC+PDF+V0//DE>

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

gelungen für gewerbliche und private Drohnenflüge vor, darunter die Ausweitung von Flugverbotszonen. Kurz zuvor hatte sich auch die Bundesregierung zur Kennzeichnungspflicht von kleinen Drohnen geäußert (vgl. BT-Drs. 18/3606). In der aktuellen bundespolitischen Diskussion kommt dem Aspekt des Datenschutzes jedoch bislang nur eine untergeordnete Bedeutung zu. Das muss sich ändern!

Die Datenschutzbehörden appellieren an die Drohnenbetreiber, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann. Der Gesetzgeber ist aufgefordert, bei der Festlegung eines neuen Rechtsrahmens für den Einsatz von Drohnen das Persönlichkeitsrecht der Betroffenen zu berücksichtigen.

11.2 Novellierung des Telemediengesetzes – Störerhaftung bei offenen WLANs

Deutschland hinkt im internationalen Vergleich bei der Verbreitung öffentlicher WLANs hinterher. Wesentliche Ursache hierfür ist die Gefahr der Haftung des Betreibers eines öffentlichen WLAN für die Handlungen seiner Nutzer.

In Deutschland sind öffentliche WLANs (WLAN = Wireless Local Area Network) wegen der bestehenden Rechtsunsicherheit bei der Frage der Haftung der WLAN-Betreiber kaum verbreitet. § 8 Absatz 3 und 4 im Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (TMG-E) soll dies durch eine Haftungsprivilegierung für Betreiber öffentlicher WLANs ändern.

Die sog. Störerhaftung der Betreiber öffentlicher WLANs geht auf verschiedene Gerichtsurteile zurück und wurde bereits höchstrichterlich bestätigt (vgl. BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08 – Sommer unseres Lebens). Demnach haftet der Betreiber eines öffentlichen WLANs für Urheberrechtsverletzungen oder sonstige rechtswidrige Handlungen seiner Nutzer, wenn er die ihm zumutbaren Prüf- und Kontrollmaßnahmen zur Verhinderung von Rechtsverletzungen verletzt hat. Da ein Betreiber öffentlicher WLAN grundsätzlich als Access-Provider einzustufen ist, sind an die Zumutbar-

keit von Maßnahmen und Pflichten besonders strenge Anforderungen zu stellen.

Nachdem bereits mehrere politische Vorstöße zur Regelung der Haftung der Betreiber öffentlicher WLANs gescheitert waren (ein Überblick über die Rechtsprechung und die politische Diskussion zur Haftung der Betreiber öffentlicher WLANs findet sich in dem Aufsatz von Mantz/Sassenberg, Computer und Recht 2015, S. 298–306), hat die Bundesregierung die Thematik im Rahmen ihrer Digitalen Agenda aufgegriffen. Am 11. März 2015 wurde der Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes vorgestellt. Ziel des Referentenentwurfs war, die Haftungsprivilegierung der WLAN-Betreiber für Rechtsverletzungen ihrer Nutzer im Telemediengesetz klarzustellen und die Voraussetzungen für eine Haftung zu präzisieren. Hierzu sollte der Referentenentwurf bestimmen, dass WLAN-Betreiber Zugangsanbieter im Sinne des § 8 TMG sind und eine Störerhaftung nicht in Betracht kommt, wenn die WLAN-Betreiber bestimmte Sorgfaltspflichten erfüllen (Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes vom 11. März 2015, S. 2).

Aufgrund der erheblichen Kritik durch Vertreter der Regierungskoalition, der Opposition, betroffener Gruppen und großer Wirtschaftsverbände veröffentlichte das Bundeswirtschaftsministerium im April 2015 eine FAQ-Liste, in der es Erläuterungen und Klarstellungen zu häufig gestellten Fragen publiziert (abrufbar unter:

http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan_did=695728.html).

U. a. stellte es klar, dass § 8 TMG-E von keinem WLAN-Betreiber fordere, dass er den Namen des Nutzers protokollieren, registrieren oder anderweitig erfassen müsse (vgl. Antwort zu Frage 5).

Am 25. September 2015 legte schließlich die Bundesregierung den Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes vor (BR-Drs. 440/15), der inhaltlich weitestgehend dem ursprünglichen Referentenentwurf entsprach. Allerdings fand die noch im Referentenentwurf enthaltene und stark kritisierte Unterscheidung zwischen geschäftsmäßigen und privaten Anbietern bei der Privilegierung der Unterlassungsansprüche gegen den Betreiber eines offenen WLANs keinen Eingang in den Gesetzentwurf der Bundesregierung.

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Die Haftungsprivilegierung des § 8 Abs. 3 und 4 TMG-E soll nach § 2 S. 1 Nr. 2a TMG-E für WLANs mit geringer Leistung und geringer Reichweite sowie mit geringem Störungsrisiko für weitere, von anderen Nutzern in unmittelbarer Nähe installierte Systeme dieser Art gelten. Privilegiert werden sollen damit sowohl die Betreiber privater WLANs als auch geschäftsmäßige Betreiber von WLANs.

Nach § 8 Abs. 3 TMG-E muss der Betreiber eines WLANs für Rechtsverletzungen seiner Nutzer nicht haften, wenn die Voraussetzungen des § 8 Abs. 1 TMG vorliegen, also wenn die Übermittlung nicht veranlasst war, der Adressat der Information nicht ausgewählt wurde, die Information weder ausgewählt noch verändert wurde und kein kollusives Zusammenwirken mit dem Rechtsverletzer stattgefunden hat. Die Haftungsprivilegierung schließt dabei sowohl zivilrechtliche Schadensersatzansprüche als auch eine strafrechtliche Verfolgung des Betreibers aus.

Darüber hinaus sieht § 8 Abs. 4 TMG-E vor, dass WLAN-Betreiber auch gegenüber Beseitigungs- und Unterlassungsansprüchen aufgrund Rechtsverletzungen ihrer Nutzer privilegiert sind, wenn sie angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Netzwerk ergriffen haben und Zugang zum Internet nur einem Nutzer gewähren, der erklärt hat, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen.

Die Regelungen des Regierungsentwurfs sind indessen voraussichtlich nicht geeignet, die Verbreitung von WLANs im öffentlichen Raum zu fördern und diesbezügliche Rechtssicherheit zu schaffen. Insbesondere § 8 Abs. 4 TMG-E stellt nichts anderes dar als die Normierung der durch die Einzelfallrechtsprechung geschaffenen derzeitigen Rechtslage. Die verwendeten unbestimmten Rechtsbegriffe wie „zumutbare Maßnahmen“ und „angemessene Sicherungsmaßnahmen“ schaffen keine Rechtsklarheit, sondern bedürfen weiterhin der Auslegung durch die Gerichte.

Betreiber öffentlicher WLANs werden daher auch weiterhin konkrete Maßnahmen ergreifen müssen, um Haftungsrisiken durch Urheberrechtsverletzungen oder Straftaten durch ihre Nutzer zu verhindern. Es besteht daher weiterhin die Gefahr, dass die Betreiber entgegen der Klarstellung des Bundeswirtschaftsministeriums personenbezogene Daten

der Nutzer erheben und speichern, um das Risiko potentieller Gerichtsverfahren zu minimieren.

Diese Bedenken werden auch vom Bundesrat geteilt, der in seiner Sitzung am 6. November 2015 eine vollständige Neuformulierung von § 8 Abs. 3 und 4 TMG-E gefordert hat (BR-Drs. 440/15 Beschluss). Der Gesetzestext soll danach lauten:

§ 8 Absatz 3: „Der Ausschluss der Verantwortlichkeit (Absatz 1) umfasst auch Diensteanbieter von drahtlosen Netzwerken und Funknetzwerken, die sich an einen nicht im Voraus namentlich bestimmten Nutzerkreis richten (öffentliche Funknetzwerke).

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.“

§ 8 Absatz 4: „Diensteanbieter nach Absatz 3 können wegen einer rechtswidrigen Handlung eines Nutzers nicht auf Beseitigung oder Unterlassung in Anspruch genommen werden.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.“

Die Empfehlungen des Bundesrates sind geeignet, freies öffentliches WLAN rechtssicher und ohne das Sammeln von personenbezogenen Daten zu verwirklichen, und daher grundsätzlich zu begrüßen.

11.3 Orientierungshilfe Smart-TV

Smart-TVs sind der Renner jeder TV-Abteilung deutscher Elektronikmärkte. Vereinfacht gesagt sind darin die Funktionen eines Fernsehgeräts und eines Computers vereint. Und weil Computer mittlerweile standardmäßig einen Internet-Zugang haben, gilt dies vielfach auch für die Smart-TVs. Somit übertragen sich etliche datenschutzrechtliche Probleme bei Computern auch auf Smart-TVs.

Smart-TVs bieten neben dem klassischen Empfang des Fernsehsignals dem Nutzer die Möglichkeit, Internet-Dienste aufzurufen und dadurch auf ergänzende Web-Inhalte der Sender oder Web-Platt-

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

formen der Smart-TV-Hersteller zuzugreifen. Im Gegensatz zum herkömmlichen Fernsehen entsteht durch die hierfür erforderliche Online-Verbindung ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten (z. B. Werbepartner oder Plattformanbieter). Dieser Rückkanal ermöglicht es dem Empfänger, das individuelle Nutzungsverhalten zu erfassen und auszuwerten. Aus datenschutzrechtlicher Sicht stellt sich insbesondere die Frage, wann welche personenbezogenen Daten bei Nutzung der unterschiedlichen Angebote fließen, wer diese Daten zu welchen Zwecken erhält und ob eine Erlaubnis oder Rechtsgrundlage für das Erheben und den weiteren Datenumgang existiert.

Angesichts des absehbaren Abschieds von der Möglichkeit des anonymen Fernsehens sahen sich die Datenschutzaufsichtsbehörden des Bundes und der Länder sowie die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten im Mai 2014 zu einer gemeinsamen Erklärung veranlasst, die auch von den Direktoren der Landesmedienanstalten unterstützt wurde (siehe Anhang 29). Darin hieß es u. a.: „Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt“.

In der Folgezeit haben Vertreter mehrerer Aufsichtsbehörden unter Federführung des Bayerischen Landesamts für Datenschutzaufsicht eine Orientierungshilfe zu den Datenschutzerfordernungen an Smart-TV-Dienste erarbeitet, die schließlich im September 2015 zur Veröffentlichung freigegeben veröffentlicht wurde⁸⁷. Adressaten der Orientierungshilfe sind alle Anbieter von Smart-TV-Diensten, wie Gerätehersteller, Portalbetreiber oder Anbieter von Empfehlungsdiensten. Besonders im Fokus stehen die Anbieter von Hybrid-TV-Diensten (HbbTV). Bei diesen Diensten werden zum eigent-

lichen Programm Zusatzinformationen bereitgehalten, die der Zuschauer mit Hilfe des sog. Red Buttons auf seiner Fernbedienung abrufen kann. Im Unterschied zum vergleichbaren Videotext-Verfahren werden die Zusatzinformationen über das Internet in das Smart-TV übertragen und mit Hilfe des Rückkanals kann der Informationsanbieter unter Umständen den Nutzer identifizieren.

Die Orientierungshilfe Smart-TV umfasst u. a. neben einer Zusammenfassung des anwendbaren Datenschutzrechts eine Klarstellung der datenschutzrechtlichen Rahmenbedingungen für Smart-TV, Anforderungen an die technisch-organisatorischen Maßnahmen sowie konkrete Anforderungen an Anbieter von Smart-TV-Diensten.

Auch wenn eine Orientierungshilfe keinen Gesetzescharakter hat, so besteht aus datenschutzrechtlicher Sicht das dringende Bedürfnis, die darin formulierten Anforderungen umzusetzen. Für die Datenschutzbehörden in Deutschland wird die Orientierungshilfe als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungsfunktion dienen. Eine datenschutzkonforme Technik wird sich sicher nicht von heute auf morgen einführen lassen, da der Großteil der am Markt angebotenen Smart-TVs derzeit hinter den in der Orientierungshilfe genannten Anforderungen zurückbleibt. Außerdem haben die meisten Anbieter von TV-Geräten ihren Unternehmenssitz außerhalb der Europäischen Union. Das Ziel von hohen Datenschutzstandards darf jedoch nicht aus den Augen verloren werden.

Alle Anbieter von Smart-TV-Diensten sollten schnellstmöglich prüfen, welche Teile der Orientierungshilfe bereits jetzt umgesetzt werden können, und ihre Verfahren entsprechend einrichten. Die Hersteller von TV-Geräten sind ihrerseits aufgefordert, ihre Smart-TVs nachzubessern, um einen praxisgerechten und rechtskonformen Einsatz zu ermöglichen.

⁸⁷ siehe http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/OH-Smart-TV_20150917_Version-1-00-clear.pdf

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

11.4 GPEN Privacy Sweep 2014

Datenschutz wird immer internationaler. Auch Kontrollmaßnahmen müssen im Zeitalter weltumspannender Kommunikation zunehmend international ausgerichtet sein.

Unter dem Titel „GPEN Privacy Sweep 2014“ hat im Jahr 2014 die kanadische Datenschutzaufsichtsbehörde (Office of the Privacy Commissioner of Canada) eine Aktion zur Prüfung des Datenschutzes bei Smartphone Apps angestoßen und koordiniert. GPEN steht für „Global Privacy Enforcement Network“⁸⁸ und ist ein informeller Zusammenschluss von 51 Datenschutzaufsichtsbehörden auf der ganzen Welt.

In der Woche vom 12. bis 18. Mai 2014 wurden 1.211 Smartphone-Apps auf Einhaltung der Datenschutzbestimmungen, die in den jeweiligen Teilnehmerländern gelten, überprüft. In den Prüfungen waren sowohl Apps mit iOS- als auch Android-Betriebssystem vertreten, darunter kostenlose und kostenpflichtige Apps sowie Apps für den öffentlichen und den privaten Sektor. Die zu prüfenden Apps deckten die vorherrschenden App-Kategorien ab, u. a. Spiele, Gesundheit/Fitness, Nachrichten und Banking.

Auch die Mitarbeiter meines technischen Referats haben sich an der Aktion beteiligt und vornehmlich Apps evaluiert, die in Baden-Württemberg entwickelt wurden oder deren Betreiber hier ansässig sind. Insgesamt wurden rund zwei Dutzend Smartphones-Apps in die Prüfung einbezogen. Dabei wurde festgestellt, dass die meisten Apps die notwendige Transparenz im Umgang mit personenbezogenen Daten vermissen ließen. Bezogen auf die globale Prüfkaktion traf dies auf rund 85 Prozent der 1.211 untersuchten Smartphone-Apps zu und spiegelt auch ziemlich exakt die Situation in Baden-Württemberg wider. Hauptmanko war das Fehlen einer Datenschutzerklärung, aus der hervorgeht, warum bestimmte Daten von einer App benötigt werden. Daher konnte auch nicht nachvollzogen werden, ob die erhobenen Daten für das Funktionieren einer App tatsächlich erforderlich waren. Bei rund einem Drittel der Apps passten die angebotenen Funktionen nicht mit den einzuräumenden Berechtigungen zusammen, d. h. es mussten mehr

Privilegien erteilt werden, als aufgrund der Funktionalität zu erwarten war.

Ich ermutige daher jeden Besitzer von mobilen Endgeräten wie Smartphones oder Tablets, stets kritisch zu prüfen, welche Zugriffsberechtigungen auf Daten eine App sich einräumt. Der Nutzer sollte darauf achten, dass eine App nur die Daten anfordert, die für den Anwendungszweck nötig und plausibel sind. So ist Skepsis angebracht, wenn etwa eine Taschenrechner-App auf die Standortdaten oder gar Kontaktdaten zugreifen will. Allzu wissbegierige Anwendungen sollten am besten gar nicht erst installiert oder gleich wieder gelöscht werden. In Zukunft wird meine Dienststelle derartige Kontrollaktionen wiederholen. Allerdings müssen wir uns dafür personell weiter verstärken, denn das erforderliche technische Know-how und der zeitliche Aufwand für solche Aktionen sind doch beträchtlich.

Mit einem offenen Brief⁸⁹ an die Betreiber von App Stores, den ich mitunterzeichnet habe, will GPEN erreichen, dass zu den von ihnen angebotenen Apps für Smartphones auch eine Datenschutzerklärung im App Store vorhanden ist. Dies sollte ausnahmslos für jede App gelten, die personenbezogene Daten verarbeitet.

Ich bemängele die bislang passive Rolle der App Store Betreiber in diesem Punkt. Wer Produkte vertreibt, müsste sich auch mitverantwortlich zeigen, wenn es um Aufklärung und Transparenz beim Datenschutz geht. Viel zu oft, so hat unsere Prüfkaktion gezeigt, bleibt die Frage unbeantwortet, warum bestimmte Daten von einer App benötigt werden. Eine Datenschutzerklärung sollte eigentlich helfen, die Ungewissheit zu beseitigen.

Durch die EU-Datenschutz-Grundverordnung wird sich auch die Rolle der Aufsichtsbehörden auf Landesebene ändern. Eine stärkere internationale Ausrichtung und eine Intensivierung technischer Prüfungen werden unausweichlich sein.

11.5 Heartbleed Bug – der GAU

Unter den Sicherheitslücken, die Webauftritte im Internet betreffen, wurde im Berichtszeitraum mit dem sogenannten „Heartbleed Bug“ eine besonders

⁸⁸ <https://www.privacyenforcement.net/>

⁸⁹ https://www.priv.gc.ca/media/nr-c/2014/nr-c_141210_e.asp

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

gravierende Schwachstelle offenkundig. Der ausgewiesene Sicherheitsexperte Bruce Schneier kommentierte diesen Bug so⁹⁰: „Katastrophal“ ist das richtige Wort. Auf einer Skala von 1 bis 10 ist dies eine 11.“

Vereinfacht gesagt, ermöglicht diese Sicherheitslücke den Zugriff auf die Passwörter von Administratoren und Benutzern der betroffenen Webauftritte, ohne dass sie davon Kenntnis erlangen. Ein Programmierfehler in der weitverbreiteten Verschlüsselungssoftware OpenSSL, die im Grunde vor unberechtigten Zugriffen schützen soll, war die Ursache für diesen „größten anzunehmenden Unfall (GAU)“ im Bereich der IT-Sicherheit und des Datenschutzes.

Obgleich nach Bekanntwerden der Sicherheitslücke im April 2014 zahlreiche Unternehmen und Organisationen nachgebessert haben, gab es Hinweise, dass nicht alle Webauftritte umgehend auf eine fehlerfreie Version umgestellt wurden.

Meine Mitarbeiter haben daher im September 2014 stichprobenartig die Webseiten von rund 11.000 hier ansässigen Unternehmen mit unserer Prüfplattform (siehe Kapitel 11.6) darauf hin geprüft, inwieweit eine durch den Heartbleed Bug anfällige Version von OpenSSL noch im Einsatz ist. Insgesamt konnten 46 Webauftritte ermittelt werden, die den Heartbleed Bug aufweisen. Ich gehe davon aus, dass bei einer Vollerhebung weitaus mehr Webauftritte diese Sicherheitslücke zeigen würden.

Die Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, um den Anforderungen des Bundesdatenschutzgesetzes zu genügen. Insbesondere zählt hierzu die Zugriffskontrolle. Sie soll gewährleisten, dass allein aufgrund definierter Zugriffsberechtigungen auf Daten zugegriffen werden kann und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Heartbleed-Lücke verursacht eine gravierende Verletzung der Zugriffskontrolle, da neben Passwörtern auch andere personenbezogene Daten unberechtigt ausgelesen werden können.

Vermutlich ist noch nicht allen von der Sicherheitslücke betroffenen Webseiten-Betreibern bewusst,

dass sie noch die anfällige Version verwenden. Ich beabsichtige auch hier, mit Wiederholungsprüfungen stärker darauf hinzuwirken, dass Webseiten von Betreibern mit Sitz in Baden-Württemberg den Anforderungen des Datenschutzes vollumfänglich genügen.

11.6 Fachkongress des IT-Planungsrats am 7. und 8. April 2014 in Stuttgart

Unter dem Titel „Datenschutzrechtliche und sicherheitsrelevante Überprüfungen von Webseiten in großer Zahl – Open Source Software im Einsatz“ waren Mitarbeiter meines technischen Referats mit einem Ausstellungsstand auf dem Fachkongress des IT-Planungsrates vertreten.

Im Datenschutz wie auch in der Informationssicherheit spielt die Überprüfung einer großen Anzahl von Webseiten im Hinblick auf die Einhaltung rechtlicher und sicherheitsrelevanter Vorgaben zunehmend eine wichtige Rolle. Beispielsweise ist zu prüfen, inwieweit Social Plugins oder sogenannte Reichweitenanalysewerkzeuge datenschutzkonform eingesetzt werden. Dabei sind in kurzer Zeit mehrere Tausend Websites (Webdomains) zu analysieren, zu bewerten und die Prüfergebnisse für jeden durchgeführten Analyseschritt zu dokumentieren.

Um die fehleranfällige und aufwendige Erstellung von individueller Software für jedes Prüfungsvorhaben zu vermeiden, haben meine Mitarbeiter basierend auf einem Business-Intelligence-Werkzeug (BI-Werkzeug) ein Vorgehen und eine Prüfplattform entwickelt, die auf einem modularen Ansatz beruhen.

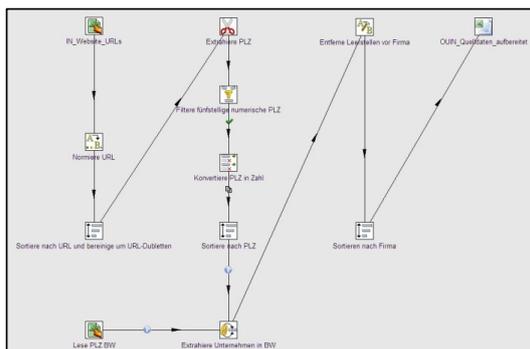
Für die eigentliche Prüfungsaufgabe wird nur ein spezifischer „Kern“ entwickelt, die restliche Umgebung mit Dateninput und Ergebnisprotokollierung kann strukturell weitgehend konstant gehalten werden. Durch eine Vielzahl funktioneller Bausteine, die das BI-Werkzeug bereitstellt, können auf einfache Weise auch komplexe Prüfaufgaben bewerkstelligt werden. Nicht zuletzt, weil es sich bei dem BI-Werkzeug um die kostenfreie Community Edition einer Open Source Software – Pentaho Open-Source-BI-Suite – handelt, hält sich der finanzielle Aufwand für die Prüfungen in engen Grenzen.

Beispielsweise bedarf es nur weniger Schritte, um aus öffentlich zugänglichen Adressen mit gespeicherten Webseitenadressen (URL) eine homogene Datenbasis zu erzeugen. In der folgenden Abbil-

⁹⁰ <https://www.schneier.com/blog/archives/2014/04/heartbleed.html>

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

derung ist beschrieben, wie die Rohdaten um Dubletten bereinigt und nach unterschiedlichen Kriterien sortiert werden. Das Ergebnis ist ein „normierter“ Datenbestand, der Eingang in die Online-Prüfung von Webseiten finden kann.



Mit der Plattform verbinden sich nach unserer Erkenntnis folgende Vorteile:

- Schnelle, kostengünstige Umsetzung der Prüfaufgabe – im Wesentlichen durch Konfiguration,
- Entwicklungs- und Ausführungsplattform sind identisch – kurze Korrektur-Test-Zyklen,
- graphische Modellierung reduziert Kommunikations- und Dokumentationsaufwand.

Kritisch anzumerken ist die teilweise zu knappe, öffentlich zugängliche Dokumentation des Open Source Werkzeugs. Ebenso ist die Erfahrung mit BI-Werkzeugen ein wesentlicher Erfolgsfaktor.

In der Diskussion mit den Besuchern des Ausstellungsstandes wurde deutliches Interesse an dieser Prüfplattform kundgetan, wenngleich vornehmlich mit dem Fokus auf Prüfungen im Bereich der IT-Sicherheit.

11.7 Vorsicht Internet! – oder worauf man achten sollte, wenn man im Internet unterwegs ist

„Betteln und Hausieren verboten“ – Früher fand sich ein Schild mit dieser Aufschrift an mancher Haus- oder Ladentüre. Heutzutage gibt es das Internet, aber das Problem ist ein Ähnliches. Unerwünschte Besucher dringen in unsere Privatsphäre ein und wollen letztendlich das Gleiche wie ehemals – Geld.

Ob beim Surfen im Internet, im Umgang mit E-Mails oder beim Online-Banking: die Gefahr, Opfer krimineller Machenschaften zu werden, ist groß und wird ohne entsprechende Gegenmaßnahmen immer bedrohlicher. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt in seinem Jahresbericht 2014 fest, dass es jeden Monat hierzulande mindestens eine Million Infektionen durch Schadprogramme gibt, Tendenz steigend. An erster Stelle zu nennen sind sogenannte Spam-Mails, also unerwünschte E-Mails, die, häufig als Werbung getarnt, auch zum Verbreiten von Schadprogrammen genutzt werden. Beliebte dabei ist das Phishing, mit dem persönliche Daten wie Passwörter oder Kontodaten durch die so verbreiteten Schadprogramme an Kriminelle übermittelt werden. Ebenso kann dies beim Besuch von manipulierten Webseiten im Internet geschehen.

Was kann man dagegen tun? Einen vollkommenen Schutz gegen die vielfältigen Bedrohungen, die im Internet lauern, gibt es nicht. Allein die Zahl der Schadprogrammvarianten, die täglich im Internet neu auftauchen, beträgt rund 300.000 – wohlgeachtet pro Tag. Angesichts dieser Flut an Bedrohungen liegt es nahe zu resignieren. Mit den folgenden fünf Maßnahmen kann zumindest ein Basisschutz erreicht werden, der die wichtigsten Bereiche Ihrer häuslichen Informationstechnik umfasst:

- Sicherheitsupdates. Fast alle Programme, die Sie auf Ihrem Computer verwenden, haben Sicherheitsschwachstellen. Die Hersteller der Programme bessern laufend nach, um die Sicherheitslücken zu schließen. Dies geschieht durch sogenannte Sicherheitsupdates. In vielen Fällen können Sie die Programme so einstellen, dass Sie automatisch benachrichtigt werden, wenn ein Update von Seiten des Herstellers vorliegt.
- Schutzprogramme sind in unserem einleitenden Beispiel wie die Haustüre, die unerwünschte Besucher fernhält und nur Berechtigten den Zugang ermöglicht. Zu den Schutzprogrammen zählen Virenschutzprogramme und Personal Firewalls. Am Markt gibt es sowohl kostenfreie Produkte wie auch kostenpflichtige. Die Stiftung Warentest prüft hin und wieder derartige Programme und gibt Empfehlungen zur Auswahl (zuletzt im Heft test 04/2015).
- Pflegen Sie ein gesundes Misstrauen. Würden Sie jedem die Türe öffnen, der Einlass begehrt?

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Wohl kaum. Wenn Sie eine E-Mail erhalten, die Ihnen verdächtig vorkommt, folgen Sie auf keinen Fall den darin enthaltenen Aufforderungen. Vor allem: öffnen Sie keine E-Mail-Anhänge. Vielfach verstecken sich hinter Anhängen die oben erwähnten Schadprogramme. Unser Tipp: ziehen Sie im Zweifelsfall jemanden zu Rate, dem Sie vertrauen. Schauen Sie sich gemeinsam die verdächtige E-Mail an und entscheiden in Ruhe, ob es sich um einen Betrugsversuch handeln könnte.

- Sichere Passwörter sind gleichsam wie Hauschlüssel – unerlässlich für einen wirksamen Schutz. Eine Haustüre mit einem Buntbartschloss stellt kein ernsthaftes Zugangshindernis dar. Entsprechend müssen Passwörter sehr sorgfältig ausgewählt werden, damit sie ihren Zweck erfüllen. Auf meiner Internetseite steht unter der Rubrik „Technik“ ein Merkblatt zum Umgang mit Passwörtern zum Abruf bereit.
- Fertigen Sie regelmäßig Sicherheitskopien Ihrer Daten an. Sie beugen dem Datenverlust durch technische Defekte ebenso vor wie auch der Bedrohung durch sogenannte Ransomware, die zu erpresserischen Zweck zunehmend eingesetzt wird. Mit Ransomware können die Daten auf Ihrem Rechner ohne Ihr Zutun verschlüsselt werden. Für die Entschlüsselung wird dann ein Lösegeld (englisch Ransom) von Ihnen gefordert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Betroffenen, den geforderten Geldbetrag keinesfalls zu zahlen.

Weiterführende Links mit praktischen Hinweisen und Tipps finden Sie zu diesem Thema unter:

<https://www.bsi-fuer-buerger.de>

<http://www.baden-wuerttemberg.datenschutz.de/technik>

<https://www.bsi.bund.de>

11.8 E-Government-Gesetz Baden-Württemberg

In meinem letzten Tätigkeitsbericht habe ich über das E-Government-Gesetz des Bundes berichtet (vgl. 31. TB 2012/2013, LT-Drs. 15/4600, Kapitel 1.4.2). Der Landesgesetzgeber hat nunmehr nachgezogen und am 16. Dezember 2015 ein Gesetz zur Förderung der elektronischen Verwaltung und zur Änderung weiterer Vorschriften (E-Government-

Gesetz Baden-Württemberg, EGovG BW, LT-Drs. 15/7724) verabschiedet, welches sich an dem Bundesgesetz orientiert. Bereits in der Phase der Erstellung des Gesetzentwurfs sowie im weiteren Gesetzgebungsverfahren wurde meine Dienststelle beteiligt. Einige meiner Anregungen wurden umgesetzt. An manchen Stellen begegnet das Gesetz jedoch aus datenschutzrechtlicher Sicht weiterhin Kritik.

Nach § 2 Absatz 1 EGovG BW ist jede Behörde ist verpflichtet, auch einen Zugang für die elektronische Kommunikation zu eröffnen. Im Unterschied zum E-Government-Gesetz des Bundes (E-GovG Bund) enthält die Regelung jedoch keine Verpflichtung, einen elektronischen Zugang auch für elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen. Vielmehr soll ausweislich der Gesetzesbegründung für die Zugangseröffnung die Bereitstellung eines E-Mail-Postfachs der Behörde ausreichen. Hierdurch wird versäumt, den Bürgern die Möglichkeit einer Übermittlung qualifiziert elektronisch signierter Dokumente einzuräumen. Obwohl § 3a des Landesverwaltungsverfahrensgesetzes (LVwVfG) auch die qualifizierte elektronische Signatur als Schriftformersatz vorsieht, spiegelt sich diese Gleichbehandlung mit anderen Formen der elektronischen Kommunikation, wie z. B. der De-Mail, im E-Government-Gesetz Baden-Württemberg nicht wider. Dabei ist keine Infrastruktur besser geeignet, dem bei einer elektronischen Kommunikation erforderlichen Nachweis der Identität, Authentizität und Integrität so vollständig Rechnung zu tragen, wie die qualifizierte elektronische Signatur. Im Gesetzgebungsverfahren hatte ich darauf hingewiesen, dass, statt die qualifizierte elektronische Signatur endgültig in ein Schattendasein zu drängen, die Praktikabilität und die Akzeptanz der qualifizierten elektronischen Signatur erhöht werden sollten. Der neue elektronische Personalausweis hat diesbezüglich großes Potenzial, denn in einigen Jahren wird jeder ausweispflichtige deutsche Staatsbürger zumindest über eine potenzielle Signaturkarte verfügen, die mit einer qualifizierten elektronischen Signatur ausgestattet werden kann. Der Verzicht auf eine Verpflichtung der Behörden zu einer Zugangseröffnung auch für qualifiziert signierte elektronische Dokumente bedeutet eine weitere Schwächung der qualifizierten elektronischen Signatur.

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Bereits früher hatte ich außerdem vorgeschlagen, die Behörden auch zur Entgegennahme verschlüsselt übertragener Dokumente zu verpflichten. In den Regierungsentwurf wurde sodann nachträglich die Regelung des § 2 Absatz 2 E-GovG BW eingefügt. Dieser enthält die Verpflichtung, mindestens einen Zugang für die elektronische Kommunikation durch angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff Dritter zu schützen. Ich habe zwar Verständnis, dass eine technikoffene Formulierung gewählt wurde. Durch die hiermit für die Behörden eingeräumten Umsetzungsmöglichkeiten ist jedoch nicht gewährleistet, dass dem Einsatz von Verschlüsselungsverfahren die notwendige Bedeutung zukommt. So erläutert die Gesetzesbegründung, dass Behörden die entsprechende Verpflichtung über „service-bw“, das Dienstleistungsportal des Landes, erfüllen können. Allerdings wird sodann folgerichtig darauf hingewiesen, dass der Bürger dort ein Servicekonto einrichten müsse, um auf diesem Weg gesichert zu kommunizieren. Setzt der Bürger auch in seiner sonstigen elektronischen Kommunikation Verschlüsselungsverfahren ein, kann er diese nun für die Behördenkommunikation nicht nutzen, sondern ist gezwungen, sich bei dem Dienstleistungsportal anzumelden. Ich halte diese Strategie des Landes für suboptimal und widersprüchlich: Einerseits werden die Bürger – gerade auch von der Politik – ständig aufgefordert, selbst mehr für die Sicherheit im Internet zu tun. Andererseits wurde mit dem E-Government-Gesetz Baden-Württemberg die Möglichkeit versäumt, ein Zeichen für die Verbreitung von Verschlüsselungssoftware zu setzen und diesen Prozess aktiv zu unterstützen. Das ausschließliche Angebot, mit einer Behörde über ein Dienstleistungsportal zu kommunizieren, welches zunächst einer Anmeldung und der Hinterlegung von Daten bedarf, greift entschieden zu kurz.

§ 2 Absatz 2 Satz 2 E-GovG verpflichtet die Behörde, grundsätzlich bei der Kommunikation in Verwaltungsverfahren den nach Satz 1 eingerichteten zugriffsgeschützten Zugang zu verwenden. Diese Verpflichtung wird von mir unterstützt. Allerdings hatte ich in meiner Stellungnahme zum Regierungsentwurf darauf aufmerksam gemacht, dass gegen die in der Gesetzesbegründung formulierte Ausnahme, bei Vorliegen einer ausdrücklichen Einwilligung des externen Kommunikationspartners ungesichert übermitteln zu können, erhebliche Bedenken bestehen. Zum einen ist unklar, wann von einer ausdrück-

lichen und wann von einer konkludenten Einwilligung ausgegangen werden kann. Wäre z. B. die Angabe einer E-Mail-Adresse neben weiteren Kontaktdaten gegenüber einer Behörde eine ausdrückliche Einwilligung? Zum andern wäre selbst wenn man davon ausgeht, dass der Kommunikationspartner explizit sein Einverständnis für eine ungesicherte Rückantwort erklärt, zu bezweifeln, ob es sich hierbei um eine wirksame Einwilligung handelt. Da der Empfänger die Antwort der Behörde nicht kennt, z. B. ob es sich um eine bloße Eingangsbestätigung oder einen Bescheid handelt, kann er nicht wissen, in was er einwilligt. Ferner ist denkbar, dass die Behördenantwort personenbezogene Daten Dritter enthält, welche nicht von der Einwilligung umfasst wären, da diese nicht zu Lasten Dritter erklärt werden kann. Schließlich bestehen wie z. B. in § 87a Absatz 1 Satz 3 der Abgabenordnung besondere Anforderungen an die elektronische Verwaltungskommunikation. Diese gesetzlich festgelegten Sicherheitsstandards sind nicht disponibel, das heißt, auf diese Verschlüsselungserfordernisse kann nicht per Einwilligung verzichtet werden. Das gleiche gilt zumindest auch für besonders schutzbedürftige personenbezogene Daten, z. B. Gesundheits- oder Sozialdaten. Erforderlich wäre daher eine Schutzbedarfsanalyse. Um hier eine Rechtsunsicherheit bei dem Behördenmitarbeiter zu verhindern, hatte ich vorgeschlagen, die Einwilligung als Ausnahme von § 2 Absatz 2 Satz 2 E-GovG BW nicht in der Gesetzesbegründung zu nennen, sondern im Grundsatz für eine Behördenantwort immer denselben gesicherten Kommunikationsweg zu wählen.

Wie bereits beim E-Government-Gesetz des Bundes ist die gleichlautende Vorschrift des § 12 E-GovG BW zur Georeferenzierung zu kritisieren. Die Vorschrift sieht vor, in elektronische Register, die Angaben mit Bezug zu Grundstücken enthalten, die Georeferenzierung mit aufzunehmen. Dies ist datenschutzrechtlich hoch problematisch. Zwar handelt es sich bei einer Geokoordinate zunächst um ein neutrales Datum, jedoch führt die inhaltliche Verknüpfung mit den sonstigen Registerdaten dazu, dass das betreffende Grundstück und damit der Eigentümer eindeutig bestimmbar werden. Deshalb dürfte in vielen Fällen die Geokoordinate als personenbezogenes Datum zu qualifizieren sein. Ausweislich der Gesetzesbegründung soll durch die Speicherung der Koordinaten eine direkte räumliche

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

und technisch einfache Zuordnung und Verknüpfung verschiedener Informationen möglich sowie eine Auswertung deutlich vereinfacht werden. Hierin liegt jedoch ein großes Risiko für das informationelle Selbstbestimmungsrecht. Es besteht die Gefahr, dass die Zweckbindung der Registerdaten nicht eingehalten wird und Daten unzulässig zusammengeführt werden. Des Weiteren sind detaillierte Profilbildungen denkbar. Angesichts der hohen datenschutzrechtlichen Gefährdungslage ist die Erforderlichkeit der Vorschrift in Frage zu stellen. Ich hatte daher für eine Streichung der Regelung plädiert.

Wie das E-Government-Gesetz des Bundes sieht das E-Government-Gesetz Baden-Württemberg in § 14 vor, dass die Pflicht zur Bekanntmachung oder Veröffentlichung in einem amtlichen Mitteilungs- oder Verkündungsblatt zusätzlich oder ausschließlich elektronisch erfüllt werden kann. Insbesondere die Veröffentlichungen von Gemeinden in ihren Mitteilungs- und Verkündungsblättern enthalten häufig personenbezogene Daten, die durch eine Veröffentlichung im Internet dauerhaft und weltweit verfügbar gemacht werden. Hieraus ergibt sich eine spezifische Gefährdung des informationellen Selbstbestimmungsrechts der Betroffenen. Die Gefährdungslage ist als gravierend einzustufen, weil durch eine Internetveröffentlichung nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche es jedem Internet-Nutzer mit Hilfe einer Suchmaschine jederzeit erlaubt, durch die Eingabe des Namens der Betroffenen sämtliche zu diesen Personen vorhandenen Angaben zu sammeln und – losgelöst vom ursprünglichen Informationszweck – Persönlichkeitsprofile anzulegen. Diese Möglichkeit einer weltweiten dauerhaften Veröffentlichung halte ich nicht für erforderlich. Aufgrund meiner in der Stellungnahme zum Referentenentwurf geäußerten Bedenken wurde in Absatz 3 zumindest eine Pflicht zur nachträglichen Unkenntlichmachung von personenbezogenen Daten aufgenommen. Unklar ist jedoch, wie der Verpflichtung zur nachträglichen Unkenntlichmachung in der Praxis technisch und organisatorisch nachgekommen werden soll. Es wäre besser gewesen, vor einer Internetveröffentlichung eine Interessenabwägung zu fordern und die Dauer der Veröffentlichung im Internet in jedem Fall zu begrenzen.

Die frühzeitige Beteiligung meiner Dienststelle bei der Entstehung des E-Government-Gesetzes des Landes ist positiv hervorzuheben. Leider wurde in einigen zentralen Punkten meiner Kritik kein Gehör geschenkt. Abzuwarten bleibt, wie die Umsetzung in der Praxis gelingt.

11.9 Die Evaluierung des Rundfunkbeitragsstaatsvertrags

Durch den 15. Rundfunkänderungsstaatsvertrag wurde das System des Rundfunkbeitrags grundlegend geändert. Die gerätebezogene Rundfunkgebühr wurde ab 2013 auf einen wohnungsbezogenen Rundfunkbeitrag umgestellt. Über die in diesem Zusammenhang aufgetretenen datenschutzrechtlichen Probleme habe ich bereits in meinem 30. Tätigkeitsbericht 2010/2011 berichtet (LT-Drs. 15/955, 9. Teil, 3.). In einer Protokollerklärung aller Länder wurde damals eine Evaluierung des Rundfunkbeitrags vereinbart. Überdies verabschiedete der Landtag einstimmig eine Entschließung, wonach in die Evaluierung explizit Aspekte der Datenschutzkonformität einbezogen werden sollten (LT-Drs. 15/671). Meine im 30. Tätigkeitsbericht 2010/2011 geäußerte Hoffnung, dass damit dem Datenschutz bei der Erhebung der Rundfunkbeiträge künftig mehr Beachtung geschenkt wird, wurde indes enttäuscht.

Anfang 2012 wurde zur Durchführung der Evaluierung des Rundfunkbeitrags eine Arbeitsgemeinschaft der Medienreferenten der Staatskanzleien unter dem Vorsitz Baden-Württembergs eingesetzt. Die Ergebnisse der Evaluierung fanden nunmehr Eingang in den 19. Rundfunkänderungsstaatsvertrag (vgl. LT-Drs. 15/7680), mit dem auch der Rundfunkbeitragsstaatsvertrag (RBStV) angepasst wird. Einige Punkte sind aus datenschutzrechtlicher Sicht durchaus zu begrüßen. So wurde in § 11 Absatz 4 Satz 2 RBStV eine Klarstellung aufgenommen, welche öffentlichen und nichtöffentlichen Stellen auskunftspflichtig sind, und in § 11 Absatz 4 Satz 5 Nr. 1 RBStV der Direkterhebungsgrundsatz als zentrales datenschutzrechtliches Prinzip ausdrücklich verankert. Ferner wurde in § 11 Absatz 7 RBStV eine Auskunftspflicht der Rundfunkanstalten gegenüber den Betroffenen über die datenübermittelnde Stelle aufgenommen. Schließlich wurde die bereits mit dem 15. Rundfunkänderungsstaatsvertrag kritisierte Datenerhebungsbefugnis durch Ankauf von

32. Tätigkeitsbericht 2014/2015 - 11. Technik und Medien

Adressdaten weiterhin bis zum 31. Dezember 2020 ausgesetzt.

Erhebliche datenschutzrechtliche Bedenken begegnet jedoch die neue Vorschrift des § 14 Absatz 9a RBStV. Zur Sicherstellung der Aktualität des Datenbestandes wird zum 1. Januar 2018 ein weiterer vollständiger Meldedatenabgleich durchgeführt. Die Meldebehörden sind danach verpflichtet, die Daten bis längstens 31. Dezember 2018 zu übermitteln. Die Rundfunkanstalten begründen die Erforderlichkeit mit der Sorge vor einer Erosion der Bestandsdaten, weil nach dem Tod des bisherigen Beitragsschuldners oder dessen Auszug aus einer Wohnung (z. B. wegen Trennung, Scheidung, Auflösung einer WG) ohne Zutun der zurückbleibenden Person nicht bekannt werden würde, wer neuer Beitragsschuldner ist. Sie gehen von einem jährlichen „Schwund“ von rund 200.000 beitragspflichtigen Wohnungen aus. Bereits der im Jahr 2013 durchgeführte vollständige Meldedatenabgleich war auf erhebliche datenschutzrechtliche Bedenken gestoßen (vgl. die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. September 2010, Anhang 8 meines 30. Tätigkeitsberichts 2010/2011, LT-Drs. 15/955). Diese wurden von den Datenschutzbeauftragten des Bundes und der Länder seinerzeit nur deshalb zurückgestellt, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern. Auch das im Auftrag von ARD und ZDF erstellte Rechtsgutachten von Herrn Prof. Dr. Bull sowie der Bayerische Verfassungsgerichtshof in seinem Urteil vom 15. Mai 2014 (Vf. 8-VII-12 und Vf. 24-VII-12, Ziff. 164 ff.) haben die mit dem Meldedatenabgleich verbundenen Grundrechtseingriffe nur aufgrund seiner Einmaligkeit für verhältnismäßig gehalten.

Die Rundfunkanstalten haben meines Erachtens nicht überzeugend dargelegt, weshalb ein erneuter vollständiger Meldedatenabgleich erforderlich sein soll. Belastbare Zahlen, die eine Bestandserosion begründen, sind nicht vorgebracht worden. Zudem unterliegen die Beitragspflichtigen selbst einer Anzeigepflicht, die gem. § 12 Absatz 1 Nr. 1 RBStV bußgeldbewehrt ist. Sollte dieser nicht nachgekommen werden und sollten die Inhaber einer Wohnung unbekannt sein, kann der Beitragsservice die Auskunft vom Eigentümer oder vom Verwalter der Wohnung nach § 9 Absatz 1 RBStV einholen. Dar-

über hinaus bietet das Melderecht mit der anlassbezogenen Meldedatenübermittlung an die Rundfunkanstalten eine angemessene und ausreichende Möglichkeit, die Aktualität des Datenbestandes auch bei Veränderungen der Meldesituation der Beitragsschuldner zu gewährleisten. Selbst wenn die Befürchtung eines Verlustes von ca. 200.000 Beitragspflichtigen jährlich zutrifft, ist ein Abgleich von 70 Mio. Datensätzen unverhältnismäßig.

Die Datenschutzbeauftragten des Bundes und der Länder erhielten zwar durch meinen Berliner Kollegen als Vorsitzenden des Arbeitskreises Medien Gelegenheit zur Stellungnahme, konnten sich jedoch kein Gehör verschaffen. Meine Dienststelle wurde erst im November 2015 zum Entwurf des Zustimmungsgesetzes gehört. Zu diesem Zeitpunkt war der Entwurf des Staatsvertrags jedoch bereits von den Ministerpräsidenten der Länder beschlossen und eine inhaltliche Änderung nicht mehr zu erwarten. Für eine frühere Information und unmittelbare Beteiligung meiner Dienststelle wäre ich dankbar gewesen.

Ein erneuter kompletter Meldedatenabgleich erscheint weder erforderlich noch verhältnismäßig und widerspricht darüber hinaus dem Gebot der Datensparsamkeit. Ich befürchte auch, dass es nicht bei dem erneuten „einmaligen“ Abgleich bleiben wird, sondern jetzt der Boden für eine „Dauerlösung“ bereitet wird. Unabhängig von den datenschutzrechtlichen Bedenken stünde ein regelmäßiger Meldedatenabgleich weder mit der Funktion des Melderegisters noch mit der staatsfernen Stellung der Rundfunkanstalten im Einklang.

32. Tätigkeitsbericht 2014/2015 - Inhaltsverzeichnis des Anhangs

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2014/2015		
Anhang Nr.	Datum	Thema
1	28.03.2014	Beschäftigtendatenschutzgesetz jetzt!
2	28.03.2014	Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!
3	28.03.2014	Gewährleistung der Menschenrechte bei der elektronischen Kommunikation
4	28.03.2014	Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!
5	28.03.2014	Zukünftige Struktur der Datenschutzaufsicht in Europa
6	25.04.2014	Ende der Vorratsdatenspeicherung in Europa!
7	09.10.2014	Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert
8	09.10.2014	Effektive Kontrolle von Nachrichtendiensten herstellen!
9	09.10.2014	Marktmacht und informationelle Selbstbestimmung
10	09.10.2014	Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar
11	09.10.2014	Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen
12	25.11.2014	Keine PKW-Maut auf Kosten des Datenschutzes!
13	16.12.2014	Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeld-beziehern!
14	07.01.2015	Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern
15	05.02.2015	Verfolgung des Nutzungsverhaltens im Internet
16	19.03.2015	Big Data zur Gefahrenabwehr und Strafverfolgung
17	19.03.2015	Datenschutz nach Charlie Hebdo
18	19.03.2015	Datenschutzgrundverordnung darf keine Mogelpackung werden
19	19.03.2015	IT-Sicherheitsgesetz nicht ohne Datenschutz
20	19.03.2015	Mindestlohngesetz und Datenschutz
21	19.03.2015	Nachbesserungen beim eHealth-Gesetz
22	19.03.2015	Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA
23	19.03.2015	Verschlüsselung ohne Einschränkungen ermöglichen
24	09.06.2015	Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken
25	02.10.2015	Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken
26	02.10.2015	Verfassungsschutzreform bedroht Grundrechte

32. Tätigkeitsbericht 2014/2015 - Inhaltsverzeichnis des Anhangs

Beschlüsse des Düsseldorfer Kreises 2014/2015		
Anhang Nr.	Datum	Thema
27	26.02.2014	Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)
28	26.02.2014	Vergabe von Prüfzertifikaten
29	20.05.2014	Smartes Fernsehen nur mit smartem Datenschutz
30	24.09.2014	Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert
31	16.09.2015	Nutzung von Kameradrohnen durch Private

Sonstiges		
Anhang Nr.	Datum	Thema
32	26.11.2015	Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge
33	22.04.2014	Landes- und branchenweite schriftliche Datenschutzkontrollen – Fragenkatalog

Anhang 1**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 27. und 28. März 2014****Beschäftigtendatenschutzgesetz jetzt!**

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

32. Tätigkeitsbericht 2014/2015

Anhang 2

**Entschließung der 83. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
am 28. März 2014**

**„Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des
Selbstbestimmungsrechts Betroffener!“**

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i.S.d. § 4a BDSG rechtmäßig erfolgen.
- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Abs. 3 BDSG, entspricht.
- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

32. Tätigkeitsbericht 2014/2015

- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

32. Tätigkeitsbericht 2014/2015

Anhang 3**Entschließung der 83. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
am 28. März 2014****„Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“**

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anhang 4**Entschließung der 83. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
am 28. März 2014****„Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!“**

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.
- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.
- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.
- Es ist sicherzustellen, dass
 - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

32. Tätigkeitsbericht 2014/2015

- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
- die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Anhang 5**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 28. März 2014****Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa**

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.
2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.
3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.
4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.
5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.
6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Ver-

32. Tätigkeitsbericht 2014/2015

verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

Anhang 6**Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 25. April 2014****Ende der Vorratsdatenspeicherung in Europa!**

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäischen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechte-Charta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z. B. der Fluggastdaten-Übermittlung in die USA und des Safe-Harbor-Abkommens.

32. Tätigkeitsbericht 2014/2015

Anhang 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Oktober 2014

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von *privacy by design* bzw. *privacy by default* zu verwirklichen.
- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.
- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.
- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.
- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Anhang 8**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Oktober 2014****Effektive Kontrolle von Nachrichtendiensten herstellen!**

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechts extremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

32. Tätigkeitsbericht 2014/2015

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Anhang 9**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Oktober 2014****Marktmacht und informationelle Selbstbestimmung**

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

32. Tätigkeitsbericht 2014/2015

Anhang 10**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Oktober 2014****Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar**

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status' als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzentwurf keine bzw. nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes – und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.
- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetz nicht der Fall.
- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

Anhang 11**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 9. Oktober 2014****Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen**

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden.

Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhaltenanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

32. Tätigkeitsbericht 2014/2015

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.
- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.
- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Anhang 12**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 14. November 2014****Keine PKW-Maut auf Kosten des Datenschutzes!**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

32. Tätigkeitsbericht 2014/2015

Anhang 13

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

Anhang 14**EntschlieÙung der Konferenz
der Datenschutzbeauftragten des Bundes und der Lander
vom 14. November 2014****Anforderungen an den Schutz der Datenbermittlungen zwischen medizinischen
Leistungserbringern und klinischen Krebsregistern**

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundeslander derzeit auf bundesgesetzlicher Grundlage ein flachendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfaltige Daten ber alle krebskranken Personen von allen niedergelassenen Arzten und Krankenhusern, die sie behandeln. Andererseits sollen die Register den behandelnden Arzten die empfangenen Patientendaten zum Abruf zur Verfgung stellen. Die hierbei bermittelten Daten sind hoch sensibel und knnen mannigfaltig missbraucht werden. Dem mssen die Manahmen zu ihrem Schutz entsprechen.

Mit dieser EntschlieÙung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundeslander auf, fr deren Erfllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

32. Tätigkeitsbericht 2014/2015

Anhang 15

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. Februar 2015

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Ver- folgung des Nutzungsverhaltens im Internet

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieter-übergreifenden Nutzungsprofilen verwendet, um Nutzern dann z. B. auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Art. 5 Abs. 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sog. Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Art. 5 Abs. 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

Anhang 16**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 18./19. März 2015****Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten**

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden (“Predictive Policing”).

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysensysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speichereicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertelgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysensysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

32. Tätigkeitsbericht 2014/2015

Anhang 17

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19. März 2015

Datenschutz nach „Charlie Hebdo“ : Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terroranschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

Anhang 18**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 18./19. März 2015****Datenschutzgrundverordnung darf keine Mogelpackung werden!**

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.
- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.
- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.
- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

32. Tätigkeitsbericht 2014/2015

Anhang 19

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19. März 2015

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beidseitiger, gerechter Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o. g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldepflicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

32. Tätigkeitsbericht 2014/2015

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

32. Tätigkeitsbericht 2014/2015

Anhang 20

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19. März 2015

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

U. a. haftet ein Unternehmen dafür, wenn ein Subunternehmer – und ggf. auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Anhang 21**Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 18./19. März 2015****Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister
bei Berufsheimnisträgern erforderlich**

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.
2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.
3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagsnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsheimnisträger deren Verantwortlichkeit für die Berufsheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

32. Tätigkeitsbericht 2014/2015

Anhang 22

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18./19. März 2015

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

Anhang 23**Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 18./19. März 2015****Verschlüsselung ohne Einschränkungen ermöglichen**

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014–2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist¹. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

¹ Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden.“

32. Tätigkeitsbericht 2014/2015

Anhang 24

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Juni 2015

Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten be- stehen erhebliche verfassungsrechtliche Bedenken

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtsbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Scherwiegeln einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiterer Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

Anhang 25**Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 1. Oktober 2015****Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken**

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

32. Tätigkeitsbericht 2014/2015

Anhang 26

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2015

Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden“ hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

Anhang 27**Beschluss der obersten Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 25./26. Februar 2014)****Unzulässigkeit von Videoüberwachung aus Fahrzeugen
(sog. Dashcams)**

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nichtöffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (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.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

32. Tätigkeitsbericht 2014/2015

Anhang 28**Beschluss der obersten Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 25./26. Februar 2014)****Modelle zur Vergabe von Prüfcertifikaten, die im Wege der Selbstregulierung
entwickelt und durchgeführt werden****I. Ausgangslage**

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,
- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,

32. Tätigkeitsbericht 2014/2015

- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,
- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungssuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

32. Tätigkeitsbericht 2014/2015

Anhang 29

**Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im
nicht-öffentlichen Bereich (Düsseldorfer Kreis)
sowie der
Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten
im Mai 2014**

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.
2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:
 - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
 - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und –verwendung informiert werden. – Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
 - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofilen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.
3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbie-

32. Tätigkeitsbericht 2014/2015

tern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

32. Tätigkeitsbericht 2014/2015

Anhang 30**Beschluss der Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 23./24. September 2014)****Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert**

Der Düsseldorfer Kreis weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.
- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.
- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.
- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.
- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirken die Datenschutzaufsichtsbehörden darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Anhang 31**Beschluss der Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 15./16. September 2015)****Nutzung von Kameradrohnen durch Private**

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 i. V. mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches [StGB]), mithin Bereiche der Intimsphäre (im Einzelnen

32. Tätigkeitsbericht 2014/2015

dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

Anhang 32

**Gemeinsame Erklärung der Datenschutzbeauftragten von Bund und Ländern
und des Verbandes der Automobilindustrie (VDA) zu:
Datenschutzrechtliche Aspekte
bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge
vom 26. November 2015**

Vorbemerkung

Bereits heute benötigt und produziert das moderne Kraftfahrzeug eine Vielzahl an Daten. Aufgrund der fortschreitenden informationstechnischen Ausstattung der Kraftfahrzeuge und deren Anbindung an das Internet sowie der Vernetzung der Verkehrsteilnehmer untereinander wird sich dieser Trend fortsetzen und in den kommenden Jahren zu weitreichenden Veränderungen im Straßenverkehr führen. Darüber hinaus entstehen zahlreiche neue Fahrzeugfunktionen und Verkehrstelematikanwendungen, z. B. in den Bereichen Service und Multimedia. Die Digitalisierung und insbesondere die Vernetzung bergen neben den unbestreitbaren Vorteilen für die Verkehrssicherheit und den Komfort zugleich auch Risiken für die Persönlichkeitsrechte der Fahrzeugnutzer. Vor diesem Hintergrund halten die unabhängigen Datenschutzbehörden des Bundes und der Länder und der VDA nachfolgende datenschutzrechtliche Aspekte für besonders relevant.⁹¹

1. **Personenbezogenheit:** Bei der Nutzung eines modernen Kraftfahrzeugs wird permanent eine Vielzahl von Informationen erzeugt und verarbeitet. Insbesondere bei Hinzuziehung weiterer Informationen können die anfallenden Daten auf den Halter oder auch auf den Fahrer und Mitfahrer zurückführbar sein und Informationen über persönliche oder sachliche Verhältnisse einer bestimmbar Person enthalten. Die bei der Kfz-Nutzung anfallenden Daten sind jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes (BDSG), wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.
2. Entscheidend ist der **Zeitpunkt der Datenerhebung** durch eine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Hier ist zu unterscheiden, ob es sich um Kraftfahrzeuge handelt, bei denen eine Datenspeicherung innerhalb des Fahrzeuges stattfindet („offline“), oder ob eine Übermittlung von Daten aus dem Fahrzeug heraus erfolgt („online“), wie etwa bei der Übermittlung und Speicherung von Fahrzeugdaten auf Backend-Servern.

Bei „Offline“-Autos ist von einer Datenspeicherung ohne vorherige Erhebung auszugehen. Eine Erhebung liegt mangels Erfüllung des Tatbestandes des § 3 Abs. 3 BDSG nicht vor; gleichwohl fallen anlässlich der Kfz-Nutzung Daten an, die im Fahrzeug abgelegt werden. Diese Daten müssen geschützt werden und machen – vergleichbar der Regelung in § 6c BDSG (Mobile personenbezogene Speicher- und Verarbeitungsmedien) – auch eine Sicherung des Rechts auf informationelle Selbstbestimmung erforderlich. Erst wenn die im Fahrzeug abgelegten Daten z. B. von einer Werkstatt für Reparaturzwecke ausgelesen werden, kommt es zu einer Erhebung durch eine verantwortliche Stelle nach § 3 Abs. 3 BDSG.

Bei „Online“-Autos findet bereits im Zeitpunkt der Datenkommunikation aus dem Fahrzeug heraus eine Erhebung durch eine verantwortliche Stelle im Sinne des § 3 Abs. 3 BDSG statt.

⁹¹ Datenschutzrechtliche Fragestellungen, die sich bei der Besitzüberlassung eines Kfz z. B. im Rahmen eines Dienst- oder Arbeitsverhältnisses oder einer Vermietung ergeben, sind nicht Gegenstand des vorliegenden Papiers.

32. Tätigkeitsbericht 2014/2015

3. **Verantwortliche Stelle:** Auch für die Identifikation der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ist zwischen „Offline“- und „Online“-Autos zu differenzieren.

Bei „Offline“-Autos wird derjenige, der personenbezogene Fahrzeugdaten aus dem Fahrzeug ausliest (d. h. erhebt) und anschließend verarbeitet, zur verantwortlichen Stelle. Hierbei wird es sich in der Regel um Werkstätten handeln.

Auch wenn die Hersteller bei „Offline“-Autos regelmäßig mangels Erhebung nicht bereits beim „Entstehen“ der Daten verantwortliche Stelle sind, trifft diese u. a. nach dem Gedanken „Privacy by Design“ dennoch eine Verantwortung im Hinblick auf den Datenschutz. Dies gilt insbesondere, weil der Hersteller im Rahmen seiner technischen Gestaltungsmöglichkeiten (Art und Umfang von Schnittstellen, Zugriffsmöglichkeiten, Verfolgung der in § 3a BDSG niedergelegten Grundsätze von Datenvermeidung und -sparsamkeit) Einfluss auf die zeitlich nach hinten verlagerte Erhebung und Verarbeitung hat (vergleichbar der Regelung in § 6c BDSG). Sofern es um die technischen Gestaltungsmöglichkeiten geht, sind die Hersteller auch bei dieser Fahrzeugkategorie als Ansprechpartner für die Datenschutzaufsichtsbehörden anzusehen.

Bei „Online“-Autos sind diejenigen als verantwortliche Stellen anzusehen, die personenbezogene Daten erhalten, d. h. in der Regel die Hersteller und gegebenenfalls dritte Dienst-Anbieter. Insbesondere wenn Hersteller Zusatzdienstleistungen für das Kfz anbieten und dabei in ihren Backend-Servern Daten speichern, sind sie verantwortliche Stelle für diese Datenverarbeitung.

4. Die **Zulässigkeit der Datenerhebung und -verarbeitung** kann sich insbesondere aus § 28 Abs. 1 S. 1 Nrn. 1 oder 2 BDSG, §§ 11 ff. Telemediengesetz oder aus einer Einwilligung ergeben, die den Voraussetzungen des § 4a BDSG genügt.

Wie die Informationen über Datenerhebungs- und -verarbeitungsvorgänge aufbereitet sein müssen, um Teil des Vertrags oder Grundlage für eine ggf. relevante informierte Einwilligung sein zu können (ausführliche Informationen im Sinne eines Verfahrensverzeichnis oder strukturierte, überblicksartige Informationen), bleibt Frage des Einzelfalls. Der Erstkäufer kann die notwendigen Informationen jedenfalls vom Verkäufer (Hersteller oder herstelleregebundener Händler) erhalten.

Grundsätzlich sind die wichtigsten Informationen zur Datenverarbeitung in allgemein verständlicher Form auch in der Borddokumentation nachlesbar vorzuhalten, die der Hersteller bereitstellt.

5. Gegenüber dem Hersteller besteht ein unentgeltliches **Auskunftsrecht** des Halters über seine durch den Hersteller erhobenen und gespeicherten personenbezogenen Daten nach § 34 BDSG. Darüber hinaus besteht aus § 34 BDSG kein datenschutzrechtliches Auskunftsrecht des Halters gegenüber dem Hersteller allein aufgrund dessen Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme. Die Fahrzeughalter von „Offline“-Autos haben die Möglichkeit des Auslesens von Daten, ggf. mithilfe von Sachverständigen, was nicht zwingend unentgeltlich sein muss. Aufgrund des Transparenzgebots muss der Betroffene sich unentgeltlich und ohne sachverständige Hilfe über die Grundsätze der Datenverarbeitungsvorgänge einschließlich zumindest der Art der verarbeiteten personenbezogenen Daten beim Hersteller informieren können.
5. In Bezug auf die Datenhoheit sollen die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können. Die Automobilhersteller streben an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status vorzusehen. Einschränkungen der Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende

32. Tätigkeitsbericht 2014/2015

Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist. Vom Nutzer eingegebene Informationen (z. B. Komfortdaten wie Sitzeinstellung, bevorzugte Radiosender, Navigationsdaten, E-Mail-/SMS-Kontaktdaten, etc.) muss der Nutzer jederzeit selbst ändern oder zurückstellen können.

32. Tätigkeitsbericht 2014/2015

Anhang 33



Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Der Landesbeauftragte für den Datenschutz Baden-Württemberg
Postfach 10 29 32 · 70025 Stuttgart

Datum 22. April 2014
Name
Durchwahl 0711/615541-...
Aktenzeichen: R 1910/...
(Bitte bei Antwort angeben)

 **Aufsichtsrechtliche Kontrolle nach § 38 des Bundesdatenschutzgesetzes (BDSG)**

Anlagen:

- **Merkblatt „Der betriebliche Beauftragte für den Datenschutz“**
- **Formular zur Meldung eines automatisierten Datenverarbeitungsverfahrens nach § 4d BDSG (einschließlich Bearbeitungshinweisen)**

Sehr geehrte ...,

der Landesbeauftragte für den Datenschutz Baden-Württemberg kontrolliert als Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich bei privatrechtlichen Unternehmen und Organisationen – also bei Unternehmen der privaten Wirtschaft, Freiberuflern, Vereinen usw. – mit Sitz in diesem Bundesland die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, § 38 Absatz 1 BDSG.

Eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat (vgl. § 4 Absatz 1 BDSG).

Die zentrale Erlaubnisnorm für die Privatwirtschaft stellt dabei § 28 Absatz 1 Satz 1 Nr.1 BDSG dar, wonach die Erhebung und Verwendung personenbezogener Daten zulässig ist, sofern dies im Rahmen eines vertraglichen Verhältnisses mit der betroffenen Person erforderlich ist (z. B. Kaufvertrag, Dienstleistungs- oder Werkvertrag).

Abweichend hiervon ist nach § 30a Absatz 1 BDSG die geschäftsmäßige Erhebung und Verwendung personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung auch ohne direkte Beziehung zwischen der

32. Tätigkeitsbericht 2014/2015

verantwortlichen Stelle und der betroffenen Person zulässig, sofern die entsprechenden Voraussetzungen bei den auszuwertenden Daten und beim angewandten Verfahren vorliegen.

Um eine ordnungsgemäße Kontrolle nach § 38 Absatz 1 BDSG gewährleisten zu können, bitten wir Sie im Rahmen eines schriftlichen Kontrollverfahrens nach § 38 Absatz 3 BDSG um die Beantwortung folgender Fragen **hinsichtlich Ihrer Tätigkeit auf dem Gebiet der Markt- und/oder Meinungsforschung**:

1. Art der Tätigkeit

Nach unserer Recherche ist Ihr Unternehmen im Bereich der Markt- und Meinungsforschung tätig.

a. Trifft dies zu? Bitte schildern Sie uns Ihre Tätigkeitsbereiche.

Falls ja:

- b. Wie viele Datensätze zu wie vielen Personen speichern Sie im Durchschnitt insgesamt (einschließlich durch gesonderte Speicherung pseudonymisierter Datensätze, ohne irreversibel anonymisierte Datensätze)? Wie viele davon enthalten besondere Arten personenbezogener Daten i.S. von § 3 Absatz 9 BDSG?
- c. Welche Quellen personenbezogener Daten (einschließlich Quellen für hinzugespeicherte Daten) nutzen Sie für Ihre Markt- und/oder Meinungsforschung (z. B. öffentliche Telefonverzeichnisse, Melderegister, Adresshändler, Kundendaten einzelner Unternehmen, nach § 15 Absatz 3 des Telemediengesetzes (TMG) erhobene Nutzungsdaten, Zufallsnummern über Telefonnummernräumen, Umfrageportale)?
- d. Aus welchen Einzeldaten besteht im Regelfall ein Datensatz (Inhalts- und Zuordnungsdaten zusammengekommen)?

2. Benennung der Rechtsgrundlagen

Auf welche Rechtsgrundlagen stützen Sie die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Ihr Unternehmen?

3. Betriebliche/r Datenschutzbeauftragte/r

Grundsätzlich ist nach § 4f Absatz 1 BDSG von Unternehmen eine Datenschutzbeauftragte / ein Datenschutzbeauftragter zu bestellen, wenn in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Davon abweichend haben Unternehmen, die personenbezogene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, nach

32. Tätigkeitsbericht 2014/2015

§ 4f Absatz 1 Satz 6 BDSG unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte / einen Datenschutzbeauftragten zu bestellen.

- a. Hat Ihr Unternehmen eine Datenschutzbeauftragte / einen Datenschutzbeauftragten bestellt? Bitte legen Sie ggf. zum Nachweis eine Kopie des Bestellungsschreibens sowie Informationen zur ihrer/seiner diesbezüglichen Aus- und Fortbildung vor.
- b. Bitte übersenden Sie uns Nachweise zur konkreten Tätigkeit Ihrer/Ihres Datenschutzbeauftragten, z. B. von ihr/ihm erstellte Jahres- oder Quartalsberichte, von ihr/ihm erarbeitete Datenschutzrichtlinien und -informationen oder Mitarbeiterschulungen.
- c. Wie ist die/der Datenschutzbeauftragte in das Unternehmen eingegliedert, wem ist sie/er unterstellt?
- d. Welche Richtlinien/Anweisungen gibt es im Unternehmen zur Einbeziehung der/des Datenschutzbeauftragten?
- e. Wer ist in Ihrem Unternehmen der Ansprechpartner für betroffene Personen, die ihre Datenschutzrechte geltend machen wollen (z. B. Auskunft über die eigenen Daten, Berichtigung, Sperrung, Löschung von Daten oder Werbewiderspruch)?
- f. Welcher Zeiteanteil steht der/dem Datenschutzbeauftragten für ihre/seine Aufgaben zur Verfügung? Welche finanziellen Mittel stehen der/dem Datenschutzbeauftragten zur Verfügung? Hat sie/er ein eigenes Budget?
- g. Mit welchen sonstigen Aufgaben hat sich Ihre Datenschutzbeauftragte / Ihr Datenschutzbeauftragter neben dieser Funktion in Ihrem Unternehmen noch zu befassen? In welchem (prozentualen) Umfang?

4. Verfahrensverzeichnis und Meldungen zum Register

- a. Gemäß § 4g Absatz 2 und Absatz 2a BDSG hat jedes Unternehmen für alle eingesetzten Verfahren der automatisierten Verarbeitung personenbezogener Daten ein Verfahrensverzeichnis zu führen und seiner/seinem Datenschutzbeauftragten zur Verfügung zu stellen, wobei dieses Verzeichnis auf Antrag jedermann in geeigneter Weise verfügbar zu machen ist („Jedermannverzeichnis“).

Bitte lassen Sie uns Ihr Jedermannverzeichnis i.S. von § 4g Absatz 2 Satz 2 BDSG zukommen.

- b. Insbesondere Markt- und Meinungsforschungsunternehmen unterliegen nach § 4d Absatz 4 Nr. 3 BDSG – zumindest hinsichtlich solcher automatisierten Datenverarbeitungsverfahren, die eine geschäftsmäßige Speicherung personenbezogener Daten für Zwecke der Markt- und Meinungsforschung einschließen – der Meldepflicht nach § 4d Absatz 1 BDSG. Gemäß § 43 Absatz 1 Nr. 1 BDSG handelt ordnungswidrig, wer vor-

32. Tätigkeitsbericht 2014/2015

sätzlich oder fahrlässig die Meldung nach § 4d Absatz 1 BDSG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

Nach unseren Unterlagen liegt uns von Ihnen keine Meldung vor. Bitte teilen Sie uns ggf. mit, warum Sie Ihrer Ansicht nach nicht zur Meldung verpflichtet sind.

5. Auftragsdatenverarbeitung

Mit Unternehmen, die als Dienstleister personenbezogene Daten weisungsgebunden im Auftrag verarbeiten (z. B. Lettershops, IT-Wartungsunternehmen, Cloud-Computing-Dienstleister, Rechenzentren), muss ein dem § 11 Absatz 2 Satz 2 BDSG entsprechender schriftlicher Vertrag abgeschlossen werden.

- a. Bitte teilen Sie uns mit, welche Dienstleistungsunternehmen Ihr Unternehmen weisungsgebunden nach § 11 BDSG einsetzt, und lassen Sie uns gegebenenfalls einen Mustervertrag zukommen.
- b. Nach welchen Kriterien wählen Sie Dienstleistungsunternehmen aus und wie wird die ordnungsgemäße Auftragsabwicklung gewährleistet?

6. Sperrung/Löschung personenbezogener Daten

Welche Regeln gibt es in Ihrem Unternehmen zur Sperrung bzw. Löschung von nicht mehr erforderlichen Daten (Datenlöschkonzeption)?

7. Sonstiges

- a. Werden E-Mails mit Personenbezug ausschließlich transport- und/oder inhaltsverschlüsselt versendet?
- b. Entsorgen Sie in Ihrem Unternehmen Altpapier datenschutzgerecht?
- c. Hat Ihr Unternehmen einen Notfallplan für den Fall einer Datenpanne i.S. von § 42a BDSG? Wie sieht die Vorbereitung auf eine etwaige Aufarbeitung einer solchen Datenpanne in Ihrem Unternehmen aus?
- d. Haben Sie im Internetauftritt Ihres Unternehmens eine Datenschutzerklärung nach den Vorgaben von § 13 Absatz 1 TMG und § 4 Absatz 3 BDSG eingebunden?

Nähere Informationen können Sie den beigelegten Anlagen entnehmen. Diese Unterlagen und Informationen zu weiteren Datenschutz-Themen finden Sie auch auf unserer Homepage www.baden-wuerttemberg.datenschutz.de unter den Rubriken „Themen A–Z“, „Technik“ und „Service“.

32. Tätigkeitsbericht 2014/2015

Wir weisen Sie darauf hin, dass die der Kontrolle durch die Aufsichtsbehörden unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen haben.

Nur vorsorglich weisen wir Sie außerdem darauf hin, dass nach § 43 Absatz 1 Nr. 10 BDSG ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 38 Absatz 3 Satz 1 BDSG der Aufsichtsbehörde eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt. Diese Ordnungswidrigkeit kann nach § 43 Absatz 3 BDSG mit einer Geldbuße von bis zu 50.000 Euro geahndet werden.

Allerdings kann der Auskunftspflichtige nach § 38 Absatz 3 Satz 2 BDSG die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Absatz 1 Nrn. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Wenn Sie von Ihrem Auskunftsverweigerungsrecht Gebrauch machen wollen, sollten Sie dies jedoch näher begründen. Wer nämlich seiner Mitwirkungsobliegenheit nach § 38 Absatz 3 Satz 1 BDSG nicht nachkommt, obwohl ihm deren Erfüllung zumutbar ist, läuft Gefahr, dass die Behörde daraus für ihn nachteilige Folgerungen zieht (vgl. Kopp/Ramsauer, VwVfG, 13. Auflage, Randnummern 12a ff. zu § 24 und Randnummern 43 f. zu § 26). Das gilt auch, wenn Behauptungen nicht ausreichend belegt werden.

Unabhängig von einem Bußgeldverfahren kann eine Auskunftserteilung mit Hilfe eines Verwaltungsverfahrens nach § 38 Absatz 3 Satz 1 BDSG angeordnet und mit Mitteln der Verwaltungsvollstreckung erzwungen werden.

Wir bitten Sie daher, uns Ihre Antwort bis spätestens zum

XX.XX.XXXX

zuzuleiten. Hierfür danken wir Ihnen im Voraus.

Mit freundlichen Grüßen

Im Auftrag

32. Tätigkeitsbericht 2014/2015

Stichwortverzeichnis

Abmahnung	177	behördliche	100
Access-Provider.....	191	Datenschutzgrundverordnung	20
ad hoc Vertrag	26	Datenschutz-Grundverordnung	17
Adresshandel.....	170	Datenschutzkontrolle, schriftliche	170
Angemessenheitsentscheidung für Drittstaaten	26	Datentransfer in Drittstaaten.....	26
Antiterrordatei	41	Datenverarbeitung im Auftrag.....	138
Arbeitsdatei Szenekundige Beamte (SKB- Datenbank).....	55	Deutsche Rentenversicherung Reha-Entlassungsberichte	122
Arbeitsunfähigkeitsbescheinigung	120	Digitale Agenda.....	191
Ärzte		Digitales Testfeld Autobahn.....	93
Verrechnungsstellen.....	128	Drohnen	189
Auftragsdatenverarbeitung	113	eCall.....	93
Abgrenzung zur Funktionsübertragung....	98	E-Government-Gesetz Baden-Württemberg	197
Auskunft		Eigenbescheinigung	84
über Grundbucheinsicht	72	Einschulungsuntersuchung Gesundheitsdienstgesetz	111
Ausweiskopie		Einstellungsuntersuchung Gesundheitsdienstgesetz	111
Banken	179	Einwendungen – Internetveröffentlichung Schwärfungsfunktion Word.....	89
Hotel	167	Einwilligung	157
Automatische Kennzeichenlesesysteme	32	Bonitätsabfrage	158
Automatisiertes Fahren.....	93	E-Mail-Werbung.....	151
Balanced Scorecard	50	Elektrromobilität Vernetzung verschiedener Mobilitätsformen	101
Big Data	8	Elektronische Strafakte.....	70
Bikesharing		E-Mail-Werbung.....	151
Polygo.....	101	eTicketing.....	101
Bodenseeschifffahrt	105	EuGH	22
Bonitätsabfragen.....	158	Europäische Datenschutzreform	17
Bundesmeldegesetz	86, 116	EU-Waffenrichtlinie	60
Carsharing		Fehlversendung	132
Polygo.....	101	Feuerwehrgesetz.....	94
Dashcams	188	Forschung	119
Datenformat „XWaffe“	60	Fotos	
Datenpanne	129, 132	Pflegeheim, Notfall- und Evakuierungspläne ..	127
Datenschutz		Fototaschen	175
Europa	19	Führungs- und Einsatzanordnung Fußball Baden-Württemberg (FEA Fußball).....	59
Datenschutzbeauftragter	165		
Beendigung der Tätigkeit eines betrieblichen DSB.....	166		
behördliche	88		
Datenschutzerklärung.....	194		

32. Tätigkeitsbericht 2014/2015

Fundsachen mit elektronischem Speicher.....	90	Krankengeldfallmanagement	120
Funktionsübertragung		Krankenhaus.....	113
Abgrenzung zur Auftragsdatenverarbeitung		Datenpanne	130
.....	98	Krankenhauseelsorge	113
Anforderungen an den Übertragungsvertrag	98	Krankenkasse	120, 124
Gerichtsvollzieher		Krankenversicherung	120
unbefugte Datenübermittlung	75	Laborauftrag durch behandelnden Arzt	128
Gesetz über den öffentlichen		Landesamt für Verfassungsschutz	41
Gesundheitsdienst.....	111	Landesgesundheitsgesetz	112
Gesetz zur Stärkung der		Landesinformationsstelle Sporteinsätze beim	
sektorenübergreifenden Zusammenarbeit		Innenministerium Baden-Württemberg (LIS)	
und der Vernetzung aller Beteiligten des		57
Gesundheitswesens in Baden-Württemberg		Landeskrankenhausgesetz.....	113
und zur Änderung anderer Gesetze		Markt- und Meinungsforschung	170
Landesgesundheitsgesetz.....	112	Medizinische Forschung	118
Gesundheitsatlas	119	Medizinischer Dienst der Krankenversicherung	
Gesundheitsdaten.....	125	123
Gesundheitsdienstgesetz	111	Medizinischer Dienst der Krankenversicherung	
GPEN Privacy Sweep 2014.....	194	(MDK)	120
Haftungsprivilegierung.....	191	Meldedaten	
Hauptzollamt.....	134	Hotel	167
Hausarzt	113	Meldedatenabgleich.....	199
Haushaltsbefragung.....	83	Mietbescheinigung.....	133
HbbTV.....	193	Mieterselbstauskunft.....	179
Heartbleed Bug.....	194	Mindestlohngesetz.....	145
Heimaufsicht.....	135	mobile Datenträger	130
Hilfsmittelerbringer.....	125	Nationalen Waffenregister (NWR)	59
Hotel.....	167	Notariat	75
Hybrid-TV-Dienste	193	Altpapierentsorgung	74
individuelle Vertragsklauseln	26	Aufbewahrung von Unterlagen	72
Industrie 4.0	13	Kontrolle	74
Informationspflicht nach § 42a BDSG	180	Urkundenarchiv	72
Infrastrukturabgabe.....	93	Notfall- und Evakuierungspläne	
Intelligente Verkehrssysteme	93	Pflegeheim, Fotos.....	127
Internationaler Datentransfer.....	26	NSA-Affäre.....	15
JI-Richtlinie	19	Öffentlichkeitsfahndung	
Jobcenter	133, 134	In sozialen Netzwerken	71
Kontoauszüge.....	133	OpenSSL	195
Kraftfahrzeug		ÖPNV	
Datenverarbeitung im Kraftfahrzeug	93	Polygo.....	101

32. Tätigkeitsbericht 2014/2015

Orientierungshilfe	Schutzprogramme	196
Krankenhausinformationssysteme (OH KIS)	Selbstvermessung	12
.....	Sicherheitskopien	197
.....	Sicherheitsupdates	196
Orientierungshilfe Smart-TV	Smart Meter	183
Passwörter	Smartphone Apps	194
Personalausweis	Smart-TV-Dienste	193
Personaldaten	Social Plugins	195
Pflege	Soziale Netzwerke	
Pflegeheim	Öffentlichkeitsfahndung	71
Notfall- und Evakuierungspläne, Fotos .	Spam-Mails	196
.....	Speichermedien	130
Pflegekasse	Staatsanwaltschaft	116
Phishing	Staatsschutz	41
Pkw-Maut	Stadtwerke	165
Polizei	Standardvertragsklauseln	26
Auskunft	Steuer	84
Datenlöschung	indirekte	84
Fahndung	Steuerschuldner	84
Löschung	Steuerträger	85
Predictive Policing	Störerhaftung	191
Verdeckte Ermittler	Strafakte	
Videobeobachtung	elektronische	70
Vorbeugende Straftatenbekämpfung	Straßenverkehr	
Polygo	Kennzeichenlesesysteme	93
Postunternehmen	Stromzähler, intelligente	183
Prüfbericht	Telefon	
Prümer Beschluss	Überwachung, Aufzeichnen, Mithören ..	147
Ransomware	Telemediengesetze	191
Rechtsanwälte	TMF	118
Aufbewahrungsfrist für Handakten	Trilog-Verhandlungen	20
.....	TwoGo by SAP	98
Red Button	Übermittlung	
Reha-Entlassungsberichte	Gerichtsvollzieher	75
Deutsche Rentenversicherung	Übernachtungssteuer	84, 85
.....	Umschlagverfahren	124
Reichweitenanalysewerkzeuge	Unterlassungsklagegesetz	177
Reservierungsbestätigung	Urkundenarchiv	
Reservierungsbestätigung	Notariat	72
Rundfunkbeitrag	Verband der Automobilindustrie (VDA)	93
Safe Harbor	Verbot mit Erlaubnisvorbehalt	89
Saisonkarten		
Erfassung von Nutzungsdaten		
.....		
Sammelprüfaktion		
Sanktionslistenabgleich		
Schadprogramme		

32. Tätigkeitsbericht 2014/2015

Verbraucherschutzorganisation	177	Verschlüsselung	130
Verbunddatei „Gewalttäter Sport“	56	Videüberwachung	185
Verfahren der „Online- Sicherheitsüberprüfungen“ (OSIP-BW)	60	Dashcams	188
Verfahrensverzeichnis		Drohnen	189
Zeitpunkt des Erstellens	144	durch Privatpersonen, EuGH-Urteil	
Zeitpunkt des Meldens an den Datenschutzbeauftragten	144	Rechtssache Ryneš	187
Verfassungsschutz	66	in öffentlichen Verkehrsmitteln	186
Strategische Fernmeldeüberwachung	35	Orientierungshilfe	185
Verkehr		Videüberwachung in Schwimmbädern	185
Reisezeitermittlung	107	Vorratsdatenspeicherung	
Verkehrsverbund		EuGH-Urteil vom 8. April 2014	69
Datenerhebung zur Einnahmenverteilung	105	Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten	69
Vermittlung datenschutzrechtliche Grundlagen	88	WLAN	191
vernetztes Fahren	93	Wohn-, Teilhabe- und Pflegegesetz	135
Verrechnungsstellen		Wohngeld	137
Einsatz durch Ärzte	128	Wohngruppenzuschlag	136
Versammlung		Zensus 2011	79
Videoaufnahme durch Versammlungsteilnehmer	31	Zentrale Informationsstelle Sporteinsätze (ZIS)	57
		Zugriffskontrolle	195