Landtag von Baden-Württemberg **Drucksache 15 / 955**

15. Wahlperiode **01. 12. 2011**

Mitteilung

des Landesbeauftragten für den Datenschutz

30. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2010/2011

Schreiben des Landesbeauftragten für den Datenschutz Baden-Württemberg vom 1. Dezember 2011:

Anbei übersende ich Ihnen unseren 30. Tätigkeitsbericht, der nach § 31 Absatz 2 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 1. Dezember 2011 zu erstatten ist.

Klingbeil

Eingegangen: 01. 12. 2011 / Ausgegeben: 21. 12. 2011

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.

30. Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz
Baden-Württemberg
2010/2011

INHALTSVERZEICHNIS

Seite

Vorwort 11

1. Teil: Zur Situation 13

1. Die Zäsur – Datenschutz aus einer Hand in Baden-Württemberg 13
   1.1 Das Urteil des Europäischen Gerichtshofs vom 9. März 2010 und seine Umsetzung 13
   1.2 Die Änderung des Landesdatenschutzgesetzes Baden-Württemberg 13
   1.3 Erste Eindrücke und Probleme 14
   1.4 Der Wechsel beginnt – auch im Datenschutz? 16
2. Entwicklung des Datenschutzrechts 2010/2011 18
   2.1 Die Neuregelung der Videoüberwachung durch öffentliche Stellen in § 20 a LDSG 18
   2.2 Ein modernes Datenschutzrecht für das 21. Jahrhundert 21
   2.3 Aktivitäten auf Bundesebene im Berichtszeitraum 22
      2.3.1 Neue Regelungen zur Informationspflicht bei Datenschutzverstößen 22
      2.3.2 Die gesetzliche Neuregelung des Beschäftigtendatenschutzes ist überfällig 24
      2.3.3 Bis hierher und nicht weiter: Rote Linien im Internet 27
      2.3.4 Ein neuer Akteur? Die Bundesstiftung Datenschutz 28
      2.3.5 Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages 29
   2.4 Novellierung des europäischen Rechtsrahmens 30
3. Internationaler Datenverkehr 31
   3.1 Das sogenannte SWIFT-Abkommen 31
   3.2 Flugpassagiere als generell Verdächtige 32
   3.3 Internationale Datenübermittlungen zwischen Unternehmen 33
   3.4 Strafverfolgung über die Grenzen – Grenzen für den Datenschutz? 34
4. Aktuelle technische Herausforderungen 35
   4.1 Von hölzernen Pferden und Holzwegen – der „Staats-Trojaner“ im Einsatz 35
   4.2 Reine Fassade? Panoramaansichten im Internet 40
   4.3 „Google Analytics“ – Reichweitenanalyse jetzt datenschutzkonform möglich 42
   4.4 Der intelligente Stromzähler 43
   4.5 Datenschutz in der Wolke? Cloud Computing 44
   4.6 Das gefällt uns (noch) nicht – Datenschutz in sozialen Netzwerken 46
5. Die Dienststelle in Zahlen 51

Seite

2. Teil: Öffentliche Sicherheit und Justiz 54

1. Abschnitt: Öffentliche Sicherheit 54

1. Gesetzgebung 54
1.1 Gesetzliche Regelungen zur Terrorismusabwehr verlängert 54
1.2 Vorratsdatenspeicherung 55
1.3 Nationales Waffenregister 55
1.4 Rechtsgrundlagen für die Tätigkeit des Bundeskriminalamts 56
1.5 Verfassungsschutz – verfassungswidrige Maßnahmen zum Schutz der Verfassung? 57
2. Datenverarbeitung durch Sicherheitsbehörden 57
2.1 1. Mai 2009 – Tag der Arbeit – mit Folgen für viele 57
2.2 Dienstanweisung POLAS-BW – ein Weg zu mehr Datenqualität 59
2.3 Die Prüffallregelung nach § 38 Absatz 2 des Polizeigesetzes auf dem datenschutzrechtlichen Prüfstand 62
2.4 Videoüberwachung bei der Polizei – wofür ist sie wirklich geeignet? 66
2.5 Die „Sport-Dateien“ der Polizei im Land und das Problem mit der Verbunddatei 69
2.6 Was gibt es Neues zur Arbeitsdatei „Politisch motivierte Kriminalität“? 71
2.7 Verdeckte Ermittlungen in Heidelberg und beim NATO-Gipfel 2009 72
2.8 „Zuverlässigkeitsüberprüfungen“ bei Großveranstaltungen weiterhin ohne gesetzliche Grundlage 75
2.9 NADIS – das nachrichtendienstliche Informationssystem des Verfassungsschutzes in neuem Gewand 77

2. Abschnitt: Justiz 79

1. Gesetzgebung 79
1.1 Schuldner bald im Internet? Das bundesweite Vollstreckungsportal 79
1.2 Eine fesselnde Angelegenheit – die elektronische Fußfessel in der Führungsaufsicht 80
1.3 Der virtuelle Überwachungsraum – Funkzellenabfrage 81
2. Grenzen der Kontrollbefugnis des Datenschutzes im Justizbereich 83
3. Eine Strafanzeige kommt selten allein – aber warum müssen Anzeigeerstatter über andere Anzeigeerstatter informiert werden? 84

3. Teil: Bildung und Forschung 87

1. Datenschutz an Schulen 87
1.1 Aktuelle Entwicklungen im Bereich der öffentlichen Schulen in Baden-Württemberg: Es tut sich etwas! 87
1.2 Sparsamkeit am falschen Platz: Datenschutz an einer Gesamtschule 88
2. Datenschutz im Hochschulbereich 89
2.1 Sicherheitsforschung – für welchen Zweck? 89
2.2 Ohne nachzudenken ins Internet eingestellt und dann vergessen? 90

Seite

4. Teil: Gesundheit und Soziales 92

1. Abschnitt: Gesundheit 92

1. Die Elektronische Gesundheitskarte – eine fast unendliche Geschichte 92
2. Datenschutz im Krankenhaus 92
2.1 Kontrollbesuch in einem Klinikum 92
2.1.1 Das Krankenhausarchiv 93
2.1.2 Die Videoüberwachung 94
2.1.3 Der Datenschutzbeauftragte im Klinikum 95
2.2 Die neue Orientierungshilfe für Krankenhausinformationssysteme 96
2.3 Terminvereinbarung an der Krankenhauspforte 97
2.4 Akteneinsicht in Patientenakte einer verstorbenen Verwandten in einem Krankenhausarchiv 98
3. Laborbeauftragung durch Arzt 100
4. Datenschutzrechtliche Fragen bei einem überbetrieblichen Dienst von Betriebsärzten 101
5. Korrektur psychiatrischer Verdachtsdiagnosen mittels des datenschutzrechtlichen Berichtigungsanspruchs? 104
6. Aufzeichnung von Anrufen bei Integrierten Leitstellen 105
7. Wie geht es weiter mit der Einschulungsuntersuchung? 106
8. Pflegestützpunkte mit datenschutzrechtlichen Startproblemen 107

2. Abschnitt: Soziales 109

1. ELENA gestoppt – ein Sieg der Vernunft und des Datenschutzes 109
2. Grundsicherung für Arbeitsuchende neu geregelt 111
3. Einzelfälle 112
3.1 Auskunftspflicht von Unterhaltspflichtigen 112
3.2 Datenerhebung beim Vermieter 113
3.3 Verstoß gegen die Unterstützungspflicht öffentlicher Stellen 114

5. Teil: Datenschutz in anderen Verwaltungsbereichen 115

1. Kommunales 115
1.1 Fertigung von Luftbildaufnahmen zur Ermittlung von kommunalen Abwassergebühren 115
1.2 So kommt der Datenschutz auf den Hund 116
1.3 Kommunale Veröffentlichungen im Internet 117
1.3.1 Die Übertragung von Gemeinderatssitzungen im Internet 118
1.3.2 Die Veröffentlichung von Alters- und Ehejubiläen im Internet 121
1.3.3 Die Einstellung von Fotos in das Internet 121
1.3.4 Videoaufnahmen von Kindergartenkindern im Internet 122
1.4 Das neue Bundesmeldegesetz kommt – ohne zentrales Bundesmelderegister 123

Seite

1.5 Meldewesen – Fehler im Meldeverfahren MeldIT 123

1.6 Der neue elektronische Personalausweis – Kontrollbesuch bei drei Kommunen 125

1.7 Bewerbungen für den Migrationsbeirat 126

1.8 Auskünfte aus Bauakten an Dritte 127

1.8.1 Grundlegendes 127

1.8.2 Datenübermittlung an einen Mieter 128

1.9 Das Ende des Subventionsprangers – der EuGH hat ein Einsehen 129

1.10 Personenbezug bei Webcams – wo fängt er an, wo hört er auf? 130

2. Steuerverwaltung 131

2.1 Datenschutzpanne beim elektronischen Lastschriftverfahren für die Kfz-Steuer 131

2.2 Auch Steuerpflichtige haben ein Recht auf Auskunft! 131

3. Volkszählung Zensus 2011: Ohne wesentliche Datenschutzmängel 132

6. Teil: Datenschutz in der Arbeitswelt 134

1. Abschnitt: Gesundheitsdaten im Arbeitsverhältnis 134

1. Erhebung von Gesundheitsdaten bei Arbeitnehmern anlässlich der Einstellung 134

2. Erhebung von Gesundheitsdaten im Rahmen von Krankenrückkehrgesprächen 135

3. Krank im Kalender? Gesundheitsdaten in elektronischen Abwesenheitsmanagementsystemen 137

4. Erhebung der Schwerbehinderteneigenschaft von Bewerbern und Arbeitnehmern 138

5. Mehr Datenschutz beim Voranerkennungsverfahren für die Beihilfefähigkeit einer ambulanten psychotherapeutischen Behandlung 139

6. Verwaltungsvorschrift zur Beihilfeverordnung – Beihilfe für berücksichtigungsfähige Angehörige 139

2. Abschnitt: Weitere Fragen des Arbeitnehmerdatenschutzes 140

1. Speicherung und Nutzung der bei Personaleinkäufen anfallenden Daten 140

2. Fragerecht des Arbeitgebers im Bewerbungsverfahren: Bewerberfragebogen 141

3. Verarbeitung personenbezogener Daten für Auslandseinsätze von Mitarbeitern durch eine Wirtschaftsprüfungsgesellschaft im Auftrag des Arbeitgebers 143

4. Datenübermittlung in die USA zur Vorbereitung einer Mitarbeiterbefragung 144

5. Dürfen Mitarbeiterdaten mit „Antiterrorlisten“ abgeglichen werden? 146

6. Compliance-Ermittlungen 147

7. Erhebung und Speicherung der Standortdaten von Dienstfahrzeugen mittels Ortungssystemen 148

Seite

8. Bei der Videobeobachtung kleine Brötchen backen! 152
9. Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung beim konzernweiten Datentransfer 154
10. Unbefugte Auskünfte aus dem Personalverwaltungssystem einer Stadt 157
11. Datenschutzrechtliche Fallstricke einer Mitarbeiterbefragung 158
12. Der überwachungsbedürftige Wachmann 158
13. Löschkonzeption für elektronische Personalakten 160

7. Teil: Datenschutz in der Wirtschaft 161

1. Abschnitt: Der Betriebliche Datenschutzbeauftragte 161

1. Grundsätzliche Anforderungen 161
2. Ist Personal mit gelegentlichem Lesezugriff auf den Kundenadressbestand ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt? 162

2. Abschnitt: Werbung und Adresshandel 163

1. Neue datenschutzrechtliche Regelungen für die Werbung und den Adresshandel 163
2. Moderne Zeiten - Wahlwerbung per E-Mail und SMS 165
3. Die Freundschaftswerbung 166

3. Abschnitt: Auskunfteien und Inkassounternehmen 167

1. Allwissend und auskunftsfreudig – die Auskunfteien 167
2. Scoring 170
3. Datenschutz bei Durchleiteauskunfteien 171
4. Personenverwechslung beim Inkasso 172
5. Rechtsanwälte und der Datenschutz 173

4. Abschnitt: Versicherungen 174

1. Das neue Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft 174
2. Neue Einwilligung und Schweigepflichtentbindungen 176
3. Der Beitrag hängt vom Fahrstil ab 177
4. Abgabe der Akten der Gebäudebrandversicherung an Archive 178

5. Abschnitt: Devisen nur gegen Identitätsnachweis? 179

6. Abschnitt: Sonstiges 180

1. Datenschutz an der Ladenkasse 180
2. Datenentsorgung in der Mülltonne 182
3. Das Leih-Notebook als Datenfundgrube 183
4. Steckbriefe im Modecenter 184

Seite

8. Teil: Datenschutz im Verein 186

1. Der wahlkämpfende Vereinskassierer 186
2. Erhebung personenbezogener Daten beim Erwerb von Eintrittskarten 187
3. Schiri, wir wissen, wann du Geburtstag hast! 187

9. Teil: Technik und Medien 189

1. Videoüberwachung 189
   - 1.1 Achtung, wachsamer Nachbar! 189
   - 1.2 Videoüberwachung in Gaststätten 190
   - 1.3 Waschen, Schneiden, Föhnen, Videobeobachten 191
2. Datenschutzprobleme im Internet 192
   - 2.1 Das Datenleck beim Dienstleister I 192
   - 2.2 Das Datenleck beim Dienstleister II – Personenbezogene Kundendaten im Internet 193
3. Abschied von der GEZ? Der 15. Rundfunkänderungsstaatsvertrag 194

Inhaltsverzeichnis des Anhangs 197

Vorwort

Der Berichtszeitraum des 30. Tätigkeitsberichts deckt die Jahre 2010 und 2011 ab und umfasst damit einen Zeitraum, der für meine Dienststelle erhebliche Herausforderungen mit sich brachte und immer noch bringt. Am 1. April 2011 trat die grundlegendste Änderung seit der Einrichtung des Amtes in Kraft: Dank eines kaum erwarteten Kurswechsels der größten damaligen Regierungsfraktion im Herbst 2009 und befördert durch ein Urteil des Europäischen Gerichtshofs vom 9. März 2010 wurden endlich die beiden Datenschutzkontrollbehörden des Landes, die bis dato im Innenministerium angesiedelte Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich und meine Dienststelle, zusammengeführt. Damit wurde endlich ein „Geburtsfehler“ der Datenschutzaufsicht in Baden-Württemberg, der seit dem Inkrafttreten des Landesdatenschutzgesetzes am 1. April 1980 bestand, korrigiert. Zugleich wurde die Dienststelle aus dem Geschäftsbereich des Innenministeriums herausgelöst und dem Landtag zugeordnet. Datenschutz aus einer Hand wird nunmehr möglich. Die mit der Zusammenlegung verbundenen personellen und organisatorischen Veränderungen haben die Arbeitsfähigkeit der Dienststelle allerdings vorübergehend erheblich beeinträchtigt, zumal wir erst Ende Oktober 2011 in gemeinsame Diensträume umziehen konnten. Gravierende Auswirkungen hatte auch der personelle Umbruch in der Aufsichtsbehörde, der für einen erheblichen Erfahrungsverlust sorgte. Auf diese Weise gibt manche Passage dieses Berichts eher die aus dem Studium der Akten als die aus eigener unmittelbarer Anschauung gewonnenen Erkenntnisse wieder. Die Startbedingungen für die Dienststelle in neuer Formation waren somit nicht ganz einfach.

Während dieser Tätigkeitsbericht für den Datenschutz im öffentlichen Bereich nahtlos an den 29. Tätigkeitsbericht vom Dezember 2009 anknüpfen kann, stellt er für den Datenschutz im nicht-öffentlichen Bereich die Entwicklung seit dem Erscheinen des Fünften Tätigkeitsberichts des Innenministeriums zum 1. Juli 2009 dar. Er deckt damit zum größten Teil den Zeitraum vor der Zusammenlegung ab, für den ich noch nicht die Verantwortung trug. Der Bericht beruht insoweit auch auf der Tätigkeit des langjährigen Leiters der Aufsichtsbehörde, dem an dieser Stelle ein herzliches Wort des Dankes für seine stets kompetente Arbeit unter schwierigen Rahmenbedingungen gebührt. Dieser Dank gilt ebenso seinen Mitarbeiterinnen und Mitarbeitern, die zum Teil jetzt auch die meinen sind. In gleicher Weise bin ich natürlich auch dem bewährten übrigen Team meiner Dienststelle zu Dank verbunden.

Die Zukunft des Datenschutzes bleibt spannend: Auf europäischer Ebene steht eine Neuordnung des Rechtsrahmens an, die aller Voraussicht nach Ende Januar 2012 der Öffentlichkeit vorgestellt werden wird und erheblichen Einfluss auf die deutsche Rechtsentwicklung haben dürfte. Insofern bin ich skeptisch, ob die überfällige Modernisierung des Datenschutzrechts noch während der laufenden Legislaturperiode des Bundestags in Angriff genommen wird. Selbst die wichtige Neuregelung des Beschäftigtendatenschutzes scheint derzeit nicht voranzukommen und droht im Sperrfeuer gegenläufiger Interessen hängenzubleiben. Dadurch besteht die Gefahr, dass sich die Bundespolitik auf Nebenkriegsschauplätze wie die Gründung einer Bundesstiftung Datenschutz begibt oder das weite Feld des Internetrechts internationalen Konzernen zur Selbstregulierung überlässt. Auf Landesebene ist zu hoffen, dass die neue Landesregierung der programmatischen Ankündigung in der Koalitionsvereinbarung, den unabhängigen Datenschutz stärken zu wollen, bald Taten folgen lässt. Durch eine Personalverstärkung könnte meine Dienststelle mehr als bisher präventiven Datenschutz betreiben.

In den nächsten Monaten wird die fusionierte Dienststelle weiter zusammenwachsen, insbesondere um diejenigen Themenschwerpunkte aufzugreifen, die sich sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich zu gemeinsamen Herausforderungen entwickelt haben. Hier sind in erster Linie das Internet und die darauf basierenden Geschäftsprozesse in Verwaltung und Wirtschaft zu nennen. Wenn ich die Bandbreite der Themen in den letzten Monaten betrachte, dann wäre dieses Spektrum mit dem Schlagwort „zwischen Staats-Trojaner und Facebook“ am besten umschrieben. Auf beide Stichworte wird in diesem Bericht eingegangen (1. Teil, Nummern 4.1 und 4.6). Daneben finden sich Ausblicke auf die europäische und nationale Weiterentwicklung des Datenschutzrechts, aber auch Bewertungen der vorhandenen Defizite, zu denen – wie gesagt – insbeson-

dere die ausstehende gesetzliche Regelung des Beschäftigtendatenschutzes zählt (1. Teil, Nummer 2.3.2). Die Darstellung des Datenschutzes in der Arbeitswelt ist erstmals ein besonderer Schwerpunkt meines Tätigkeitsberichts (6. Teil), zumal hierzu immer wieder Anfragen und Eingaben von Betriebs- und Personalräten eingehen. Wie gewohnt bilden die im Bericht dargestellten Einzelfälle nur die Spitze des Eisbergs der tagtäglichen Beratungs- und Kontrollpraxis meiner Mitarbeiterinnen und Mitarbeiter ab.

Im Laufe des kommenden Jahres soll unser Internet-Auftritt überholt werden, der mittlerweile optisch und hinsichtlich der Benutzerfreundlichkeit in die Jahre gekommen ist. Auch für meine Dienststelle wird das Internet zu einem immer wichtigeren Kanal für Kommunikation und Interaktion. Den gewandelten Mediengewohnheiten der Bürgerinnen und Bürger wollen wir auf diese Weise Rechnung tragen. Für Anregungen und Verbesserungsvorschläge – auch hinsichtlich der bisherigen Form des Tätigkeitsberichts – bin ich weiterhin dankbar.

Jörg Klingbeil

1. Teil: Zur Situation

1. Die Zäsur – Datenschutz aus einer Hand in Baden-Württemberg

1.1 Das Urteil des Europäischen Gerichtshofs vom 9. März 2010 und seine Umsetzung

Die Entscheidung kam für viele überraschend und bestätigte die Position der Datenschutzbeauftragten auf eindrucksvolle Weise: Mit Urteil vom 9. März 2010 (C-518-07) gab der Europäische Gerichtshof (EuGH) der Klage in dem Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland statt und stellte fest, dass die für die Kontrolle der Datenverarbeitung im nicht-öffentlichen Bereich zuständigen Stellen der Länder nicht völlig unabhängig seien, wie es Artikel 28 der Europäischen Datenschutzrichtlinie 95/46/EG fordert. Beanstandet wurde insbesondere die bis dato bestehende Rechts- und Fachaufsicht von Regierungsstellen über die Kontrollbehörden und das damit verbundene Risiko einer direkten oder indirekten Einflussnahme auf deren Kontrolltätigkeit. Mit dem – von den Datenschutzbeauftragten des Bundes und der Länder einhellig begrüßten (vgl. Entschließung vom 17./18. März 2010, Anhang 4) – Urteil des Europäischen Gerichtshofs war das entscheidende Signal für eine weitreichende Strukturveränderung bei den deutschen Aufsichtsbehörden der Länder gegeben. Peu à peu wurden seither die entsprechenden Rechtsgrundlagen geändert und – soweit noch nicht geschehen – die Aufsichtsbehörden für den nicht-öffentlichen Bereich mit den Dienststellen der jeweiligen Landesbeauftragten für den Datenschutz zusammengelegt. Eine Ausnahme bildet weiterhin Bayern, wo die Zweigleisigkeit mit dem Landesamt für Datenschutzaufsicht einerseits und dem Landesbeauftragten für den Datenschutz andererseits beibehalten wurde. Die Fach- und Rechtsaufsicht wurde durchgängig abgeschafft und allenfalls eine eingeschränkte Dienstaufsicht belassen. Als letztes Land hat Thüringen sein Landesgesetz geändert und die beiden Aufsichtsbehörden ebenfalls beim Landesbeauftragten zusammengeführt. Die zwischenzeitlich im Innenausschuss des Bundesrates aufgekommene Idee, die Europäische Datenschutzrichtlinie zu ändern und die dort normierte „völlige Unabhängigkeit“ der Datenschutzaufsicht wieder einzuschränken[1], ist damit hoffentlich vom Tisch.

1.2 Die Änderung des Landesdatenschutzgesetzes Baden-Württemberg

Obwohl die CDU-Landtagsfraktion bereits im Oktober 2009, also schon einige Monate vor der EuGH-Entscheidung, ihren langjährigen Widerstand gegen eine Zusammenlegung der Datenschutzaufsichtsbehörden in Baden-Württemberg aufgegeben hatte, dauerte es noch mehr als ein Jahr, bis die Regierungsfraktionen endlich im Dezember 2010 einen Entwurf zur Änderung des Landesdatenschutzgesetzes (LDSG) in den Landtag von Baden-Württemberg einbrachten (LT-Drucksache 14/7313).

Außer der überfälligen, weil verfassungsrechtlich gebotenen Anpassung der Vorschrift über die nichtpolizeiliche Videoüberwachung durch öffentliche Stellen, die durch den Beschluss des Bundesverfassungsgerichts vom 23. Februar 2007 erforderlich geworden war und auf die noch näher eingegangen wird (1. Teil, Nr. 2.1), sah der Entwurf die angesprochene Zusammenfassung der Datenschutzaufsicht über öffentliche und nicht-öffentliche Stellen bei meiner Dienststelle und deren Zuordnung zum Landtag vor. Die bisher für den nicht-öffentlichen Bereich gegebene Fach- und Rechtsaufsicht entfiel. Als Folge meiner An-

[1] Anlass der Beratung war die Mitteilung der Kommission an das Europäische Parlament u. a.: Gesamtkonzeption für den Datenschutz in der Europäischen Union, KOM (2010) 609 endg., BR-Drucksache 707/10.

bindung an den Landtag unterstehe ich nunmehr der Dienstaufsicht des Präsidenten des Landtags, die aber – wie bisher schon im öffentlichen Bereich – stark eingeschränkt ist, da meine europarechtlich gebotene völlige Unabhängigkeit hierdurch nicht beeinträchtigt werden darf. Insofern ist die Dienstaufsicht ähnlich wie bei Mitgliedern des Rechnungshofs oder Richtern auf Lebenszeit ausgestaltet. Hingegen wurde die landesweite Zuständigkeit für die Verfolgung von datenschutzrechtlichen Ordnungswidrigkeiten – die zuvor für den nicht-öffentlichen Bereich bei der Aufsichtsbehörde im Innenministerium und für den öffentlichen Bereich bei allen vier Regierungspräsidium angesiedelt war – dem Regierungspräsidium Karlsruhe übertragen. Ich hätte mir in diesem Punkt eine mutigere Entscheidung gewünscht. Die geltend gemachten verfassungsrechtlichen Bedenken, mir auch die Zuständigkeit für Bußgeldverfahren im Datenschutz zu übertragen, überzeugten mich schon deshalb nicht, weil sie in anderen Ländern, wo die Datenschutzbeauftragten auch für die Verfolgung und Ahndung entsprechender Ordnungswidrigkeiten zuständig sind, offenbar keine Rolle spielten. In Anbetracht des engen Zeitrahmens, der so knapp vor Ende der Legislaturperiode für die Verabschiedung des Gesetzentwurfs durch den Landtag noch zur Verfügung stand, war es denn auch kein Wunder, dass meine Anregungen und Bedenken nicht mehr berücksichtigt wurden. Meine Stellungnahme zu dem Gesetzentwurf ist in LT-Drucksache 14/7482 nachzulesen.

Das Änderungsgesetz wurde vom Landtag am 2. Februar 2011 beschlossen und im Gesetzblatt vom 7. Februar 2011 verkündet (S. 43). Am 1. April 2011 trat es in Kraft. Damit wurde genau 31 Jahre nach der Einrichtung meiner Dienststelle am 1. April 1980 die wohl größte Zäsur in ihrer Geschichte vorgenommen und – wie die erste Landesdatenschutzbeauftragte Dr. Ruth Leuze schon in ihrem ersten Tätigkeitsbericht (LT-Drucksache 8/830, S. 13) schrieb – die „alles andere als bürgerfreundliche Zuständigkeitszersplitterung der Kontrolle im Datenschutz“ beendet.

1.3 Erste Eindrücke und Probleme

Mit der Zusammenlegung der Datenschutzaufsichtsbehörden hatte der Landesgesetzgeber den organisatorischen Rahmen abgesteckt. Nun galt und gilt es ihn mit Leben zu erfüllen. Angesichts des kurzen Zeitraums seit der Zusammenlegung lässt sich noch nicht von umfangreichen Erfahrungen, sondern mehr von ersten Eindrücken berichten. Daher an dieser Stelle nur ein knappes Zwischenfazit:

- Die Arbeitsbelastung im nicht-öffentlichen Bereich ist erheblich. Das belegt auch die Zahl der Eingaben und Beschwerden, obwohl die Statistiken im öffentlichen und im nicht-öffentlichen Bereich aufgrund etwas unterschiedlicher Erhebungsmethoden und Zählweisen nur schlecht zu vergleichen sind. Dem stand und steht eine unzureichende Personalausstattung gegenüber, wie auch ein Vergleich mit den Aufsichtsbehörden anderer Länder zeigt. Zwar hat der Landtag meiner Dienststelle dankenswerterweise im Dritten Nachtrag zum Staatshaushaltsplan 2011 drei Neustellen zugehen lassen, damit wurde aber unterm Strich noch kein nennenswerter Kapazitätszuwachs erreicht, weil das Innenministerium als Ergebnis der zähen „Fusionsverhandlungen“ drei hochwertige Stellen der Aufsichtsbehörde für ministerielle und andere Zwecke zurückbehielt.
- Bereits im Jahr 2010 gab es massive personelle Veränderungen in der Aufsichtsbehörde im nicht-öffentlichen Bereich und damit verbunden einen erheblichen Know-how-Verlust. Um es plastisch auszudrücken: Zum Zeitpunkt der Zusammenlegung waren nur eine Sachbearbeiterin und die Registraturkraft wesentlich länger als ein halbes Jahr im Datenschutzgeschäft der Aufsichtsbehörde tätig; die anderen Kolleginnen und Kollegen waren entweder erst kurze Zeit mit der Aufgabe befasst oder mussten – da einige Stellen zunächst unbesetzt waren – noch gefunden werden. Die letzte vakante Stelle konnte erst

im September 2011 besetzt werden. Für meine neue Aufgabe waren das keine günstigen Startbedingungen. Da der Berichtszeitraum der Aufsichtsbehörde bis zu deren letztem, dem Fünften Tätigkeitsbericht vom Juli 2009 zurückreicht, musste mancher Beitrag dieses Berichts insofern eher nach „Aktenlage“ als aus eigener Erfahrung geschrieben werden.

– Erst vor wenigen Wochen konnten meine Mitarbeiter und ich in gemeinsame Diensträume umziehen. Mehr als ein halbes Jahr waren wir – wie zuvor – an zwei Standorten in Stuttgart untergebracht, zum einen in der Urbanstraße 32, zum andern als „Untermieter“ auf drei verschiedenen Stockwerken im Innenministerium, Dorotheenstraße 6. Dass dies Doppelstrukturen bedingte und für das Zusammenwachsen der Dienststelle nicht gerade förderlich war, liegt auf der Hand. Seit dem 24. Oktober 2011 haben sich aber die äußeren Arbeitsbedingungen wesentlich verbessert: Die neuen Diensträume befinden sich in der unteren Königstraße in der Nähe des Hauptbahnhofs, damit auch verkehrsgünstig für ratsuchende Bürgerinnen und Bürger zu erreichen. Da ich selbst nicht über ein Budget für die Anmietung und Unterhaltung von Büros verfüge – so weit reicht meine europarechtlich eigentlich gebotene „Unabhängigkeit“ nun doch nicht –, war ich bei der Suche nach einer neuen Bleibe vor allem auf die Unterstützung der Liegenschaftsverwaltung angewiesen. Dem Amt Stuttgart des Landesbetriebs Vermögen und Bau Baden-Württemberg sei deshalb ein herzliches Wort des Dankes für die im Ergebnis erfolgreich bewältigte Unterbringung gesagt.

– Die Qualität meines Amtes steht und fällt mit der Qualität meiner Mitarbeiterinnen und Mitarbeiter. Auch dieser Tätigkeitsbericht ist nicht das Werk eines Einzelnen, sondern das Produkt einer Teamarbeit. Bereits bei der Novellierung des Landesdatenschutzgesetzes habe ich deshalb auf gute Rahmenbedingungen für eine vernünftige Personalpolitik großen Wert gelegt. Hierzu gehört zum einen, dass ich Bewerberinnen und Bewerbern attraktive Arbeitsplätze bieten kann, wo sie sich beruflich weiterentwickeln können. Zum andern soll eine Verwendung bei mir für sie aber auch nicht zur beruflichen Einbahnstraße oder gar Sackgasse werden, denn das wirkt sich wiederum unmittelbar auf die Neigung fähiger Köpfe aus, überhaupt zu mir zu kommen. Außerdem ist weder ihnen noch dem Datenschutz noch unseren „Kunden“ gedient, wenn es nur noch reine „Datenschutzkarrieren“ mit einer einseitigen Fokussierung von Mitarbeitern ohne Verwaltungserfahrung auf Datenschutzprobleme geben sollte und wenn sich für meine Mitarbeiterinnen und Mitarbeiter keine interessante Anschlussverwendung finden ließe. Der Landesgesetzgeber schien das ähnlich zu sehen, denn in dem neuen § 26 Absatz 4 Satz 4 LDSG wurde die Landesregierung verpflichtet, die Einbeziehung meiner Mitarbeiterinnen und Mitarbeiter in den allgemeinen Personalaustausch der Landesverwaltung zu gewährleisten. Laut Gesetzesbegründung sollte das Nähere in einer schriftlichen Vereinbarung zwischen der Landesregierung und mir geregelt werden. Auch mir war diese Regelung wichtig, denn ich befürchtete seit jeher, dass die neue unabhängige Stellung, die in der Zuordnung meiner – nunmehr größeren – Dienststelle zum Landtag zum Ausdruck kam, in gewisser Weise auch ihre Kehrseite haben könnte, nämlich in der Herauslösung aus der Personalpolitik des Innenministeriums. Die Innenverwaltung war schon aufgrund ihres großen Personalkörpers bis dato in der Lage gewesen, der Dienststelle bei der Personalrekrutierung oder bei Anschlussverwendungen flexibel zu helfen. Aus diesem Grund schrieb ich Ende Juli 2011 an den neuen Amtschef des Staatsministeriums, man möge die Verhandlungen über die in der Gesetzesbegründung vorgesehene Vereinbarung doch alsbald aufnehmen und Lösungsansätze für die künftige Rekrutierung und Anschlussverwendung meiner Mitarbeiterinnen und Mitarbeiter entwickeln. Das Antwortschreiben fiel allerdings ausgesprochen ernüchternd aus. Darin

wurde zwar dem wichtigen Anliegen einer Personalrotation allgemein zugestimmt, aber sogleich Wasser in den Wein gegossen, indem auf ähnliche Probleme in anderen Dienststellen sowie gesetzliche und personalwirtschaftliche Zwänge hingewiesen wurde, die auch durch eine mögliche Vereinbarung zwischen der Landesregierung und mir nicht außer Kraft gesetzt werden könnten. Insofern könne eine derartige Vereinbarung „allenfalls deklaratorischen Charakter“ haben. Als Trostpflaster wurde mir angeboten, meine Vorstellungen den Ressorts in einer der turnusmäßigen Personalreferentenrunden vorzutragen, was ich vor kurzem getan habe. Immerhin wurden dabei bilaterale Verhandlungen bei konkretem Bedarf und gegebenenfalls „pragmatische Lösungen“ in Aussicht gestellt. Unter der vom Gesetzgeber vorgesehenen „Vereinbarung“ zwischen der Landesregierung und mir konnte man sich indessen nichts Rechtes vorstellen, was die künftigen Probleme ahnen lässt. Als ressortübergreifende Aufgabe scheint die Unterstützung meiner Dienststelle in Personalfragen noch nicht unbedingt angesehen zu werden. Immerhin hatte ich bereits zuvor mit dem Innenministerium abgesprochen, dass ich mich bei der Besetzung neuer oder vakanter Stellen am allgemeinen Bewerberauswahlverfahren der Innenverwaltung beteiligen darf und dass Bewerber nach einer Verwendung bei mir auch wieder in die Innenverwaltung übernommen werden, wenn sie im Auswahlverfahren zuvor auch vom Innenministerium für tauglich befunden wurden. Dieses Verfahren dürfte aber nur die „Einstiegsseite“ bei Berufsanfängern abdecken und zudem nur bis zu einer nicht allzu hohen Besoldungsgruppe funktionieren. Wenn es um den „Ausstieg“, also den Wechsel auf Funktionsstellen in der übrigen Verwaltung geht, drohen die vom Staatsministerium genannten Restriktionen zu greifen. Eine gewisse Lösung könnte in der verstärkten Abordnung von Mitarbeitern der übrigen Landesverwaltung für eine bestimmte Zeit zu meiner Dienststelle liegen, sofern das stellentechnisch darstellbar ist. Davon könnten beide Seiten profitieren, so wie es sich schon in Bezug auf das Innenministerium durch die Abordnung eines Beamten des höheren Polizeivollzugsdienstes (seit Oktober 2009) und in Bezug auf das Kultusministerium durch die Abordnung eines IT-Fachlehrers (seit September 2011) gezeigt hat. Ein vergleichbares Vorgehen könnte sich anbieten, wenn tatsächlich die Zuständigkeit für die Verfolgung und Ahndung von datenschutzrechtlichen Ordnungswidrigkeitenverfahren auf meine Dienststelle verlagert werden sollte; jedenfalls habe ich schon positive Signale aus dem Justizministerium als Reaktion auf diesen Vorschlag vernommen. Ich werde jetzt aufmerksam beobachten, ob sich die Ministerien tatsächlich kooperativ zeigen und in konkreten Personalfällen befriedigende Lösungen anbieten werden, damit aus einer beruflichen Station in meiner Dienststelle keine Sackgasse wird.

1.4 Der Wechsel beginnt – auch im Datenschutz?

Die nächsten Monate werden auch zeigen, ob sich durch das Ergebnis der Landtagswahl vom 27. März 2011 die Vorzeichen für den Datenschutz im Land grundlegend verändert haben. Die die neue Landesregierung tragenden Parteien haben sich jedenfalls in ihrer Koalitionsvereinbarung (S. 67 f.) zu dem Ziel bekannt, den unabhängigen Datenschutz in Baden-Württemberg zu stärken. Unter diesem rundum erfreulichen Oberziel wird eine ganze Reihe von weiteren positiven Maßnahmen ins Auge gefasst, denen eine rasche Umsetzung zu wünschen ist:

– So soll meine Dienststelle „bei angemessener Ausstattung mit Personal und Sachmitteln“ den Status einer obersten Landesbehörde „mit eigenen Sanktionsbefugnissen für die Verfolgung und Ahndung von Ordnungswidrigkeiten“ erhalten. Die dafür erforderliche Novellierung des Landesdatenschutzgesetzes solle rasch in Angriff genommen werden. Es wird jetzt auf die konkrete Ausgestaltung des Entwurfs ankommen. Im Extremfall könnte der Status einer obersten

Landesbehörde bedeuten, dass sich meine relativ kleine Dienststelle um wirklich alles selber kümmern und dafür Personalkapazitäten aufbringen muss, die für das „Kerngeschäft“, die eigentliche Beratungs- und Aufsichtstätigkeit, dann nicht zur Verfügung stehen. Ob dies Sinn macht, wird zu diskutieren sein. Mit der Beratung und Betreuung durch die Landtagsverwaltung (zum Beispiel in Haushalts- und Personalfragen) bin ich bis jetzt durchaus zufrieden. So wie in anderen Ländern wäre es daher auch denkbar, meiner Dienststelle zwar den Status einer obersten Landesbehörde zu verleihen, aber dennoch bestimmte Aufgaben von einer anderen Stelle wahrnehmen zu lassen. Eine (Rück-)Verlagerung der Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten würde meiner Behörde zwar mehr Durchschlagskraft verleihen, wäre aber ohne ausreichende Personalverstärkung nicht zu verantworten. Ohnehin bestünde aus meiner Sicht die wirksamste „Stärkung“ des unabhängigen Datenschutzes in einer Verstärkung der personellen Kapazitäten meiner Dienststelle.

– In der Koalitionsvereinbarung wird Datenschutz endlich als Bildungsaufgabe anerkannt. Diese Aussage ist sehr zu begrüßen, denn sie entspricht einer langjährigen Forderung der Datenschutzbeauftragten (vgl. hierzu auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011, „Datenschutz als Bildungsaufgabe“, Anhang 21). Damit wird dem Umstand Rechnung getragen, dass viele, nicht nur junge Menschen von der digitalen Welt zunehmend überfordert werden und teilweise den Überblick darüber verloren haben, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Daten verknüpft oder gegebenenfalls weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch sein informationelles Selbstbestimmungsrecht nicht ausüben. Ungeachtet der lobenswerten, aber mittlerweile in ihrer Vielfalt nahezu unübersehbaren Aktivitäten zahlreicher öffentlicher, gemeinnütziger und gewerblicher Einrichtungen, die Aufklärungsarbeit hinsichtlich der Internet-Nutzung betreiben, sollte das Augenmerk künftig stärker auf der Integration des Themas in die reguläre Bildungsarbeit liegen. Aus Sicht der Datenschutzbeauftragten sollte die Vermittlung von Datenschutzwissen als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert werden. Ebenso sollten Medien- und Datenschutzkompetenz zum verbindlichen Gegenstand der Lehreraus- und -fortbildung gemacht werden.

– Die Koalitionsvereinbarung spricht sich außerdem dafür aus, die behördlichen und betrieblichen Datenschutzbeauftragten als wichtiges Element der Eigenkontrolle zu stärken. Da die betrieblichen Datenschutzbeauftragten dem Bundesdatenschutzgesetz (BDSG) und damit nicht dem Gestaltungsspielraum des Landesgesetzgebers unterfallen, verstehe ich diese Zielsetzung so, dass im Land die bisher ins Belieben der Behörden gestellte Bestellung behördlicher Datenschutzbeauftragter einer gesetzlichen Verpflichtung hierzu weichen sollte. Es ist ja auch nicht einzusehen, warum der Gesetzgeber von Unternehmen etwas verlangen sollte, was er den Behörden freistellt. Bedenken kleiner Behörden ließen sich durch eine „Bagatellgrenze“ beziehungsweise durch eine entsprechende Betreuung durch die behördlichen Datenschutzbeauftragten übergeordneter Behörden nach § 10 Absatz 2 LDSG ausräumen.

Die Koalitionsvereinbarung enthält natürlich noch eine ganze Reihe weiterer politischer Absichtserklärungen, deren datenschutzrechtliche Relevanz nicht gleich auf den ersten Blick erkennbar ist. Immerhin leuchtet ein, dass die auf Seite 66 in Aussicht genommene „individualisierte anonymisierte Kennzeichnung der Polizei bei sog. Großlagen“ für die betroffenen Einsatzbeamten datenschutzrechtlich von Bedeutung sein kann, zumal das Recht auf informationelle Selbstbestimmung explizit angesprochen wird. Gemeint ist mit dem Vorschlag, der sicher

noch näher zu konkretisieren sein wird, dass Polizeibeamte in bestimmten Einsatzsituationen eine Art Kennzeichen (zum Beispiel eine Buchstaben-Zahlen-Kombination) auf ihrer Kleidung tragen sollen, um gegebenenfalls später leichter identifiziert werden zu können. Es handelt sich zwar nicht um eine echte Anonymisierung, aber ich halte das für einen datenschutzgerechten Kompromiss, um gerade bei Demonstrationen einerseits den Rechten von Versammlungsteilnehmern gerecht zu werden und andererseits den Schutz von Polizeibeamten oder deren Familienangehörigen vor Vergeltungsangriffen und Aggressionen zu gewährleisten. Im demokratischen Rechtsstaat sollte die Polizei nichts zu verbergen haben. Von manchen Politikern, aber auch von Gewerkschaftsseite wird zwar immer wieder der Eindruck erweckt, dass die Kennzeichnung eine Art kollektives Misstrauensvotum gegenüber der Polizei darstellen könnte, ich halte diese nachvollziehbaren Einwände aber für überwindbar, wenn Sinn und Zweck der Maßnahme hinreichend verdeutlicht werden. Dabei gehe ich davon aus, dass nicht pauschales Misstrauen gegenüber Polizeivollzugsbeamten den Hintergrund des Vorschlags gebildet hat, sondern die verfassungsrechtlichen Grundsätze der Transparenz und der Überprüfbarkeit staatlichen Handelns im demokratischen Rechtsstaat. Sofern es zur Umsetzung kommt, bin ich gerne bereit, bei der weiteren Konzeption des Verfahrens beratend zur Seite zu stehen.

2. Entwicklung des Datenschutzrechts 2010/2011

2.1 Die Neuregelung der Videoüberwachung durch öffentliche Stellen in § 20 a LDSG

Bereits im 29. Tätigkeitsbericht (LT-Drucksache 14/5500; 1. Teil, Nr. 4) hatte ich auf den Beschluss des Bundesverfassungsgerichts vom 23. Februar 2007 (1 BvR 2368/06) hingewiesen, wonach eine Videoüberwachung durch öffentliche Stellen einer speziellen und eindeutigen Rechtsgrundlage bedarf. Damit war der bisherigen Praxis, eine Überwachungsmaßnahme auf die allgemeinen Vorschriften der §§ 13 ff. LDSG zu stützen, die Grundlage entzogen. Bereits unter meinem Vorgänger wurde stets die Auffassung vertreten, dass Videoüberwachungsmaßnahmen in schwerwiegender Weise in das Recht auf informationelle Selbstbestimmung der Betroffenen eingreifen und nur unter engen Voraussetzungen überhaupt zulässig sein können. Mit dem Gesetz zur Änderung des Landesdatenschutzgesetzes und anderer Rechtsvorschriften vom 7. Februar 2011 (GBl. S. 43) wurde nunmehr die Vorschrift des § 20 a LDSG eingeführt, die am 1. April 2011 in Kraft getreten ist. Die Neuregelung formuliert strenge Anforderungen an eine Videoüberwachung durch öffentliche Stellen. Auch wenn die Schaffung einer expliziten Rechtsgrundlage grundsätzlich zu begrüßen ist, kann ich mit der Norm nicht gänzlich zufrieden sein.

Im Rahmen des Gesetzgebungsverfahrens waren von meiner Seite einige Bedenken geäußert worden (vgl. LT-Drucksache 14/7482), die jedoch bedauerlicherweise keinen Eingang in das Gesetz gefunden haben:

So wird in der Gesetzesbegründung (LT-Drucksache 14/7313, S. 17) etwa ausgeführt, dass das Aufstellen einer Kameraattrappe nicht unter § 20 a LDSG falle, da es sowohl am Tatbestandsmerkmal der Beobachtung als auch an einer optisch-elektronischen Einrichtung fehle. Dieser Einschätzung soll nicht widersprochen werden, unklar bleiben jedoch die Konsequenzen, die sich hieraus ergeben. In der aufsichtlichen Praxis erfahre ich immer wieder von Fällen, in denen öffentliche Stellen den Einsatz von Kameraattrappen erwägen. Im Lichte des Volkszählungsurteils (BVerfGE 65, 1 ff.) dürfte es sich auch beim Einsatz einer Kameraattrappe wegen des damit verbundenen psychischen Überwachungsdrucks um einen Grundrechtseingriff handeln, der einer gesetzlichen Grundlage bedarf. Aus meiner Sicht ist der Gesetzgeber nicht daran gehindert, diese im Landesdatenschutzgesetz zu schaffen. Mit der neuen Vorschrift des § 20 a LDSG wurde es versäumt, eine Einrichtung,

von der lediglich der Anschein einer Videobeobachtung ausgeht, ebenfalls den Voraussetzungen des § 20 a Absätze 1 und 2 LDSG zu unterwerfen. Man hätte sich hier ein Beispiel an der von der Bundesregierung geplanten gesetzlichen Regelung des Beschäftigtendatenschutzes (vgl. § 32 f Absatz 1 Satz 4 BDSG-E, BT-Drucksache 17/4230), aber auch an den Landesdatenschutzgesetzen anderer Länder (vgl. zum Beispiel § 30 Absatz 9 HmbDSG, § 34 Absatz 6 LDSG RP) nehmen können.

Nach § 20 a Absatz 1 Satz 2 Nummer 2 LDSG ist die Videobeobachtung nur zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In der Einzelbegründung hierzu (LT-Drucksache 14/7313, S. 19) ist zu lesen, dass „etwa die Videoüberwachung besonders sensibler Örtlichkeiten (zum Beispiel von Toiletten und Umkleidekabinen) regelmäßig nicht zulässig sein“ wird. Diesbezüglich hätte ich mir aufgrund des schwerwiegenden Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen die Klarstellung gewünscht, dass eine Videoüberwachung in diesen Bereichen ausnahmslos unzulässig ist. Ferner hätte ich eine Ergänzung des Klammerzusatzes zur Umschreibung „sensibler Örtlichkeiten“ um weitere Räume, wie Ruheräume, befürwortet. Selbst wenn Fallkonstellationen denkbar sind, in denen eine Videoüberwachung als ultima ratio in Betracht kommt, hätte in der Gesetzesbegründung eine konkrete Darstellung erfolgen sollen, an welche Ausnahmefälle gedacht wurde.

Bedenken bestehen meines Erachtens auch hinsichtlich der Kennzeichnungspflicht. Nach § 20 a Absatz 2 LDSG sind die Videobeobachtung und die verantwortliche Stelle „durch geeignete Maßnahmen erkennbar“ zu machen. Eine Kennzeichnungspflicht soll ausweislich der Gesetzesbegründung (LT-Drucksache 14/7313, S. 19) jedoch nicht bestehen, wenn „die Kameras für jedermann sichtbar angebracht sind und nicht nur die Tatsache der Überwachung, sondern auch die dafür verantwortliche Stelle offenkundig ist“. Diese Ausnahmeregelung dürfte unpraktikabel sein und in der Kontrollpraxis zu erheblichen Meinungsverschiedenheiten mit den kontrollierten Stellen führen. Die Kennzeichnungspflicht sollte daher aus den nachstehenden Erwägungen ausnahmslos gelten: Zum einen muss die „Sichtbarkeit“ der Kamera gegeben sein, bevor der Betroffene in den „Erfassungsbereich“ der Kamera gerät. Es kann den Bürgerinnen und Bürgern aber nicht zugemutet werden, ihre Umgebung ständig daraufhin zu überprüfen, ob eine Videokamera sichtbar wird, die – zum Beispiel an einem öffentlichen Gebäude – einer bestimmten verantwortlichen Stelle ohne Weiteres zugeordnet werden kann und nach allgemeiner Lebenserfahrung der Überwachung dienen dürfte. Zum andern weiß ich nicht, wann für einen Betroffenen die Tatsache der Überwachung „offenkundig“ sein soll. Jemand, der eine Videokamera erblickt, kann nicht feststellen, ob sie überhaupt funktionsfähig ist, in welcher Auflösung und in welchem Bildausschnitt die Aufnahmen erfolgen und welchen Zwecken die Kamera dient, ob sie etwa mit Hilfe von Übersichtsbildern nur Verkehrsströme erfassen und der Ampelsteuerung dienen soll oder ob sie auch in der Lage ist, die Gesichter von Passanten zu erkennen, ob sie eine Zoom- und Schwenkfunktion hat, ob jemand an dem Überwachungsmonitor sitzt, auf den die Bilder übertragen werden, und ob eine Aufzeichnung erfolgt. All dies ist für den Betroffenen, der eine Videokamera erblickt, nicht zu beurteilen und für ihn schon gar nicht „offenkundig“. Aus diesem Grund sollte bei Videobeobachtungsmaßnahmen ausnahmslos eine Kennzeichnung erfolgen, damit die Betroffenen ihr Verhalten gegebenenfalls danach ausrichten und dem Erfassungsbereich einer Videokamera ausweichen können.

Leider blieb auch meine Kritik daran unberücksichtigt, dass nach § 20 a Absatz 3 Satz 2 LDSG eine Zweckänderung der erhobenen und gespeicherten Daten nicht nur zulässig ist, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder für die Verfolgung von Straftaten erforderlich ist, sondern auch zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung. Die Voraussetzungen der

Zweckänderung hätten entsprechend der Regelung in § 6 b Absatz 3 Satz 2 BDSG auf die Abwehr von Gefahren für die öffentliche Sicherheit und die Verfolgung von Straftaten beschränkt werden sollen. Ferner halte ich die in § 20 a Absatz 5 LDSG normierte maximale Speicherdauer von vier Wochen für zu lang. Eine Speicherdauer von maximal zwei Wochen erscheint ausreichend.

Nach § 20 a Absatz 6 Satz 1 LDSG bedarf der erstmalige Einsatz optisch-elektronischer Einrichtungen der vorherigen schriftlichen Freigabe durch die verantwortliche Stelle. Meiner Auffassung nach hätte die Gesetzesbegründung klarstellen sollen, dass es für bereits vor Inkrafttreten der Regelung des § 20 a LDSG (möglicherweise rechtswidrig) in Betrieb genommene Videoüberwachungseinrichtungen keinen „Bestandsschutz“ geben kann. Eine schriftliche Freigabe mit den im Gesetz genannten inhaltlichen Anforderungen ist auch für „Altanlagen“ zu fordern, zumal der oben genannte Beschluss des Bundesverfassungsgerichts bei Inkrafttreten des Änderungsgesetzes des Landesdatenschutzgesetzes bereits über vier Jahre zurücklag. Außerdem wäre klarzustellen gewesen, dass von der verantwortlichen Stelle regelmäßig zu überprüfen ist, ob die für die Freigabe erforderlichen Voraussetzungen noch gegeben sind. Dies wäre zwar de lege lata ohnehin geboten, findet aber in der Praxis nicht immer die gewünschte Beachtung. Um die dauerhafte Verfestigung einmal freigegebener Maßnahmen zu verhindern, wäre es zudem empfehlenswert gewesen, die Freigabe zeitlich zu befristen beziehungsweise regelmäßig zu erneuern.

Videoüberwachungsmaßnahmen durch öffentliche Stellen bedeuten einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen und erfordern eine sorgfältige Prüfung der differenzierten Kriterien. Dieses Erfordernis hat auch der Gesetzgeber gesehen und die verantwortlichen Stellen in § 20 a Absatz 6 LDSG zu der bereits genannten schriftlichen Freigabe verpflichtet. Gemäß § 20 a Absatz 6 Satz 3 LDSG ist der Entwurf der schriftlichen Freigabe dem behördlichen Datenschutzbeauftragten zur Prüfung vorzulegen, sofern ein solcher bestellt ist. Diesem ist nach der Gesetzesbegründung (LT-Drucksache 14/7313, S. 21) für seine Prüfung ausreichend Zeit einzuräumen. Eine Videoüberwachungsmaßnahme ist damit auch nach Ansicht des Gesetzgebers datenschutzrechtlich nicht einfach zu beurteilen. Ich halte es daher für geboten, öffentliche Stellen, die Videoüberwachungsmaßnahmen durchführen wollen, zur Bestellung eines behördlichen Datenschutzbeauftragten zu verpflichten. Sofern diese Stellen über keinen Datenschutzbeauftragten verfügen, dürfen sie optisch-elektronische Einrichtungen für Zwecke der Videoüberwachung erst dann einsetzen, wenn ein behördlicher Datenschutzbeauftragter bestellt ist und dieser die datenschutzrechtliche Zulässigkeit der Maßnahme geprüft hat. Ungeachtet der Tatsache, dass ich die Einführung einer generellen Verpflichtung zur Bestellung behördlicher Datenschutzbeauftragter – wie in anderen Ländern längst eingeführt – für überfällig halte, wäre zumindest im Zusammenhang mit der Planung des Einsatzes von Videoüberwachungstechnik eine Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten angezeigt gewesen.

Alles in allem hat die neue Vorschrift des § 20 a LDSG und ihre Konkretisierung in der Gesetzesbegründung einige Schwachstellen. Umso enttäuschender, dass meine im Gesetzgebungsverfahren geäußerten Bedenken vom Gesetzgeber nicht aufgegriffen wurden. Es bleibt zu hoffen, dass die Zusage im Koalitionsvertrag der neuen Landesregierung, bei der Neuregelung der Videoüberwachung „insbesondere die Forderungen des Landesdatenschutzbeauftragten um[zu]setzen“ (S. 67) eingelöst wird. Abzuwarten bleibt, wie sich die Anwendung des Gesetzes in der Praxis darstellt. Die ersten Monate nach dem Inkrafttreten der neuen Vorschrift deuten darauf hin, dass sich meine Sorge, § 20 a LDSG könnte eine erhebliche Ausweitung der Videoüberwachung durch öffentliche Stellen zur Folge haben, bestätigt.

2.2 Ein modernes Datenschutzrecht für das 21. Jahrhundert

Mit der überfälligen grundlegenden Modernisierung des deutschen Datenschutzrechts ist in dieser Legislaturperiode kaum noch zu rechnen.

Eine grundlegende Modernisierung des deutschen Datenschutzrechts ist überfällig. Schon im Jahre 2001 hatten die Professoren Roßnagel, Garstka und Pfitzmann im Auftrag des Bundesinnenministeriums ein Gutachten zum Modernisierungsbedarf erarbeitet, das in der Folgezeit aber nur punktuell umgesetzt wurde. Um die Diskussion über die notwendige Reform erneut zu beleben, haben die Datenschutzbeauftragten des Bundes und der Länder unter der Überschrift „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ im Jahr 2010 Eckpunkte vorgelegt und hierzu am 4. Oktober 2010 ein Symposium im Berliner Abgeordnetenhaus durchgeführt[2]. Das Eckpunktepapier kann von meiner Homepage heruntergeladen werden. Die wesentlichen Forderungen seien hier zusammengefasst:

Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die für konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen

[2] Der Verlauf der Veranstaltung wird ausführlich im 23. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Kap. 1.4, dargestellt. (vgl. http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.pdf?__blob=publicationFile). Im Anhang des Berichts ist auch das Eckpunktepapier abgedruckt.

zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Hierfür sollten für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa ein pauschalierter Schadensersatzanspruch, eingeführt werden. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

Trotz des Reformstaus ist mit einer umfassenden Modernisierung des deutschen Datenschutzrechts wie schon vor zehn Jahren meines Erachtens in nächster Zeit nicht zu rechnen. Vielmehr scheint die Bundespolitik – ebenfalls wie vor zehn Jahren – erneut auf Europa warten zu wollen. Diesmal sind es die Vorschläge der Europäischen Kommission für ein Gesamtkonzept für den Datenschutz in der Europäischen Union[3] vom November 2010, die einer Generalrevision des deutschen Datenschutzrechts offenbar im Wege stehen (siehe 1. Teil, 2. Abschnitt, Kapitel 4).

2.3 Aktivitäten auf Bundesebene im Berichtszeitraum

2.3.1 Neue Regelungen zur Informationspflicht bei Datenschutzverstößen

Die Regelungen zur Informationspflicht von unrechtmäßiger Kenntniserlangung personenbezogener Daten haben sich bewährt. Die Publizitätspflicht motiviert die verantwortlichen Stellen, mehr für den Datenschutz und die Datensicherheit zu tun und versetzt den Betroffenen zugleich in die Lage, negative Konsequenzen rechtzeitig abzuwenden und Sicherheitsmaßnahmen zu ergreifen.

[3] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Gesamtkonzept für den Datenschutz in der Europäischen Union [KOM(2010)0609].

Im 29. Tätigkeitsbericht (LT-Drucksache 14/5500) und insbesondere im Fünften Tätigkeitsbericht der Aufsichtsbehörde im Innenministerium wurde 2009 ausführlich über die drei Novellen berichtet, durch die das Bundesdatenschutzgesetz seinerzeit geändert wurde; insoweit kann ich auf die damalige Berichterstattung verweisen. An anderer Stelle in diesem Bericht wird auf die inzwischen gewonnenen Erfahrungen in Teilbereichen (vgl. etwa zur Werbung 7. Teil, 2. Abschnitt Nr. 1) und die nach wie vor vorhandenen Defizite (insbesondere hinsichtlich des Themas Arbeitnehmerdatenschutz, vgl. das folgende Kapitel) eingegangen. Im Folgenden möchte ich auf eine zunächst eher kritisch bewertete Neuerung eingehen, die sich bislang bewährt hat.

Seit dem 1. September 2009 müssen gemäß § 42 a BDSG nichtöffentliche Stellen und ihnen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen gravierende Datenschutzpannen der zuständigen Aufsichtsbehörde anzeigen sowie die Betroffenen informieren und ihnen Handlungsempfehlungen unterbreiten. Anzeigepflichtige Datenschutzverstöße liegen vor, wenn sensible personenbezogene Daten unrechtmäßig in die Hände Dritter gelangt sind und schwerwiegende Beeinträchtigungen für die Betroffenen drohen.

Im August 2010 erfolgte eine Anpassung des Sozialdatenschutzes an das Bundesdatenschutzgesetz. Die Regelung des § 83 a des Zehnten Buchs des Sozialgesetzbuchs (SGB X) verpflichtet die dem Sozialgeheimnis unterliegenden Stellen, im Fall der unrechtmäßigen Kenntniserlangung von Sozialdaten unverzüglich die Aufsichtsbehörde nach § 90 des Vierten Buchs des Sozialgesetzbuchs (SGB IV), die zuständige Datenschutzaufsichtsbehörde und den oder die Betroffenen zu informieren. Im Hinblick auf die Art der Benachrichtigung verweist die Norm auf § 42 a BDSG.

Um den betroffenen Behörden eine Hilfestellung bei der Anwendung dieser Vorschriften zu geben, hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu § 42 a BDSG FAQ (Häufig gestellte Fragen mit Antworten) erstellt *(http://www.datenschutz-berlin.de/attachments/809/535.4.7.pdf?1311923219)*. Die FAQ sollen die betroffenen Stellen dabei unterstützen, mitteilungspflichtige Sachverhalte zu erkennen und die entstehenden Handlungspflichten umzusetzen. Ich kann den Verantwortlichen nur empfehlen, diese wertvollen Hinweise zu Rate zu ziehen.

Meiner Behörde wurden bislang insgesamt rund 50 Datenschutzverstöße gemeldet. Überwiegend hat es sich dabei um den Verlust von Speichermedien (zum Beispiel Notebooks, Rechner, USB-Sticks), um Fehler beim Versand von E-Mail und Fax oder die Kompromittierung von Webseiten gehandelt. Häufig war auch meine Beratung gefragt, ob es sich im konkreten Einzelfall überhaupt um einen meldepflichtigen Vorgang handelt. Aber selbst wenn dies nicht der Fall war, so boten auch diese Anfragen eine gute Gelegenheit, mit den betroffenen Unternehmen über den datenschutzrechtlichen Optimierungsbedarf ins Gespräch zu kommen. Auf diese Weise kann die Anzeigepflicht nebenbei dazu beitragen, die Hemmschwellen vor einem Kontakt mit der Aufsichtsbehörde abzusenken.

Wenngleich die Zahl der gemeldeten Fälle belegt, dass die verantwortlichen Stellen die Informationspflicht durchaus ernst nehmen, gehe ich davon aus, dass eine Vielzahl von Datenschutzverstößen nach wie vor nicht gemeldet wird. Betroffene Stellen sollten sich darüber im Klaren sein, dass bei nicht angezeigten Datenpannen ein Bußgeld von bis zu 300.000 Euro oder mehr droht. Auch insofern gilt, dass die Vermeidung von Datenschutzpannen im Vorfeld – etwa durch ein klares Datenschutzmanagement im Unternehmen – allemal besser ist als die vom Gesetzgeber nun verordnete Pflicht zur Unterrichtung, wenn das Kind bereits in den Brunnen gefallen ist.

2.3.2 Die gesetzliche Neuregelung des Beschäftigtendatenschutzes ist überfällig

Nachdem in mehreren spektakulären Datenschutzskandalen in den Jahren 2006, 2007 und 2008 die rechtswidrige Verarbeitung von Beschäftigtendaten durch Arbeitgeber bekannt geworden war, sagte die Bundesregierung im Frühjahr 2009 eine gesetzliche Neuregelung des Arbeitnehmerdatenschutzrechts zu und nahm die Umsetzung einer von den Datenschutzbeauftragten des Bundes und der Länder bereits seit längerer Zeit erhobenen Forderung in Angriff. Die Datenschutzkonferenz hat seinerzeit entsprechende Eckpunkte einer Neuregelung aufgezeigt (vgl. 29. Tätigkeitsbericht 2009, LT-Drucksache 14/5500, Anhang 19). In einem ersten Schritt fügte der Gesetzgeber mit § 32 BDSG eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten in das Bundesdatenschutzgesetz ein. Die Vorschrift trat mit der BDSG-Novelle II zum 1. September 2009 in Kraft und konnte wegen ihrer Kürze und Allgemeinheit den Beschäftigtendatenschutz nicht umfassend regeln und eine detaillierte gesetzliche Neuregelung daher nicht entbehrlich machen.

Noch vor der Bundestagswahl 2009 veröffentlichte das Bundesministerium für Arbeit und Soziales (BMAS) den Entwurf eines Beschäftigtendatenschutzgesetzes. Diesen brachte die SPD-Fraktion nach der Bundestagswahl unverändert in den Deutschen Bundestag ein (BT-Drucksache 17/69). Während dieser Entwurf die Materie des Beschäftigtendatenschutzes in einem eigenständigen Beschäftigtendatenschutzgesetz regelt, beschlossen die Regierungsparteien der 17. Legislaturperiode in ihrer Koalitionsvereinbarung vom 26. Oktober 2009, die erforderlichen Neuregelungen zum Arbeitnehmerdatenschutz in das Bundesdatenschutzgesetz aufzunehmen.

Ende März 2010 legte das Bundesministerium des Innern einen Referentenentwurf vor, den die Konferenz der Datenschutzbeauftragten des Bundes und der Länder inhaltlich in vielen Punkten als unzureichend kritisierte (Entschließung vom 22. Juni 2010, Anhang 6). Nachdem Ressortabstimmungen zu einer Überarbeitung in einzelnen Punkten geführt hatten, beschloss die Bundesregierung am 25. August 2010 den überarbeiteten Referentenentwurf als Gesetzesentwurf (vgl. BR-Drucksache 535/10). Der Bundesrat hat dazu im Rahmen seiner Stellungnahme zahlreiche Ergänzungs- und Änderungsvorschläge vorgebracht (BT-Drucksache 17/4230, Anlage 3, S. 26 bis 37), die von der Bundesregierung allerdings nur teilweise zustimmend aufgegriffen wurden (vgl. BT-Drucksache 17/4230, Anlage 4, S. 38 bis 43).

Zu Beginn des Jahres 2011 legte schließlich die Fraktion Bündnis 90/Die Grünen einen eigenen Entwurf zur Regelung des Beschäftigtendatenschutzes vor (BT-Drucksache 17/4853). Dieser Entwurf sieht ebenso wie der Entwurf der SPD die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes vor.

Der Entwurf der Bundesregierung wurde vom Bundestag am 25. Februar 2011 in erster Lesung beraten (BT-Plenarprotokoll 17/94, S. 10735A – 10745A). Im Anschluss daran wurde der Gesetzesentwurf zur weiteren Beratung an die Ausschüsse unter Federführung des Innenausschusses verwiesen. Der Innenausschuss führte am 23. Mai 2011 eine öffentliche Anhörung durch (BT-Protokoll Nr. 17/40). Dabei wurde deutlich, dass die Ansichten der Sachverständigen und Fraktionen bei mehreren bedeutsamen Themenkomplexen noch weit auseinander liegen. Nach der Sommerpause haben die Ausschüsse des Bundestags die Beratungen zum Beschäftigtendatenschutz wieder aufgenommen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich inzwischen ebenfalls mit den vorgelegten Gesetzentwürfen beschäftigt und hierbei konkrete Vorschläge für alternative oder zusätzliche Regelungen gemacht (Entschließung vom 16./17. März 2011, Anhang 14).

Bei der öffentlichen Anhörung am 23. Mai 2011 haben sich besonders folgende Punkte als weiterhin diskussionswürdig und -bedürftig erwiesen:

– Unterschreitung des gesetzlichen Datenschutzniveaus durch betriebliche Vereinbarungen oder Einwilligungen

  Der Gesetzentwurf der Bundesregierung sieht vor, dass Betriebs- und Dienstvereinbarungen nicht zu Ungunsten der Beschäftigten von den gesetzlichen Vorgaben im Beschäftigtendatenschutz abweichen dürfen. Außerdem soll eine Verarbeitung von Arbeitnehmerdaten auf der Grundlage individueller Einwilligungen nur in vom Gesetz ausdrücklich vorgesehenen Fällen zulässig sein. Zwischen Arbeitgeber- und Arbeitnehmerseite ist umstritten, ob durch diese Regelungen angemessene betriebsindividuelle Lösungen nicht unzumutbar erschwert werden. Hierbei ist zu bedenken, dass die im Datenschutzrecht häufig vorkommenden unbestimmten Rechtsbegriffe wie beispielsweise der Begriff der „Erforderlichkeit“ Auslegungs-, Interpretations- und Wertungsspielräume eröffnen und Raum für eine Präzisierung der gesetzlichen Regelungen auf betrieblicher Ebene lassen. Die Beschränkung der Einwilligung von Arbeitnehmern als Rechtfertigungsgrund für eine Datenverarbeitung soll dem Umstand Rechnung tragen, dass im Verhältnis zwischen Arbeitgebern und Arbeitnehmern keine volle „Waffengleichheit“ besteht, sondern der Arbeitnehmer sich in der Regel von vornherein in der schwächeren Position befindet. Neben den im Gesetzentwurf für Einwilligungen vorgesehenen Fällen sind allerdings noch weitere Konstellationen denkbar, in denen die Einwilligung des Arbeitnehmers trotz seiner schwächeren Verhandlungsposition auf seiner freien Entscheidung beruhen und damit freiwillig sein kann. Es erscheint daher durchaus überlegenswert, über eine Erweiterung der Einwilligungsfälle (Positivliste) nachzudenken.

– Videoüberwachung

  Die vorgesehene Erlaubnis zur offenen Videobeobachtung begegnet insoweit Bedenken, als eine Videobeobachtung nichtöffentlich zugänglicher Betriebsstätten zu dem relativ unbestimmten Zweck der Qualitätskontrolle zulässig sein soll. Einmal installiert, können solche Anlagen leicht auch zur Verhaltens- und Leistungskontrolle der Arbeitnehmer genutzt werden. Auf der anderen Seite erscheint es nicht ausgemacht, dass das vom Gesetzentwurf vorgesehene ausnahmslose Verbot der heimlichen Videoüberwachung den betrieblichen Erfordernissen und den berechtigten Interessen der Arbeitnehmer tatsächlich in vollem Umfang Rechnung trägt. Immerhin ist bislang nach der Rechtsprechung des Bundesarbeitsgerichts in eng begrenzten Ausnahmefällen eine heimliche Videobeobachtung zulässig, auch wenn sich die Frage stellt, ob damit nicht die originär staatlichen Aufgaben der präventiven und repressiven Verbrechensbekämpfung partiell „privatisiert“ wurden.

– Recht der Arbeitnehmer zur Anrufung der Datenschutzaufsichtsbehörde

  Die vom Gesetzentwurf vorgesehene Beschränkung des Rechts der Arbeitnehmer zur Anrufung der Datenschutzaufsichtsbehörde – Voraussetzung hierfür ist, dass der Arbeitnehmer sich zuvor erfolglos an seinen Arbeitgeber gewandt hat – ist aus datenschutzrechtlicher Sicht nicht hinnehmbar und im Übrigen europarechtswidrig. Die europäische Datenschutzrichtlinie sieht ein individuelles Recht jedes Betroffenen zur direkten Anrufung der jeweils zuständigen Aufsichtsbehörde vor.

– Konzernweiter Datentransfer

Anders als die Gesetzentwürfe der Fraktion Bündnis 90/ Die Grünen und der Fraktion der SPD sieht der Gesetzentwurf der Bundesregierung keine Erleichterungen für den konzernweiten Transfer von Beschäftigtendaten vor. Ob die vorhandenen und derzeit in der Praxis genutzten Instrumente (insbesondere die Auftragsdatenverarbeitung) insoweit praktikabel sind und den betrieblichen Erfordernissen ausreichend Rechnung tragen, ist zwischen Arbeitnehmern und Arbeitgebern umstritten. Die geringeren Rechtsschutzmöglichkeiten der Betroffenen im EU-Ausland sprechen gegen eine zu weitgehende Privilegierung eines konzernweiten Datentransfers ins Ausland. Bei dieser Frage geht es allerdings nicht nur um Beschäftigtendaten. Auch Kunden-, Abnehmer- und Lieferantendaten können hiervon betroffen sein, sodass es sich nicht um eine originäre Frage des Beschäftigtendatenschutzes, sondern um eine allgemeine datenschutzrechtliche Frage handelt, die im allgemeinen Datenschutzrecht ihren Platz hat und auch dort geregelt werden sollte.

– Erhebung von Bewerber- und Beschäftigtendaten im Internet

Der Gesetzentwurf gestattet Arbeitgebern, Bewerberdaten aus sozialen Netzwerken, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind (zum Beispiel XING), zu erheben. Eine Erhebung von Daten aus sonstigen sozialen Netzwerken wie etwa Facebook soll dagegen ausgeschlossen sein. Kontrollieren lässt sich die Einhaltung eines solchen Verbots in der Praxis kaum. Sinnvoll erscheint das Verbot daher nur zusammen mit entsprechenden Informationsverwertungsverboten.

– Automatisierter Datenabgleich zur Aufdeckung von Straftaten und anderen schwerwiegenden Pflichtverletzungen durch Beschäftigte im Beschäftigungsverhältnis

Der Entwurf sieht einen automatisierten Abgleich von zu anderen Zwecken erhobenen Beschäftigtendaten vor, um Straftaten und andere schwerwiegende Pflichtverletzungen durch Beschäftigte aufzudecken. In der Praxis wird die Sicherstellung einer umfassenden Regelkonformität im Unternehmen (nicht nur mit Hilfe von Datenabgleichen) häufig mit dem Begriff „Compliance“ bezeichnet. Nach dem Gesetzentwurf soll ein solcher Abgleich auf einer ersten Stufe in anonymisierter und pseudonymisierter Form möglich sein, ohne dass Anhaltspunkte für ein Fehlverhalten einzelner Mitarbeiter vorliegen müssten. Der Gesetzentwurf schreibt dem Arbeitgeber zwar vor, die „näheren Umstände“, die ihn zu einem solchen Abgleich veranlassen, zu dokumentieren. Nähere Anforderungen an diese Umstände und insbesondere an den daraus abzuleitenden Verdachtsgrad sieht der Gesetzentwurf jedoch nicht vor. Soweit hierbei Beschäftigtendaten nicht nur in anonymisierter, sondern in pseudonymisierter und damit in personenbeziehbarer Form Verwendung finden, geht die Neuregelung über das, was nach geltendem Recht zulässig ist, hinaus. Hier scheint es erwägenswert, zunächst immer einen Abgleich in anonymisierter Form vorzuschreiben. Aus einem solchen Abgleich, der für sich genommen nicht dem Anwendungsbereich des Bundesdatenschutzgesetzes unterfiele, weil keine personenbezogenen oder -beziehbaren Daten verwendet werden, können sich dann konkrete Anhaltspunkte für ein Fehlverhalten seitens einzelner – namentlich nicht bekannter – Mitarbeiter ergeben, aufgrund derer dann ein Abgleich mit den Mitarbeiterdaten in personalisierbarer Form verhältnismäßig sein kann. Jede Verwendung von Mitarbeiterdaten durch den Arbeitgeber steht unter dem Vorbehalt der Verhältnismäßigkeit. Für Zwecke der Revision

und herkömmliche Geschäftsprüfungen können unter Umständen bereits sichtprobenweise Überprüfungen und Prüfungsmaßnahmen in besonders fehleranfälligen Bereichen ausreichen. Das Gesetz sollte daher zumindest eine entsprechende Einschränkung der Befugnis von Arbeitgebern zur Durchführung von Datenabgleichen vorsehen.

– Kontrolle der Nutzung von Telekommunikationsdiensten durch Beschäftigte

Der Gesetzentwurf klammert die private Nutzung von Telekommunikationsdiensten am Arbeitsplatz und die Folgen, die sich daraus für die Befugnis des Arbeitgebers zur Kontrolle seiner Beschäftigten und zum Zugriff auf die Daten und Inhalte der Kommunikation ergeben, aus. Insoweit besteht ein akuter Regelungsbedarf. Den Aufsichtbehörden und der Rechtsprechung ist es bislang beispielsweise nicht gelungen, eine einheitliche Antwort auf die Frage zu finden, ob und unter welchen Voraussetzungen Arbeitgeber auf empfangene oder versandte E-Mails ihrer Mitarbeiter zugreifen dürfen, wenn sie die private Nutzung des Internets ausdrücklich gestattet oder zumindest geduldet haben. Bereits die Frage, ob ein Arbeitgeber, der seinen Mitarbeitern die private Nutzung dienstlicher Telekommunikationsanlagen gestattet oder diese duldet, Diensteanbieter im Sinne von § 3 Nummern 6 und 10 des Telekommunikationsgesetzes (TKG) und daher dem Fernmeldegeheimnis unterworfen ist, wird in Rechtsprechung und Literatur nicht einheitlich beantwortet. Angesichts der erheblichen praktischen Bedeutung dieser Frage und der gegenwärtigen Rechtsunsicherheit erscheint eine gesetzliche Regelung dringend angezeigt.

Auf der Homepage des Deutschen Bundestags *(www.bundestag.de)* findet man unter dem Stichwort „Öffentliche Anhörung des Innenausschusses am 23. Mai 2011“ den weiterhin aktuellen Diskussionsstand mit den divergierenden Standpunkten der Verbandsvertreter beziehungsweise der Sachverständigen. Ob in absehbarer Zeit noch ein Kompromiss zustande kommt, erscheint mir mittlerweile mehr als fraglich, denn seit der Anhörung ist – zumindest nach außen – kein Verfahrensfortschritt zu erkennen.

2.3.3 Bis hierher und nicht weiter: Rote Linien im Internet

Das Bundesministerium des Innern hat einen Gesetzentwurf zur Festlegung einer „roten Linie“ zum Schutz des Persönlichkeitsrechts im Internet angekündigt. Ob ein solches Vorhaben geeignet ist, den Einzelnen effektiv vor beeinträchtigenden Online-Veröffentlichungen zu schützen, ist bislang ungewiss.

Es war nicht zuletzt die Diskussion um die Zulässigkeit öffentlich zugänglicher Panoramaansichten im Internet, die die Bundesregierung zu dem Versuch veranlasste, das Persönlichkeitsrecht des Einzelnen wirksam gegen beeinträchtigende Online-Veröffentlichungen zu schützen: Das Bundesministerium des Innern veröffentlichte am 1. Dezember 2010 ein Eckpunktepapier zum Datenschutz im Internet und kündigte darin einen Gesetzentwurf zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht an. Das Gesetz solle eine „rote Linie“ festlegen, die durch Publikationen im Internet nicht überschritten werden darf.

Der Gesetzentwurf ist zwar – möglicherweise aufgrund des Wechsels an der Spitze des Bundesinnenministeriums – bislang noch nicht erschienen. Das Eckpunktepapier nennt jedoch einige Grundpfeiler des Vorhabens. So soll insbesondere vermieden werden, durch den Erlass von Einzelfallgesetzen ein lückenhaftes und daher stets in hohem Maß aktualisierungsbedürftiges Regelungsgefüge zu etablieren. Vielmehr soll der Gesetzentwurf, anders als zum Beispiel der Datenschutz-Kodex des IT-Branchen-

verbands BITKOM (siehe hierzu 1. Teil Nr. 4.2), nicht nur für die Veröffentlichung von Geodaten, sondern für jede Art personenbezogener Daten in Telemedien gelten. Er soll Vorgaben sowohl für öffentliche als auch für nicht-öffentliche Stellen enthalten. Kern des Gesetzesvorhabens soll sein, solche Veröffentlichungen im Grundsatz zu verbieten, die einen besonders schweren Eingriff in das Persönlichkeitsrecht des Betroffenen darstellen. Auch beeinträchtigende Veröffentlichungen sollen nur aufgrund einer Abwägung der Interessen des Betroffenen mit den Grundrechten der Meinungs- und Berufsfreiheit der Diensteanbieter zulässig sein. Unzulässig sollen jedenfalls ehrverletzende Veröffentlichungen sein beziehungsweise solche, durch die sich ein umfangreiches Persönlichkeits- und Bewegungsprofil des Betroffenen ergeben kann. Die Schwelle für einen besonders schweren Eingriff in das Persönlichkeitsrecht soll nach den Angaben des Ministeriums hoch angesetzt werden. Dies sei dem Umstand geschuldet, dass das Internet als öffentlicher Raum grundsätzlich frei von staatlichen Restriktionen bleiben soll. Um dennoch einen umfassenden Schutz zu realisieren, setzt das Bundesministerium des Innern auf Selbstverpflichtungen der Telemedienanbieter. Das Eckpunktepapier stellt weiterhin in Aussicht, dass der Gesetzentwurf Regelungen für Gesichtserkennungsdienste, Profilbildungen anhand von Suchmaschinenanfragen sowie für die Erhebung von Standortdaten im Rahmen der Nutzung von Smartphones enthalten werde.

Der Versuch, das Persönlichkeitsrecht des Einzelnen vor beeinträchtigenden Online-Veröffentlichungen zu schützen, ist aus meiner Sicht zwar grundsätzlich zu begrüßen. Doch ist der im Eckpunktepapier des Bundesministeriums gewählte Regelungsansatz datenschutzrechtlich kontraproduktiv. Das geltende Datenschutzrecht beruht auf dem Grundsatz des Verbots mit Erlaubnisvorbehalt und geht damit davon aus, das jeder Umgang mit personenbezogenen Daten rechtfertigungsbedürftig ist. Ein Gesetz, das nur besonders schwere Eingriffe in das Persönlichkeitsrecht definiert und verbietet, kann dazu führen, dass Beeinträchtigungen unterhalb dieser Schwelle als grundsätzlich legitim angesehen werden und unsanktioniert bleiben. Je nach dem Kontext der Veröffentlichung können aber auch einzelne und zunächst belanglos erscheinende Daten, wie etwa das Kfz-Kennzeichen, für den Betroffenen unangenehme Folgen haben. Überdies kann sich der Betroffene bereits nach geltendem Recht vor den ordentlichen Gerichten gegen ehrverletzende Veröffentlichungen zur Wehr setzen. Ob der angekündigte Gesetzentwurf die Position der Betroffenen zu bessern vermag, ist daher fraglich.

Eine sinnvolle und nachhaltige Grenzziehung zwischen der (freiwilligen) Selbstregulierung durch die Wirtschaft und der Regulierung durch den Gesetzgeber wird angesichts der dynamischen Entwicklung in der Internet-Welt zwar schwierig bleiben. Ich halte es aber ordnungspolitisch für verfehlt, den Schutz der Privatsphäre deshalb den Kräften des Marktes zu überlassen.

2.3.4 Ein neuer Akteur? Die Bundesstiftung Datenschutz

In ihrem Koalitionsvertrag haben die die Bundesregierung tragenden Parteien 2009 die Gründung einer „Stiftung Datenschutz“ angekündigt, die den Datenschutz in Deutschland stärken solle. Lange Zeit blieb jedoch unklar, was darunter zu verstehen ist und welche Aufgaben diese Einrichtung konkret erhalten soll. Dass es sich um ein Lieblingsprojekt des kleineren Koalitionspartners innerhalb der Bundesregierung handelte, wurde durch entsprechende konzeptionelle Überlegungen aus dieser Ecke deutlich[4]. Danach soll die geplante Bundesstiftung als Tätigkeitsschwerpunkte

[4] vgl. insbesondere den Aufsatz von Gisela Piltz MdB und RA Sebastian Schulz „Die Stiftung Datenschutz – moderner Datenschutz neu gedacht“, RDV 2011, 117 ff.

Bildung und Aufklärung in Datenschutzfragen, eigenverantwortliche Tests von Produkten und Dienstleistungen unter Datenschutzaspekten sowie bundesweit einheitliche Zertifizierungsverfahren in Angriff nehmen. Insgesamt soll die Stiftung quasi als dritter Akteur neben den Gesetzgeber und die Aufsichtsbehörden treten. Im Haushalt des Bundesinnenministeriums für 2011 wurde inzwischen ein Finanzierungsbeitrag von 10 Millionen Euro ausgewiesen. Ob die Erträge eines Stiftungskapitals in dieser Höhe ausreichen werden, um die angedachten Aufgaben abzudecken, erscheint fraglich. Dem Vernehmen nach sollen inzwischen Wirtschaftskreise wegen einer Mitfinanzierung angesprochen worden sein. Diese Entwicklung ist aus meiner Sicht bedenklich. Zwar ist jeder neue Akteur, der die Anliegen des Datenschutzes gegenüber Öffentlichkeit und Interessengruppen aktiv vertritt, uneingeschränkt zu begrüßen. Eine Mitfinanzierung durch die Wirtschaft würde jedoch die Unabhängigkeit und Unbeeinflussbarkeit der neuen Einrichtung, insbesondere bei Tests und Testaten, in Zweifel ziehen. Die Stiftung kann meines Erachtens nur dann glaubwürdig agieren, wenn sie ihre Aufgaben strikt unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft und zudem in völliger Transparenz wahrnimmt. Verfassungsrechtlich wäre noch zu klären, ob die Bundesregierung hier nicht in Handlungsfelder der Länder eingreift. Schließlich darf die Stiftung nur solche Aufgaben wahrnehmen, die nicht ausschließlich den Datenschutzaufsichtsbehörden zugewiesen sind. Unter diesen Voraussetzungen bieten die Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung und der Stiftung Datenschutz gerne ihre partnerschaftliche Unterstützung und Zusammenarbeit an (siehe auch Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010, Anhang 12).

2.3.5 Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages

Am 4. März 2010 hat der Deutsche Bundestag einstimmig die Einsetzung einer Enquete-Kommission „Internet und digitale Gesellschaft“ beschlossen. Im Antragstext der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN (BT-Drucksache 17/950) heißt es: *„Die digitale Gesellschaft bietet neue Entfaltungsmöglichkeiten für jeden Einzelnen ebenso wie neue Chancen für die demokratische Weiterentwicklung unseres Gemeinwesens, für die wirtschaftliche Betätigung und für die Wissensgesellschaft. (...) Das Internet ist nicht länger nur eine technische Plattform, sondern entwickelt sich zu einem integralen Bestandteil des Lebens vieler Menschen, denn gesellschaftliche Veränderungen finden maßgeblich im und mit dem Internet statt.“* Das Themenfeld der Enquete-Kommission war dementsprechend breit angelegt und betraf zahlreiche Politikfelder[5]. Wie die Kommission selbst konstatierte, sind dabei Fragen nach der Zukunft des Rechts auf informationelle Selbstbestimmung, der Wahrung des Persönlichkeitsrechts und des Datenschutzes von zentraler Bedeutung. Der Umgang mit personenbezogenen Daten habe sich im digitalen Zeitalter erheblich verändert. Dies würden Bürgerinnen und Bürger unmittelbar im täglichen Umgang mit dem Internet erleben. Die daraus folgenden Fragestellungen nähmen auch in der öffentlichen Diskussion großen Raum ein. Aus diesem Grund wurde eine Projektgruppe „Datenschutz, Persönlichkeitsrechte“ eingerichtet. Deren Ergebnisse wären aus meiner Sicht auch für das Land von Interesse gewesen. Die bis zur Som-

[5] vgl. insoweit Zwischenbericht der Enquete-Kommission vom 19. April 2011, BT-Drucksache 17/5625. Auf der Internetseite der Enquete-Kommission finden sich zudem zahlreiche weitere Dokumente sowie die Live-Mitschnitte der öffentlichen Anhörungen, http://www.bundestag.de/internetenquete/index.jsp.

merpause 2011 angekündigten Handlungsempfehlungen der Projektgruppe verzögerten sich allerdings um mehrere Monate, weil es – so war im Internet zu lesen – zu unerwarteten Abstimmungsergebnissen zu den Themen Netzneutralität und Urheberrecht gekommen sei und die Beratungen daraufhin vertagt wurden. Seit der letzten Projektgruppensitzung am 27. Juni 2011 war bis zum Redaktionsschluss dieses Berichts kein Fortschritt zu erkennen. Ob der Auftrag wie geplant bis zur Sommerpause 2012 erfüllt werden kann, ist mittlerweile fraglich geworden. Ohnehin dürfte der praktische Nutzen der Handlungsempfehlungen der Kommission in Anbetracht der offenkundig einzugehenden politischen Kompromisse begrenzt sein. Die notwendigen politischen Entscheidungen werden momentan ohnehin viel stärker durch die aktuelle Weiterentwicklung des Rechtsrahmens für den Datenschutz auf europäischer Ebene bestimmt.

2.4 Novellierung des europäischen Rechtsrahmens

Bereits im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, 1. Teil, Nr. 2.1) bin ich ausführlich auf die sich abzeichnende Modernisierung des europäischen Datenschutzrechts eingegangen, die sich aus dem im Dezember 2009 in Kraft getretenen Vertrag von Lissabon ergibt, insbesondere aus dem Wegfall der Säulenstruktur, generell aber auch aus der rasanten technologischen Weiterentwicklung. Eine Grundüberholung ist auch deshalb dringend notwendig, weil die maßgebliche Rechtsgrundlage, die europäische Datenschutzrichtlinie 95/46/EG, bereits aus dem Jahr 1995 stammt. Im Juli 2009 hatte die Europäische Kommission deshalb ein Konsultationsverfahren zum künftigen Rechtsrahmen eingeleitet und – darauf aufbauend – am 4. November 2010 ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“[6] vorgestellt und ein Konsultationsverfahren auch hierzu eingeleitet. Das Dokument ist – ebenso wie die im Zuge der ersten Konsultation abgegebene gemeinsame Stellungnahme der Artikel 29-Gruppe und der Arbeitsgruppe Polizei und Justiz (WP 168 „Die Zukunft des Datenschutzes“) und die zahlreichen Rückmeldungen von öffentlichen Stellen, Verbänden und Privatpersonen – im Internet auf der Seite der Generaldirektion Justiz der EU-Kommission abzurufen *(http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf)*.

Der Konsultationsbeitrag behandelte folgende Themenbereiche:

- Stärkung des Grundrechtsschutzes und Stärkung der individuellen Rechtsposition (einschließlich Prüfung der Einführung einer Verbandsklage),
- verstärkter Rechtsschutz im Internet und Schutz vor Profilbildung,
- Anwendbarkeit des nationalen Rechts,
- besondere Kategorien personenbezogener Daten („sensitive Daten“),
- Form des künftigen EU-Rechtsrahmens,
- betrieblicher Datenschutzbeauftragter,
- Datenschutz in den Bereichen Polizei und Strafjustiz,
- globale Dimension des Datenschutzes,
- verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules/BCR),
- Stärkung der Datenschutzbehörden.

[6] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010)0609, BR-Drucksache 707/10.

Im Rahmen des Konsultationsverfahrens nahmen auch zahlreiche Institutionen und Verbände aus Deutschland Stellung. So begrüßte der Bundesrat in seiner Stellungnahme vom 11. Februar 2011 (Drucksache 707/10) zwar die generelle Zielrichtung des Konzepts, warnte unter anderem aber vor zusätzlicher Bürokratie, kritisierte die Ausweitung der Datenschutzvorschriften im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf innerstaatliche Vorgänge, äußerte Vorbehalte gegen eine Verordnungsregelung und lehnte ein Verbandsklagerecht ab.

Die Datenschutzbeauftragten des Bundes und der Länder gaben eine gemeinsame Stellungnahme ab, die stellvertretend der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit am 13. Januar 2011 der Vizepräsidentin der EU-Kommission, Viviane Reding, übermittelte. Darin wurde der Leitgedanke der Europäischen Kommission für die Reform des EU-Datenschutzrechts begrüßt, das Grundrecht auf Datenschutz nach Artikel 8 der EU-Grundrechte-Charta vollumfänglich zur Geltung zu bringen. Um nationale Rechtstraditionen zu berücksichtigen und eine Absenkung des Datenschutzniveaus zu vermeiden, wurde als Rechtsrahmen eine Richtlinie favorisiert. Wegen der Einzelheiten wird auf den Konsultationsbeitrag der Datenschutzbeauftragten verwiesen, der von meiner Homepage abgerufen werden kann.

Um die hohe Bedeutung der Weiterentwicklung des europäischen Rechtsrahmens für den Datenschutz auch gegenüber der Öffentlichkeit zu unterstreichen, wurde die zentrale Veranstaltung der deutschen Datenschutzbeauftragten anlässlich des 5. Europäischen Datenschutztages am 28. Januar 2011 unter das Motto „Datenschutz in Europa – quo vadis?“ gestellt. Als Vorsitzender der Datenschutzkonferenz im Jahr 2010 hatte ich die ehrenvolle Aufgabe, die Veranstaltung in der baden-württembergischen Landesvertretung in Berlin zu organisieren. In Redebeiträgen von Bundesjustizministerin Sabine Leutheusser-Schnarrenberger MdB, des Europaabgeordneten Manfred Weber und von Professor Alexander Roßnagel (Universität Kassel) sowie in einer hochkarätig besetzten Podiumsdiskussion wurden vor zahlreichen interessierten Zuhörern Lösungsansätze für eine moderne Datenschutzstrategie auf europäischer und nationaler Ebene umrissen. Die Redebeiträge können von meiner Homepage heruntergeladen werden.

Ankündigungen, die unter Berücksichtigung der zahlreichen Stellungnahmen weiterentwickelte Gesamtkonzeption der EU-Kommission für den Datenschutz in der Europäischen Union werde kurz vor oder nach der Sommerpause 2011 das Licht der Öffentlichkeit erblicken, haben sich als verfrüht erwiesen. Mittlerweile ist davon die Rede, dass das Konzept erst Ende Januar 2012 veröffentlicht werden wird. Wie man schon an der Stellungnahme des Bundesrats gesehen hat, dürfte ein rasches Inkrafttreten der in Aussicht genommenen Regelungen nicht zu erwarten sein.

3. Internationaler Datenverkehr

3.1 Das sogenannte SWIFT-Abkommen

Im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 20) hatte ich noch der Hoffnung Ausdruck gegeben, dass die Belange des Datenschutzes bei der Übermittlung von Finanztransaktionsdaten in die USA zukünftig stärkere Beachtung finden. Diese Hoffnung wurde enttäuscht. Zwar ist am 1. August 2010 das sogenannte SWIFT-Abkommen zwischen den USA und der EU in Kraft getreten. Eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ließ aber gravierende Mängel erkennen. Nicht einmal die im Abkommen festgelegten Datenschutzregeln wurden beachtet.

Die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dazu am 16./17. März 2011 zum wiederholten Mal eine Entschließung gefasst:

Das Europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

(Der vollständige Wortlaut der Entschließung ist dem Anhang 13 zu entnehmen.)

Die EU arbeitet derzeit an einem eigenen EU-System zum Aufspüren der Terrorismusfinanzierung. Dieser Ansatz ist zunächst zu begrüßen. Denn dadurch kann die massenhafte Datenübermittlung, die europäischen Datenschutzstandards nicht einmal ansatzweise genügt, beendet werden. Erfreulich ist auch, dass sich die Europäische Kommission in ihrer Mitteilung vom 13. Juli 2011 zu den Optionen für das geplante EU-System ausdrücklich auch mit den Themen Datenschutz und Datensicherheit befasst. Allerdings steckt dieses Projekt noch in den Kinderschuhen. Mit einem raschen Ende des bisherigen Abkommens ist nicht zu rechnen.

3.2 Flugpassagiere als generell Verdächtige

Anfang des Jahres 2011 stellte die EU-Kommission einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vor. Nach ihren Überlegungen sollen systematisch die Daten aller Flugpassagiere, die die Außengrenzen der Gemeinschaft überqueren, aus den Buchungssystemen der Fluggesellschaften an die jeweilige nationale Zentralstelle der Sicherheitsbehörden übermittelt werden. Diese sollen dann die Daten regelmäßig für fünf Jahre speichern, wenn auch nach einem Monat vordergründig anonymisiert. Damit hofft man Personen aufspüren zu können, die als mögliche Verdächtige von terroristischen Straftaten oder sonstiger schwerer Kriminalität in Frage kommen können. Das Ergebnis wären riesige Datenbanken auf nationaler Ebene, in denen die Daten von vielen Millionen Flugpassagieren, egal ob sie in den Urlaub fliegen oder ob sie beruflich auf das Verkehrsmittel Flugzeug angewiesen sind, gespeichert wären. Eine solche Vorratsdatenspeicherung – auch wenn sie zur Terrorismusabwehr gedacht ist – würde in einem unverhältnismäßigen Umfang in das informationelle Selbstbestimmungsrecht einer Vielzahl unbescholtener Bürgerinnen und Bürger eingreifen. Dazu hatte das Bundesverfassungsgericht in seinem Urteil vom 2. März 2010 zur Vorratsdatenspeicherung von Telekommunikationsdaten wie schon in früheren Entscheidungen daran erinnert, dass es mit den Freiheitsrechten der Bürgerinnen und Bürger nicht vereinbar ist, wenn diese total erfasst und registriert werden. Gerade dazu würden die PNR-Daten (passenger name record) genutzt. Und diese umfassen eben nicht nur Name, Geburtsdatum und Adresse, sondern beispielsweise auch Informationen über Mobiltelefonnummern, Kreditkartendaten, Passinformationen und – nicht zu vergessen – die persönlichen Vorlieben während des Aufenthalts im Flugzeug.

Erfreulicherweise hat neben den Datenschutzbeauftragten des Bundes und der Länder, die in ihrer Entschließung vom 16./17. März 2011 (vgl. Anhang 17) ihre Bedenken gegen die Datensammelwut der EU-Kommission und vor allem der staatlichen Vertragspartner aus Übersee artikuliert haben, auch der Bundesrat in seinem Beschluss vom 18. März 2011 (BR-Drucksache 73/11) deutlich den auch nach datenschutzrechtlichen Kriterien mangelhaften Vorschlag kritisiert.

Nicht zu übersehen ist, dass Verordnungen, Richtlinien und sonstige Rechtsakte der EU-Kommission zur Terrorismusabwehr seit dem 11. September 2001 bis heute nicht in ein schlüssiges Gesamtkonzept eingebracht wurden, um gerade die Persönlichkeitsrechte der vielen betroffenen Flugpassagiere adäquat zu berücksichtigen. Stattdessen hat

die Kommission parallel zu dem Richtlinienentwurf einen Vorschlag vorgelegt, der auch für Flugreisen innerhalb der Europäischen Union vergleichbare Datensammlungen ermöglichen soll.

Zu hoffen ist, dass die Abkommen über die Flugpassagierdaten mit Australien, Kanada und den USA und die Überlegungen der Kommission, für den innergemeinschaftlichen Flugverkehr vergleichbare Regelungen zu treffen, von dem zu beteiligenden Europäischen Parlament kritisch auf ihre Vereinbarkeit mit dem Vertrag von Lissabon und dem darin verankerten Recht auf den Schutz der eigenen personenbezogenen Daten jedes Flugpassagiers überprüft werden.

Was das Abkommen mit den USA angeht: Am 17. November 2011 gab die EU-Kommission den Abschluss der Verhandlungen bekannt. Alle gesammelten Datensätze sollen nun nach sechs Monaten anonymisiert werden. Die Speicherfrist werde auf 10 (statt 15) Jahre verkürzt. Weiterhin würden von Flugreisenden 19 Datensätze erhoben, wie etwa Personaldaten oder Reiseroute. Zum Schutz vor unberechtigten Zugriffen sei jetzt vorgesehen, dass nur das US-Heimatschutzministerium zum Auslesen der Daten berechtigt sei und nicht etwa Fluggesellschaften oder andere Dritte. Außerdem würden die Fluggäste eine Einspruchsmöglichkeit erhalten, um ihre Daten einsehen und gegebenenfalls löschen lassen zu können. Das neue Abkommen, für das eine Laufzeit von sieben Jahren mit automatischer Verlängerung vorgesehen ist, solle nun so rasch wie möglich vom EU-Parlament beraten und freigegeben werden. Dass es dort nicht durchgewunken wird, bleibt zu hoffen.

Außer den bilateralen Abkommen sind auch die Planungen innerhalb der EU kritisch zu bewerten. Die Entwürfe der EU-Kommission ermöglichen, fast unbegrenzt Daten von Flugpassagieren zu speichern. Der Nachweis, dass dies generell terroristisch oder sonst schwerkriminell Verdächtige aufzuspüren hilft, fehlt bisher. Die Daten einer europaweit nach Millionen zählenden Personengruppe für fünf Jahre zu speichern, ist kaum als verhältnismäßig und grundrechtskonform anzusehen. Wenn dann noch Forderungen für die Speicherung vergleichbarer Daten der Nutzer anderer Verkehrsmittel wie Eisenbahn und Schiff realisiert würden, käme dies einem Verlust von Bürgerrechten in der EU gleich.

3.3 Internationale Datenübermittlungen zwischen Unternehmen

Zwei bedeutsame Entwicklungen aus dem Berichtszeitraum sind zu vermelden:

Am 5. Februar 2010 hat die Europäische Kommission die Standardvertragsklauseln vom 27. Dezember 2001 für die Datenübermittlung an Auftragsdatenverarbeiter in Drittländern mit Wirkung zum 15. Mai 2010 aufgehoben und durch eine neue Fassung ersetzt. Die vor dem Stichtag 15. Mai 2010 abgeschlossenen Standardverträge nach dem alten Vertragsmuster gelten fort. Werden für solche Altverträge allerdings Vertragsanpassungen vorgenommen, ist der bisherige Vertrag durch das neue Standardvertragsmuster zu ersetzen.

Mit Beschluss vom 28./29. April 2010 (siehe Anhang 32) haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) Anforderungen an Unternehmen, die Daten an ein nach den Grundsätzen des „sicheren Hafens“ (Safe Harbor) zertifiziertes Unternehmen in den USA übermitteln, formuliert.

Im Hinblick darauf, dass eine flächendeckende Kontrolle der Selbstzertifizierung US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA bislang nicht stattfindet, sollen Unternehmen in Deutschland zur Prüfung gewisser Mindestkriterien verpflichtet sein, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln. Allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs darf sich das Daten exportierende Unternehmen aber nicht verlassen. Stattdessen muss der Datenexporteur zumindest prüfen, ob die Safe Harbor-Zertifizierung noch nicht durch Zeitablauf erloschen ist, und sich zudem nach-

weisen lassen, wie das importierende Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nachzukommen gedenkt. Die Prüfung ist vom exportierenden Unternehmen zu dokumentieren und auf Nachfrage der Aufsichtsbehörde nachzuweisen.

Anzumerken ist, dass nach Meinung vieler Experten in der Vergangenheit ein erhebliches Vollzugsdefizit bei der Umsetzung des Safe Harbor-Abkommens festzustellen war: So kam ein Gutachten des US-Beratungsunternehmens Galexia unter dem Titel „Safe Harbor – Fact or Fiction?“ bereits im Jahr 2008 zu ernüchternden Erkenntnissen: So hätten zum Beispiel 206 befragte Unternehmen zwar behauptet, Mitglied von Safe Harbor zu sein, seien es in Wirklichkeit aber gar nicht gewesen. Auch deutsche Datenschützer machten ein Fragezeichen hinter die Aussagekraft des Abkommens, weil die Mitgliedschaft keine Fremdzertifizierung voraussetzt. Sanktionen sind von Europa aus allerdings kaum möglich. Die Bundesregierung hat übrigens in einer Antwort gegenüber dem Bundestag keinen wesentlichen Korrekturbedarf hinsichtlich des transatlantischen Datenschutzes gesehen (vgl. BT-Drucksache 17/3375) und insoweit auf die zuständigen EU-Gremien verwiesen.

3.4 Strafverfolgung über die Grenzen – Grenzen für den Datenschutz?

Bereits im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500) hatte ich über das sog. Stockholmer Programm der Europäischen Union berichtet, das „ein offenes und sicheres Europa im Dienste der Bürger“ als Zielsetzung versprach. Schon im Jahre 2009 hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 8./9. Oktober 2009 Datenschutzdefizite des Programms benannt. So war es dann nicht überraschend, dass die vom Bundestagsinnenausschuss am 19. September 2011 durchgeführte Anhörung zu dem „Entwurf eines Gesetzes über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedsstaaten der Europäischen Union“ (BT-Drucksache 17/5096) ein überwiegend kritisches Meinungsbild der Experten ergab. So wurde einhellig moniert, dass der Informationstransfer zwischen europäischen Strafverfolgungsbehörden nicht ohne umfassende Auflagen erleichtert werden könne, da in der EU kein einheitliches und ausreichendes Datenschutzniveau bestehe. Es sei realitätsfern anzunehmen, die deutsche Polizei könne selbst prüfen, ob eigene Informationen in anderen Mitgliedsstaaten, beispielsweise in Malta oder Ungarn, nach hiesigen Schutzstandards aufbewahrt werden. Kritik wurde aber nicht nur an dem aktuellen Gesetzentwurf, sondern auch an dem unzulänglichen Rahmenbeschluss geübt, der zeitlich vor dem Lissabonner Vertrag zustande kam. Dies hat zur Folge, dass Rechtsgrundlagen wie Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union und Artikel 8 der Grundrechte-Charta letztlich ohne Auswirkungen auf die Umsetzung der Schwedischen Initiative (Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006) bleiben würden. Die Realisierung des Gesetzentwurfs würde zu erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung führen. Denn zusammengefasst wäre dann möglich, dass die deutschen Polizeidienststellen – also nicht etwa die Staatsanwaltschaften – Informationen an Strafverfolgungsbehörden in anderen Mitgliedsstaaten der Union nach sehr weitgefassten Vorgaben übermitteln dürfen. Vor allem könnte bei der Übermittlung nicht darauf abgestellt werden, ob die empfangende Strafverfolgungsbehörde einem vergleichbaren Datenschutzstandard wie die deutschen Stellen unterliegt. Damit bliebe im Gegensatz zu der für die deutschen Polizeidienststellen geltenden Zweckbindung offen, ob diese auch im Empfängerstaat so greifen würde, von der Frage, ob die Informationen dann auch an weitere Stellen außerhalb der Europäischen Union übermittelt werden dürften, ganz zu schweigen. Die in der Bundestags-Drucksache nachzulesende Stellungnahme des Bundesrates lässt allerdings erkennen, dass dort weniger der Schutz der Individualrechte von Bedeutung war als vielmehr die Klarstellung der regelungskonformen Anwendung und die Ausweitung des Anwendungsbereichs auf die Schengen-Staa-

ten sowie auf die Steuerfahndung. Dass der Gesetzentwurf von der Polizei wegen der Verbesserung der Kriminalitätsbekämpfung positiv gesehen wird, ist zwar nachvollziehbar, zeigt aber auch eine fehlende Sensibilität für das Anliegen, die Bürgerrechte in einem zusammenwachsenden Europa bestmöglich zu berücksichtigen.

4. Aktuelle technische Herausforderungen

4.1 Von hölzernen Pferden und Holzwegen – der „Staats-Trojaner“ im Einsatz

Die Überwachung der Telekommunikation von Tatverdächtigen ist unter engen Voraussetzungen seit langem zulässig, um schwere Straftaten aufzuklären; Rechtsgrundlage für diesen Eingriff in das Fernmeldegeheimnis (Artikel 10 Absatz 1 GG) sind in erster Linie §§ 100 a, 100 b der Strafprozessordnung (StPO). Wenn Tatverdächtige bei der Telekommunikation aber Verschlüsselungstechniken einsetzen, ergeben sich Probleme für die Strafverfolgungsbehörden. Diese haben sich in den letzten Jahren insbesondere durch die immer beliebtere Internet-Telefonie (auch Voice over IP – VoIP – genannt) verstärkt, bei der Kommunikationsinhalte ohne großen Aufwand verschlüsselt werden können. Nach Angaben des Branchenverbandes BITKOM nutzen in Deutschland mittlerweile mindestens 12 Millionen Bürger regelmäßig den Computer zum Telefonieren – Tendenz steigend. Eine Überwachung von verschlüsselten Telefongesprächen über das Internet kann deshalb nur auf dem Umweg über die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) erfolgen. Dazu muss auf dem Computer der zu überwachenden Zielperson eine entsprechende Software (Erfassungssoftware) installiert werden, die auf die Daten der laufenden Kommunikation (Internet-Telefonie, aber auch E-Mail-Verkehr) zugreift und diese an die jeweilige Ermittlungsbehörde weiterleitet, bevor die Daten verschlüsselt werden bzw. nachdem sie entschlüsselt worden sind. Die dabei eingesetzte Technik und das Vorgehen entsprechen im Grunde der umstrittenen Online-Durchsuchung (vgl. 29. Tätigkeitsbericht 2009, LT-Drucksache 14/5500, S. 13). Damit ist das verfassungsrechtliche und technische Minenfeld an der Nahtstelle zwischen Online-Durchsuchung und Quellen-TKÜ aufgezeigt, auf die das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) eingegangen ist. Darin wurde die Regelung über die Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz für nichtig erklärt. Zugleich zeigte das Gericht die verfassungsrechtlichen Grenzen für ein heimliches Eindringen des Staates in private Rechner deutlich auf und schuf bei dieser Gelegenheit mit dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme einen neuen Maßstab, an dem staatliches Handeln sich künftig auszurichten hat.

„Wird ein komplexes informationstechnisches System zum Zwecke der Telekommunikationsüberwachung technisch infiltriert (‚Quellen-Telekommunikationsüberwachung‘), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können die auf dem Personalcomputer abgelegten Dateien zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. … Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Artikel 10 Absatz 1 GG nicht oder nicht hinreichend begegnet werden. Artikel 10 Absatz 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung‘, wenn sich die Überwachung ausschließlich auf Daten aus dem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.“ (Rdnr. 188–190)

Das Gericht ließ zwar weiterhin die Überwachung der Telekommunikation auch mit den Methoden der Quellen-TKÜ und – unter noch engeren Voraussetzungen – sogar die Online-Durchsuchung zu, verlangte aber zugleich, dass die Grenze zwischen dem Belauschen eines Internet-Telefonats und dem Seitenblick auf die Festplatte oder den Bildschirm desselben Rechners strikt einzuhalten ist. In welchem Umfang die Ermittlungsbehörden das Mittel der Quellen-TKÜ einsetzen, blieb lange Zeit im Dunkeln. Schon wegen der Komplexität der Maßnahme und der nicht unerheblichen Kosten[7] war nicht mit einer allzu großen Verbreitung zu rechnen. Dass die Versuchung, auf dem Zielrechner auch andere Daten als die aus laufender Telekommunikation abzugreifen, nicht nur theoretischer Natur ist, wurde durch den Beschluss des Landgerichts Landshut vom 14. Januar 2011, 4 QS 346/10, NStZ 2011, S. 479, deutlich: Im Rahmen eines Ermittlungsverfahrens war die Telekommunikationsüberwachung eines Geschäftsmanns, der des gewerbsmäßigen unerlaubten Handels mit Betäubungsmitteln verdächtig war, richterlich angeordnet worden. Da er verschlüsselt über das Internet zu kommunizieren pflegte, wurde auf seinen Laptop anlässlich einer Sicherheitskontrolle am Flughafen heimlich ein Spionageprogramm aufgespielt. Dieses Programm zeichnete dann aber nicht nur Telefongespräche und E-Mails auf, sondern fertigte auch noch Screenshots des Bildschirms im 30-Sekunden-Abstand an und speicherte diese. Im Unterschied zur Vorinstanz hielt das Landgericht die Screenshots für unzulässig, weil diese nicht den Telekommunikationsvorgang selbst betrafen; die Quellen-TKÜ auf der Grundlage von § 100 a StPO wurde als solche hingegen nicht in Frage gestellt.

Frühzeitig haben Experten darauf hingewiesen, dass sich der Einsatz der verwendeten Spionage-Software auf Dauer nicht verheimlichen lässt. Insofern erstaunte es nicht, dass eine Festplatte, auf der die Erfassungssoftware installiert war, auch den Weg zum Chaos-Computer-Club (CCC) fand. Dieser sezierte die auf der Platte gespeicherten Dateien, stieß auf technische Ungereimtheiten und machte diese Anfang Oktober 2011 publik. Der baden-württembergische Innenminister musste am 10. Oktober 2011 vor der Presse einräumen, dass Varianten der Erfassungssoftware bis April 2011 viermal auch von Strafverfolgungsbehörden des Landes eingesetzt worden waren. Gleichzeitig gab er bekannt, dass der Einsatz der Erfassungssoftware bis auf Weiteres gestoppt worden sei. Einzelheiten wurden inzwischen gegenüber dem Landtag offengelegt; insoweit verweise ich auf die LT-Drucksache 15/669. Ich habe den Einsatz und die Verwendung der Software am 11. Oktober 2011 einer Kontrolle beim Landeskriminalamt unterzogen. Diese und der sich anschließende Schriftwechsel mit der Behörde brachten bisher folgende Erkenntnisse:

– Infiltration

  Im Gegensatz zu Trojanern in freier EDV-Wildbahn darf sich die Erfassungssoftware nicht auf jedem Rechner einnisten. Da die Überwachungsmaßnahme regelmäßig verdeckt erfolgt, ist zunächst tatsächlich und rechtlich das Problem zu lösen, wie die Maßnahme auf einem Personalcomputer realisiert werden kann, auf den man im Allgemeinen keinen Zugriff hat. Zudem muss sichergestellt werden, dass die Erfassungssoftware genau auf dem oder den Rechnern der zu überwachenden Zielperson installiert wird. Das Landeskriminalamt hat erklärt, dass die modular aufgebaute Software bei jedem Einsatz speziell angepasst worden sei. Insbesondere hätten die Anpassungen die im Allgemeinen einen Computer kennzeichnenden Eigenschaften wie MAC-Adresse oder WLAN-Adresse berücksichtigt. Die hierzu ergangenen richterlichen Anordnungen habe ich von den be-

[7] vgl. hierzu bereits Buermeyer/Bäcker: Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100 a StPO, Online-Zeitschrift HRRS 2009, S. 433 f., unter Bezugnahme auf ein Anfang 2008 durch den Chaos-Computer-Club veröffentlichtes Papier aus dem Bayerischen Staatsministerium der Justiz.

teiligten Staatsanwaltschaften angefordert und erhalten; sie enthielten jeweils spezifische technische Beschränkungen hinsichtlich der Zielperson und der Überwachungsmaßnahmen.

Die meinen Mitarbeitern gegenüber aufgezeigten Wege, sich eindeutige Merkmale des zu infiltrierenden Rechners zu beschaffen und die Erfassungssoftware so zu parametrisieren, dass sie nur auf diesem PC installiert werden kann, sind aus datenschutzrechtlicher Sicht nur bedingt überzeugend. Weitere Einzelheiten können an dieser Stelle aus Gründen der Geheimhaltung nicht offengelegt werden.

– Kommunikationsinhaltsdaten

Im Urteil des Bundesverfassungsgerichts wird meiner Meinung nach unmissverständlich erklärt, dass für eine Quellen-TKÜ-Maßnahme nur die Daten ausgeleitet werden dürfen, die im Rahmen einer laufenden Kommunikation anfallen. Hierunter fallen beispielsweise Daten von Programmen zur Internet-Telefonie, dem sogenannten Instant Messaging und E-Mail. Nicht davon erfasst werden beispielsweise Programme zur Textverarbeitung, Tabellenkalkulation oder Datenbanken. Ebenso ist es nach dem Urteil des Bundesverfassungsgerichts im Rahmen einer Quellen-TKÜ-Maßnahme nicht zulässig, den gesamten Bildschirminhalt zu kopieren (Screenshot; siehe hierzu auch die o. g. Entscheidung des LG Landshut), die Webcam eines Computers einzuschalten, das Mikrofon zu aktivieren oder alle Betätigungen der Tastatur aufzuzeichnen (key logger).

Das Landeskriminalamt hat erklärt, dass dem Unternehmen, von dem es die Erfassungssoftware angemietet hat, mitgeteilt werden musste, welche Kommunikationsprogramme ausgeleitet werden sollen. Das Unternehmen habe die modulare Erfassungssoftware so angepasst, dass nur die mitgeteilten Programme abgehört werden konnten. Das Landeskriminalamt hat weiter erklärt, die Software sei in einem Testlabor vor dem Einsatz getestet worden.

Hierzu ist zu sagen, dass solche Tests prinzipiell nicht vollständig sein können, da gezielte Tests nur zeigen, ob eine bestimmte Funktionalität implementiert ist, aber nicht, dass beispielsweise eine andere nicht implementiert ist. Es ist daher grundsätzlich möglich, dass die Erfassungssoftware Funktionalitäten realisiert, die nicht zulässig sind und die bei Tests nicht erkannt werden können.

– Verschlüsselung

Die bei einer Quellen-TKÜ-Maßnahme gewonnenen Daten werden aus naheliegenden Gründen nicht auf dem Computer der Zielperson gespeichert. Daher müssen die Daten an einen anderen Rechner übertragen und dort gesichert werden. Da in öffentlichen Netzen das Risiko besteht, dass die Datenübertragung von Dritten mitgelesen (oder sogar manipuliert) werden kann, bin ich der Auffassung, dass die Übertragung der personenbezogenen Daten verschlüsselt zu erfolgen hat. Sofern Verschlüsselungen nur mit einem „Universalschlüssel“ vorgenommen werden, besteht – wie das Vorgehen des CCC gezeigt hat – die Gefahr, dass Dritte in den Besitz des Schlüssels geraten und damit die Vertraulichkeit nicht mehr gewährleistet ist.

Das Landeskriminalamt hat zwar erklärt, dass die ausgeleiteten Daten verschlüsselt zu einem Server übertragen worden seien. Auf Nachfrage räumte es aber ein, dass bei der Verschlüsselung wohl noch Verbesserungsmöglichkeiten bestünden. Von einem Test im Labor, bei dem die verschlüsselten Daten mit einem Netzwerkmonitor aufgezeichnet und die Güte der Verschlüsselung hätte analysiert werden können, erwähnte das Landeskriminalamt nichts.

– Fernsteuerungsfunktion

Sich darauf zu verlassen, dass mit zeitgesteuerter Erfassung kriminalistisch aufschlussreiche Daten erhoben werden, ist nicht zielführend. Daher – und das schließt das Urteil des Bundesverfassungsgerichts

nicht aus – kann die Erfassungssoftware über entsprechende Kommandos aus der Ferne gesteuert werden. Auf Knopfdruck können Fensterinhalte von Kommunikationsprogrammen kopiert oder Sprachdaten von den Programmen für Internet-Telefonie ausgeleitet werden.

Aus meiner Sicht muss die Übertragung der Kommandos an die Erfassungssoftware verschlüsselt erfolgen. Das Landeskriminalamt hat hierzu erklärt, dass es davon ausgehe, dass die Steuerungskommandos verschlüsselt übertragen würden. Ganz sicher war es sich aber nicht. In diesem Zusammenhang ist ein weiterer Punkt zu beachten: Allein mit der Verschlüsselung kann nicht mit letzter Sicherheit verhindert werden, dass Unbefugte Steuerungskommandos an die Erfassungssoftware schicken könnten. Daher bin ich der Auffassung, dass derjenige, der Kommandos an die Erfassungssoftware schickt, nachweisen muss, dass er dazu berechtigt ist. Im Allgemeinen geschieht dies im Rahmen eines Authentifizierungsverfahrens. Auf die Frage, wie die Steuerungsstation sich an dem zu überwachenden Rechner authentisieren würde, wurde erklärt, dass darüber keine Kenntnisse vorlägen. Von einem Test unter Laborbedingungen, an dem die Kommunikation zwischen einem Steuerungs-Computer und einem Test-Computer mit einem Netzwerkmonitor nachvollzogen wurde und der den Sachverhalt hätte erhellen können, erwähnte das Landeskriminalamt nichts.

– Nachladefunktion

Bei der Kontrolle hat das Landeskriminalamt eingeräumt, dass die Erfassungssoftware über eine Funktion verfügte, mit der nach der Infiltration nachträglich weitere Dateien und Programme auf den Rechner der Zielperson hätten übertragen werden können. Der Rechner, von dem die Datei(en) kopiert worden wäre(n), konnte frei bestimmt werden.

Für die Nachladefunktion sollten meines Erachtens die gleichen Anforderungen wie für die Fernsteuerungsfunktion gelten. Ohne Authentifikationsverfahren und Verschlüsselung sollte diese Funktionalität nicht genutzt werden können. Wenn die Nachladefunktion ohne Authentifizierung erfolgen kann und die nachzuladenden Dateien auf beliebigen Rechnern bereitgestellt werden können, stellt eine Erfassungssoftware ein Sicherheitsrisiko dar, das das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme verletzt.

Ob die Nachladefunktion diesen Anforderungen gerecht wird, konnte das Landeskriminalamt nicht mit Bestimmtheit sagen.

– Kernel-Modul

Eine „Schlüssel-Funktion“ im wahrsten Sinne des Wortes hat das sogenannte Kernel-Modul, das Teil der Erfassungssoftware ist. Diese Art von Software klinkt sich in das Betriebssystem ein und wird ein Bestandteil davon. Dadurch sind dem Modul weitreichende Zugriffsmöglichkeiten eröffnet, da das Betriebssystem dafür zuständig ist zu regeln, wer wann wie auf Daten, Dateien oder Geräte wie beispielsweise Mikrofon, Webcam, Tastatur oder Bildschirmspeicher zugreifen kann. Über dieses Kernel-Modul hätte die Erfassungssoftware möglicherweise auf Geräte und Dateien zugreifen können. Andererseits ist es für die Erfassungssoftware erforderlich, auf die zu überwachenden Anwendungen zugreifen zu können. Dies kann im Allgemeinen nur im Rahmen eines Kernel-Moduls geschehen, da alle Programme auf einem Computer der Steuerung durch das Betriebssystem unterliegen.

Es ist meiner Auffassung nach wichtig, die Funktionalität des Kernel-Moduls genau zu kennen. Hierüber konnte das Landeskriminalamt keine hinreichend konkreten Angaben machen. Da es sich bei dem Kernel-Modul um die kritischste Komponente der Erfassungssoftware hinsichtlich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme handelt, halte ich es für erfor-

derlich, dass alle darin enthaltenen Funktionalitäten offengelegt werden.

– Löschfunktion

  Nach erfolgter Überwachungsmaßnahme darf die Erfassungssoftware nicht auf dem Rechner verbleiben, sondern muss gelöscht werden.

  Das Landeskriminalamt erklärte hierzu, dass sich die Erfassungssoftware selbst löschen würde, wenn die Frist für die Überwachungsmaßnahme abgelaufen sei. Es sei aber auch möglich, die Löschung der Erfassungssoftware bereits vor Ablauf der Frist über einen Steuerungsbefehl vorzunehmen.

  In einem Fall wurde die Maßnahme über die sonst übliche Dauer von drei Monaten verlängert. Nach derzeitigem Stand ist es anscheinend möglich, die automatische Löschung vor Erreichen der Frist auszusetzen. Dieser Punkt muss noch detailliert geklärt werden.

– Server in den USA

  Wenn die Erfassungssoftware installiert ist, muss sie die gewonnenen Daten an einen Rechner übertragen. Dabei hatte sich das Landeskriminalamt eines Servers bedient, der sich in einem Rechenzentrum in den USA befand. Auf die Frage, warum ein Server in den USA genutzt wurde, erklärte das Landeskriminalamt, dies sei zur Legendenbildung geschehen.

  Ich halte es für einen schweren Fehlgriff, dass eine deutsche Strafverfolgungsbehörde eine Quellen-TKÜ-Maßnahme mit technischen Gerätschaften durchführte, die sich nicht in einem Land der EU befanden, und an der Personal mitwirkte, das nicht der EU-Jurisdiktion unterlag. Daran kann auch der Umstand nichts ändern, dass mit dem Freistaat Bayern eine Kooperation bestand, wie das Innenministerium dem Landtag mitteilte (vgl. LT-Drucksache 15/669). Die Durchführung einer Überwachungsmaßnahme außerhalb der Verantwortung der zuständigen Justizorgane ist meiner Meinung nach mehr als bedenklich.

Dass die Sicherheitsbehörden in den Stand versetzt werden müssen, ermittlungstaktisch mit potenziellen Straftätern mithalten zu können, dürfte bei emotionsloser Betrachtung unstreitig sein. Hierzu kann als strafprozessuale Maßnahme bei Bedarf auch die Quellen-TKÜ gehören. Aufgrund der Brisanz des Eingriffs, der häufig das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme tangiert, sind die Strafverfolgungsbehörden aber gefordert, die Maßnahme mit höchster Präzision durchzuführen. Nur dann kann die Quellen-TKÜ datenschutzrechtlich zulässig durchgeführt werden. Diesen Anforderungen kann man nicht entsprechen, wenn man nur über oberflächliche Kenntnisse der eingesetzten Software verfügt. Es genügt meiner Auffassung nach nicht, dass die Strafverfolgungsbehörden von einem Unternehmen die Erfassungssoftware anmieten und sich darauf verlassen, dass das Unternehmen die erforderlichen Anpassungen vorgenommen hat und die Funktionalität der Software nicht über den gesetzlich zulässigen bzw. richterlich angeordneten Rahmen hinausgeht. Hier muss zukünftig sorgfältiger vorgegangen werden. Notwendig ist meiner Meinung nach, dass die Ermittlungsbehörden anhand des Quellcodes wirklich beurteilen können, was die Erfassungssoftware kann. Sofern der Quellcode wegen urheberrechtlicher Beschränkungen nicht zur Verfügung gestellt wird, sollte er bei einer unabhängigen Stelle hinterlegt werden und gegebenenfalls eingesehen und geprüft werden können. Schließlich ist auch der Gesetzgeber selbst gefordert, die rechtlichen Voraussetzungen für eine Quellen-TKÜ präziser zu regeln. Die Datenschutzbeauftragten des Bundes und der Länder haben entsprechende Forderungen bereits in ihrer Entschließung vom 16./17. März 2011 (vgl. Anhang 16) erhoben.

Mittlerweile ist Bewegung in die politische Diskussion über die Zukunft der Quellen-TKÜ gekommen. Parteiübergreifend wird gefordert, dass die Ermittlungsbehörden wieder „Herr des Verfahrens“ werden und in die Lage versetzt werden müssen, die technischen Möglichkeiten der Erfassungssoftware anhand des Quell-Codes abschätzen zu können. Auch eine Konkretisierung der gesetzlichen Voraussetzungen wird nicht mehr ausgeschlossen.

4.2 Reine Fassade? Panoramaansichten im Internet

Verschiedene Diensteanbieter haben begonnen, auch in Deutschland Panoramaansichten von Straßenzügen zu fertigen und im Internet zu veröffentlichen. Beim Angebot solcher Dienste ist die informationelle Selbstbestimmung des Einzelnen unbedingt zu wahren.

Die Diskussion um die Veröffentlichung personenbezogener Daten im Internet hat sich besonders am Beispiel der Panoramaansichten von Straßenzügen entzündet. Verschiedene Diensteanbieter, allen voran international operierende Akteure wie Google Inc. und die Microsoft Corporation, haben mit ihren Diensten Google Street View beziehungsweise Bing Maps Streetside begonnen, die Straßen deutscher Großstädte nahezu vollständig fotografisch zu erfassen, um die Bilder in Form von nahtlos aneinander gereihten Panoramaansichten im Internet zu veröffentlichen. Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hat bereits in ihrem Fünften Tätigkeitsbericht 2009 (Abschnitt B 10.2) die Funktionsweise und die rechtliche Bewertung solcher Dienste durch die Datenschutzaufsichtsbehörden dargelegt.

– Die Dienste im Einzelnen:

Google Inc. hält unter seinem Angebot Google Street View Panoramaaufnahmen von den Straßenzügen der zwanzig größten Städte Deutschlands im Internet zum Abruf bereit. Die Veröffentlichung von Abbildungen aus weiteren deutschen Städten ist darüber hinaus nicht geplant. Da die Google Germany GmbH als deutsche Tochter von Google Inc. ihren Sitz in Hamburg hat, unterliegt das inländische Angebot von Google Street View der datenschutzrechtlichen Aufsicht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Dieser hat im Jahr 2010 mit Google einen 13-Punkte-Plan ausgehandelt, nach dem sich das Unternehmen unter anderem dazu verpflichtet hat, den Betroffenen die Möglichkeit einzuräumen, der Veröffentlichung der in ihrem Eigentum befindlichen oder von ihnen bewohnten Häuser vorab online oder auf dem Postweg zu widersprechen. Auch ein nachträglicher Widerspruch ist immer noch möglich. Der Widerspruch führt dazu, dass das entsprechende Haus unkenntlich gemacht (verpixelt) wird.

Die von Google eingesetzten Fahrzeuge haben zeitweise neben den für die Panoramaansichten benötigten Bilddaten auch Daten über die örtlich vorhandenen WLAN-Netze gesammelt. Dabei wurden sogar Kommunikationsinhalte in Form von E-Mail-Fragmenten rechtswidrig erfasst. Google beendete diese Praxis jedoch auf Betreiben der hamburgischen Aufsichtsbehörde.

Im Mai 2011 haben auch die Aufnahmen für die Panoramaansichten von Bing Maps Streetside in Deutschland begonnen. Der Dienst wird von der Firma Microsoft betrieben, deren deutsche Tochter, die Microsoft Deutschland GmbH, ihren Sitz in Unterschleißheim bei München hat. Nach einem intensiven Dialog mit dem Bayerischen Landesamt für Datenschutzaufsicht räumte auch Microsoft den betroffenen Grundstückseigentümern und Mietern vom 1. August bis zum 30. September 2011 die Möglichkeit zur Einlegung eines Vorab-Widerspruchs ein. Auch beim Dienst Bing Maps Streetside ist ein nachträglicher Widerspruch jederzeit möglich.

– Regulierungsansätze

Durch verschiedene Regelungsinitiativen ist versucht worden, den mit der Veröffentlichung von Panoramaansichten verbundenen Datenschutzrisiken wirksam zu begegnen. Gegenstand dieser Bemühungen ist teilweise eine Selbstregulierung der Diensteanbieter, teilweise eine staatliche Regulierung.

Eingedenk der mit den Diensten verbundenen Risiken für die Persönlichkeitsrechte der Bürger hat der Bundesminister des Innern im September 2010 den Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) aufgefordert, einen Kodex für eine Selbstregulierung der Diensteanbieter im Bereich von online abrufbaren Panoramaansichten vorzulegen. Dabei hatte das Ministerium dem BITKOM nahe gelegt, den Kodex zuvor mit den Datenschutzbehörden des Bundes und der Länder abzustimmen. Der Verband hat jedoch auf eine solche Konsultation verzichtet.

BITKOM hat am 1. März 2011 den vom Bundesministerium des Innern gewünschten Datenschutzkodex für Geodatendienste vorgelegt. Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben ihn in ihrem Beschluss vom 8. April 2011 (vgl. Anhang 37) für unzureichend befunden. Einem effektiven Schutz der Betroffenen steht insbesondere entgegen, dass der Kodex für diese lediglich die Möglichkeit vorsieht, der Veröffentlichung der Aufnahmen nachträglich zu widersprechen. Das kann zu spät sein, weil die ins Internet gestellten Aufnahmen bis zur Unkenntlichmachung längst kopiert und weitergeleitet sein können. Außerdem wird bereits mit der Veröffentlichung in die Persönlichkeitsrechte der Betroffenen eingegriffen. Da der Kodex zudem nur für Panoramaansichten aus der Straßenperspektive gelten soll, bleiben Schrägaufnahmen aus der Luft unberücksichtigt. Der Kodex beachtet daher im Ergebnis nicht in ausreichender Weise die Interessen der Betroffenen.

Angesichts der Defizite dieses Selbstregulierungsversuchs ist eine gesetzliche Regelung für Panoramadienste im Internet vorzuziehen, zumal es auch Anbieter von Panoramaaufnahmen geben kann, die nicht Mitglied des Verbandes BITKOM sind und sich deswegen an dessen Kodex nicht gebunden zu fühlen brauchen. Der Bundesrat hat im August 2010 einen von allen Ländern gebilligten Gesetzentwurf in den Bundestag eingebracht (BT-Drucksache 17/2765), der für das Angebot von Panoramaansichten im Internet die folgenden datenschutzrechtlichen Mindeststandards formuliert:

- Diensteanbieter haben sicherzustellen, dass Gesichter und amtliche Kennzeichen von Fahrzeugen nicht identifizierbar sind.
- Nach dieser Unkenntlichmachung sind die unveränderten Rohdaten unverzüglich zu löschen.
- Die Betroffenen sind spätestens eine Woche vor der Datenerfassung von der hierfür verantwortlichen Stelle durch öffentliche Bekanntmachung in einer örtlichen Tageszeitung und im Internet auf das Vorhaben hinzuweisen.
- Den Betroffenen ist schon vor der Veröffentlichung der Bilder im Internet eine Widerspruchsmöglichkeit einzuräumen, auf die ausdrücklich durch öffentliche Bekanntmachung hinzuweisen ist.
- Der Entwurf soll nur die Aufnahme und Bereitstellung von Bildern erlauben, die nicht unter Entfernung oder Überwindung blickschützender Vorrichtungen aufgenommen worden sind; solche Bilder bedürfen daher der Einwilligung des Betroffenen.
- Die Verletzung dieser Pflichten soll nach dem Gesetzentwurf als Ordnungswidrigkeit mit Bußgeld geahndet werden können.

Obwohl der Gesetzentwurf zumindest eine geeignete Diskussionsgrundlage für eine datenschutzgerechte Ausgestaltung der Panoramadienste darstellt, ist er im Bundestag bislang nicht beraten worden.

Um die Persönlichkeitsrechte der Betroffenen effektiv zu schützen, bedarf das Angebot von Panoramaansichten im Internet weiterhin einer gesetzlichen Regelung. Der Gesetzgeber darf den Schutz der Privatsphäre nicht den Kräften des Marktes überlassen.

4.3 „Google Analytics“ – Reichweitenanalyse jetzt datenschutzkonform möglich

Betreiber von Internet-Angeboten interessieren sich vielfach dafür, wie die Besucher ihrer Webseiten die Angebote nutzen, welche Seiten sie häufig aufrufen, und was sie vielleicht hindern könnte, eine Bestellung oder einen Download auszuführen. Dazu greifen die Webseitenbetreiber gerne auf einfach bedienbare Werkzeuge zur sogenannten Reichweitenmessung zurück. Der Konflikt zwischen dem geschäftlichem Interesse der Webseitenbetreiber und dem Schutz der sensiblen Besucherdaten ist vorprogrammiert.

Google Analytics ist ein solches weitverbreitetes und zudem kostenlos nutzbares Werkzeug. In den meisten Fällen wird man beim Surfen auf Webseiten nicht bemerken, dass Google Analytics nahezu unsichtbar im Hintergrund Daten sammelt. Hat der Webseitenbetreiber ein paar Zeilen Javascript-Code in seine Webseiten aufgenommen, wird der Google Analytics-Code im Webbrowser des Besuchers ausgeführt. Beim Aufruf einer derart präparierten Webseite werden Informationen erhoben und an die Google Inc. in die USA weitergeleitet, unter anderem über den Zeitpunkt des Seitenaufrufs, wie lange die Seite im Browser geladen gewesen ist, welcher Browser eingesetzt und von welcher Seite dorthin gewechselt wurde.

Aus datenschutzrechtlicher Sicht ist die Weiterleitung der IP-Adresse, die mittels der Javascripte erfolgt, besonders problematisch. Die Datenschutzaufsichtsbehörden vertreten schon seit langem – so auch der Düsseldorfer Kreis in seinem Beschluss vom 27. November 2009 zur „Datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ (vgl. Anhang 29) – die Auffassung, dass die IP-Adresse ein personenbezogenes Datum ist. Dies gilt unabhängig davon, ob die IP-Adresse statisch oder dynamisch vom Internet Service Provider vergeben wird.

Bei Internet-Angeboten regelt § 12 Absatz 1 des Telemediengesetzes (TMG) die Erhebung und Verwendung von personenbezogenen Daten. Danach muss der Webseitenbesucher einwilligen, wenn „seine“ Daten erhoben oder verwendet werden sollen, es sei denn, das Telemediengesetz selbst oder eine andere Rechtsvorschrift erlauben dieses auch ohne seine Einwilligung.

Zweck der Reichweitenmessung ist die bedarfsgerechte Gestaltung von Webseiten durch den Anbieter. Das Telemediengesetz sieht zwar vor, dass dafür Nutzungsprofile erstellt werden dürfen (§ 15 Absatz 3 TMG), allerdings nur bei Verwendung eines Pseudonyms statt einer Nutzeridentifikation und nur, falls der Nutzer dem nicht widersprochen hat.

Hier kam es in der Vergangenheit zum datenschutzrechtlichen Konflikt. Einerseits durften Nutzungsprofile für die Reichweitenmessung nur pseudonym erfasst werden, andererseits wurde die vollständige IP-Adresse, und damit ein personenbezogenes Datum, ohne Einwilligung des Webseitenbesuchers an die Firma Google weitergeleitet. Ein möglicher Ausweg: Wie bei einer Telefonnummer wird durch Weglassen der letzten Ziffern die IP-Adresse anonymisiert. Damit wäre der Personenbezug nicht mehr gegeben. Für Google bliebe bei verkürzter IP-Adresse noch ausreichend Information erhalten, um den Webseitenbesucher einem Land oder einer Region zuordnen zu können, was für die Reichweitenmessung ein wesentlicher Punkt ist. Zusätzlich zur anonymisierten IP-Adresse muss der Nutzer sein Widerspruchsrecht ausüben können. Am einfachsten lässt sich dies durch sog. Browser-Add-Ons, die der Webseitenbesucher für seinen Browser herunterladen und aktivieren kann, bewerkstelligen. Diese verhindern, dass die Javascripte von Google Analytics ausgeführt und damit Nutzungsprofile erstellt werden.

Im Zuge der seit Ende 2009 mit dem Unternehmen Google geführten Verhandlungen hat mein Hamburger Kollege in Abstimmung mit den anderen Datenschutzaufsichtsbehörden in Deutschland diese beiden technischen Maßnahmen zur Einhaltung des § 15 Absatz 3 TMG eingefordert. Zur Jahresmitte 2011 hat Google dann sowohl ein Javascript zur Anonymisierung der IP-Adresse als auch Browser-Add-Ons für die am Markt führenden Internet-Browser bereit gestellt. Google sichert zu, dass die Anonymisierung noch innerhalb Europas stattfindet und eine Weiterleitung der ungekürzten IP-Adresse in die USA ausgeschlossen ist.

Nun sind die Webseitenbetreiber in der Pflicht. Zum einen müssen sie das Javascript für die Anonymisierung in ihre Webseiten „einbauen" *(http://code.google.com/intl/de/apis/analytics/docs/gaJS/gaJSApi_gat.html#_gat._anonymizeIp)*, zum anderen einen Auftragsdatenverarbeitungsvertrag mit Google nach § 11 BDSG abschließen *(http://www.google.de/intl/de/analytics/tos.pdf)*. Webseitenbetreiber beauftragen danach im Grunde die Google Inc. mit der Verarbeitung der Daten, die Besucher ihrer Webseiten ihnen zur Verfügung stellen. Google selbst liefert das Werkzeug Google Analytics und gibt die aufbereiteten anonymisierten Besuchsstatistiken an die Webseitenbetreiber zurück.

Und schließlich sind die Webseitenbesucher über ihr Widerspruchsrecht gegen das „Tracking" durch Google Analytics aufzuklären. Zusammen mit dem Link *http://tools.google.com/dlpage/gaoptout?hl=de* zum Herunterladen des passenden Add-Ons ist in die Datenschutzerklärung ein entsprechender Hinweis durch den Webseitenbetreiber aufzunehmen.

Grundsätzlich empfiehlt es sich, die Datenschutzbedingungen der Webseiten daraufhin durchzusehen, ob und wie ein Widerspruchsrecht ausgeübt werden kann. Gerade bei der Nutzung von Internet-Diensten sollte man darauf achten, wie man dieses Recht zur Anwendung bringen kann. Wie das Beispiel Google Analytics zeigt, ist die praktische Mitwirkung des Betroffenen besonders gefragt.

Das Verhandlungsergebnis in Sachen Google Analytics kann sich sehen lassen. Es zeigt, dass sich die wirtschaftlichen Interessen großer amerikanischer Internet-Unternehmen durchaus mit europäischen Datenschutzstandards in Einklang bringen lassen. Das macht Mut auch hinsichtlich anderer Marktakteure, insbesondere des sozialen Netzwerks Facebook.

4.4 Der intelligente Stromzähler

„Smart Meter verraten Fernsehprogramm": Mit dieser Schlagzeile wurde am 20. September 2011 in der elektronischen Publikation „heise Security" ein Beitrag eingeleitet, der die datenschutzrechtliche Problematik beim Einsatz von sog. Smart Metern plakativ deutlich macht. Doch der Reihe nach:

Das Energiewirtschaftsgesetz (EnWG) verpflichtet seit dem Jahr 2010 zum Einbau von digitalen Zählern, sogenannten Smart Metern, beim Neubau oder bei umfangreicheren Renovierungen von Häusern oder Wohnungen. Denn im Zusammenhang mit der verstärkten Nutzung regenerativer Energien (zum Beispiel Sonne, Wind) ist mit Schwankungen der Energieproduktion zu rechnen, auf die auf der Abnahmeseite flexibel reagiert werden muss. Mit Smart Metern soll der tatsächliche Energieverbrauch, zum Beispiel bei elektrischem Strom oder bei Gas, und die tatsächliche Nutzungszeit gemessen werden. Der Vorteil für den Kunden liegt auf der Hand: Er kann seine Energiekosten optimieren, indem er den Verbrauch seiner Geräte und Einrichtungen nach zeitlich variablen Tarifen der Energieversorger ausrichtet. Die Verbrauchsdaten werden an die Versorger übermittelt und ermöglichen diesen wiederum, die Netzauslastung besser zu steuern und schneller auf Lastspitzen zu reagieren.

Die zeitliche Auflösung der Verbrauchsdatenerfassung durch Smart Meter kann bis in den Sekundenbereich herabreichen. Und damit lassen

sich personenbezogene Nutzungsprofile erstellen, die mehr über die Lebensgewohnheiten aussagen, als man zunächst vermuten könnte. Forscher der Fachhochschule Münster haben in einem vom Bundesministerium für Bildung und Forschung geförderten Projekt (DaPriM – Data Privacy Management) gezeigt, dass bei sekundengenauer Messauflösung sogar ein auf einem üblichen Fernsehgerät angezeigtes Programm oder ein eingespielter Film identifiziert werden kann. Ermöglicht wird dies durch die charakteristischen Schwankungen im elektrischen Energieverbrauch, die mit den Hell-Dunkel-Wechseln bei der Darbietung des Programms oder beim Abspielen des Films entstehen. Und genau diese Schwankungen lassen sich mit einem Smart Meter erfassen und auswerten.

In der Entschließung zum „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs“ der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010 (vgl. Anhang 10) wird daher zu Recht darauf hingewiesen, dass die detaillierte Erfassung des Verbrauchs ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich birgt.

Im konkreten Fall lässt sich das Ausforschungspotenzial dadurch verringern, dass die zeitlich hoch aufgelösten Messdaten vor ihrer Übermittlung an den Energieversorger in Zeitintervallen von einer Viertelstunde aggregiert werden und ein Rauschsignal beigemischt wird, um das Verbrauchsprofil zu entschärfen. Die aggregierten Daten sind dabei ausreichend genau, um den Verbrauch im Sinne des Nutzers zu steuern, aber keinerlei Rückschlüsse auf die Lebensgewohnheiten zuzulassen.

Für das Smart Metering wird in der Entschließung folglich gefordert, dass

- detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden, und
- die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen nicht davon abhängig gemacht werden darf, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Erst zusammen mit der verschlüsselten Übermittlung der Verbrauchsdaten an den Versorger erhält der Nutzer die Gewissheit, dass er Herr seiner Daten bleibt. Dazu gehört auch, dass die Verbrauchsdaten nur so lange gespeichert werden, wie dies zum Beispiel für Abrechnungszwecke notwendig ist. Außerdem müssen die Messgeräte vor Manipulation geschützt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat deshalb ein Schutzprofil entwickelt, das einen einheitlichen Sicherheitsstandard für Smart Meter schaffen soll.

Smart Meter stehen als Basistechnologie am Anfang weiterer Entwicklungsstufen, die zu sogenannten intelligenten Versorgungsnetzen (Smart Grids) führen werden. Diese Art von Verteilnetzen wird beim Übergang von zentralen zu dezentralen Energieerzeugungsanlagen zum Einsatz kommen. Nur durch größtmögliche Transparenz im Sinne des Datenschutzes kann bei den Kunden das Vertrauen in eine neuartige Technologie geschaffen werden, die zukünftig tiefgreifend unsere Lebensgewohnheiten beeinflussen wird.

4.5 Datenschutz in der Wolke? Cloud Computing

Was ist das Besondere an Cloud Computing? Die in herkömmlichen Rechenzentren zur Verfügung gestellten Rechenleistungen und Speicherkapazitäten können nur sehr begrenzt an den zuweilen stark schwankenden Bedarf der Kunden angepasst werden. Mit neuartigen Technologien wie der Virtualisierung von Rechnern und Speichern lassen sich auch sehr kurzfristig Anpassungen an unterschiedliche Lastsituationen erreichen.

Cloud Computing zeichnet sich durch die massive Konzentration von (virtualisierter) Rechenleistung und Speicherkapazität aus, sodass Cloud-Anwender diese flexibel und bedarfsgerecht über ein Rechner-

netz in einfacher Weise nutzen können. Wesentlich dabei ist, dass die technischen und organisatorischen Details des Betriebs dem Cloud-Anbieter überlassen werden. Und: der Cloud-Anwender zahlt nur für in Anspruch genommene Leistungen, seine Fixkosten reduzieren sich.

Der Cloud-Anbieter wiederum kann durch die zentrale Steuerung seine Ressourcen besser auslasten und somit seine Kosten senken. Drohenden Engpässen bei Rechner- oder Speicherkapazitäten kann er durch Verlagerung der Prozesse und Daten zwischen seinen Rechenzentren begegnen. Dazu bedient er sich besonders leistungsfähiger und hochverfügbarer Rechnernetze, vielfach mit Hilfe des Internets.

Eine Marktsegmentierung wird durch differenzierte Leistungserbringung der Cloud-Anbieter realisiert. Im Wesentlichen haben sich drei Modelle etabliert. Beim Modell *Infrastructure as a Service* (IaaS) stellt der Cloud-Anbieter die essentiellen IT-Ressourcen zur Verfügung. Hier sind Speicherressourcen, Rechnerleistung und Kommunikationsverbindungen zu nennen, wobei die Angebote nicht notwendig alle drei Hardwarekategorien umfassen müssen. Beim Modell *Platform as a Service* (PaaS) bietet der Cloud-Anbieter die Infrastruktur zur Entwicklung von Cloud-Anwendungen an. Der Anwender muss auf der Grundlage dieser Entwicklungsumgebung die für ihn relevanten Anwendungen realisieren. Dies kann sowohl auf der Service-Infrastruktur des Plattform-Anbieters als auch auf der Service-Infrastruktur von Dritten realisiert werden. Innerhalb des Modells *Software as a Service* (SaaS) bietet der Cloud-Anbieter eine oder mehrere Anwendungen als Dienstleistung an. Die Bandbreite erstreckt sich von einfachen E-Mail-Systemen für Kleingruppen bis zu Planungssystemen (Enterprise Resource Planning) für Unternehmen und Verwaltung. Aufgrund der unterschiedlichen Gestaltung der angebotenen Dienste müssen modellspezifisch Risiken betrachtet und datenschutzrechtliche Anforderungen implementiert werden. Wesentlich ist dabei, dass die Anforderungen innerhalb der Modelle realisiert werden können.

Beim Thema Cloud Computing tritt sehr deutlich hervor, dass die Regelungen des Bundesdatenschutzgesetzes ursprünglich nicht auf eine derartige Technik ausgerichtet sind und deshalb hier nicht mehr umfassend greifen (können). Denn das Bundesdatenschutzgesetz stammt konzeptionell aus der Zeit der Großrechner, als die Zuordnung von Verantwortlichkeiten noch einfach und Speicherplatz und Datenleitungen noch knapp und teuer waren. Die Virtualisierung bedingt die Auflösung der zeitlich-räumlichen Bindung der Daten und deren Verarbeitung. Der Cloud-Anwender erfährt in der Regel nicht, wo seine Daten gerade verarbeitet werden. Eine wirksame Kontrolle ist ihm damit praktisch nicht mehr möglich.

Andererseits ist der Cloud-Anwender im datenschutzrechtlichen Sinne verantwortliche Stelle und nach § 11 Absatz 1 BDSG für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen der Auftragsdatenverarbeitung verantwortlich. Er muss sich beispielsweise als Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Cloud-Anbieter als Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Faktisch hat der Cloud-Anwender allerdings nur einen sehr eingeschränkten administrativen, operativen und kontrollierenden Zugriff auf die Infrastruktur des Cloud-Anbieters, was durch die Besonderheiten des Cloud Computing bedingt ist.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher in ihrer Entschließung vom 28./29. September 2011 (vgl. Anhang 22 „offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen“ gefordert. Zudem werden transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel verlangt.

Wenn der Cloud-Anwender nicht die Mittel und Möglichkeiten hat, die ordnungsgemäße Verarbeitung seiner Daten beim Cloud-Anbieter zu überprüfen, könnten aktuelle und aussagekräftige Nachweise, beispielsweise Zertifikate von anerkannten und unabhängigen Prüfungsorganisationen, herangezogen werden. Für die Auftragserfüllung sind die Prüfergebnisse der genutzten Infrastruktur, insbesondere im Hinblick auf die Informationssicherheit, die Portabilität und die Interoperabilität, vorzulegen.

Befindet sich der Cloud-Anbieter nicht im Europäischen Wirtschaftsraum oder in der Europäischen Union, ist eine Auftragsdatenverarbeitung dann nicht möglich, wenn eine Übermittlung personenbezogener Daten in Staaten ohne ausreichendes Datenschutzniveau erfolgt. Ausnahmen sieht das Bundesdatenschutzgesetz vor, falls zum Beispiel die sogenannten Standardvertragsklauseln zur Anwendung kommen.

Aber selbst bei Nutzung von Rechenzentren in Europa sollten Cloud-Anwender im Hinterkopf behalten, was im Sommer 2011 für Schlagzeilen in einschlägigen Fachmagazinen sorgte: Soweit diese Rechenzentren von US-Firmen betrieben werden, besteht das Risiko, dass US-Sicherheitsbehörden aufgrund entsprechender US-Bestimmungen, wie etwa dem US Patriot Act, auch auf die Daten europäischer Cloud-Anwender zugreifen dürfen – Safe Harbor-Abkommen hin oder her. Dabei können die Kunden nicht einmal sicher sein, von dem Zugriff zu erfahren, denn schließlich kann das FBI gegebenenfalls mit einem National Security Letter dem amerikanischen Cloud-Anbieter ein „Redeverbot“ auferlegen. Aus meiner Sicht stellt die mögliche Datenweitergabe aus dem EU-Gebiet heraus die Inanspruchnahme derartiger Cloud-Angebote grundsätzlich in Frage.

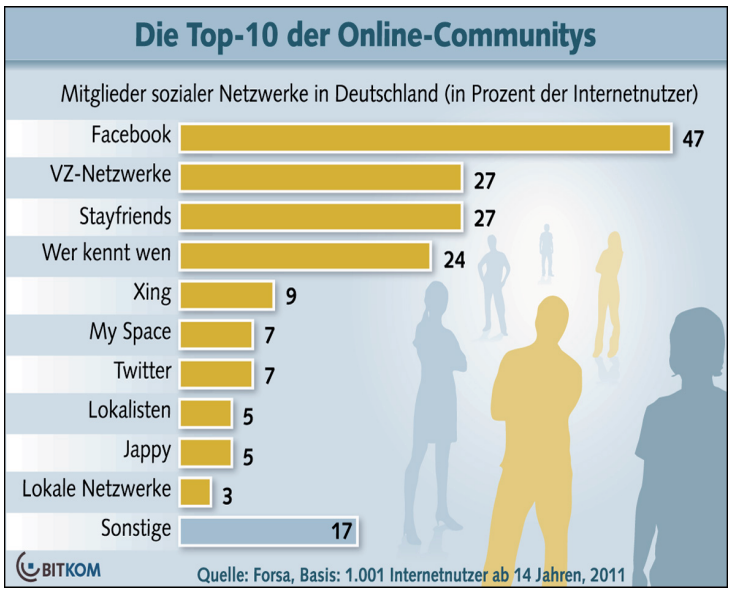
In der „Orientierungshilfe Cloud Computing“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Version 1.0, Stand: 26. September 2011) wird ausführlich auf die kurz aufgezeigten datenschutzrechtlichen Probleme eingegangen. Gerade für Cloud-Anwender, aber auch für Cloud-Anbieter, ist die Handreichung, die von meiner Homepage heruntergeladen werden kann, eine wertvolle Hilfe, um die Regelungen des Datenschutzes rechtskonform umzusetzen.

4.6 Das gefällt uns (noch) nicht – Datenschutz in sozialen Netzwerken

Soziale Netzwerke boomen: Waren im Jahr 2010 noch 30 Millionen Bundesbürger in einem solchen Netzwerk registriert, so sind es im Jahr 2011 bereits rund 40 Millionen Internet-Nutzer über 14 Jahren gewesen. Eine Steigerung um ein Drittel in nur einem Jahr! Dies geht aus einer Pressemitteilung des Branchenverbandes BITKOM vom 13. April 2011 hervor. Bei den unter 30-Jährigen sind sogar schon 96 % Mitglied einer Social Community.

Offensichtlich gibt es einen großen Bedarf, sich in sozialen Netzwerken kommunikativ auszutauschen. Die Beweggründe für die Teilnahme sind durchaus unterschiedlich. Stehen bei Facebook, Google+, Schüler VZ und anderen die privaten Beziehungen im Vordergrund, suchen bei beruflich genutzten Netzwerken wie XING, LinkedIn und vergleichbaren Anbietern die Mitglieder nach neuen geschäftlichen Kontakten oder sind in Gruppen organisiert, die gemeinsame berufliche Interessen verfolgen. Dass ein soziales Netzwerk allein offenbar nicht ausreicht, um die Bedürfnisse seiner Mitglieder vollständig abzudecken, zeigt sich daran, dass im Durchschnitt jedes Mitglied bei 2,4 sozialen Netzwerken angemeldet ist.

Nach einer BITKOM-Studie vom April 2011 ist eindeutiger Marktführer mittlerweile der US-amerikanische Anbieter Facebook; 47 % der befragten Internet-Nutzer waren dort Mitglied (siehe Grafik). Weltweit sollen es zurzeit schon mehr als eine halbe Milliarde Menschen sein.



Grafik: © BITKOM 2011

Beachtlich ist auch die Bindungswirkung, die soziale Netzwerke offenkundig entfalten: Nach einer BITKOM-Erhebung vom September 2011 verbringen deutsche Internet-Nutzer schon mehr als 16 % ihrer Online-Zeit bei Facebook; vor einem Jahr sind es erst 4,1 % gewesen. Dies zeigt, dass Facebook sich offenbar zum zentralen Anlaufpunkt im Web entwickelt hat. Im Laufe der Zeit hat Facebook immer mehr Funktionalitäten eingebunden, um die Nutzer auf seine Seiten zu ziehen. Aktuell unternimmt Facebook weitere Anstrengungen, um die Nutzer noch stärker an sich zu binden, nach Möglichkeit ein Leben lang: Mit der „Timeline“ offeriert Facebook eine Art digitales Tagebuch, das die Lebensgeschichte des Nutzers grafisch darstellen und sogar ohne sein Zutun gefüttert werden kann, insbesondere durch Applikationen (sog. Apps), die den Status des Nutzers von selbst posten sollen, also dem „Freundeskreis“ gegebenenfalls verraten, was man gerade so treibt oder wo man sich gerade aufhält.

Mit dem wachsenden Angebot an vermeintlich kostenlos zu nutzenden sozialen Netzwerken geht die Sorge der Nutzer einher: Was passiert überhaupt mit meinen Daten? In der Tat ist die Entwicklung auf diesem Gebiet so rasant, dass der Datenschutz ins Hintertreffen geraten ist und die Nutzer sich zunehmend Gedanken über die eigenen Kontrollmöglichkeiten ihrer Daten machen. Manchen ist mittlerweile bewusst geworden, dass sie die kostenlosen Angebote vielfach mit ihren eigenen Daten bezahlen, die dann zum Rohstoff für eine möglichst individuelle, auf die jeweiligen Interessen des Nutzers zugeschnittene Werbung werden. Um ein kürzlich gehörtes Bonmot zu zitieren: Wenn ein Produkt nichts kostet, kann es sein, dass man selber das Produkt ist.

Dreh- und Angelpunkt der datenschutzrechtlichen Kritik an sozialen Netzwerken ist die Missachtung des Grundrechts auf informationelle Selbstbestimmung. Dabei geht es um das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Ob er Informationen über sich im Internet veröffentlicht oder nicht, soll er selbst entscheiden. Werden seine Daten ohne seine Einwilligung veröffentlicht, soll er dagegen vorgehen können.

Die Einwilligung muss bewusst und eindeutig erteilt werden und jederzeit für die Zukunft widerrufen werden können. In einem bereits 2008 gefassten Beschluss haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich an die gesetzlichen Verpflichtungen erinnert (vgl. auch Fünfter Tätigkeitsbericht der Aufsichtsbehörde 2009, B 10.1.1, S. 168) und darauf hingewiesen, dass Anbieter sozialer Netzwerke ihre Nutzer umfassend über die Verarbeitung ihrer perso-

nenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten müssen. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

Für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung von Telemedien, wozu auch die sozialen Netzwerke zählen, dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden, sofern der Nutzer dem nicht widerspricht. Die Geschäftsmodelle der kostenfrei zu nutzenden sozialen Netzwerke beruhen aber im Wesentlichen auf der kommerziellen Vermarktung derartiger Nutzungsprofile. Insofern überrascht der Widerstand einiger Betreiber gegen datenschutzrechtliche Restriktionen nicht.

Mit sog. Social Plug-ins wie dem Like-Button von Facebook wird die Erstellung von Nutzungsprofilen sozusagen en passant ermöglicht. Ein Mausklick auf den Button und schon wird ein Cookie, eine kleine Datei, auf dem Rechner des Internet-Nutzers – in der Regel unbemerkt – abgelegt. In dem Cookie ist eine Zeichenfolge über längere Zeit gespeichert, die den Internet-Nutzer gegenüber dem sozialen Netzwerk jederzeit identifizieren soll. Auch wenn der Nutzer gar nicht bei dem sozialen Netzwerk registriert ist, so kann doch mit Hilfe des Cookies sein „Surfverhalten“ beobachtet und zum Beispiel für Werbezwecke ausgewertet werden. Wenn er sich später dann noch bei dem betreffenden Netzwerk registriert, wird aus dem Inhalt des Cookies ein personenbezogenes Datum, ohne dass der Nutzer bewusst und eindeutig eingewilligt hat, wie es das Telemediengesetz verlangt. Diejenigen, die es vorziehen, pseudonym gegenüber dem sozialen Netzwerk zu bleiben, können ihr Widerspruchsrecht de facto nicht ausüben. Es fehlt einfach ein „Widerspruchs-Button“.

Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Webseitenbetreiber verantwortlich, der Social Plug-ins in seine Webseiten einbindet. Ihm kommt die Aufgabe zu, auf die Widerspruchsmöglichkeit gegen die pseudonyme Nutzungsprofilerstellung nach § 15 Absatz 3 des Telemediengesetzes (TMG) hinzuweisen und nach § 13 Absatz 1 TMG die Nutzer seiner Webseiten über Art, Umfang und Zwecke der Erhebung und Verarbeitung personenbezogener Daten aufzuklären. Dies gilt insbesondere, wenn die bei der Interaktion mit einem Social Plug-in erzeugten Daten an das soziale Netzwerk weitergeleitet werden und im Rahmen einer Reichweitenanalyse aggregiert und statistisch aufbereitet von dort an ihn zurückfließen.

Bei sog. Fanpages, ausgestattet mit Social Plug-ins, ist die Rolle der verantwortlichen Stelle noch nicht abschließend geklärt. Facebook betrachtet sich selbst als verantwortliche Stelle, jedoch nicht deutschem Datenschutzrecht unterliegend. Allerdings gibt es nicht von der Hand zu weisende rechtliche Argumente, die auch den Fanpage-Betreiber in der Pflicht sehen. Neben der erwähnten Pflicht zur Aufklärung der Nutzer seiner Fanpage über das ihnen zustehende Widerspruchsrecht könnte eine Impressumspflicht nach § 5 Absatz 1 TMG oder nach § 55 des Rundfunkstaatsvertrages hinzukommen.

Inzwischen gibt es auch immer mehr öffentliche Stellen, die bei Facebook eigene Fanpages eröffnen und auf „moderne“ Art und Weise mit den Bürgerinnen und Bürgern kommunizieren wollen. Eine Große Kreisstadt im Lande gab neulich bekannt, auch sie zähle jetzt zu den modernen „flotten“ Kommunen. Mit dieser plakativen Bezeichnung sollte die Öffentlichkeit darüber unterrichtet werden, dass die Gemeinde soeben eine eigene Fanpage bei Facebook eröffnet hatte, auf der Neuigkeiten aus dem Rathaus oder örtliche Veranstaltungstipps nachzulesen seien. Flott, aber gedankenlos, kann ich da nur sagen. Denn auch wenn die rechtliche Verantwortung bei Fanseiten noch nicht hinreichend geklärt beziehungsweise zwischen dem fraglichen Betreiber des sozialen Netzwerks und den Datenschutzaufsichtsbehörden umstritten ist, so sollten sich gerade öffentliche Stellen ihrer Vorbildfunktion bewusst sein und darauf achten, dass sie nur solche sozialen Netzwerke in ihre Internet-Auftritte einbinden beziehungsweise dass sie selbst nur

solche Netzwerke zur Kommunikation und Außendarstellung nutzen, die die geltenden Standards nach europäischem und deutschem Datenschutzrecht einhalten. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen.

In Anbetracht der datenschutzrechtlichen Unzulänglichkeiten bei der Verwendung von Social Plug-ins und Fanpages haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 28./29. September 2011 („Datenschutz bei sozialen Netzwerken jetzt verwirklichen!“, vgl. Anhang 24) daher alle öffentlichen Stellen aufgefordert, von der Nutzung von Social Plug-ins abzusehen, die den geltenden Datenschutzregelungen nicht genügen, und auf solchen Plattformen auch keine Profilseiten oder Fanpages einzurichten. Dieser Forderung möchte ich an dieser Stelle nochmals Nachdruck verleihen.

Soziale Netzwerke sind mehr als nahezu unübersehbare Sammlungen von Profilseiten ihrer Mitglieder. Zwei Sichten auf den Datenbestand lassen sich unterscheiden: zum einen gibt es eine Sichtbarkeit zwischen den Mitgliedern, die durch entsprechende Einstellungen steuerbar ist. Wer welche Seiten ansehen oder kommentieren darf, bestimmt das Mitglied durch mehr oder weniger fein einstellbare Zugriffsrechte. Datenschutzfreundlich sind Standardeinstellungen, durch die die Privatsphäre der Mitglieder, insbesondere für neu hinzugekommene, möglichst umfassend geschützt wird. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern, dass Standardeinstellungen besonders restriktiv gefasst werden müssen, wenn sich das soziale Netzwerk an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

Zum anderen werden vom Betreiber des sozialen Netzwerks, für die Mitglieder unsichtbar, die gesammelten Daten in neue, möglicherweise nur statistisch abgesicherte, Beziehungen gesetzt. Mit den Methoden des Data-Mining können Mitglieder in Cluster zusammengefasst werden, die mehr oder weniger lukrative Zielgruppen für die Werbung darstellen. Je differenzierter diese Cluster für Werbemaßnahmen gestaltet werden können, umso größer ist der monetäre Gewinn, der sich mit den gewonnenen Daten erzielen lässt. Und je mehr Mitglieder ein soziales Netzwerk hat, umso größere und „passgenauere“ Cluster lassen sich zuschneiden.

Beabsichtigt ein Mitglied, sein soziales Netzwerk zu verlassen, sind daher die Hürden besonders hoch gelegt. Das Löschen aller Daten eines Mitglieds scheint aber bei den meisten sozialen Netzwerken ein schwieriges Unterfangen zu sein. Nach einer Pressemitteilung der Europäischen Kommission vom 16. Juni 2011 wünschen sich 75 % der Internet-Nutzer, ihre persönlichen Angaben jederzeit online löschen zu können, um so von ihrem Recht, vergessen zu werden, Gebrauch zu machen. Nicht zuletzt aus diesem Grund hat der Bundesrat am 17. Juni 2011 einen Gesetzentwurf eingebracht (BR-Drucksache 156/11), durch den der Verbraucherschutz im Internet und insbesondere bei sozialen Netzwerken verbessert werden soll. Kernanliegen ist die Schaffung zusätzlicher Pflichten für die Anbieter von Telemedien, zum Beispiel hinsichtlich der Einrichtung eines „Nutzerkontos“, das vom Nutzer jederzeit selbst gelöscht werden kann, oder hinsichtlich der Information des Nutzers über seine Rechte sowie über Inhalt und Umfang der Datenverarbeitung durch den Anbieter. Leider hat die Bundesregierung auf diese Vorschläge eher ausweichend reagiert und will die Entwicklung des Datenschutzrechts auf europäischer Ebene abwarten (vgl. Stellungnahme der Bundesregierung in BT-Drucksache 17/6765, Anlage 2).

Anfang November 2011 ist von Bundesseite die Entwicklung eines allgemeinen Kodex für soziale Netzwerke angeregt worden. Die Federführung hierfür hat der Verein der Freiwilligen Selbstkontrolle der Multimediaanbieter (FSM) übernommen. Diese Bemühungen können als Schritt in die richtige Richtung betrachtet werden. Entscheidend werden aber die erzielten Ergebnisse sein, die bei der CeBIT 2012 präsentiert

werden sollen. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) haben in diesem Zusammenhang am 8. Dezember 2011 darauf hingewiesen, dass Selbstverpflichtungen von den Aufsichtsbehörden nach § 38 a BDSG anzuerkennen sind, aber dass ungeachtet dessen die Betreiber sozialer Netzwerke bereits heute das Datenschutzrecht in Deutschland beachten müssten. Dies gelte wegen § 1 Absatz 5 Satz 2 BDSG grundsätzlich auch für Anbieter, die außerhalb des Europäischen Wirtschaftsraums ansässig sind. Der Beschluss der Aufsichtsbehörden ist in Anhang 43 nachzulesen. Unter den Aufsichtsbehörden besteht überdies Konsens, dass etwaige Selbstverpflichtungen nicht hinter den europäischen Datenschutzstandards zurückbleiben dürfen. Vorrangig sollten soziale Netzwerke größtmögliche Transparenz anstreben und in allen Punkten dem Prinzip der informierten Einwilligung folgen. Das heißt beispielsweise, dass die Voreinstellungen – etwa hinsichtlich der Weitergabe von Informationen an Dritte – zunächst möglichst restriktiv sein müssen und erst durch ausdrückliche Einwilligung des Nutzers erweitert werden dürfen (sog. opt-in). Umgekehrt wäre eine „offene“ Voreinstellung, die erst durch einen Widerspruch wieder einzugrenzen ist (opt-out), nicht rechtmäßig. Außerdem ist der Nutzer in leicht verständlicher Form darüber zu informieren, welche Daten erhoben werden und für welchen Zweck. Diese Information darf auch nicht irgendwo in umfangreichen Nutzungsbedingungen des Anbieters versteckt werden, sondern muss leicht zugänglich sein. Ferner müssen die Betroffenen ihre Ansprüche auf Auskunft, Berichtigung und Löschung einfach durchsetzen können.

Was Social Plug-ins angeht, so bin ich vorübergehend bereit, Ersatzlösungen wie zum Beispiel den von einem Verlag entwickelten und auch vom Südwestrundfunk (SWR 3) propagierten sog. Zwei-Klick-Button zu tolerieren, der vor der Aktivierung des eigentlichen Like-Buttons eine vorgelagerte Freigabe vorsieht. Ich sehe aber insbesondere die Betreiber von sozialen Netzwerken selbst in der Pflicht, die bisherigen Mängel zu beseitigen und endlich von sich aus technische Lösungen für datenschutzkonforme Voreinstellungen (privacy by default) anzubieten.

Ein besonderes datenschutzrechtliches Ärgernis ist die auf der Facebook-Plattform im Frühjahr 2011 – ohne vertiefte Aufklärung der Nutzer – eingeführte Gesichtserkennung. Dabei erstellt und speichert Facebook nach den Feststellungen meines Hamburger Kollegen biometrische Profile von Facebook-Nutzern, deren Gesichter durch andere Nutzer auf Fotos markiert („getagt“) worden sind. Durch einen Abgleich mit der so gebildeten biometrischen Datenbank werden beim Hochladen weiterer Fotos dem hochladenden Nutzer Markierungsvorschläge unterbreitet, wenn Facebook darauf Gesichter von Nutzern aus seiner „Freundesliste“ (wieder-)erkennt. Zwar lässt sich das Unterbreiten von Markierungsvorschlägen, die die eigene Person betreffen, über bestimmte Navigationspunkte umständlich deaktivieren. Die bei der Einführung der Gesichtserkennung für alle Nutzer gewählte Voreinstellung war jedoch „aktivieren“. Ob die Deaktivierung dazu führt, dass keine weiteren biometrischen Daten erhoben beziehungsweise verarbeitet werden oder gar das biometrische Profil des Nutzers bei Facebook gelöscht wird, ließ sich von der Hamburger Aufsichtsbehörde bislang nicht zweifelsfrei klären. Der Kollege in Hamburg erwägt gegenwärtig rechtliche Schritte; auf seine Pressemitteilung vom 10. November 2011 darf ich verweisen *(http://www.datenschutz-hamburg.de/news/)*.

Wer am 27. Juli 2011 die Frankfurter Allgemeine Zeitung aufschlug, bekam eine Vorahnung, was unserer Gesellschaft durch freiwillig munitionierte Gesichtserkennungssoftware blühen kann: Dort war eine Menschenmenge bei einem Musikfestival in Großbritannien abgebildet; zahlreiche Besucher hatten auf dem Foto über ihren Köpfen etwas schweben, was für Uneingeweihte wie kleine grüne Ballons oder Sprechblasen aussah. Diese Besucher hatten dem Festival-Betreiber – zugegebenermaßen freiwillig – für einen Weltrekordversuch ihr Facebook-Profilbild zur Verfügung gestellt, das mit Hilfe der Gesichtserkennungssoftware in der Menschenmenge wiedererkannt und mit dem

passenden „Tag“ versehen wurde. Für Facebook-Mitglieder waren die Namen zu lesen, für jeden Betrachter aber auch die Personen einwandfrei zu erkennen. „Gigatagging“ nennt sich das zweifelhafte Phänomen, bei dem auf Fotos von Massenveranstaltungen einzelnen Personen ihr jeweiliges Facebook-Profil zugeordnet wird, entweder durch die Betroffenen selbst oder durch Dritte. Noch arbeitet das Verfahren nicht fehlerfrei, aber nach meinem Eindruck wird es nur eine Frage der Zeit sein, bis die Fehlerrate sinkt. Die wissenschaftliche Forschung in verschiedenen Ländern arbeitet mit Hochdruck an biometrischen Bilderkennungsverfahren (vgl. hierzu auch den Beitrag im 3. Teil, Nr. 2.1), die auch aus dem Verhalten von Personen Schlüsse ziehen sollen. In Anbetracht der eingangs genannten weiten Verbreitung von sozialen Netzwerken würde die Beschränkung des Zugriffs auf registrierte Mitglieder kaum einen wirksamen Schutz bieten. Mit der biometrischen Erkennung von Individuen im öffentlichen oder halböffentlichen Raum würden auf jeden Fall weitere Freiräume der Privatheit verloren gehen.

5. Die Dienststelle in Zahlen

Durch die Zusammenlegung meiner Dienststelle mit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zum 1. April 2011 hat sich die Ausstattung mit Personal und Sachmitteln naturgemäß erheblich verändert. Da die Änderung unterjährig erfolgte und im Wege des Haushaltsvollzugs 2011 umgesetzt wurde, lässt sie sich noch nicht dem Staatshaushaltsplan 2011 entnehmen, der insoweit im Kapitel 0303 noch das Bild vor der Zusammenlegung widerspiegelt. Stimmigere Zahlen wird erst der Staatshaushaltsplan 2012 liefern können.

Im 29. Tätigkeitsbericht (LT-Drucksache 14/5500, 1. Teil, Nr. 5) hatte ich berichtet, dass meine Dienststelle zum damaligen Zeitpunkt über elf Beamtenstellen und fünf Angestelltenstellen verfügte (einschließlich meiner Stelle). Die personelle Ausstattung der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich war vor der Zusammenlegung allenfalls für Insider oder aufgrund parlamentarischer Berichtsanträge zu erkennen. So wurde insbesondere in LT-Drucksache 14/5333 berichtet, dass für die Kontrolltätigkeit der Aufsichtsbehörde 6,1 Stellen zur Verfügung stünden. In dieser Zahl, die auch Teilzeitstellen umfasste, waren allerdings noch keine Assistenzkräfte, insbesondere Schreibkräfte, eingerechnet. Im Zuge der Zusammenlegung übertrug das Innenministerium auf meine Dienststelle (nunmehr Kapitel 0103) 6,5 Stellen (einschließlich einer halben, mit einer Schreibkraft besetzten Stelle). Drei Stellen des Datenschutzreferats behielt das Innenministerium für die im Datenschutz weiterhin zu erledigenden ministeriellen Aufgaben und für andere Zwecke zurück. Erfreulicherweise stellte der Landtag im Dritten Nachtrag des Staatshaushaltsplans 2011 drei Neustellen zur Verfügung, sodass der personelle Schwund der Aufsichtsbehörde unterm Strich ausgeglichen wurde. Aktuell verfügt meine Dienststelle über 25,5 Planstellen, die allerdings im Hinblick auf vorhandene Teilzeitstellen nicht vollständig besetzt werden konnten. Hierin zeigt sich ein gewisser Nachteil der unabhängigen Stellung meiner kleinen Dienststelle, weil ich stellenmäßig vorsorgen muss, falls in Teilzeit beschäftigte Beamte ihren Anteil wieder aufstocken wollen. In der Vergangenheit war es dem Innenministerium aufgrund des großen Personalkörpers der Innenverwaltung gelungen, derartige Schwankungen mit eigenen Kapazitäten aufzufangen und mich von der Bildung von stellenmäßigen Reserven zu verschonen.

Eine gewisse Verbesserung der personellen Situation meiner Dienststelle hat sich durch die Abordnung eines Beamten des höheren Polizeivollzugsdienstes zu meiner Dienststelle ab 1. Oktober 2009 ergeben. Die Abordnung, die sich ausgesprochen bewährt hat, läuft demnächst aus. Es bleibt zu hoffen, dass die entstehende Lücke möglichst bald mit einem kompetenten Nachfolger geschlossen wird. Von einem derartigen Erfahrungs- und Wissensaustausch können beide Seiten profitieren. Ebenso erfreulich ist eine weitere Abordnung, die mir das Kultusministerium im Frühjahr 2011 noch kurz vor dem Regierungswechsel in Aussicht gestellt hatte und die zum Schuljahresbeginn 2011/2012 realisiert wurde: Seit 12. September 2011 ist

ein IT-Fachlehrer, der weiterhin themenbezogen in der Lehrerfortbildung tätig ist, zunächst für ein Jahr zu 80 % an meine Dienststelle abgeordnet. Wir hoffen, dass wir dadurch dem Ziel, Datenschutz als Bildungsziel und integralen Bestandteil der Lehreraus- und -fortbildung zu verankern, ein Stück weit näher kommen werden.

Für sachliche Verwaltungsausgaben standen mir im Jahr 2009 – wie im 29. Tätigkeitsbericht berichtet wurde – rund 65 T€ zur Verfügung. Im Jahre 2010 wurde der Sachtitel wegen meines Vorsitzes in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorübergehend aufgestockt. Im Zuge der Zusammenlegung übertrug das Innenministerium einen nach Personen bemessenen Pauschalbetrag in Höhe von 20.000 € auf das Kapitel meiner Dienststelle, durch den der mit dem Personalzuwachs verbundene gestiegene Finanzbedarf für Büroausstattung, Reisekosten, Zeitschriften, Bücher usw. aufgefangen werden soll. Im Vergleich zu der Finanzausstattung anderer Datenschutzbeauftragter ist aber immer noch die vielzitierte „schwäbische Hausfrau“ stilprägend.

Auf der „Leistungsseite“ stehen dem folgende Kennzahlen gegenüber, wobei ein Vergleich zwischen den Zahlen meiner Dienststelle und denen der Aufsichtsbehörde aufgrund der teilweise unterschiedlichen Erfassungskriterien nur bedingt möglich ist.

Die Zahlen für den öffentlichen Bereich seit Erstellung meines letzten Tätigkeitsberichts haben sich folgendermaßen entwickelt:

		2009	2010	2011	2012	2013
Anzahl der Eingaben	Soll	2000	2000	2000	2000	2000
	Ist	2532	2540	2010*		
Anzahl der Kontrollen	Soll	20	20	20	20	20
	Ist	19	25	21		
Anzahl der Beratungen	Soll	1000	1000	1000	1000	1000
	Ist	820	712	870*		

Der Rückgang der Zahl der Eingaben im Jahre 2011 ist unter anderem dadurch zu erklären, dass mit dem 1. April 2011 die Eingaben nicht mehr erfasst wurden, die zuvor – nach teilweise mühsamer Klärung der Zuständigkeiten – an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich abgegeben wurden.

Der Berichtszeitraum für den nicht-öffentlichen Bereich weicht von dem des öffentlichen Bereichs ab:

	ab 01. 07. 2009	2010	2011
Anzahl der Beschwerden	356	940	1020*
Anzahl der schriftlichen Beratungen	119	256	230*

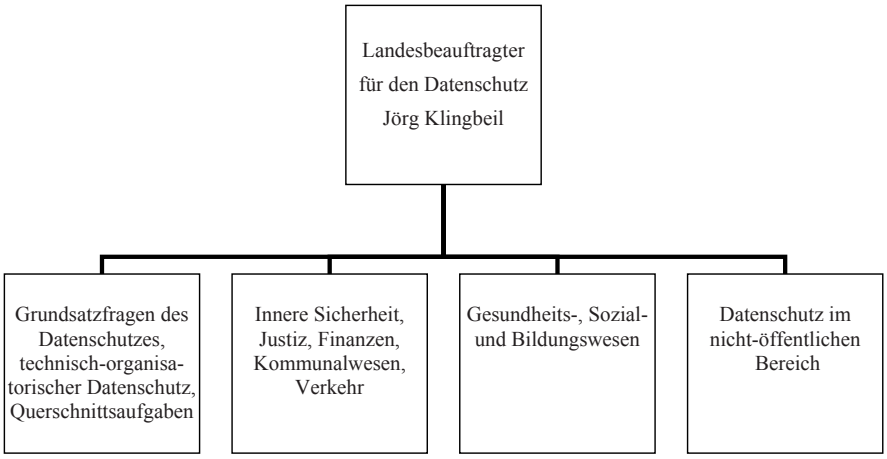
Erfasst wurden bisher nur schriftliche Beschwerden bzw. Beratungen. Die Zahl der Überprüfungen vor Ort bewegte sich in den Jahren 2009 bis 2011 jeweils fast in einer ähnlichen Größenordnung wie im öffentlichen Bereich.

Für die Zukunft werde ich mit meinen Mitarbeiterinnen und Mitarbeitern neue Kennzahlen erarbeiten, die einen besseren Überblick über die Arbeitsbelastung geben sollen. Eine Trennung in die Bereiche öffentlich bzw. nicht-öffentlich wird sich dabei nur teilweise durchhalten lassen, da viele Themen übergreifend zu bearbeiten sind.

In organisatorischer Hinsicht habe ich der gestiegenen Mitarbeiterzahl und der dadurch erweiterten Führungsspanne, aber auch der Notwendigkeit themenübergreifender Zusammenarbeit Rechnung getragen: Seit dem Umzug der Dienststelle am 24. Oktober 2011 ist meine Dienststelle daher in vier

* Hochrechnung aufgrund der Zahlen des 1. bis 3. Quartals 2011.

Referate gegliedert (vgl. Organigramm). Die Bildung eines weiteren Referats für die Aufgabenbereiche des technisch-organisatorischen Datenschutzes sowie des Medien- und Internetrechts ist beabsichtigt.



2. Teil: Öffentliche Sicherheit und Justiz

1. Abschnitt: Öffentliche Sicherheit

1. Gesetzgebung

1.1 Gesetzliche Regelungen zur Terrorismusabwehr verlängert

Bereits der 27. Tätigkeitsbericht 2006 meines Amtsvorgängers befasste sich ausgiebig mit der Rechtsetzung zur Abwehr der Gefahren des internationalen Terrorismus. Das Gesetzespaket vom 5. Januar 2007 sah unter dem Titel „Terrorismusbekämpfungsergänzungsgesetz“ eine Vielzahl von Gesetzesänderungen in vielen Bundesgesetzen vor, die vor allem den Nachrichtendiensten mehr Befugnisse zur Abschöpfung von Informationen bieten sollten. Da – wie aus der Stellungnahme des Innenministeriums zum damaligen Bericht (vgl. LT-Drucksache 14/650) zu entnehmen war – der Bundestag entgegen dem Wunsch der Länder die Gesetze mit einem Verfallsdatum zum 10. Januar 2012 versah, war wegen des drohenden Ablauftermins nunmehr eine rasche politische Einigung zwischen den verantwortlichen Bundesministerien des Inneren und der Justiz erforderlich. Der zunächst titulierte „Entwurf eines Gesetzes zur Stärkung von Rechtsschutz und Aufsicht im Bereich der Nachrichtendienste des Bundes (ND-Rechtsschutzstärkungsgesetz)“ wurde im August 2011 dem Bundesrat unter dem Titel „Entwurf eines Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes“ (BR-Drucksache 476/11) zugeleitet. Ob der Rechtsschutz mit dem Vorhaben verbessert wird, muss sich nach dem Inkrafttreten am 10. Januar 2012 erweisen, jedenfalls werden einige Gesetze und nicht nur das Bundesverfassungsschutzgesetz geändert. Inhaltlich wurde der Entwurf mit den Ergebnissen der Evaluierung des Terrorismusbekämpfungsergänzungsgesetzes begründet. Diese im Wesentlichen vom verantwortlichen Bundesministerium selbst durchgeführte Auswertung kann meines Erachtens nicht unbedingt als wissenschaftlich fundiert bewertet werden. Gerade wegen der mit den gesetzlichen Regelungen ermöglichten Eingriffe in das informationelle Selbstbestimmungsrecht wäre dies aber notwendig. Insoweit ist Artikel 9 des Gesetzentwurfs möglicherweise eine Folge der Erfahrung mit einer Evaluierung nach „Hausmacher Art“, denn er bestimmt:

> *Die Anwendung der durch das Terrorismusbekämpfungsgesetz, das Terrorismusbekämpfungsergänzungsgesetz und dieses Gesetz geschaffenen und geänderten Vorschriften des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes und des Sicherheitsüberprüfungsgesetzes ist von der Bundesregierung vor dem 10. Januar 2016 unter Einbeziehung eines oder mehrerer wissenschaftlicher Sachverständiger, die im Einvernehmen mit dem Deutschen Bundestag bestellt werden, zu evaluieren. Bei der Untersuchung sind auch die Häufigkeit und die Auswirkungen der mit den Eingriffsbefugnissen verbundenen Grundrechtseingriffe einzubeziehen und in Beziehung zu setzen zu der anhand von Tatsachen darzustellenden Wirksamkeit zum Zweck der Terrorismusbekämpfung. Die Sachverständigenauswahl muss dem Maßstab der Evaluierung gemäß Satz 2 Rechnung tragen.*

Jedenfalls hat man in dem Gesetzentwurf auf eine Weitergeltung der Regelung verzichtet, die in dem Evaluierungszeitraum des Terrorismusbekämpfungsergänzungsgesetzes nicht angewendet wurde. Dafür wurde aber eine Regelung eingeführt, die zunächst in einigen Ländern Begehrlichkeiten weckte. Denn das Bundesamt für Verfassungsschutz soll im Einzelfall Kontostammdaten beim Bundeszentralamt für Steuern abrufen können. Hier wollten einige Länder erreichen, dass dies auch den jeweiligen Landesämtern für Verfassungsschutz ermöglicht werden sollte. Aber der Bundesrat beschloss am 23. September 2011, keine Stellungnahme zu dem Gesetzentwurf abzugeben.

Wie schon in der Vergangenheit ist auch in diesem Gesetzentwurf die Kontrolle der nachrichtendienstlichen Aktivitäten der G 10-Kommission übertragen, dem eigentlich nur für die Eingriffe in das Post- und Fernmeldegeheimnis zuständigen parlamentarischen Kontrollgremium nach dem Artikel 10-Gesetz. Es ist zu hoffen, dass die Stärkung des Rechtsschutzes bei der weiteren Umsetzung nicht auf der Strecke bleibt.

1.2 Vorratsdatenspeicherung

Mit Urteil vom 2. März 2010 (1 BvR 256/08 u. a.) hat das Bundesverfassungsgericht die damaligen Regelungen zur Vorratsdatenspeicherung für nichtig erklärt. Die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten bewertete das Bundesverfassungsgericht als besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kenne.

Die Diskussion um die Wiedereinführung einer modifizierten Vorratsdatenspeicherung reißt seither nicht ab. Während sich die Innenministerkonferenz für eine Neuregelung der Vorratsdatenspeicherung aussprach, hat das Bundesjustizministerium vorgeschlagen, die bei den Telekommunikationsunternehmen bereits vorhandenen Verkehrsdaten nur anlassbezogen zu sichern („einzufrieren“, sog. quick freeze) und den Strafverfolgungsbehörden unter Richtervorbehalt eine begrenzte Zeit zur Verfügung zu stellen. Außerdem soll zur Sicherstellung von Auskünften über die Bestandsdaten von Anschlussinhabern bei Internet-Zugangsdiensten eine Speicherung von wenigen Tagen erfolgen.

Die Europäische Kommission wiederum hat wegen der Nichtumsetzung der Richtlinie über die Vorratsdatenspeicherung (006/24/EG) zwischenzeitlich ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet. Gleichzeitig befindet sich die Richtlinie in der Überarbeitung, da in einem Evaluationsbericht der Kommission vom April 2011 erhebliche Mängel bei der Zielerreichung festgestellt wurden.

Weil die Vorratsdatenspeicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung in einer Entschließung vom 17./18. März 2010 (Anhang 5) grundsätzlich abgelehnt und die Bundesregierung aufgefordert, sich für eine Aufhebung der europäischen Richtlinie über die Vorratsdatenspeicherung einzusetzen.

Es bleibt abzuwarten, wie sich die Angelegenheit auf europäischer und auf Bundesebene weiter entwickelt. Ich vertrete die Ansicht, dass das vom Bundesjustizministerium vorgeschlagene Modell „quick freeze“, das wesentlich datenschutzfreundlicher ist als die ursprüngliche Regelung der Vorratsdatenspeicherung, eine faire Chance verdient.

1.3 Nationales Waffenregister

Der Bundesgesetzgeber hat mit der Regelung in § 43 a des Waffengesetzes eine Vorgabe der Waffenrichtlinie der Europäischen Union (91/477/EWG) umgesetzt, nach der die Mitgliedsstaaten bis zum 31. Dezember 2014 ein computergestütztes Waffenregister einzuführen haben. In Deutschland wird dies schon zum Ende des Jahres 2012 Wirklichkeit. Notwendig für dieses Waffenregister ist allerdings eine gesetzliche Regelung, deren Entwurf gerade zwischen den verantwortlichen Ministerien in Bund und Ländern abgestimmt wird. Erfreulicherweise hatte das Innenministerium den übersandten Arbeitsentwurf auch meiner Dienststelle zur Verfügung gestellt, sodass ich Anregungen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) für dessen Äußerung gegenüber dem federführenden Bundesministerium des Innern geben konnte.

Der für das Nationale Waffenregister notwendige Aufwand kann nur unvollkommen in diesem Zusammenhang beschrieben werden. In Deutschland ist es erforderlich, 577 Waffenbehörden, von denen eine überdurchschnittlich hohe Zahl, nämlich 147 in Baden-Württemberg beheimatet ist und die mit höchst unterschiedlichen Verfahren bisher

ihre Register führen, auf einen Standard hin zu vereinheitlichen. Nur so wird die registerführende Behörde, das Bundesverwaltungsamt, im elektronischen Datenaustausch mit den Waffenbehörden kommunizieren können. Für den Datenaustausch zwischen Waffenbehörden und Bundesverwaltungsamt wurde daher das Verfahren XWaffe entwickelt. Außer den Angaben zu den Waffenbesitzern sollen insbesondere Angaben zu den Waffen, zu der jeweiligen waffenrechtlichen Berechtigung und zu den Gründen für die Berechtigung gespeichert werden. Diese Angaben sollen allerdings nur unter einer Ordnungsnummer gespeichert werden, die keine personenbezogenen Angaben enthalten darf. Ebenso müssen zukünftig neben den für den automatisierten Abruf berechtigten Waffenbehörden die Sicherheitsbehörden, zu denen außer den Polizeien des Bundes und der Länder die Verfassungsschutzbehörden und Nachrichtendienste, die Staatsanwaltschaften und Zollfahndungsdienststellen gehören, über die geeignete Technik verfügen.

Ein wesentlicher datenschutzrechtlicher Aspekt, der mir in dem Gesetzentwurf auffiel, war die nur unzulänglich berücksichtigte Kontrollfunktion der Landesbeauftragten für den Datenschutz. Da ein wesentlicher Teil der datenschutzrechtlichen Verantwortung für die personenbezogenen Daten trotz der Zuständigkeit des Bundesverwaltungsamts bei den hiesigen Waffenbehörden und damit bei den von meiner Dienststelle zu kontrollierenden öffentlichen Stellen liegen wird, habe ich vorgeschlagen, verschiedene Regelungen dieser gesetzlich vorgegebenen Kompetenzverteilung zwischen dem Bundesgesetzgeber und den zum Vollzug dieser Gesetzgebung verantwortlichen Länder anzupassen.

Das Nationale Waffenregister soll zukünftig aber nicht nur die Waffenbesitzer unter einem Dach zusammenführen, sondern wird auch die Hersteller von Waffen und Händler umfassen, die nach dem Waffengesetz bereits verschiedene Nachweispflichten zu erfüllen haben. Diese Nachweise sollen im Nationalen Waffenregister in einer zentralen Komponente abgebildet werden.

1.4 Rechtsgrundlagen für die Tätigkeit des Bundeskriminalamts

– Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt:

  In meinem letzten Tätigkeitsbericht hatte ich über die Änderung des Bundeskriminalamtsgesetzes berichtet, die dem Bundeskriminalamt präventiv-polizeiliche Gefahrenabwehraufgaben im Bereich des internationalen Terrorismus zugestanden hat. Diese Gesetzesänderung forderte alle diejenigen heraus, die für ein ausgewogeneres Verhältnis zwischen der Gewährleistung der Sicherheit und dem informationellen Selbstbestimmungsrecht eintreten. In dieser Hinsicht ließ das neue BKA-Gesetz erheblich zu wünschen übrig, denn – um nur einige Kritikpunkte zu nennen – es verwischte die Grenzen zwischen Polizei- und Geheimdienstmethoden noch mehr und schützte das Zeugnisverweigerungsrecht bestimmter Berufsgruppen nur unzureichend. Die Folge waren mehrere Verfassungsbeschwerden verschiedener Bürgerrechtsorganisationen, Anwalts- und Ärzteverbände, Journalisten und einiger Bundestagsabgeordneter, über die das Bundesverfassungsgericht noch zu entscheiden hat. Unter den Beschwerdeführern befindet sich auch ein ehemaliger Bundesinnenminister, der in den letzten Jahren schon wiederholt mit Verfassungsbeschwerden gegen Sicherheitsgesetze (Vorratsdatenspeicherung, Online-Durchsuchung, Luftsicherheitsgesetz, „Großer Lauschangriff“) erfolgreich war.

– Rechtsverordnung nach § 7 Absatz 6 des Bundeskriminalamtsgesetzes:

  Im Juni 2009 brachte es das Bundesministerium des Innern mit Unterstützung des Bundesrates fertig, die von den Datenschutzbeauftragten des Bundes und der Länder schon seit einiger Zeit geforderte Verordnung zu den Daten, die nach dem Bundeskriminalamtsgesetz verarbeitet werden dürfen, zu erlassen. Damit kam man gerade noch rechtzeitig, um eine drohende Niederlage vor dem Bundesverwal-

tungsgericht zu vermeiden. Es ging um die Speicherung von Daten in der Datei „Gewalttäter Sport“ (vgl. hierzu auch den Beitrag im 2. Abschnitt, Nummer 2.5). Ohne die Verordnung, deren Lektüre nur den im Gestrüpp von Verweisungen sich wohl fühlenden Lesern Genuss bereiten dürfte, wären zahlreiche Dateien des Bundeskriminalamts, die von dort zentral und im Verbund mit den Landeskriminalämtern geführt werden, ohne Rechtsgrundlage und damit kaum zu halten gewesen. Der drohende Datenverlust durch Gerichtsentscheidungen leistet für die Gesetzgebung und Politik offenbar eher Schrittmacherdienste als die rechtzeitigen Hinweise der Datenschutzbeauftragten von Bund und Ländern, leider!

1.5 Verfassungsschutz – verfassungswidrige Maßnahmen zum Schutz der Verfassung?

Durch meinen Kollegen aus Rheinland-Pfalz wurde ich darauf aufmerksam gemacht, dass dort kurz vor der Landtagswahl am 27. März 2011 eine gemeinsame Initiative aller damals im Landtag vertretenen Parteien zu einer Änderung des Landesverfassungsschutzgesetzes führte. Hintergrund war das Urteil des Bundesverfassungsgerichts vom 3. März 2004 – 1 BvR 2378/98, in dem die strafprozessualen Vorschriften zur akustischen Wohnraumüberwachung für unzureichend erklärt wurden. Die Landtagsfraktionen hatten daraufhin ein Rechtsgutachten des Wissenschaftlichen Dienstes des Landtags zur „Notwendigkeit einer Fortentwicklung verfassungsschutzrechtlicher Vorschriften“ eingeholt. Aus diesem Gutachten vom 10. Februar 2010 ergab sich wegen des Schutzes des Kernbereichs privater Lebensgestaltung gesetzlicher Änderungsbedarf, dem mit der Verabschiedung am 9. März 2011 Genüge getan wurde.

Als ich mich im Sommer 2011 beim Innenministerium erkundigte, ob eine vergleichbare Änderung im baden-württembergischen Landesverfassungsschutzgesetz vorgesehen sei, erhielt ich eine prompte, aber auch aufschlussreiche Antwort in zwei Sätzen. Zunächst wurde bestätigt, dass die Regelung in § 6 Absatz 3 des Landesverfassungsschutzgesetzes zur akustischen Wohnraumüberwachung noch nicht an die Rechtsprechung des Bundesverfassungsgerichts angepasst worden sei. Sodann wurde – nicht wirklich überraschend – darauf verwiesen, dass über den konkreten Regelungsbedarf im Rahmen eines Gesetzgebungsverfahrens zu entscheiden sei.

Bemerkenswerterweise hatte dasselbe Innenministerium im Rahmen der Novellierung des Polizeigesetzes im Jahr 2008 in der Begründung des Gesetzentwurfs zur Änderung des § 23 des Polizeigesetzes (LT-Drucksache 14/3165, S. 53) eben dieses Urteil des Bundesverfassungsgerichts angeführt. Warum nun der Polizeivollzugsdienst schon seit November 2008 auf einer verfassungsrechtlich sauberen Grundlage akustische Wohnraumüberwachungen durchführen kann, die Verfassungsschützer drei Jahre später – und über sieben Jahre nach dem Urteil – immer noch in vergleichbarer Situation aber auf einer verfassungsrechtlich renovierungsbedürftigen Rechtsgrundlage die Verfassung schützen dürfen, bleibt zumindest mir verborgen. Aber vielleicht bereitet das Innenministerium schon einen Gesetzentwurf – natürlich zunächst im Verborgenen – vor.

2. Datenverarbeitung durch Sicherheitsbehörden

2.1 1. Mai 2009 – Tag der Arbeit – mit Folgen für viele

Der Tag der Arbeit wird bundesweit immer mehr zu einem Tag widerstreitender Demonstrationen. So auch am 1. Mai 2009, für den nicht nur eine Gewerkschaftskundgebung im Ulmer Rathaus angemeldet worden war, sondern auch die Demonstration einer rechtsgerichteten Partei. Daraufhin mischten sich unliebsame „Gäste“ unter die Gewerkschaftsveranstaltung, die bewusst die Kundgebung für Auseinandersetzungen mit der Polizei und den politischen Gegnern nutzen wollten. Der Polizeivollzugsdienst bemühte sich zwar nach Kräften, gewalttätige Aus-

einandersetzungen zwischen den verfeindeten Demonstrationsgruppen zu verhindern; im Ergebnis waren aber vor allem Polizeibeamte die Angegriffenen. Das Ergebnis war vorauszusehen, es folgten polizeirechtliche und strafprozessuale Maßnahmen wie Einkesselungen, Platzverweise, Gewahrsamsanordnungen und natürlich strafrechtliche Ermittlungen wegen verschiedener Straftaten, die dann die Justizorgane beschäftigten. Die Zuständigkeit meiner Dienststelle schien zunächst nicht gefragt zu sein. In derartigen Fällen bin ich zumeist gefordert, wenn es um die Verarbeitung der personenbezogenen Daten Betroffener durch die beteiligten öffentlichen Stellen geht.

Das sollte sich 2010 ändern, als zwei zeitlich und auch räumlich weit auseinander liegende Einzelfälle meine Mitarbeiter und mich dazu veranlassten, das damalige Geschehen in Ulm näher unter die Lupe zu nehmen. In der Folge kam es zu einem Kontrollbesuch bei der Polizeidirektion Ulm und einer ausführlichen Besprechung im Landeskriminalamt. Daneben beanstandete ich die unzulässige Datenverwendung durch einen Oberbürgermeister und sprach gegenüber beteiligten Polizeidienststellen weitere Empfehlungen zum Datenschutz aus. Erfreulich war, dass Daten der beiden jungen, kommunalpolitisch aktiven Betroffenen, die zunächst nicht nur im landesweiten polizeilichen Informationssystem, sondern auch bundesweit als verdächtige Personen im Zusammenhang mit durchaus habhaften strafrechtlichen Vorwürfen gespeichert wurden, nach entsprechenden Schriftwechseln gelöscht wurden. Die beiden Betroffenen waren bei der Einkesselung von Gruppen, aus denen heraus Straftaten begangen worden waren, festgesetzt worden. Vorwürfe, dass sie sich an den Auseinandersetzungen aktiv beteiligt hatten, waren weder durch die Videoaufzeichnungen der Polizei noch durch Feststellungen der Polizeibeamten und auch nicht nach der körperlichen Durchsuchung der Betroffenen beweisbar. Damit entfiel der für die Speicherung in den polizeilichen Informationssystemen notwendige Resttatverdacht. Wie der polizeiliche Einsatzleiter als Zeuge in einem anschließend angestrengten Verwaltungsgerichtsverfahren, bei dem es um die Rechtmäßigkeit einer Ingewahrsamnahme vor einem Ausschluss aus einer Versammlung ging, auch einräumte, sei es schwierig gewesen, zwischen verschiedenen Teilen des sogenannten „Schwarzen Blocks“ – also häufig gewaltbereiten Personen, die aus einer Menschenmenge agieren – und friedlichen Versammlungsteilnehmern zu unterscheiden. Wenn dem so ist – und daran habe ich auch nach der Sichtung der Unterlagen durch meine Mitarbeiter keine Zweifel –, dann hat der Polizeivollzugsdienst die von ihm selbst erhobenen Beweismittel kritisch auf ihre Relevanz für eine Datenspeicherung zu überprüfen.

Wenn es damit sein Bewenden gehabt hätte, wäre dieser Einsatz eigentlich wegen der Vielzahl solcher Fälle in der täglichen Arbeit meiner Dienststelle kaum einer Erwähnung wert gewesen.

Aber in einem der beiden Fälle fiel bei der Durchsicht der vorgelegten Akten und Unterlagen eine Meldung von 127 Personen an das Landeskriminalamt auf, die von dort in einer bundesweiten Falldatei zur „inneren Sicherheit“ gespeichert worden waren. Diese Liste führte zwangsläufig zu der Frage, wie in derartigen Fällen die Speicherung der Daten von Demonstrationsteilnehmern begründet wird. Diese stellte sich auch das Landeskriminalamt aufgrund seiner fachaufsichtlichen Verantwortung und prüfte mit der sachbearbeitenden Polizeidirektion die Datensätze auf die rechtliche Zulässigkeit der Speicherung. Schon dies führte zu einer deutlichen Reduzierung der Zahl der gespeicherten Personen. Nachdem ich einen Kontrollbesuch durch meine Mitarbeiter für erforderlich hielt, wurden die gesamten Umstände im konkreten Fall, aber auch generell für vergleichbare zukünftige Einsätze, betrachtet und mit der betroffenen Polizeidirektion sowie dem Innenministerium und dem Landeskriminalamt erörtert.

Letztlich wurden insgesamt 50 Datensätze von den genannten 127 Personen gelöscht; bei den restlichen Personen waren die den Resttatverdacht begründenden Umstände so, dass ich aus datenschutzrechtlicher

Sicht dagegen keine Bedenken geltend machen konnte. Generell hatte sich schon vor der Erörterung im Landeskriminalamt für den Polizeivollzugsdienst die Notwendigkeit ergeben, Überlegungen für die Planung zukünftiger Einsätze anzustellen, die für die Feststellung strafrechtlich relevanter Sachverhalte und damit auch die Grundlagen der Speicherung personenbezogener Daten Auswirkungen haben werden. Dass die Anforderungen an die Qualität der Datenverarbeitung dabei erfüllt werden sollten, ist in meinen Augen eine Selbstverständlichkeit.

Der andere Fall hatte einen kommunalpolitischen Hintergrund. In einer Stadt sollte sich ein Arbeitskreis um die Aufarbeitung der nationalsozialistischen Vergangenheit kümmern und den Gemeinderat dabei beraten. An einem jungen, politisch besonders interessierten Mann entzündete sich in einer Sitzung des Gremiums der Streit über dessen Beteiligung im Arbeitskreis. Dabei kamen Vorwürfe auf, die den Vorsitzenden veranlassten, über die Verwaltung beim Polizeivollzugsdienst nach Erkenntnissen zu fragen. Was zu diesem Zeitpunkt noch niemand wusste: Auch der junge Mann war durch die eingangs genannten Ereignisse in Ulm der Polizei aufgefallen und zunächst gespeichert worden. Bei der Abfrage im Auftrag des Oberbürgermeisters, die streng vertraulich sein sollte, kümmerte sich niemand um die Frage, ob für den Zweck überhaupt eine Information beim Polizeivollzugsdienst eingeholt werden durfte. Es kam, wie es kommen musste: Die polizeilichen Erkenntnisse wurden der Stadtverwaltung mitgeteilt und dann in der – allerdings nicht-öffentlichen – Sitzung dem Gemeinderat übermittelt. Dass der Betroffene später dem Vorsitzenden dieses Gremiums erläutern musste, dass an den Vorwürfen aufgrund der Einstellungsverfügung der Staatsanwaltschaft nichts dran war, machte das Ganze nicht ungeschehen.

Für mich war der gesamte Vorgang Anlass, der Stadtverwaltung mit einer Beanstandung Nachhilfe in Sachen Datenschutz zu geben. Sowohl die Abfrage beim Polizeivollzugsdienst als auch die Übermittlung der unzulässigerweise verschafften Daten an den Gemeinderat haben das informationelle Selbstbestimmungsrecht des jungen Mitbürgers in nicht zu rechtfertigender Weise verletzt. Nicht zuletzt deshalb, weil die Speicherung der Daten mangels Grundlage unzulässig war.

Der Polizeidirektion, die nach der Rechtslage etwas besser dran ist, da sie bei Abfragen einer Stadtverwaltung nur zu prüfen hat, ob das Auskunftsersuchen im Rahmen von deren Aufgaben (zu denen die der Polizeibehörde gehören) liegt, hat auf meine Empfehlungen, zukünftig bei Abfragen von kommunalen Verwaltungen genauer hinzuschauen, in erfreulich deutlicher Weise reagiert. Es soll zukünftig darauf hingewiesen werden, dass derartige Übermittlungen nur zweckgebunden erfolgen. Denn wie diese beiden Fälle zeigen, können die für die vorbeugende Bekämpfung von Straftaten durch den Polizeivollzugsdienst gespeicherten Daten, die ebenso für Gefahrenabwehraufgaben genutzt werden dürfen, häufig nur dann qualifiziert beurteilt werden, wenn die entsprechenden Akten beigezogen werden.

Die Qualität der vom Polizeivollzugsdienst gespeicherten Verdachtsdaten muss in einem permanenten Verbesserungsprozess gesteigert werden. Dies bedingt entsprechende Zielvorgaben des Innenministeriums und die konsequente Umsetzung durch die Angehörigen des Polizeidienstes im Land.

2.2 Dienstanweisung POLAS-BW – ein Weg zu mehr Datenqualität

Als Hilfsmittel polizeilicher Verbrechensbekämpfung und -prävention kann POLAS-BW nur so gut sein, wie es die eingegebenen Daten erlauben. Sowohl aus ermittlungstaktischen Gründen als auch aus Sicht des Betroffenen ist deshalb in besonderem Maße auf die Richtigkeit, Erforderlichkeit und Zulässigkeit der einzuspeichernden Daten zu achten. Zudem ist eine unverzügliche Dateneingabe unabdingbare Voraussetzung für eine höchstmögliche Aktualität des Systems.

So endet die Einleitung der Dienstanweisung POLAS-BW, die im Juli 2011 vom Landeskriminalamt Baden-Württemberg den Dienststellen

zur Verfügung gestellt wurde. Sie fasst zusammen, was die Polizeidienststellen mit dem Landeskriminalamt in vielen Jahren an Erfahrungen in der polizeilichen Praxis mit der vorläufigen Dienstanweisung POLAS-BW gesammelt haben. Sie stellt den Leitfaden dar, der die gesetzlichen Vorgaben und die systemseitigen Anforderungen des polizeilichen Auskunftssystems für deren Nutzer erschließen soll.

Datenverarbeitung bedeutet permanente Bereitschaft, neue Entwicklungen zu erfassen und für die praktischen Bedürfnisse nutzbar zu machen. Davon ist gerade die polizeiliche Datenverarbeitung nicht ausgenommen. Die aktuelle Verfügbarkeit von wesentlichen Informationen gerade über einzelne Personen wird unter den Gesichtspunkten der vorbeugenden Straftatenbekämpfung und der Gefahrenabwehr als unverzichtbar angesehen. Für diese Informationen sind aber gesetzliche Rahmenbedingungen gesetzt, die unter dem Aspekt der datenschutzrechtlichen Zulässigkeit der Speicherung, Nutzung und Übermittlung der Daten von grundsätzlicher Bedeutung sind. Damit die polizeiliche Praxis bei der Nutzung ihrer Informationssysteme nicht nur die gesetzlichen Regelungen, sondern auch die zur Funktionsfähigkeit notwendigen internen Regelungen beachtet, werden neben den Datenschutz- und Datensicherheitskonzepten auch Dienstanweisungen erlassen, die dazu beitragen sollen, dass möglichst einheitliche Standards in jedem Arbeitsschritt von den Sachbearbeitern bis zu den Datenstationen beachtet werden. Dies hängt auch damit zusammen, dass ohne solche Vorgaben Bemühungen um eine möglichst hohe Qualität der gespeicherten Daten kaum erfolgreich sind. Nach einer längeren Diskussionsphase, in der meine Dienststelle in beispielhafter Weise mit dem Landeskriminalamt dessen Überlegungen für die endgültige Fassung der Dienstanweisung erörtern konnte, wurde diese in diesem Jahr erlassen. Ich bin insgesamt mit dieser Regelung zufrieden, auch wenn zu einzelnen Punkten anzumerken ist, dass zwischen meiner Dienststelle und der polizeilichen Praxis keine Übereinstimmung in der Beurteilung bestimmter Vorgänge zu erzielen war und vermutlich weiterhin nicht zu erzielen sein wird. Entscheidend ist aber, dass in der Zielsetzung „höchstmögliche Qualität der Datensätze“ keine Differenzen bestehen. Dieses Ziel werden weder das Landeskriminalamt noch meine Dienststelle bei der Betrachtung der vielen Einzelfälle, die auf unseren Schreibtischen zu bearbeiten sind, aus den Augen verlieren.

Zu diesen Qualitätsverbesserungsmaßnahmen gehört unbedingt die Erfassung des justiziellen Ausgangs eines Ermittlungsverfahrens. Nach der Strafprozessordnung ist die Staatsanwaltschaft verpflichtet, einer ermittelnden Polizeidienststelle den Ausgang eines von dieser geführten Ermittlungsverfahrens mitzuteilen. Wie meine Mitarbeiter in der Vergangenheit immer wieder feststellen mussten, war das entscheidende Feld in den Datensätzen häufig nicht ausgefüllt. Diese Mitteilung über den Ausgang eines Verfahrens soll aber gerade dazu dienen, die spätestens mit der Abgabe der Ermittlungsakte an die Staatsanwaltschaft erfolgte Speicherung in dem polizeilichen Auskunftssystem aufgrund des justiziellen Ergebnisses nochmals zu überprüfen und zu aktualisieren. Dies betrifft neben der Frage, ob ein Datensatz zu löschen sei, viel häufiger die weiteren Inhalte eines Datensatzes wie die Straftat, wegen der ermittelt wurde, oder ob die Löschfrist, die zunächst 60 Monate beträgt, verändert werden muss. Das Landeskriminalamt hat insoweit mein Anliegen aufgegriffen, als es inzwischen eine Änderung des Programms vorgenommen hat, welches in einer Art automatisierten Wiedervorlage den Datenstationen nach Ablauf einer angemessenen Frist die Datensätze anzeigt, in denen das entscheidende Feld nicht befüllt ist. Dann hat die Datenstation den betreffenden Sachbearbeiter zu veranlassen, den Datensatz zu überprüfen, gegebenenfalls durch Rückfrage bei der Staatsanwaltschaft den Ausgang des Verfahrens zu ermitteln. Eine generelle Verbesserung dürfte sich zukünftig dann ergeben, wenn der elektronische Datenaustausch zwischen Staatsanwaltschaft und Polizei weiter entwickelt wird. Jetzt wurde bereits die elektronische Übermittlung des staatsanwaltschaftlichen Aktenzeichens realisiert, zukünftig sollen viele Vorgänge ebenfalls auf diesem Wege erledigt werden.

Dazu gehört dann auch die Mitteilung des Verfahrensausgangs. Mehrere meiner Mitarbeiter konnten sich in einer Informationsveranstaltung, die die gemeinsame Arbeitsgruppe Justiz/Polizei für die betroffenen Dienststellen der Staatsanwaltschaften und der Polizei durchführte, über die erreichten Fortschritte informieren. Wenn es gelingt, die Vorgangsbearbeitung bei den Ermittlungsbehörden so zu gestalten, dass damit die Qualität des Datenbestandes in POLAS-BW gesteigert wird, ist dies begrüßenswert.

Eine entscheidende Aufgabe bei der Speicherung personenbezogener Daten in den polizeilichen Informationssystemen obliegt dem Prüfdienst und der Datenstation. Diese haben aus den vorgelegten Erfassungsbelegen der Sachbearbeiter und den möglicherweise schon übersandten Mitteilungen der Staatsanwaltschaften zu überprüfen, ob die Datenfelder zutreffend ausgefüllt wurden und ob die Entscheidungen über Speicherungsinhalt und Speicherungsdauer plausibel getroffen wurden. Dass dabei Anspruch und Wirklichkeit im Hinblick auf Intensität und Qualität der Überprüfung teilweise auseinanderklaffen, kann bei der Fülle der bei den Datenstationen eingehenden Erfassungsbögen nicht verwundern. Inzwischen hat eine Organisationsuntersuchung der Datenstationen stattgefunden. Als Ergebnis konnten auch qualitätssichernde Maßnahmen in die Geschäftsprozesse integriert werden. Die Umsetzung der Empfehlungen aus dieser Arbeitsgruppe erfordern aber auch noch ablauf- und aufbauorganisatorische Änderungen, die im Kontext zu der aktuell anstehenden Gesamtorganisationsuntersuchung der Polizei zu sehen seien, teilte mir das Innenministerium vor wenigen Wochen mit.

Was aber bereits jetzt erledigt werden kann, ist die kontinuierliche Fortbildung der für die Datenspeicherung eigentlich entscheidenden Sachbearbeiterebene. Gerade hier könnte ein Mehr an Sensibilität für die rechtlichen Anforderungen und eine nicht nur schematische Behandlung helfen, einerseits die Qualität der Datensätze zu verbessern, andererseits aber auch die Rechte der Betroffenen angemessen zu achten. Ich möchte hier nur zwei Beispiele erwähnen, die deutlich machen, welche Auswirkungen eine mangelnde Sensibilität haben kann:

Ein Bürger wurde beschuldigt, ein Fahrrad in einer Tiefgarage beschädigt zu haben. Dass dieses nicht absichtlich geschah, war zweifelsfrei aus den Schilderungen der Beteiligten erkennbar. Damit war der Straftatbestand der Sachbeschädigung mangels vorsätzlicher Handlungsweise nicht erfüllt und der Vorgang hätte erst gar nicht gespeichert werden dürfen. Zu allem Übel war dieser Mensch aber schon einmal viele Jahre zuvor wegen des Vorwurfs einer Straftat mit sexuellem Hintergrund verurteilt worden. Und diese Erkenntnis wurde in Übereinstimmung mit den rechtlichen Vorgaben für 20 Jahre gespeichert. Da diese Straftat auch in dem bundesweiten Kriminalaktennachweis (KAN) gespeichert war, wurde nach dem teilweise üblichen Schema „einmal KAN, immer KAN“ die (fahrlässige) Sachbeschädigung für zehn Jahre gespeichert. Nach einigen schriftlichen Bemühungen gelang es, diesen Teil des zu dem Betroffenen gespeicherten Datensatzes zu löschen. Grundsätzlich bin ich der Auffassung, dass nur die Vorgänge im bundesweiten KAN gespeichert werden dürfen, die in jedem Einzelfall die Kriterien für die Aufnahme in diesem Aktennachweis erfüllen und nicht jede Straftat, vor allem wenn wie in diesem Fall nur einmal die Voraussetzungen für die Erfassung des Bürgers im KAN vorgelegen hatten. In diesem Punkt konnte ich mit dem Landeskriminalamt bei der Abfassung der neuen Dienstanweisung für das polizeiliche Auskunftssystem leider keine völlige Übereinstimmung erzielen.

Zwischen dem Landeskriminalamt und meiner Dienststelle wird immer wieder diskutiert, ob in den bundesweiten Dateien gespeicherte Erkenntnisse zu einer betroffenen Person für die Wiederholungsprognose und vor allem für die Frage der Verlängerung der Speicherfrist genutzt werden können. Ein sicherlich bisher einmaliger Fall wurde im Rahmen eines Kontrollbesuchs aufgedeckt. Die betroffene Person hatte sich mehrfach an meine Dienststelle gewandt, da sie die Speicherungsinhalte als unzutreffend ansah. Zu einem bereits Jahre zurückliegenden Vor-

fall, der dieser Person eine Verurteilung einbrachte, hatte die Polizeidienststelle einen erkennungsdienstlichen Datensatz angelegt. Die zugehörigen Unterlagen wurden nach einiger Zeit wegen fehlender Notwendigkeit vernichtet und der Datensatz in dem landesweiten System gelöscht. Dieser Datensatz wurde auch in dem bundesweiten System gespeichert. Nach der Löschung im Landessystem erfolgte aber keine Löschung in dem Bundessystem. Vielmehr erklärt sich das Bundeskriminalamt in derartigen Fällen zum Datenbesitzer mit Hinweis auf den früheren Vorbesitzer. Als nun die Akte im Rahmen der fristgerechten Aussonderungsprüfung des Speicherungsinhalts auf den Tisch des Sachbearbeiters kam, entschied dieser aufgrund der vorhandenen Speicherung in dem Bundessystem eine Verlängerung der Speicherung für weitere drei Jahre zu veranlassen. Wie die Polizeidienststelle aber bereits bei der Anforderung der Akte durch meine Dienststelle erkannte, war der Sachbearbeiter bei seiner Entscheidung einem klassischen Zirkelschluss erlegen. Die Speicherung in dem Bundessystem betraf allein die erkennungsdienstliche Behandlung, die im Lande schon längst gelöscht war. Konsequenterweise wurde der gesamte Speicherungsinhalt vor der Vorlage der Akten an meine Dienststelle sofort gelöscht und auch das Bundeskriminalamt um Löschung des erkennungsdienstlichen Datensatzes gebeten.

Auch diese – zugegebenermaßen extremen – Einzelfälle belegen für mich die Notwendigkeit einer kritischen Auseinandersetzung jedes einzelnen Sachbearbeiters im Polizeivollzugsdienst mit den Voraussetzungen einer Datenspeicherung. Dies ist nicht nur im Interesse der Betroffenen, sondern auch der anderen polizeilichen Nutzer der Informationen im Rahmen ihres gesetzlichen Auftrags.

Worauf es trotz aller Vorgaben und Regelungen entscheidend ankommt, ist die Bereitschaft jedes Einzelnen, daran mitzuarbeiten, dass die einleitend genannten Ziele bei der Nutzung der polizeilichen Informationssysteme verwirklicht werden.

2.3 Die Prüffallregelung nach § 38 Absatz 2 des Polizeigesetzes auf dem datenschutzrechtlichen Prüfstand

Im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, 2. Teil, 1. Abschnitt, Nr. 1.1) hatte ich mich mit der vom Landtag im November 2008 verabschiedeten Änderung des Polizeigesetzes befasst und vor allem grundsätzliche Bedenken gegen die nunmehr in § 38 Absatz 2 des Polizeigesetzes (PolG) enthaltene Prüffallregelung erhoben. Diese Bestimmung lautet:

> *Zur vorbeugenden Bekämpfung von Straftaten ist die Speicherung, Veränderung und Nutzung personenbezogener Daten bis zu einer Dauer von zwei Jahren erforderlich, wenn aufgrund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person eine Straftat begangen hat. Ein solcher Verdacht besteht nicht, wenn die betroffene Person im Strafverfahren rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen sie unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt ist und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Straftaten nicht oder nicht rechtswidrig begangen hat.*

Im Klartext heißt dies: Wenn ein Bürger im Verdacht steht, eine Straftat begangen zu haben, und keine Prognose über eine erneute Straffälligkeit gegeben werden kann, weil er weder bisher vergleichbar aufgefallen war noch aus der einen Tat auf weitere Taten geschlossen werden kann, so können dennoch seine Daten bis zu zwei Jahren in dem landesweiten polizeilichen Auskunftssystem POLAS-BW gespeichert werden. Ich halte diese Datensammelei auf Vorrat nach wie vor für verfassungsrechtlich bedenklich, weil sie das Prinzip der Gefahrenabwehr, aber auch die in das Polizeirecht allmählich eingesickerte Idee der vorbeugenden Straftatenbekämpfung unterläuft. Für die Abwehr von Gefahren ist das Vorliegen einer Gefahr beziehungsweise die Prognose eines

Schadenseintritts unverzichtbar, ebenso für das Ziel, durch polizeiliche Maßnahmen einer künftigen Straftat vorzubeugen. Wenn eine solche Prognose nicht abgegeben werden kann, dann liegt streng genommen keine drohende Gefahr vor, vor der es die Allgemeinheit zu schützen gilt. Es ist auch daran zu erinnern, dass bevor es diese gesetzliche Regelung gab – derartige Vorgänge weitgehend nur statistische Relevanz hatten, das heißt als sogenannte PKS-Fälle (PKS = Polizeiliche Kriminalstatistik) für eine deutlich kürzere Dauer gespeichert wurden und für Auskünfte aus dem polizeilichen Informationssystem grundsätzlich nicht zur Verfügung standen.

Nachdem die gesetzliche Prüffallregelung aber nun einmal vom Landesgesetzgeber in die Welt gesetzt worden ist, kann ich ihre Anwendung weder stoppen noch ignorieren. Daher stand für mich und meine Mitarbeiter nach der technischen Umsetzung durch das für die polizeiliche Datenverarbeitung verantwortliche Landeskriminalamt im Februar 2009 die stichprobenweise Kontrolle der praktischen Anwendung auf dem Programm. Ausgewählt wurde dabei eine große Dienststelle mit entsprechendem Einzugsbereich und eine Dienststelle im ausgeprägt ländlichen Raum. Ausgangspunkt der Kontrolle war zunächst die summarische Erhebung geeigneter Fälle, in denen nur ein einziger Vorgang gespeichert war, durch einen entsprechenden Rechenlauf des Landeskriminalamts. Für die Kontrolle der ersten Dienststelle baten wir um Mitteilung aller in einem bestimmten Zeitraum gespeicherten Fälle, differenziert nach den unterschiedlichen Fristen für die Aussonderungsprüfung nach § 38 Absatz 4 PolG in Verbindung mit § 5 der Durchführungsverordnung zum Polizeigesetz (DVO PolG). Nach diesen Bestimmungen können Daten bis zu zwei Jahren (bei Kindern unter bestimmten Voraussetzungen), drei Jahren (sogenannte Fälle geringer Bedeutung), fünf Jahren (Normalfrist für alle Vorgänge), zehn Jahren (überregional bedeutsame Delikte, gewerbs- oder gewohnheitsmäßige Delikte, besonders schwere Delikte) oder sogar für zwanzig Jahre (Delikte mit sexuellem Hintergrund) gespeichert werden. Nach den vorab schon mitgeteilten Summen in den einzelnen Gruppen nach den Fristen wurde dann für jede Gruppe ein Stichprobenmaßstab festgelegt, sodass sich 250 Fälle ergaben. Von diesen wurden insgesamt 123 Fälle überprüft, die sich auf typische, massenweise vorkommende Delikte wie „Beleidigungen“, „Ladendiebstahl“, „Körperverletzung“, „allgemeine Betäubungsmittelkriminalität nach § 29 des Betäubungsmittelgesetzes“ und „Beförderungserschleichung“ bezogen. Für die zweite Dienststelle baten wir nach den Erfahrungen in der ersten Dienststelle um die Übermittlung aller Fälle mit einer einzigen Eintragung aus dem Bereich der vorgenannten Delikte für einen vergleichbaren Zeitraum, jedoch ohne das Delikt „Beförderungserschleichung“, da es im ländlichen Raum eher selten vorkommen dürfte. Aus den insgesamt 1257 Fällen wurden dann 130 Fälle für die Kontrolle vorgesehen. Dabei wurde gerade nach den Erfahrungen in der ersten Dienststelle ein Augenmerk auf die Speicherung der Daten von strafunmündigen Kindern zwischen dem 7. und 14. Lebensjahr gelegt, für die es nach den allgemeinen Speicherungsvoraussetzungen darauf ankommt, dass gerade kein kindtypisches, entwicklungsbedingtes Fehlverhalten vorliegt und Anhaltspunkte für die Begehung weiterer Straftaten gegeben sind. In diesem Fall können auch die Daten von Kindern für die Dauer von zwei Jahren gespeichert werden. Da die Prüffallregelung aber keine Wiederholungsprognose voraussetzt, wurde, ohne dass dies im Gesetz oder gar in der Gesetzesbegründung (vgl. LT-Drucksache 14/3165, S. 73 f.) explizit berücksichtigt worden wäre, die Dauer der Speicherung von Kindern durch den Einführungserlass des Landeskriminalamts aus dem Januar 2009 auf ein Jahr begrenzt.

Beiden Dienststellen wurde nach dem Kontrollbesuch Gelegenheit gegeben, zu kritischen Anmerkungen meiner Mitarbeiter in Bezug auf die Speicherungsgründe, die Aussonderungsprüffristen, die Wiederholungsprognose bei Datenspeicherungen von mehr als zwei Jahren, die Gründe für eine Speicherung im bundesweiten Kriminalaktennachweis (KAN) oder zu der Verneinung eines kindtypischen, entwicklungsbedingten Fehlverhaltens bei Kindern noch einmal vertiefend Stellung zu nehmen.

Die daraufhin übermittelten Ergebnisse der erneuten Überprüfung durch die speichernden Stellen waren für mich nachvollziehbar. Die in einem Teil der überprüften Fälle erfolgten Veränderungen an den Datensätzen, die von der Löschung bis zur deutlichen Verringerung der Speicherfristen reichten, bestätigten mir allerdings, dass die polizeiliche Speicherpraxis von den Verantwortlichen dennoch verbessert werden kann. Hierfür wäre allerdings auch eine Verstärkung der personellen Ressourcen notwendig.

Die im Rahmen der Kontrollen festgestellte Speicherpraxis in Bezug auf Kinder verdient eine etwas eingehendere Betrachtung: Bei Kindern, also noch nicht Strafmündigen, werden Ermittlungsverfahren von der Staatsanwaltschaft unter Hinweis auf § 152 Absatz 2 der Strafprozessordnung eingestellt. Für die ermittelnden Polizeibeamten stellt sich dann hinsichtlich der Datenspeicherung die Frage, ob die Handlung des Kindes noch als kindtypisch und entwicklungsbedingt einzuordnen ist oder nicht. In diesen Fällen haben meine Mitarbeiter vor allem die Erkenntnisse überprüft, die einerseits in den Ermittlungsakten (E-Akten) und andererseits in den Kriminalakten (K-Akten), die vor allem als Aktenrückhalt für die in den Informationssystemen gespeicherten Daten eines Betroffenen von Bedeutung sind, dokumentiert waren. Dabei fielen in diesem Zusammenhang überraschende Formulierungen beziehungsweise Wertungen auf. So kam es beispielsweise vor, dass in den Ermittlungsergebnissen auch festgehalten wurde, ob das Kind in geordneten Verhältnissen lebt, ob es durch die Eltern wegen der Tat sanktioniert wurde oder durch die Ermittlungen hinreichend beeindruckt schien. Teilweise wurde schon vermerkt, dass mit weiteren Straftaten nicht gerechnet werden muss; nach Eingang der Verfahrensnachricht der Staatsanwaltschaft über die Einstellung konnte es dann in dem Erfassungsbogen für die Datenspeicherung aber entgegen der bisherigen Darstellung heißen, dass nicht nur der Tatverdacht, sondern auch die Wiederholungsgefahr gegeben sei, die mit Begriffen wie „Umfeld“, „polizeiliche Erfahrung“ oder ähnlichen begründet wurde. In solchen Fällen wurde dann aber – inkonsequent nach der Rechtslage – nur für ein Jahr gespeichert, also die Prüffallregelung angewendet, obwohl diese gerade keine Wiederholungsprognose voraussetzt.

Eine Dienststelle sah in der festgestellten Diskrepanz zwischen dem Inhalt der für die Staatsanwaltschaft gefertigten Aktenvermerke und der im Rahmen der Aussonderungsprüfungen abgegebenen Wiederholungsprognose einen Anlass, diesen Befund mit den Jugendsachbearbeitern zu erörtern. Nach ihrer Ansicht war die Anwendung der Prüffallregelung bei den meisten Ersttätern – abhängig von den jeweiligen Erkenntnissen zur Person – naheliegend. Die bei der Begründung einer Wiederholungsgefahr häufig gebrauchten erwähnten Standardhinweise seien aber ohne Aktenvorlage nur schwer nachvollziehbar, weshalb die Angaben auf dem Prüfformular künftig konkretisiert werden sollten, insbesondere wenn die Umstände aus dem Aktenrückhalt nicht ersichtlich seien.

Die andere Dienststelle räumte zu den Nachfragen meiner Mitarbeiter ein, dass die Dokumentation von Änderungen an den Datensätzen verbessert werden könne. Zu der Speicherung von Daten zu Kindern im Alter von 7 bis 14 Jahren fehlte in einigen Fällen die nachvollziehbare Erläuterung, warum kein kindtypisches Fehlverhalten angenommen wurde. Diese Dienststelle wies auf aus dem Sachverhalt erkennbare Tatsachen wie den Wert des erlangten Gegenstands oder auf spezifische Verhaltensweisen hin, die untypisch für Kinder seien. Ich halte es in solchen Fällen aber für richtig, dass das Nichtvorliegen eines kindtypischen Fehlverhaltens durch den Sachbearbeiter näher zu begründen ist.

Bei der Erfassung von Fällen geringer Bedeutung kommt es nach der Regelung in § 5 Absatz 3 DVO PolG zunächst darauf an, ob der Einzelfall dem Regelkatalog zuzuordnen ist. Soweit Begehungsformen und Umstände, die selbst bei geringer Schadenshöhe beispielsweise eine gewerbs- oder gewohnheitsmäßige Tatbegehung begründen können, belegbar sind, gibt § 5 Absatz 4 DVO PolG die Möglichkeit, die Normal-

frist von fünf Jahren für die Speicherung des Vorgangs festzulegen. Insoweit bestand auch Konsens mit der kontrollierten Dienststelle.

In beiden Fällen habe ich die allgemeinen Erläuterungen und die in den angesprochenen Einzelfällen getroffenen nachträglichen Entscheidungen der kontrollierten Dienststellen uneingeschränkt akzeptieren können, zumal die Datenspeicherungen größtenteils korrigiert wurden. Ich bin davon überzeugt, dass unsere Prüfungsbemerkungen bei den betroffenen Mitarbeiterinnen und Mitarbeitern der Dienststelle bis hin zur Leitungsebene das Gespür für die Bedeutung einer korrekten Datenverarbeitung verbessert haben. Dass es noch weitere Zeit braucht, bis alles gut wird, ist mir wohl bewusst.

Aus diesen Erkenntnissen möchte ich durchaus eine generelle Schlussfolgerung zu der Qualität der Datenspeicherungen ziehen:

- *Ein schlüssiges Aus- und Fortbildungskonzept sowie ein Fortbildungsangebot, das von den Polizeibeamten auch angenommen wird, könnten wesentlich zu einer Verbesserung der Datenqualität beitragen.*
- *Die teilweise mangelnde Qualität dürfte vor allem an der – durch welche Umstände auch immer verursachten – unzureichenden Schulung der Sachbearbeiter liegen. Dabei geht es einerseits um die Veranlassung der Speicherung oder die Aussonderungsprüfung, andererseits um die Nachvollziehbarkeit dieser Entscheidungen durch Prüfdienst und Datenstation.*
- *Insoweit kommt es entscheidend auf die personelle Ausstattung des Prüfdienstes und der jeweiligen Datenstation an, die die vom Sachbearbeiter vorgegebenen Daten auf Richtigkeit und Plausibilität zu prüfen haben.*
- *Auf die Dokumentation im Aktenrückhalt ist von allen Beteiligten ein besonderes Gewicht zu legen, damit nicht nur Sachbearbeiter und erfahrene Mitarbeiter in der Datenstation erkennen, welche Entscheidung warum getroffen wurde. Die sogenannte E-Akte und die für die Datenspeicherung als Aktenrückhalt geführte K-Akte unterscheiden sich in ihrem Umfang, abhängig vom jeweiligen Einzelfall, manchmal ganz erheblich. Die Dokumentation in der K-Akte ist übrigens der wesentliche Anknüpfungspunkt für eine datenschutzrechtliche Kontrolle. Daher sind in der Dienstanweisung POLAS-BW in einem Anhang auch ausdrücklich Beispiele für die Begründung einer Wiederholungsgefahr aufgelistet worden, damit eine qualifiziertere interne Überprüfung vor der erstmaligen oder wiederholten Speicherung eines Datensatzes möglich ist.*

Das Innenministerium hat mich kürzlich über die im Rahmen der polizeilichen Aus- und Fortbildung angebotenen Inhalte und Seminare zu allen Themen rund um Datenschutz und Datenverarbeitung unterrichtet. Abstrakt klingt die Darstellung durchaus schlüssig. Konkret habe ich aber Zweifel, ob der Vermittlung derartiger Inhalte, die für die originäre Aufgabenerfüllung der Polizei ebenso wichtig sind wie die Beachtung der Betroffenenrechte, genügend Raum verschafft wird. Wichtig wäre aus meiner Sicht, dass Veranstaltungen zu Datenschutzthemen nicht nur regelmäßig angeboten, sondern auch entsprechend angenommen werden. Hierfür bedarf es auch der intensiven Unterstützung des Themas durch die Führungskräfte der Polizei auf allen Ebenen. Ergänzend könnten die bei den Polizeidienststellen ausnahmslos bereits vorhandenen behördlichen Datenschutzbeauftragten als Multiplikatoren wirken.

Eine gewisse Hoffnung setze ich in Bezug auf eine Qualitätsverbesserung der polizeilichen Datenverarbeitung übrigens auch in die laufende Organisationsuntersuchung der Datenstationen in den Polizeidienststellen und in die anstehende Gesamtorganisationsuntersuchung der Polizei. Für die neue Landesregierung böten diese jedenfalls eine gute Gele-

genheit, eingefahrene Gleise der polizeilichen Datensammelei, zum Beispiel hinsichtlich der Bagatelldelikte, zu verlassen oder zumindest mit dem Ziel der Reduzierung des erheblichen Aufwands auf den Prüfstand zu stellen.

2.4 Videoüberwachung bei der Polizei – wofür ist sie wirklich geeignet?

Videoüberwachung ist ein alltägliches Thema auf Bahnhöfen, in Supermärkten und Kaufhäusern, im öffentlichen Personennahverkehr, in Parkhäusern und Tiefgaragen und bei vielen anderen Nutzern. Die Videotechnik ist auch bei der Polizei von großer Bedeutung, zu allererst für die Dokumentation von strafrechtlichem oder ordnungswidrigem Verhalten. Aber auch für die Lenkung großer Einsätze durch eine abgesetzte Führungs- und Einsatzzentrale oder für die Überwachung des Zugangs zu den Räumlichkeiten, die von der Polizei genutzt werden, wird diese Technik inzwischen auf breiter Front eingesetzt. Da die Polizei als staatliche Stelle über weitgehende Eingriffsbefugnisse verfügt, ist jedoch im Vergleich mit anderen Videoüberwachungen stets ein besonders kritischer Blick angezeigt.

Die Rechtslage für den Einsatz von Videokameras durch die Polizei ist inzwischen durch gesetzliche Regelungen und die Rechtsprechung weitgehend geklärt. Mit der letzten Änderung des Polizeigesetzes wurde auch eine Rechtsgrundlage dafür geschaffen, dass die Gewahrsamszellen, in die oft genug Personen aus Gründen des Eigenschutzes oder zur Verhinderung von Fremdgefährdungen verbracht werden müssen, mit Hilfe einer Kamera beobachtet werden können.

Kurz gefasst ist ein Eingriff in das informationelle Selbstbestimmungsrecht eines Einzelnen gegeben, wenn diese Überwachung mehr ermöglicht, als nur eine Menschenmenge ohne Identifizierung des Einzelnen zu beobachten und gegebenenfalls diese Aufnahmen zu speichern. Das Verwaltungsgericht Berlin und das Oberverwaltungsgericht Nordrhein-Westfalen haben in zwei Entscheidungen des letzten Jahres deutlich gemacht, dass nur für die Lenkung des Einsatzes genutzte Kameras ohne Bildaufzeichnung, die von der Polizei vor Demonstrationszügen mitgeführt wurden, eine Einschränkung der persönlichen Freiheit der Teilnehmer dann darstellen, wenn gerade die in unmittelbarer Nähe solcher Kameras befindlichen Personen ohne Weiteres erkennbar sind. Damit war der Einsatz der Kameras nach Auffassung der beiden Gerichte rechtswidrig (VG Berlin, Urteil vom 5. Juli 2010 – 1 K 905.09; OVG NRW, Beschluss vom 23. November 2010 – 5 A 2288/09).

Ein Eingriff in das informationelle Selbstbestimmungsrecht und bei Versammlungen und Aufzügen in das Grundrecht auf Versammlungsfreiheit ist bereits dann gegeben, wenn die technischen Gegebenheiten es zulassen, beispielsweise durch den Einsatz von Kameras mit Zoomfunktion, Personen oder Gegenstände so aufzunehmen, dass eine Person identifizierbar wird, selbst wenn keine Aufzeichnungen angefertigt werden.

Ob ein solcher Eingriff zulässig und erforderlich ist, ist anhand der Rechtslage und den im Einzelnen gegebenen Umständen zu beurteilen. So hatten sich meine Mitarbeiter im Berichtszeitraum insbesondere um Videoüberwachungen gekümmert, die in Mannheim seit 2001 mit der Kriminalitätsbekämpfung im Innenstadtbereich und in Stuttgart im Zusammenhang mit den Demonstrationen gegen das Projekt „Stuttgart 21“ mit der Lenkung der polizeilichen Einsätze begründet wurden. Außerdem wurde das Innenministerium zum Umsetzungsstand der Videoüberwachung in Gewahrsamszellen befragt.

– Mannheim – Nach schwierigen Anfängen zum Musterbeispiel entwickelt!

Im Tätigkeitsbericht 2001 hatte mein Vorvorgänger im Amt von den diversen Schwierigkeiten aus datenschutzrechtlicher Sicht berichtet, die die Videoüberwachung in der Mannheimer Innenstadt bereitet hatte. Damals hatten die Stadt und das Polizeipräsidium verschiedene Örtlichkeiten bestimmt, in denen nach dortiger Auffassung eine Vi-

deoüberwachung zur präventiven Kriminalitätsbekämpfung geboten schien. Im 29. Tätigkeitsbericht 2009 konnte ich bereits über die Fortschritte berichten, die diese erste Mannheimer Maßnahme erreicht hatte. Bereits 2007 konnten die Kameras an den Beobachtungspunkten in der Innenstadt stillgelegt werden, da sich das Kriminalitätsgeschehen positiv entwickelt hatte, es hatte nämlich deutlich ab- und erfreulicherweise nicht wieder zugenommen. Die Beobachtung wurde daher auf die später begonnene Überwachung des Willy-Brandt-Platzes vor dem Hauptbahnhof konzentriert, weil dort das Kriminalitätsgeschehen immer noch signifikant ausgeprägter ist als in allen anderen Bereichen der Stadt. Bei einem Kontrollbesuch konnten meine Mitarbeiter feststellen, dass fast alle datenschutzrechtlichen Vorgaben, die § 21 des Polizeigesetzes (PolG) und § 48 PolG in Verbindung mit § 9 LDSG für solche Videoüberwachungen festlegen, eingehalten wurden. Allein die Lesbarkeit der Hinweise für die aus dem Hauptbahnhof kommenden Passanten war behindert, da die Beschriftungen der Deutschen Bahn AG auf den automatisch öffnenden Türen diese Hinweise stets verdeckten. Dieses Hinweisproblem wurde nach entsprechenden Kontakten mit dem Unternehmen durch das Polizeipräsidium und die Stadt behoben. Entscheidend für die präventive Wirkung dieser Videoüberwachung ist aber weiterhin die unmittelbare Interventionsmöglichkeit bei erkannten Gefahren oder Straftaten durch das nahegelegene Polizeirevier.

– Stuttgart 21 – Was kann und was darf wo und warum aufgenommen werden?

  Die Auseinandersetzungen um die Realisierung des Projektes „Stuttgart 21“ sind hinreichend bekannt. Dass es dabei auch um den Datenschutz gehen kann, wurde uns klar, als uns das Polizeipräsidium Stuttgart an seinen Überlegungen beteiligte. Ich wurde nämlich darüber informiert, in welchem Umfang eine Videoüberwachung der Umgebung des Hauptbahnhofs geplant sei. Außerdem erreichten mich mehrere Anfragen besorgter Bürger, die sich nach dem polizeilichen Videoeinsatz erkundigten und ihre Rechte zum friedlichen Protest in Gefahr sahen.

  Soweit das Polizeipräsidium zur Lenkung des Einsatzes rund um den Hauptbahnhof mittels Videoüberwachung Übersichtsaufnahmen nutzt, bestehen keine durchgreifenden datenschutzrechtlichen Bedenken dagegen, da dieser Maßnahme der Eingriffscharakter fehlt. Anders wird es jedoch dann, wenn die technische Möglichkeit vorhanden ist, aus der Übersichtsaufnahme auf bestimmte Personen oder einer Person zuzuordnende Sachen zu zoomen, um entsprechende Informationen zu gewinnen. Wenn diese technische Möglichkeit mit dem eingesetzten System zwar möglich ist, aber nur nach entsprechenden Weisungen genutzt werden darf, ist es nach meiner Auffassung trotzdem geboten, den überwachten Bereich nach § 21 Absatz 5 PolG zu kennzeichnen. Interessant waren für mich beispielsweise Presseberichte über die Polizeidirektion Hannover, die in einem verwaltungsgerichtlichen Verfahren im Juli 2011 verurteilt worden war, für eine entsprechende Kennzeichnung der in Hannover videoüberwachten Bereiche zu sorgen. Sie verzichtete auf eine Berufung gegen das Urteil und beschaffte Klebefolien mit einer entsprechenden Aufschrift, um in den jeweils überwachten 43 Bereichen geeignete Masten zu beschildern. Ich werde daher weiter mit dem Polizeipräsidium in Kontakt bleiben, um zu klären, ob ein vergleichbarer Aufwand nicht auch in Stuttgart im Umfeld des Hauptbahnhofs leistbar wäre.

  Anders ist der Videoeinsatz zu beurteilen, wenn Angehörige des Polizeivollzugsdienstes, die durch ihre Uniformen zweifelsfrei erkennbar sind, diese Technik nutzen, um während des Einsatzes Störungen im polizeirechtlichen oder versammlungsrechtlichen Sinn oder die Begehung von Straftaten aufzuzeichnen. Diese Datenerhebungen sind bei Vorliegen der einschlägigen Voraussetzungen sowohl nach § 21 PolG als auch nach §§ 12 a, 19 a des Versammlungsgesetzes sowie nach § 163 der Strafprozessordnung zulässig. Die von diesen

Polizeibeamten angefertigten Aufzeichnungen werden ungekürzt für eine gewisse Zeit gespeichert, um nicht nur den jeweiligen Vorwurf gegenüber einem Betroffenen belegen zu können, sondern auch möglichen Manipulationsvorwürfen zu begegnen. In Hinblick auf die einleitend erwähnten Urteile der Verwaltungsgerichte in anderen Ländern wurde von den Verantwortlichen des Polizeipräsidiums versichert, dass die dort festgestellten Grundsätze bei der Begleitung von Demonstrationszügen beachtet würden.

– Gewahrsamszellen – Ort für kurze, aber sichere Aufenthalte

Es ist sicher nicht ein Ort erster Wahl, wenn man im polizeilichen Gewahrsam untergebracht wird. Häufig dürfte er nur wenige Stunden dauern, denn zumeist trifft es hilflose Personen, die sich selbst in diese Lage gebracht haben.

Der polizeirechtliche Gewahrsam nach § 28 Absatz 1 PolG kann nach dem Gesetzeswortlaut gegenüber einer Person angeordnet werden, wenn

1. *auf andere Weise eine unmittelbar bevorstehende erhebliche Störung der öffentlichen Sicherheit oder Ordnung nicht verhindert oder eine bereits eingetretene erhebliche Störung nicht beseitigt werden kann, oder*
2. *der Gewahrsam zum eigenen Schutz einer Person gegen drohende Gefahr für Leib oder Leben erforderlich ist und die Person*
   a) *um Gewahrsam nachsucht oder*
   b) *sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in einer hilflosen Lage befindet oder*
   c) *Selbsttötung begehen will, oder*
3. *die Identität einer Person auf andere Weise nicht festgestellt werden kann.*

Grundsätzlich ist für diese freiheitsentziehende Maßnahme eine richterliche Entscheidung notwendig, wenn sie länger als bis zum Ende des darauffolgenden Tages dauern würde. Wenn der Grund für den Gewahrsam schon vor einer richterlichen Entscheidung entfällt, dann ist der Gewahrsam ohne diese Entscheidung zu beenden.

Für die Durchführung des Gewahrsams hat das Innenministerium im letzten Jahr die bisherigen Regelungen durch eine Gewahrsamsordnung neu gefasst. Von besonderer Bedeutung für betroffene Personen ist dabei, dass zum Beispiel die Prüfung ihrer Haftfähigkeit durch Hinzuziehung eines Arztes geklärt werden darf. Dies dient nicht nur dem Schutz des Betroffenen, sondern ist auch für die Entscheidung eines Polizeibeamten oder des Richters über den Gewahrsam erforderlich. In der Gewahrsamsordnung wurde festgelegt, dass die Intimsphäre einer in Gewahrsam genommenen Person in geeigneter Weise zu schützen ist und in Anlehnung an § 29 Absatz 3 PolG (Durchsuchung von Personen) beim Betreten einer Gewahrsamszelle möglichst ein Bediensteter des gleichen Geschlechts wie die verwahrte Person anwesend ist.

Wenn ein Betroffener in der Gewahrsamszelle untergebracht ist, sind die mit der Verwahrung betrauten Bediensteten verpflichtet, zum Schutz der betroffenen Person, zum Eigenschutz und zur Verhinderung von Beschädigungen an der Einrichtung regelmäßige Kontrollen durchzuführen. Die letzte Novellierung des Polizeigesetzes im November 2008 eröffnete die Möglichkeit, diese Kontrollen teilweise mit dem Kamera-Monitor-Verfahren – also einer Bildbetrachtung ohne Aufzeichnungen – zu erledigen. Zum Zeitpunkt einer Anfrage meiner Dienststelle im Frühjahr 2011 war dies in 130 Gewahrsamseinrichtungen möglich, von denen etwa 60 Zellen vorrangig zu Ausnüchterungszwecken genutzt werden. Das Innenministerium stellte im Übrigen

ausdrücklich darauf ab, dass eine Videoüberwachung eine persönliche Zellenkontrolle nicht ersetzen könne. Wenn die Rahmenbedingungen eingehalten werden, kann diese Beobachtung aus datenschutzrechtlicher Sicht nicht kritisiert werden. Wir werden uns aber zu gegebener Zeit vor Ort einige Gewahrsamseinrichtungen im Rahmen eines Kontrollbesuchs anschauen, um die konkrete Umsetzung zu prüfen.

2.5 Die „Sport-Dateien" der Polizei im Land und das Problem mit der Verbunddatei

Zu Wochenbeginn können wir es leider immer öfter in der Zeitung lesen: Randale am Rande von Fußballspielen von der 1. bis zur 3. Bundesliga, Auseinandersetzungen der verfeindeten Fangruppen untereinander oder mit der Polizei; Platzverweise, Stadionverbote, Personalienfeststellungen und Ingewahrsamnahmen sind die Folge. Doch was geschieht mit den personenbezogenen Daten, die anlässlich derartiger Einsätze in teilweise erheblichem Umfang erhoben werden?

Bereits im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 24) habe ich auf das Urteil des Niedersächsischen Oberverwaltungsgerichts vom 16. Dezember 2008, 11 LC 229/08, hingewiesen, in dem die Unzulässigkeit der Speicherung personenbezogener Daten in der Verbunddatei „Gewalttäter Sport" mangels hinreichender Rechtsgrundlage festgestellt wurde. Die Datei „Gewalttäter Sport" sei errichtet und betrieben worden, so das Gericht, ohne dass der Bundesminister des Innern eine gemäß § 7 Absatz 6 des Gesetzes über das Bundeskriminalamt (BKAG) vorgesehene Verordnung über die Art der zu speichernden Daten erlassen habe. Dies galt übrigens auch für alle anderen von den Polizeien des Bundes und der Länder betriebenen Verbunddateien. Wie entwickelte sich diese Geschichte weiter?

Die vom Ursprungssachverhalt betroffene Polizeidirektion in Niedersachsen legte gegen das Urteil des Oberverwaltungsgerichts Lüneburg Revision ein. Gerade noch rechtzeitig vor der Revisionsentscheidung des Bundesverwaltungsgerichts trat nach Zustimmung des Bundesrats die BKA-Daten-Verordnung (BKADV) in Kraft. Nach geringfügigen Änderungen in den Errichtungsanordnungen zu den jeweiligen Verbunddateien war die Speicherung der personenbezogenen Daten nunmehr auf eine rechtliche Grundlage gestellt. Damit waren zunächst auch die Forderungen der Datenschutzbeauftragten von Bund und Ländern nach einer präzisen rechtlichen Festlegung der Speicherungsinhalte in den Verbunddateien erfüllt (vgl. Entschließung vom 26./27. März 2009, Anhang 11 im 29. Tätigkeitsbericht 2009, LT-Drucksache 14/5500, S. 160). Mit Urteil vom 9. Juni 2010, 6 C 5.09, wies das Bundesverwaltungsgericht daraufhin die Klage des ursprünglich auf unverzügliche Löschung seiner in der „Gewalttäterdatei Sport" gespeicherten personenbezogener Daten klagenden Fußballfans ab. Auf Grundlage des § 8 Absatz 5 BKAG in Verbindung mit §§ 4 und 9 Absatz 1 Nummer 3 b BKADV konnten die Daten des Klägers nun in der Datei gespeichert bleiben (vgl. auch den Beitrag oben unter Nr. 1.4).

Die Medienberichterstattung über diese Entwicklung sorgte für zahlreiche Anfragen betroffener Stadionbesucher nicht nur bei der Polizei, sondern auch bei meiner Behörde. Der Mehrzahl der Anfragen zur Verbunddatei „Gewalttäter Sport" war die jeweils zuvor eingeholte Antwort des Landeskriminalamts bereits beigefügt. Dieser Antwort wiederum war zu entnehmen, dass die Speicherung in der Datei in den meisten Fällen aufgrund polizeirechtlicher Ingewahrsamnahmen am Rande eines bestimmten Fußball-Bundesligaspiels im Jahre 2009 erfolgt war. Da es sich allesamt um reine polizeirechtliche Maßnahmen ohne gleichzeitig eingeleitete strafrechtliche Ermittlungsverfahren handelte, schien mir eine Überprüfung der Speichermodalitäten vor Ort im Rahmen eines Kontrollbesuchs bei der für die Speicherung verantwortlichen Polizeidienststelle angebracht. Aufgrund der dort erlangten Erkenntnisse und der Tatsache, dass zwischenzeitlich die für die Speicherung in der Datei erforderliche Rechtsgrundlage geschaffen war, konnten gegen die Speicherung derartiger Datensätze im Zusammenhang mit der genann-

ten Bundesligabegegnung keine grundsätzlichen Bedenken geltend gemacht werden. Eine Speicherung von Personen in dieser Datei ist nach der Rechtslage tatsächlich möglich, ohne dass der Verdacht der Begehung einer Straftat vorliegt. Polizeirechtliche Maßnahmen wie Platzverweis oder Gewahrsam und selbst die bloße Personalienfeststellung reichen hierfür aus, sofern die Maßnahmen zur Verhinderung von anlassbezogenen Straftaten durchgeführt wurden.

Ist der Erwachsene oder Jugendliche in der Datei erst mal gespeichert, so erfolgt grundsätzlich frühestens nach fünf Jahren eine Überprüfung, ob die Daten ausgesondert werden können.

Doch das ist nicht die einzige Datei, in der Personen gespeichert werden, die im Zusammenhang mit Sportveranstaltungen bei der Polizei auffällig werden. In der „Arbeitsdatei für szenekundige Beamte“, kurz SKB-Datenbank, werden auf Landesebene Erkenntnisse aus der und im Zusammenhang mit der gewaltgeneigten Sport-, insbesondere Fußballszene zum Zwecke der Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten in Baden-Württemberg zusammengeführt und verarbeitet. Auf diese Datei habe ich ebenfalls bereits im 29. Tätigkeitsbericht 2009 hingewiesen. Damals war sie mir im Zusammenhang mit von der Polizei durchgeführten „Gefährderansprachen“ anlässlich der Fußball-Europameisterschaft 2008 in Österreich und der Schweiz aufgefallen und auch überprüft worden. Erfreulicherweise wurde die Datei seither weiterentwickelt und meinen Forderungen, insbesondere nach einer besseren Sicherstellung des Auskunftsanspruchs der Bürger, nachgekommen. Zwischenzeitlich wird die Datei zentral unter der Verantwortung der Landesinformationsstelle Sporteinsätze beim Innenministerium in Form des Web-gestützten Analyse-Werkzeugs „Crime“ betrieben. Zugriff haben alle Dienststellen, die bislang im Rahmen ihrer Aufgabenwahrnehmung „eigene“ SKB-Datenbanken führten und im Falle eines Auskunftsersuchens einzeln abgefragt werden mussten. Dieser Fortschritt in der Qualität der Auskunftserteilung hat allerdings auch zur Folge, dass nun alle zugriffsberechtigten Beschäftigten der Polizei sofort und jederzeit Zugriff auf die auch von anderen Dienststellen gespeicherten Daten haben.

Da die Voraussetzungen für die Speicherung in der Datei „Gewalttäter Sport“ enger gefasst sind als die für die Speicherung in der SKB-Datenbank, erfolgt im Falle einer Speicherung einer Person aus Baden-Württemberg in der erstgenannten Verbunddatei die gleichzeitige Speicherung in der landesweiten Datei, der SKB-Datenbank. Umgekehrt führt eine Speicherung in der SKB-Datenbank jedoch nicht zwingend auch zu einer Erfassung in der Datei „Gewalttäter Sport“. Durch Einbindung meiner Behörde in die Fortentwicklung der SKB-Datenbank konnte ich eine noch weitere Beschränkung erreichen. So wurde zum Beispiel die grundsätzliche Speicherdauer von Personen, gegen die keine Ermittlungsverfahren eingeleitet und die somit unter der Rolle „Potenzielle Straftäter“ gespeichert werden, von fünf auf drei Jahre reduziert. Eine Überprüfung hinsichtlich der Erforderlichkeit einer weiteren Speicherung in der SKB-Datenbank erfolgt nun jährlich zum Ende der Fußball-Bundesligasaison. Wird eine Person über einen Zeitraum von zwei Jahren in der Datei als „inaktiv“ geführt, so werden deren Daten auch vor Ablauf der festgelegten grundsätzlichen Speicherdauer gelöscht. Dies wiederum kann dann Auswirkungen auf die gleichzeitige Speicherung in der Verbunddatei „Gewalttäter Sport“ haben, indem die personenbezogenen Daten auch dort noch vor Ablauf der ursprünglich festgelegten Frist gelöscht werden. Ich werde mit Interesse beobachten, wie von dieser Regelung Gebrauch gemacht wird.

Auch wenn ich die teilweise parallele Speicherung personenbezogener Daten in Landesdateien und in den Bund-/Länder-Verbunddateien weiterhin kritisch betrachte, so wurden zwischenzeitlich wenigstens die erforderlichen Rechtsgrundlagen hierfür geschaffen. Auskunftsersuchen betroffener Bürger können nun qualitativ besser beantwortet werden, die Qualität der polizeilichen Datenhaltung in diesem Bereich wurde insgesamt gesteigert. Ein Kontrollbesuch bei einer besonders betroffe-

nen Dienststelle erbrachte keine Erkenntnisse, die eine Beanstandung gerechtfertigt hätten.

2.6 Was gibt es Neues zur Arbeitsdatei „Politisch motivierte Kriminalität“?

In den Tätigkeitsberichten 2005, 2006 und 2007 meines Amtsvorgängers hatten die Zweifel an den Datenspeicherungen in der Arbeitsdatei „Politisch motivierte Kriminalität“ (AD PMK) einen breiten Raum eingenommen. Im Nachgang konnte ich aufgrund der regelmäßigen Informationen des Innenministeriums und des Landeskriminalamts feststellen, dass dort und im Gefolge auch bei den Staatsschutzreferaten in den Polizeidienststellen sich letztlich die Überzeugung durchgesetzt hatte, dass der Nutzen einer Arbeitsdatei nur erreicht werden kann, wenn die Informationen zu den Personen, aber auch zu deren politischer Motivation stichhaltig begründet werden und sich streng an der Erforderlichkeit für die weitere polizeiliche Arbeit orientieren. Daher wurde im Fortbildungsbereich seit Mitte des Jahres 2009 einiges getan, um die Fehlerquellen bei der Speicherung personenbezogener Daten in dieser Arbeitsdatei letztlich zu vermindern. In 13 Seminaren der Akademie der Polizei wurden sämtliche Staatsschutzdienststellen aus dem Land beteiligt. Eine weitere Entwicklung folgte aus einem Urteil des Verwaltungsgerichtshofs Baden-Württemberg vom 12. Juli 2010 – 1 S 349/10. Dieser hatte ein Konzert, dessen Ausrichtung als politisch extremistisch angesehen wurde, aufgrund seiner Gesamtprägung als Versammlung nach dem Versammlungsgesetz angesehen. Daher wurden die Staatsschutzdienststellen vom Landeskriminalamt gebeten, diese rechtliche Einordnung bei der Überprüfung gespeicherter Daten zu berücksichtigen. Alle Maßnahmen trugen offensichtlich dazu bei, die Zahlen der in der AD PMK gespeicherten Personen von Bericht zu Bericht zu senken und damit die Datenqualität zu verbessern.

Nachdem Ende des Jahres 2010 mit rund 10 000 Personendatensätzen ein erfreulicher Tiefstand gegenüber einer Ausgangszahl von über 40 000 Datensätzen erreicht worden war, konnten meine Mitarbeiter Mitte des Jahres 2011 bei einem Kontrollbesuch in einer Polizeidienststelle diese Entwicklung anhand konkreter Einzelfälle überprüfen. Das Ergebnis war im Vergleich zu den früheren Feststellungen bemerkenswert. In Einzelfällen ist es zwar immer wieder notwendig zu fragen, ob sich diese Person oder jener Vorgang zu Recht für eine Erfassung in der AD PMK eignet. In der fachlichen Diskussion lässt sich dieses inzwischen leichter klären, selbst wenn meine Bedenken manchmal nicht ganz ausgeräumt werden können.

Eine ergänzend eingeholte Stellungnahme des Landeskriminalamts zu den Fallzahlen in der AD PMK ergab Mitte Oktober 2011 folgendes Bild:

Von 10 979 gespeicherten Rollen entfielen 8 976 auf potenzielle Straftäter und 529 auf Kontakt- und Begleitpersonen. 808 Zeugen und 312 Beschuldigte in strafprozessualen Ermittlungsverfahren waren ebenso enthalten. Weitere Rollen wie 24 Verdächtige oder 30 Geschädigte in solchen Ermittlungsverfahren oder die insgesamt 300 polizeirechtlichen Tatverdächtigen, sonstigen Personen, potenziellen Opfer, Störer, Umfeldpersonen und andere Personen waren zahlenmäßig im Einzelnen zwischen 155 mal (Tatverdächtige) und einmal (andere Person) erfasst. Die anderen Rollen bewegten sich jeweils im zweistelligen Zahlenbereich.

Die Bezugsgröße „Rolle“ ist deshalb von Bedeutung, da Personen nur einmal erfasst werden, diesen aber aufgrund verschiedener Vorgänge – teilweise auch von mehreren Dienststellen – verschiedene Rollen in der Datenbankverarbeitung zugeordnet werden können. Da dieses in der Systematik der Datenbankverarbeitung begründet ist, kann die einleitend genannte Zahl der Rollen nicht identisch mit der Zahl der in dieser Datei gespeicherten Personen sein, diese beträgt nämlich 10 123. Für eine statistische Auswertung ist diese Datenbank nach Mitteilung des Landeskriminalamts nur eingeschränkt geeignet. Wer nun mit wie vielen Rollen im Einzelnen in der AD PMK enthalten ist, habe ich nicht weiter ermitteln lassen, da diese Aussage nur wenig ergiebig für die

Frage der datenschutzrechtlichen Zulässigkeit dieser Datenverarbeitung an sich ist.

2.7 Verdeckte Ermittlungen in Heidelberg und beim NATO-Gipfel 2009

Heidelberg und seine Akteure in der linken Szene

Im Dezember 2010 wurde in Heidelberg bekannt, dass dort ein Verdeckter Ermittler des Landeskriminalamts Baden-Württemberg tätig gewesen war. Enttarnt wurde er durch eine Person, die ihn während eines früheren Urlaubsaufenthaltes kennengelernt hatte, bei der er von seiner Tätigkeit bei der Polizei berichtete. Daher sprach sie ihn während einer Veranstaltung darauf an, informierte aber auch andere Bekannte. Einige von diesen konfrontierten den Beamten mit dieser Erkenntnis, die er aufgrund der Eindeutigkeit der Situation umgehend einräumte. Auch die Medien erfuhren davon, sodass man fast täglich in Zeitungen, Zeitschriften, diversen Internet-Foren und Magazinen viele Einzelheiten und Meinungen zu dem Einsatz nachlesen konnte. In Internet-Foren konnte man sogar Informationen aus dessen persönlichem Lebenskreis abrufen. Auch im Landtag wurden mehrere Berichtsanträge gestellt (LT-Drucksachen 14/7375, 14/7404, 14/7510, 14/7569, 14/7656).

Der Fall ließ nicht nur bei mir Erinnerungen an das Jahr 1992 wach werden, als in Tübingen zwei Verdeckte Ermittler enttarnt worden waren. Die seinerzeitige politische Diskussion (vgl. zum Beispiel LT-Drucksache 11/1696) über die Zulässigkeit des Einsatzes, der in den Tätigkeitsberichten der Landesbeauftragten für den Datenschutz für die Jahre 1992, 1993 und 1994 seinen Niederschlag fand und zudem Gegenstand eines verwaltungsgerichtlichen Verfahrens war, war Anlass genug, auch den aktuellen Fall näher zu kontrollieren.

Die rechtlichen Voraussetzungen der Erhebung personenbezogener Daten von Störern, potenziellen Straftätern und deren Kontakt- und Begleitpersonen durch Verdeckte Ermittler sind in den §§ 20 und 22 des Polizeigesetzes enthalten:

§ 22 – Besondere Mittel der Datenerhebung

(1) Besondere Mittel der Datenerhebung sind:

…….

4. der Einsatz von Polizeibeamten unter Geheimhaltung ihrer wahren Identität (Verdeckte Ermittler).

(2) …….

(3) Der Polizeivollzugsdienst kann personenbezogene Daten durch ……. oder durch den Einsatz Verdeckter Ermittler

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 Absatz 2 genannten Personen oder

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

(4) Daten dürfen auch dann nach Absatz 2 und 3 erhoben werden, wenn Dritte unvermeidbar betroffen werden.

(5) Straftaten mit erheblicher Bedeutung sind

1. Verbrechen,

2. Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie

a) sich gegen das Leben, die Gesundheit oder die Freiheit einer oder mehrerer Personen oder bedeutende fremde Sach- oder Vermögenswerte richten,

b) auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- oder Wertzeichenfälschung oder des Staatsschutzes (§§ 74 a und 120 des Gerichtsverfassungsgesetzes) begangen werden,

c) gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen werden.

(6) Der Einsatz von Mitteln nach Absatz 1, ……, bedarf der Anordnung eines Regierungspräsidenten oder des Leiters des Landeskriminalamts, eines Polizeipräsidiums oder einer Polizeidirektion. Die Regierungspräsidenten, der Leiter des Polizeipräsidiums Stuttgart sowie der Leiter des Landeskriminalamts können die Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes übertragen.

(7) ……..

(8) Der Betroffene ist von einer Maßnahme nach Absatz 2 oder 3 zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Maßnahme geschehen kann. Die Unterrichtung unterbleibt, wenn hierdurch die weitere Verwendung des Verdeckten Ermittlers für Maßnahmen nach Absatz 1 Nr. 4 oder Leben oder Gesundheit einer Person gefährdet würde, sich an den die Maßnahme auslösenden Sachverhalt ein Ermittlungsverfahren gegen den Betroffenen anschließt oder seit Beendigung der Maßnahme fünf Jahre verstrichen sind.

§ 20 – Befragung und Datenerhebung

(1) ……

(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,

3. ……

4. ……

5. ……

soweit dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist.

(4) ……

(5) ……

(6) ……

Ergänzend hat das Innenministerium aufgrund der seinerzeitigen Erfahrungen durch eine nicht öffentlich zugängliche Verwaltungsvorschrift, die regelmäßig angepasst wurde, den Dienststellen eine Grundlage für derart gravierende Eingriffe in das informationelle Selbstbestimmungsrecht an die Hand gegeben.

Einzelheiten des Falles kann ich wegen der von Seiten des Landeskriminalamts verfügten Geheimhaltung an dieser Stelle nicht ausbreiten, eines lässt sich nach einer Kontrolle der in diesem Fall angelegten Akten festhalten: Die Mängel, die in den 90er Jahren festgestellt wurden, waren nunmehr aufgrund der generellen Regelungen des Innenministeriums einerseits und durch eindeutige Anordnungen im konkreten

Fall andererseits behoben. Jedenfalls ergab sich aus den Akten, dass es nicht um das Ausspähen einer bestimmten politischen Szene – wie in der Öffentlichkeit vermutet – ging. Das wäre auch eher eine Aufgabe des Landesamts für Verfassungsschutz gewesen. Vielmehr sollten Daten bestimmter Personen in ihren gesetzlich präzisierten Rollen erhoben werden. Jedoch kann die Befugnis des Verdeckten Ermittlers, mit einer anderen Identität als seiner eigenen in dem Umfeld der betroffenen Personen zu agieren, den Eindruck nicht vermeiden, dass auch dieses Umfeld ausgekundschaftet werden soll. Dass ein Verdeckter Ermittler aufgrund der Einsatzform zwangsläufig eine Vielzahl Kontakte zu anderen Personen hat, wurde in den gesetzlichen Voraussetzungen durch die Formulierung in § 22 Absatz 4 PolG berücksichtigt. Es ist verständlich, dass ein Verdeckter Ermittler alles vermeiden sollte, was zu einer Enttarnung führen könnte. Allerdings ist das Verbot der Begehung von Straftaten, das bei dem Einsatz stets beachtet werden muss, auch in der erwähnten Verwaltungsvorschrift ausdrücklich festgehalten.

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. Dabei kann es nicht darauf ankommen, dass Straftaten tatsächlich verhindert wurden, das würde bei einem gescheiterten Einsatz wie hier sonst automatisch zur Rechtswidrigkeit des Einsatzes führen. Nicht von mir zu beurteilen war die Angemessenheit des Einsatzes aus taktischer oder gar wirtschaftlicher Sicht.

Die Unterrichtung der betroffenen Personen war zum Zeitpunkt des Kontrollbesuchs noch nicht erfolgt, aber vorgesehen. Insoweit hatte ich um ergänzenden Bericht gebeten, der mir noch im Laufe des Novembers 2011 zuging. Die Ziel- und Kontaktpersonen des Einsatzes sowie drei vom Einsatz unvermeidbar betroffene dritte Personen sind inzwischen benachrichtigt worden. Sieben Personen haben mittlerweile verwaltungsgerichtliche Verfahren zur Überprüfung des Einsatzes des Verdeckten Ermittlers angestrengt, davon eine Zielperson und eine unvermeidbar betroffene dritte Person. Die weiteren Personen waren nach Darstellung des Landeskriminalamts weder Ziel- noch Kontaktperson noch unvermeidbar betroffene Dritte bei dem Einsatz.

Zum Schluss eine persönliche Anmerkung: Was ich im Hinblick auf den Verdeckten Ermittler nach dessen Enttarnung aus bestimmten Internet-Foren und Zeitungsartikeln entnehmen konnte, lässt gewisse Zweifel an dem Verständnis der jeweiligen Verfasser an dem Recht auf informationelle Selbstbestimmung dieser Person selbst und vor allem zu dessen persönlichem Umfeld aufkommen. Dass der von dem Verdeckten Ermittler genutzte E-Mail-Account nach Aussage des Landeskriminalamts nachträglich gehackt wurde, ist dann nur noch eine Fußnote wert.

NATO-Gipfel – die Aktionen dagegen und spezielle polizeiliche Aktivitäten

Nicht nur in Heidelberg war im Jahr 2010 ein Verdeckter Ermittler unterwegs gewesen. Das Innenministerium gab mit einer Pressemitteilung vom 28. Januar 2011 zu, dass auch vor und beim NATO-Gipfel im April 2009 ein Verdeckter Ermittler im Umfeld der Aktionsgruppen eingesetzt worden war, die gegen die NATO und deren Politik demonstrierten. In der Mitteilung wurde der Einsatz auch gleich mit dem Erfolg verknüpft, dass auf baden-württembergischer Seite seinerzeit alles friedlich verlaufen sei.

Das Besondere war in diesem Fall, dass dieser Verdeckte Ermittler ein Polizeibeamter aus dem Vereinigten Königreich von Großbritannien und Nordirland war, der allerdings schon bei verschiedenen G 8-Veranstaltungen, so auch in Heiligendamm im Jahr 2007, aktiv gewesen sein soll.

Nachdem ich eigentlich gedacht hatte, mit dem 29. Tätigkeitsbericht 2009 die Datenverarbeitung durch den Polizeivollzugsdienst beim NATO-Gipfel aus datenschutzrechtlicher Sicht abschließend abgehandelt zu haben, musste ich nun doch erneut in die Kontrolle dieses weiteren Vorganges einsteigen. Allerdings musste ich nach einer ersten Stellungnahme des Innenministeriums, die mir erst nach fast fünf Monaten zuging, ergänzend verschiedene Fragen zu den einzelnen Voraussetzungen für den Einsatz und zu weiteren Aspekten der Verarbeitung der personenbezogenen Daten der Ziel- und Kontaktpersonen in den polizeilichen Informationssystemen stellen. Zu diesem Schreiben habe ich bis zum Redaktionsschluss dieses Berichts noch keine Antwort erhalten.

Eine Erkenntnis konnte ich aus der ersten Stellungnahme aber bereits gewinnen: Bei den Personen, die als potenzielle Straftäter oder deren Kontakt- und Begleitpersonen als Ziel der Datenerhebungen genannt worden waren, hatte man meine Anforderung zum Anlass genommen, die Datenbestände in verschiedenen polizeilichen Informationssystemen zu bereinigen. Kurz – es wurden Daten gelöscht. Ob dies geschah, weil sie nun nicht mehr benötigt wurden, oder ob dies schon zu Beginn des Einsatzes notwendig gewesen wäre, konnte ich bisher nicht überprüfen. Außerdem sieht das Polizeigesetz in § 78 ausdrücklich vor, dass mit Zustimmung des Innenministeriums auch ausländische Polizeibeamte in Baden-Württemberg eingesetzt werden können. Dass dabei auch die bereits erwähnten Grundsätze für den Einsatz Verdeckter Ermittler beachtet wurden, versicherte mir das Innenministerium unter Berufung auf entsprechende Absprachen.

Auch wenn seit dem Einsatz schon mehr als zwei Jahre ins Land gegangen sind, werde ich am Ball bleiben.

2.8 „Zuverlässigkeitsüberprüfungen“ bei Großveranstaltungen weiterhin ohne gesetzliche Grundlage

Was haben U-20-Frauen-Fußball-WM 2010, Frauen-Fußball-WM 2011 und der Papstbesuch Ende September 2011 gemeinsam? Auf den ersten Blick nicht viel. Bei genauerem Hinsehen wird deutlich, dass bei derartigen Ereignissen von den dabei eingesetzten Helfern – wie schon bei der Fußball-WM 2006 – mit der „Zuverlässigkeitsüberprüfung“ eine wesentliche Hürde zu überwinden ist. Was 2006 noch als einmalige Ausnahme verharmlost wurde, entwickelt sich allmählich zum Regelfall. Eine gesetzliche Grundlage gibt es hierfür weiterhin nicht.

Die zunehmende Praxis, bei sportlichen und anderen Großveranstaltungen gewisse Personen, die beruflich oder ehrenamtlich dort zu tun haben, einer Nachschau in den zahlreichen Dateien von Polizei und Nachrichtendiensten zu unterziehen und dies auf „freiwillige“ Einwilligungen der Betroffenen zu stützen, halte ich nach wie vor für datenschutzrechtlich schwer erträglich. Zwar gibt es mittlerweile gegenüber früheren Veranstaltungen gewisse Erleichterungen bei der Akkreditierung. Anlass war unter anderem der Boykott der Berichterstattung über die Leichtathletik-WM 2009 in Berlin durch einige Medien, da sich seinerzeit dort auch alle Journalisten einer Durchleuchtung durch Polizei und Geheimdienst unterwerfen sollten. Der Deutsche Journalistenverband verurteilte das Procedere im September 2009 als „nicht mit der Pressefreiheit vereinbar“. Nunmehr erhalten Journalisten im Regelfall eine Akkreditierung ohne eine Zuverlässigkeitsüberprüfung. In einem Eckpunktepapier aller betroffenen Medienverbände und -unternehmen vom Juni 2010 wurden die wesentlichen Kriterien zusammengefasst, die die Freiheit der Berichterstattung grundsätzlich sicherstellen und nur in besonders gelagerten Einzelfällen eine Zuverlässigkeitsüberprüfung eines Journalisten zulassen sollen. Tatsächlich fanden bei der Frauen-Fußball-WM 2011 nach Aussage des Innenministeriums Baden-Württemberg überhaupt keine Zuverlässigkeitsüberprüfungen von Journalisten statt.

Eine weitere Änderung in der Verfahrensweise bestand darin, dass Polizei und Verfassungsschutz den anfragenden Stellen nur noch mitteilten, ob Erkenntnisse vorliegen oder nicht, ohne diese zu spezifizieren.

Zuvor musste aber jeder, der in einem bestimmten, als Sicherheitsbereich klassifizierten Bereich tätig werden sollte, eine immerhin sechsseitige Erläuterung zum Verfahren gelesen und aufgrund dieser sein Einverständnis gegeben haben, damit ein summarisches Ergebnis aus den Informationssystemen der Sicherheitsbehörden an den Veranstalter übermittelt werden konnte. Dabei gaben die Sicherheitsbehörden nur weiter, ob Erkenntnisse im Sinne der Erläuterung vorlagen oder nicht, ohne eine Wertung abzugeben, ob die betroffene Person von dem Veranstalter nun eine Berechtigung zu einer Tätigkeit im Sicherheitsbereich erhalten solle oder nicht. Diese wurde allein dem Veranstalter überlassen. Allerdings konnte eine betroffene Person erst dann Kenntnis von dem summarischen Ergebnis erhalten, wenn auch der Veranstalter schon Bescheid wusste. Ob Gegenvorstellungen dann Erfolg hatten, konnte ich mangels Zuständigkeit nicht überprüfen.

Exemplarisch habe ich nach Abschluss der Frauen-Fußball-WM 2011 erhoben, in wie vielen Fällen Erkenntnisse an das Organisationskomitee in summarischer Form übermittelt wurden und welche Weiterungen sich ergeben hatten. Das federführende Landeskriminalamt Nordrhein-Westfalen forderte für 106 Personen eine Überprüfung durch das Landeskriminalamt Baden-Württemberg an. Von diesen 106 Personen sollten 75 als Security-Kräfte, 27 beim Catering, drei in der medizinischen Versorgung und eine als Hostess beschäftigt werden.

In 48 Fällen wurden Erkenntnisse übermittelt, davon teilweise mehrere zu derselben Person. Diese Erkenntnisse betrafen „rechtmäßige Verurteilungen“ wegen folgender Tatbestände

- Leben, Gesundheit oder Freiheit: 16 Fälle
- Sach- oder Vermögenswerte: 22 Fälle
- Betäubungsmittelgesetz: 12 Fälle
- Waffengesetz: 2 Fälle
- Geld- oder Wertzeichenfälschung: 2 Fälle

Außerdem war in vier Fällen die Identität nicht geklärt, da die vorgelegten Personalausweise zur Fahndung ausgeschrieben waren.

In fünf Fällen hat das Landeskriminalamt den betroffenen Personen nochmals die Stelle mitgeteilt, bei der sie Gegenvorstellungen erheben können. Ob diese Personen davon Gebrauch machten und zu welchem Ergebnis dies führte, war dem Amt nicht bekannt.

Das Landesamt für Verfassungsschutz wurde in zwei Fällen entsprechend beteiligt. In welchen Bereichen die betroffenen Personen eingesetzt werden sollten, sei für das Amt nicht zu erkennen gewesen, hieß es. In beiden Fällen hätten zu den Personen polizeiliche Erkenntnisse vorgelegen, auf die verwiesen werden konnte. In einem Fall sei auch auf Erkenntnisse des Amtes hingewiesen worden. Welche Folgerungen die betroffenen Personen gezogen haben, war dem Amt ebenfalls nicht bekannt.

Bei allem Verständnis für die Sicherheitsbedürfnisse der Organisatoren: Für Zuverlässigkeitsüberprüfungen bei Großveranstaltungen gibt es keine gesetzliche Grundlage. Sie immer wieder auf die vermeintliche Alternative einer informierten Einwilligung zu stützen (vgl. § 4 Absatz 1 LDSG) ist unstatthaft.

Das entscheidende Problem bei allen Großveranstaltungen ist und bleibt die Freiwilligkeit der Einwilligungserklärungen der betroffenen Personen, die für das Betreten von Sicherheitsbereichen eine Akkreditierung benötigen. Die Zuverlässigkeitsüberprüfung wird nämlich nur durchgeführt, wenn die Einwilligung die Anfrage bei den Sicherheitsbehörden umfasst. Einfach gesagt ist der Betroffene vor die Wahl gestellt, entweder nach Abfrage der Informationssysteme der Sicherheitsbehörden eine Chance für eine Tätigkeit zu erhalten oder auf die Abfrage und damit möglicherweise auf eine Tätigkeit in einem sicherheitsempfind-

lichen Bereich überhaupt zu verzichten. Diese Wahlmöglichkeit entspricht nach meiner Auffassung, wie sie auch schon in den früheren Tätigkeitsberichten wiedergegeben wurde, und nach der einhelligen Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, wie in einer Entschließung vom Oktober 2007 nach der Fußball-WM 2006 deutlich gemacht wurde, nicht den gesetzlichen Voraussetzungen einer Einwilligung in eine Verarbeitung personenbezogener Daten. Freiwillig geht anders!

Andererseits wird von niemandem bezweifelt, dass eine wie auch immer geartete Überprüfung von Personen in sicherheitsempfindlichen Bereichen bei bestimmten Veranstaltungen unter Umständen erforderlich ist. Das muss dann aber auch der Gesetzgeber regeln, wie er das beispielsweise im Sicherheitsüberprüfungsgesetz schon getan hat. Dementsprechend hatte ich das Innenministerium auf neue polizeirechtliche Bestimmungen in Berlin und Sachsen hingewiesen, die hier eine spezielle Rechtsgrundlage geschaffen haben (vgl. etwa § 44 des sächsischen Polizeigesetzes). Die Antwort fiel eher kühl aus: Man halte eine Regelung im Polizeigesetz aus rechtssystematischen Gründen nicht für angezeigt, denn die Zuverlässigkeitsüberprüfung sei keine polizeiliche Aufgabe, auch wenn die Polizei daran mitwirke. Bemerkenswert ist immerhin, dass nach dem geltenden Polizeigesetz die Polizei befugt ist, auf Antrag von Personen und Stellen außerhalb des öffentlichen Bereichs personenbezogene Daten zu übermitteln, soweit der Auskunftsbegehrende ein näher bestimmtes rechtliches Interesse glaubhaft oder geltend machen kann. In welcher Form oder unter welchen Umständen dieser Auskunftsbegehrende eine Einverständniserklärung eines Betroffenen erlangt, scheint dem Innenministerium relativ egal zu sein. Denn mein Anliegen war explizit nicht auf das Polizeigesetz allein gerichtet, sondern auf alle in Frage kommenden Gesetze. Vielleicht lässt sich bei einer Novellierung des Landesdatenschutzgesetzes, wie sie im Koalitionsvertrag in Aussicht genommen wird, doch noch eine ausgewogene Lösung finden.

2.9 NADIS – das nachrichtendienstliche Informationssystem des Verfassungsschutzes in neuem Gewand

§ 6 Gegenseitige Unterrichtung der Verfassungsschutzbehörden

Die Verfassungsschutzbehörden sind verpflichtet, beim Bundesamt für Verfassungsschutz zur Erfüllung der Unterrichtungspflichten nach § 5 gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Diese Dateien enthalten nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Die Speicherung personenbezogener Daten ist nur unter den Voraussetzungen der §§ 10 und 11 zulässig. Der Abruf im automatisierten Verfahren durch andere Stellen ist nicht zulässig. Die Verantwortung einer speichernden Stelle im Sinne der allgemeinen Vorschriften des Datenschutzrechts trägt jede Verfassungsschutzbehörde nur für die von ihr eingegebenen Daten; nur sie darf diese Daten verändern, sperren oder löschen. Die eingebende Stelle muss feststellbar sein. Das Bundesamt für Verfassungsschutz trifft für die gemeinsamen Dateien die technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes. Die Führung von Textdateien oder Dateien, die weitere als die in Satz 2 genannten Daten enthalten, ist unter den Voraussetzungen dieses Paragraphen nur zulässig für eng umgrenzte Anwendungsgebiete zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten. Die Zugriffsberechtigung ist auf Personen zu beschränken, die unmittelbar mit Arbeiten in diesem Anwendungsgebiet betraut sind; in der Dateianordnung (§ 14) ist die Erforderlichkeit der Aufnahme von Textzusätzen in der Datei zu begründen.

So lautet die gesetzliche Grundlage im Bundesverfassungsschutzgesetz (BVerfSchG) für den Datenverbund unter Führung des Bundesamts für Verfassungsschutz mit den Landesämtern für Verfassungsschutz.

Seit geraumer Zeit bemüht sich das Bundesamt, den bisherigen Informationsverbund mit den Landesämtern, das Nachrichtendienstliche Informationssystem (NADIS), auf eine neue Basis zu stellen. Angestrebt werden dabei zwei wesentliche Veränderungen gegenüber dem bisherigen Aufbau:

Bisher war das System nach § 6 Satz 2 BVerfSchG als Index aufgebaut, das heißt bei der Suche nach Personen musste das einspeichernde Bundes- oder Landesamt auf herkömmlichem Wege um Mitteilung der vorhandenen Erkenntnisse zu bestimmten Personen oder Ereignissen gebeten werden. Zukünftig soll der Informationsaustausch beschleunigt werden. Deshalb sollen Erkenntnisse, die nach § 6 Satz 8 BVerfSchG zulässig gespeichert werden, so vorgehalten werden, dass diese vom Bundesamt oder anderen Landesämtern – abhängig von der betroffenen Person, von dem jeweiligen Ereignis und von der jeweiligen Berechtigung des Bearbeiters – elektronisch abgerufen werden können. Auf entsprechende Intervention der Datenschutzbeauftragten wurde vom Bundesinnenminister eine klare Entscheidung zu den Daten dritter, verfassungsschutzmäßig nicht relevanter Personen getroffen, die sich naturgemäß in den Berichten der Dienste ebenfalls finden. Diese sind vor der Speicherung der Unterlagen dauerhaft unkenntlich zu machen beziehungsweise, wenn sie erst später irrelevant werden, dann zu „schwärzen“. Damit wurde eine Forderung der Datenschutzbeauftragten aus der Entschließung vom 3./4. November 2010 (Keine Volltextsuche in den Dateien der Sicherheitsbehörden, vgl. Anhang 11) erfüllt.

Die zweite Veränderung betrifft die für die neue Ausrichtung von NADIS notwendige Softwareumstellung. Gegenüber einer Indexdatei sind umfangreiche Änderungen notwendig, die von der Verfügbarkeit der einzelnen Information bis zur Berechtigung des einzelnen Mitarbeiters zum Abruf und natürlich auch darüber hinaus bis hin zur technischen Betreuung reichen. Es ist bei aller notwendigen Geheimhaltung ein offenes Geheimnis, dass eine solche Umstellung eine Menge Zeit braucht und ambitionierte Zeitpläne ins Rutschen geraten können.

Bei der Entwicklung dieses Projekts wurde eine Beteiligung der Landesbeauftragten für den Datenschutz unter Hinweis auf die umfassende Verantwortung des Bundesamts leider bislang abgelehnt, auch wenn die Landesämter, die nicht wenige Informationen in diesem System speichern werden, daran laufend beteiligt wurden. Nach Meinung des Bundesinnenministeriums und des Bundesamtes ist die datenschutzrechtliche Kontrolle des Systems vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorzunehmen. Soweit die Landesämter verantwortliche Stellen für die Speicherung von Daten sind, seien die jeweiligen Landesbeauftragten für den Datenschutz zur Kontrolle gefordert. Diese könne jedoch nur in dem jeweiligen Landesamt für Verfassungsschutz erfolgen. Eine Kontrolle der relevanten Protokolldaten für ein Landesamt kann aber nur dann stattfinden, wenn das Bundesamt vorher diesen Datenbestand zur Verfügung stellt. Damit wird eine Kontrolle im Land nur mit einer zeitlichen Verzögerung möglich. Ad-hoc-Kontrollen meiner Dienststelle können daher nur in Einzelfällen stattfinden, umfangreichere Prüfungen werden dadurch unnötig erschwert. Immerhin hat sich das Bundesamt durch regelmäßige Beteiligung an Sitzungen des Arbeitskreises Sicherheit der Datenschutzkonferenz sowie eine für Dezember 2011 anberaumte Informationsveranstaltung bemüht, den weiteren Fortgang des Projekts und die Klärung kritischer Punkte auch in Richtung der Landesbeauftragten zu kommunizieren.

Die Umstellung wird auch Folgen für das amtsinterne System des Landesamts für Verfassungsschutz haben, was wiederum von dem Fortschritt auf Bundesebene abhängig ist. Mein Augenmerk werde ich weiterhin auf eine mit den datenschutzrechtlichen Grundsätzen vereinbare Lösung richten. Nach meinem Eindruck ist das Landesamt ebenfalls an einem konstruktiven Dialog interessiert.

2. Abschnitt: Die Justiz

1. Gesetzgebung

1.1 Schuldner bald im Internet? Das bundesweite Vollstreckungsportal

Durch das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vom 29. Juli 2009 (BGBl. I 2009, S. 2258), dessen Neuregelungen am 1. Januar 2013 in Kraft treten, soll im Wesentlichen die Informationsbeschaffung des Gläubigers in der Zwangsvollstreckung verbessert und die Führung der Schuldnerverzeichnisse der Länder modernisiert werden. Hierzu soll unter anderem ein Internet-Portal geschaffen werden, durch das zentral und länderübergreifend Abrufe aus den Schuldnerverzeichnissen der Länder ermöglicht werden.

Auch heute schon werden bei den Vollstreckungsgerichten Schuldnerverzeichnisse geführt, in die – bei Vorliegen bestimmter Voraussetzungen – auch Privatpersonen Einsicht nehmen können. Künftig wird das Schuldnerverzeichnis für jedes Land von einem zentralen Vollstreckungsgericht geführt werden. Der Inhalt dieser Schuldnerverzeichnisse soll dann über eine zentrale und länderübergreifende Abfrage im Internet – im sogenannten bundesweiten Vollstreckungsportal – eingesehen werden können. In diesem Zusammenhang hat das Bundesministerium der Justiz im Frühjahr 2011 den Entwurf einer Verordnung über die Führung des Schuldnerverzeichnisses vorgelegt. Dieser Verordnungsentwurf ist aus datenschutzrechtlicher Sicht verbesserungsbedürftig. In meiner Stellungnahme an das Justizministerium habe ich unter anderem folgende Punkte angesprochen:

- Das Zusammenspiel zwischen den zentralen Vollstreckungsgerichten der Länder und dem bundesweiten Vollstreckungsportal als zentralem und länderübergreifendem elektronischen Informations- und Kommunikationssystem wirft Fragen auf, die im Entwurf nicht eindeutig beantwortet werden. Unklar bleibt zum Beispiel, ob die Daten ausschließlich bei den zentralen Vollstreckungsgerichten oder ob sie zum Zweck der Einsichtsgewährung zusätzlich beim Vollstreckungsportal gespeichert werden. Sollte letzteres der Fall sein, müsste dies durch die Verordnung klargestellt werden. Es stellt sich außerdem die Frage, welche Stelle die datenschutzrechtliche Verantwortung für die vom Vollstreckungsportal übernommenen Aufgaben trägt. Soll das Vollstreckungsportal für die Speicherung der Daten und die Gewährung der Einsichtnahme verantwortlich sein oder soll das Vollstreckungsportal diese Tätigkeiten im Auftrag der zentralen Vollstreckungsgerichte erledigen? Letzteres hätte zur Folge, dass die zentralen Vollstreckungsgerichte für die Datenverarbeitung durch das Vollstreckungsportal verantwortlich bleiben. Welche Stelle verantwortlich ist, hat datenschutzrechtlich weitreichende Folgen und sollte daher durch den Verordnungsgeber eindeutig geregelt werden.
- Die Einsichtnahme in das Schuldnerverzeichnis ist nur zu bestimmten Zwecken gestattet. Da die Entscheidung über die Gewährung der Einsichtnahme aber automatisiert erfolgen wird, also ohne Vorabprüfung, ist die nachträgliche Kontrolle der Zulässigkeit der Abrufe besonders bedeutsam. Um effektive nachträgliche Kontrollen zu ermöglichen, sollte der Verwendungszweck so konkret wie möglich angegeben werden, zum Beispiel in einem Freitextfeld, in dem das Aktenzeichen oder der Anlass für die Abfrage eingegeben werden kann.
- Darüber hinaus halte ich die im Entwurf vorgesehene Aufbewahrung der Protokolldaten der Einsichtnahmen für die Dauer von sechs Monaten für zu kurz, um eine ausreichende Kontrolle der Zugriffe zu ermöglichen. Die Protokolldaten sollten vielmehr für die gesamte Dauer der Speicherung der Schuldnerdaten und auch nach der Löschung der Schuldnerdaten noch für einige Zeit (zum Beispiel drei Monate) aufbewahrt werden.

– Auch die im Verordnungsentwurf vorgesehene Möglichkeit der Registrierung mittels Kreditkartendaten ist datenschutzrechtlich abzulehnen. Neben der Möglichkeit, sich mit dem elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes zu identifizieren, halte ich eine weitere Identifizierungsmöglichkeit über private Anbieter für problematisch. So gewährleistet die Identifizierung über Verfahren, die von privaten Anbietern bereitgestellt werden, nicht unbedingt das gleiche Sicherheitsniveau wie die Identifizierung mittels elektronischem Personalausweis.

Vor allem ist die im Verordnungsentwurf vorgesehene Vorgehensweise bei der Suche nach Schuldnern im Schuldnerverzeichnis aus datenschutzrechtlicher Sicht nachzubessern. So sieht der Entwurf vor, dass die gesuchte Person zunächst mit mindestens zwei Suchdaten anzugeben ist. Dann soll der anfragenden Person eine Ergebnisübersicht angezeigt werden, aus der der gesuchte Datensatz auszuwählen ist. Durch die Angabe von zwei Suchdaten ist eine Identifizierung jedoch nicht hinreichend sicher. Vor allem bei Personen mit gängigen Namen kann es zu Personenverwechslungen kommen. Auch die Anzeige einer Ergebnisliste löst dieses Problem nicht. Denn falls die anfragende Person keine weiteren Identifizierungsmerkmale kennt, kann sie die gesuchte Person auch anhand der Trefferliste nicht identifizieren. Dies gilt umso mehr, als nicht zwingend davon ausgegangen werden kann, dass die gesuchte Person überhaupt im Schuldnerverzeichnis eingetragen ist. Die Anzeige der Ergebnisliste ist zur Identifizierung daher ungeeignet und stellt eine unzulässige Übermittlung personenbezogener Daten dar. Auf die Anzeige einer Trefferliste sollte deshalb verzichtet werden. Die Suche sollte vielmehr so gestaltet werden, dass nur eine bereits anhand der eingegebenen Suchkriterien eindeutig identifizierbare Person angezeigt wird. Dies sollte durch die zwingende Vorgabe einer ausreichenden Anzahl von Suchkriterien sichergestellt werden.

Die Einsichtnahme in Schuldnerverzeichnisse über ein bundesweites Vollstreckungsportal muss – angesichts der Sensibilität der betroffenen Daten – so ausgestaltet werden, dass das informationelle Selbstbestimmungsrecht der Betroffenen gewahrt wird.

1.2 Eine fesselnde Angelegenheit – die elektronische Fußfessel in der Führungsaufsicht

Mit dem „Gesetz zur Neuordnung des Rechts der Sicherungsverwahrung und zu begleitenden Regelungen“ vom 22. Dezember 2010 (BGBl. I 2010, S. 2300), das am 1. Januar 2011 in Kraft getreten ist, hat der Bundesgesetzgeber die Möglichkeit geschaffen, den Aufenthalt entlassener Straftäter als Maßnahme der Führungsaufsicht elektronisch zu überwachen.

Gemäß § 68 b Absatz 1 Satz 1 Nr. 12 des Strafgesetzbuchs (StGB) kann das Gericht Verurteilte nunmehr für die Dauer der Führungsaufsicht anweisen, „die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen“. Diese Überwachung erfolgt mittels einer sogenannten elektronischen Fußfessel. Als Maßnahme der Führungsaufsicht dient die elektronische Aufenthaltsüberwachung vor allem dem Zweck, eine erneute Straffälligkeit von Straftätern mit ungünstiger Sozialprognose, die ihre Freiheitsstrafe vollständig verbüßt haben, zu verhindern.

Mit dem im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 58) erwähnten Einsatz elektronischer Fußfesseln aufgrund des Landesprojektes nach dem „Gesetz über elektronische Aufsicht im Vollzug der Freiheitsstrafe“ vom 30. Juli 2009, das den Einsatz elektronischer Fußfesseln als alternative Form des Strafvollzugs vorsieht, hat die elektronische Aufenthaltsüberwachung in der Führungsaufsicht dagegen nichts zu tun.

Die Erhebung und Verarbeitung personenbezogener Daten im Rahmen der Durchführung einer elektronischen Aufenthaltsüberwachung in der

Führungsaufsicht richtet sich nach § 463 a Absatz 4 der Strafprozessordnung. Nach dieser Vorschrift sind Erhebung und Speicherung aller Aufenthaltsdaten einschließlich der Daten über eine Beeinträchtigung der Erhebung zulässig. Die Verwendung der Daten ist an bestimmte, abschließend aufgezählte Zwecke gebunden. Die Daten sind gegen unbefugte Kenntnisnahme besonders zu sichern und – soweit kein Weisungsverstoß festgestellt wird – zwei Monate nach ihrer Erhebung zu löschen. Innerhalb der Wohnung dürfen, zum Schutz des Kernbereichs privater Lebensführung, keine über den Umstand der Anwesenheit hinausgehenden Daten erhoben werden, soweit dies technisch möglich ist; andernfalls dürfen diese Daten nicht verwendet und müssen umgehend gelöscht werden.

Da die vorgenannten Vorschriften bereits am 1. Januar 2011 in Kraft traten, standen die Länder Anfang des Jahres 2011 vor der Herausforderung, aus dem Stand heraus passende Systeme zu entwickeln und die elektronische Aufenthaltsüberwachung organisatorisch umzusetzen.

Im Mai 2011 haben sich die Länder auf eine bundesweit einheitliche Lösung geeinigt; danach soll in Hessen eine Gemeinsame elektronische Überwachungsstelle der Länder eingerichtet werden, die die Aufgaben der Führungsaufsichtsstellen wahrnehmen soll. Diese Überwachungsstelle soll eingehende Ereignismeldungen entgegennehmen, bewerten und abhängig vom Ergebnis die zuständigen polizeilichen und justiziellen Stellen der Länder unterrichten. Grundlage hierfür ist ein Staatsvertrag. Einige Länder, darunter auch Baden-Württemberg, haben diesen zwischenzeitlich unterschrieben, der Beitritt weiterer Bundesländer wird folgen. Auf der Grundlage einer Verwaltungsvereinbarung der beteiligten Länder soll durch die hessische Zentrale für Datenverarbeitung darüber hinaus eine technische Überwachungszentrale eingerichtet werden, die den technischen Betrieb des Systems zur elektronischen Aufenthaltsüberwachung gewährleistet.

Die datenschutzgerechte Umsetzung des gewählten Konzeptes erfordert eindeutige Regelungen über Zuständigkeiten und die Zusammenarbeit der beteiligten Stellen, insbesondere der Führungsaufsichtsstellen der Länder mit der Gemeinsamen elektronischen Überwachungsstelle oder zwischen dieser und der technischen Überwachungszentrale. Außerdem ist die Erstellung von Datenschutz- und Sicherheitskonzepten erforderlich, die unter anderem eindeutige und datenschutzrechtlich angemessene Zugriffs-, Löschungs- und Protokollierungsregelungen enthalten müssen.

So ist für die Frage nach der datenschutzrechtlichen Verantwortung von Bedeutung, dass im Staatsvertrag geregelt ist, dass die Länder hoheitliche Kompetenzen der Führungsaufsicht auf eine gemeinsame öffentliche Stelle übertragen und diese öffentliche Stelle nicht lediglich als verlängerter Arm der einzelnen Aufsichtsstellen handelt. Ebenso bedeutsam ist die auf Anregung meines bayerischen Kollegen erfolgte Aufnahme einer Regelung in den Staatsvertrag, durch die klargestellt wird, dass auf die Tätigkeit der Gemeinsamen elektronischen Überwachungsstelle der Länder das hessische Datenschutzgesetz Anwendung findet und diese Stelle der Aufsicht des hessischen Datenschutzbeauftragten unterliegt.

Angesichts der Fülle der datenschutzrechtlichen Fragestellungen, die mit der Einführung der elektronischen Aufenthaltsüberwachung in der Führungsaufsicht verbunden sind, werde ich die weitere Entwicklung der Angelegenheit im Auge behalten und begleiten. Das Justizministerium jedenfalls hat zugesagt, mich auch künftig an der weiteren Ausgestaltung des Konzeptes zu beteiligen.

1.3 Der virtuelle Überwachungsraum – Funkzellenabfrage

Die nichtindividualisierte Funkzellenabfrage im Sinne des § 100 g Absatz 2 Satz 2 der Strafprozessordnung (StPO) ist eine verdeckte Ermittlungsmaßnahme zum Zweck der Strafverfolgung. Die genannte Vorschrift ist so allgemein gefasst, dass sie die massenhafte Erfassung von

Menschen gestattet, die keinerlei Anlass für einen staatlichen Eingriff gegeben haben.

Im Rahmen einer nichtindividualisierten Funkzellenabfrage werden über einen bestimmten Zeitraum hinweg Telekommunikationsverbindungsdaten aller in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur die bestimmter einzelner Tatverdächtiger, abgefragt. Dass dabei nicht die Gesprächsinhalte, sondern „nur“ die Verkehrsdaten erfasst werden, ändert nichts daran, dass die mit einer solchen Maßnahme verbundenen Eingriffe in die Rechte der Betroffenen schwerwiegend sind. Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt (vgl. insbesondere das Urteil vom 2. März 2010, 1 BvR 256/08 u. a., zur Vorratsdatenspeicherung). Verkehrsdaten können die sozialen Beziehungen der Betroffenen widerspiegeln, ihnen kann zum Beispiel auch die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen entnommen werden.

Welches Ausmaß Funkzellenabfragen annehmen können, zeigte folgender Fall:

Sächsische Strafverfolgungsbehörden hatten am 19. Februar 2011 anlässlich von Neonaziaufmärschen und hiergegen gerichteter Demonstrationen Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmer, darunter Landtags- und Bundestagsabgeordnete, Rechtsanwälte sowie Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und in ihrem Kommunikationsverhalten erfasst worden.

Dieser Vorfall macht deutlich, dass die im Jahr 2001 in die Strafprozessordnung eingefügte Vorschrift des § 100 g Absatz 2 Satz 2 StPO unzureichend ist.

Für eine nichtindividualisierte Funkzellenabfrage im Sinne der genannten Vorschrift bedarf es nicht der Angabe der Rufnummer oder einer anderen Kennung des Anschlusses bestimmter Tatverdächtiger, sondern lediglich einer räumlich und zeitlich hinreichend bestimmten Bezeichnung der Telekommunikation. Voraussetzungen sind weiter das Vorliegen einer Straftat von erheblicher Bedeutung und, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Bereits die Verwendung des unbestimmten Rechtsbegriffs „Straftat von erheblicher Bedeutung“ zeigt, dass die bisherige Regelung zu unbestimmt ist. Wann eine Straftat von „erheblicher Bedeutung“ vorliegt, bedarf der Auslegung und ist nur schwer zu bestimmen. Die Annahme, dass eine solche Straftat „mindestens dem mittleren Kriminalitätsbereich“ zuzurechnen sein muss, hilft nur bedingt weiter und wirft außerdem die Frage nach der Verhältnismäßigkeit auf. Auch die genannte allgemeine Subsidiaritätsklausel ist nicht geeignet, den Anwendungsbereich der nichtindividualisierten Funkzellenabfrage eindeutig zu bestimmen und sicherzustellen, dass nur in verhältnismäßigem Umfang in Rechte Dritter eingegriffen wird. In der Strafprozessordnung ist außerdem nicht näher geregelt, wie die Behörden mit den erhobenen Daten umzugehen haben, zum Beispiel über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiterverwendet werden dürfen. Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. Juli 2011 eine Entschließung gefasst (vgl. Anhang 19), in der der Bundesgesetzgeber aufgefordert wird, den Anwendungsbereich der nichtindividualisierten Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken sowie die Löschungsvorschriften zu präzisieren.

Zwischenzeitlich hat der Freistaat Sachsen dem Bundesrat einen Gesetzentwurf zur Neuregelung der nichtindividualisierten Funkzellenabfrage vorgelegt (BR-Drucksache 532/11). Dieser trägt den vorstehenden Forderungen in großem Umfang Rechnung. So sieht der Entwurf zum Beispiel vor, den Anwendungsbereich der nichtindividualisierten Funkzellenabfrage auf den in § 100 a Absatz 2 StPO (§ 100 a StPO regelt die Telekommunikationsüberwachung, die auf die Erhebung von Inhaltsdaten der Kommunikation bestimmter Personen abzielt) genannten Straftatenkatalog beziehungsweise auf Straftaten zu beschränken, die im Mindestmaß mit einer Freiheitsstrafe von sechs Monaten bedroht sind. Er hebt außerdem die Verhältnismäßigkeitsprüfung besonders hervor; wenn das Ausmaß der Betroffenheit Dritter im Hinblick auf die aufzuklärende Straftat unangemessen erscheint, muss die Maßnahme unterbleiben. Der Entwurf sieht außerdem die Dokumentation der Verhältnismäßigkeitsprüfung vor. Für die Verwendung von nach § 100 g Absatz 2 Satz 2 StPO erhobenen Daten in anderen Fällen enthält der Entwurf einen Richtervorbehalt. Er sieht außerdem die Einführung einer festen Löschungsprüffrist vor.

Der Entwurf enthält jedoch keine Regelung, die dazu verpflichtet, den erhobenen Gesamtdatenbestand unverzüglich auf die zur Strafverfolgung erforderlichen Daten zu reduzieren. Eine entsprechende Regelung halte ich angesichts dessen, dass sich die nichtindividualisierte Funkzellenabfrage gegen alle Personen richtet, die sich in der Funkzelle aufhalten, für erforderlich.

Was aus dem sächsischen Gesetzentwurf wird, ist ungewiss. Die mit dem Entwurf befassten Bundesratsausschüsse haben Ende September 2011 beschlossen, die Beratung der Vorlage um vier Sitzungen zu vertagen. Ob der Gesetzentwurf jemals im Bundestag beraten werden wird, bleibt abzuwarten.

Aus datenschutzrechtlicher Sicht sind die Regelungen zur nichtindividualisierten Funkzellenabfrage gemäß § 100 g Absatz 2 Satz 2 StPO grundlegend zu überarbeiten.

Obwohl der eingangs geschilderte Vorfall in Dresden vom Februar 2011 außerhalb meiner Zuständigkeit liegt, verdient der weitere Fortgang eine kurze Nachbetrachtung, denn nicht nur in Sachsen müssen die unabhängigen Datenschutzbeauftragten gelegentlich dem Ansinnen entgegentreten, sie hätten sich aus der Überprüfung des Verhaltens von Polizei und Staatsanwaltschaft herauszuhalten, wenn hierfür eine richterliche Anordnung vorliegt.

Mit Bericht vom 9. September 2011 hat der Sächsische Datenschutzbeauftragte den Sächsischen Landtag über die Ergebnisse seiner datenschutzrechtlichen Prüfung der nichtindividualisierten Funkzellenabfragen und anderer Maßnahmen der Telekommunikationsüberwachung durch die Polizei und die Staatsanwaltschaft Dresden informiert. Daraufhin wurde seine Zuständigkeit zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld beziehungsweise nach einer richterlichen Anordnung von einigen Justizvertretern massiv in Zweifel gezogen. Dem ist entschieden entgegenzutreten. Auch im Bereich der Strafverfolgung ist es eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Dies haben die Datenschutzbeauftragten des Bundes und der Länder inzwischen in ihrer Entschließung vom 28./29. September 2011 (vgl. Anhang 25) noch einmal betont.

2. Grenzen der Kontrollbefugnis des Datenschutzes im Justizbereich

Regelmäßigen Lesern meines Tätigkeitsberichts ist bekannt, dass zwischen dem Justizministerium und meiner Dienststelle vor allem in früheren Zeiten regelmäßig Meinungsverschiedenheiten bestanden hinsichtlich der Frage, inwiefern der Landesbeauftragte für den Datenschutz die Gerichte des Lan-

des kontrollieren darf. Dass es auch zwischen Bürgern und meiner Dienststelle diesbezüglich zu Meinungsverschiedenheiten kommt, ist in den früheren Tätigkeitsberichten dagegen kaum erwähnt.

Ausgangspunkt für derartige Meinungsverschiedenheiten ist § 2 Absatz 3 LDSG. Nach dieser Vorschrift darf meine Dienststelle Gerichte nur insofern kontrollieren, soweit diese in Verwaltungsangelegenheiten tätig werden. Diese eingeschränkte Kontrollbefugnis ist auf die in Artikel 97 des Grundgesetzes verankerte richterliche Unabhängigkeit zurückzuführen.

Wie weit die richterliche Unabhängigkeit reicht beziehungsweise wie eng der Begriff der Verwaltungsangelegenheit im Bereich der gerichtlichen Rechtspflege zu fassen ist, ist für Laien oftmals schwer verständlich. Im Berichtszeitraum kam es sogar zu einer Klage eines Petenten gegen meine Dienststelle. Zugrunde lag folgender Sachverhalt:

Der Petent hatte sich an meine Dienststelle gewandt, weil er der Ansicht war, dass ein Richter im Rahmen eines arbeitsgerichtlichen Verfahrens unzulässigerweise aus dem bei den Arbeitsgerichten geführten elektronischen Verfahrensregister Informationen über ihn erhoben und diese in einem Beschluss verwendet habe.

Meine Dienststelle hatte dem Petenten daraufhin mitgeteilt, dass das Gericht diesen Beschluss im Rahmen eines anhängigen Rechtsstreits erlassen habe, die im Beschluss genannten personenbezogenen Daten des Petenten somit zu Zwecken der gerichtlichen Rechtspflege und nicht in einer Verwaltungsangelegenheit aus dem Verfahrensregister erhoben und genutzt habe, weshalb meine Dienststelle nicht befugt sei, seine Beschwerden zu überprüfen.

Der Petent war dagegen der Meinung, dass die – seiner Ansicht nach – datenschutzwidrige Vorgehensweise des Richters nichts mit der richterlichen Unabhängigkeit zu tun habe. Nur der Beschluss selbst falle unter die richterliche Unabhängigkeit, nicht jedoch die – aus Sicht des Petenten – missbräuchliche Datenverarbeitung durch den Richter. Aus diesem Grund klagte der Petent vor dem Verwaltungsgericht auf sachliche Bescheidung seiner Beschwerden durch meine Dienststelle. Das Verwaltungsgericht hat diese Klage als unbegründet abgewiesen. In den Entscheidungsgründen bestätigte das Verwaltungsgericht, dass die bei meiner Dienststelle eingelegten Beschwerden des Petenten eine richterliche Tätigkeit betreffen und deshalb außerhalb der Prüfungsbefugnis meiner Dienststelle liegen.

Nicht nur richterliche Entscheidungen, wie Urteile oder Beschlüsse, sondern alle richterlichen Tätigkeiten anlässlich eines anhängigen Rechtsstreits, sind von der Kontrollkompetenz meiner Dienststelle ausgenommen.

3. Eine Strafanzeige kommt selten allein – aber warum müssen Anzeigeerstatter über andere Anzeigeerstatter informiert werden?

Nach der Strafprozessordnung (StPO) ist ein Anzeigeerstatter von der Staatsanwaltschaft darüber zu informieren, wenn diese es – mangels konkreten Verdachts – ablehnt, Ermittlungen durchzuführen. Nicht einzusehen ist dagegen, warum Anzeigeerstatter im Rahmen dieser Mitteilung von der Staatsanwaltschaft auch die vollständigen Namen von anderen Personen erfahren müssen, die in der gleichen Angelegenheit ebenfalls eine Anzeige erstattet haben.

In einem an meine Dienststelle herangetragenen Fall hatte eine Staatsanwaltschaft in einer abschließenden Verfügung, in der begründet worden war, weshalb den zugrundeliegenden Anzeigen keine Folge gegeben wurde, die vollständigen Namen aller Anzeigeerstatter – es handelte sich um sechs Personen – genannt, die in der gleichen Angelegenheit Anzeigen erstattet hatten. Diese sechs Anzeigeerstatter erhielten jeweils eine Mehrfertigung der abschließenden Verfügung der Staatsanwaltschaft zur Kenntnis.

Auf Anfrage meiner Dienststelle bei der betreffenden Staatsanwaltschaft, auf welche Rechtsgrundlage diese Datenübermittlung gestützt werde, wurde mir von dort mitgeteilt, dass diese Vorgehensweise auf § 171 Satz 1 StPO beruhe, wonach die Staatsanwaltschaft nach ihrer Entscheidung, den An-

zeigen keine Folge zu geben, die Anzeigeerstatter zu bescheiden habe. Soweit in der abschließenden Verfügung auf das Vorbringen der Anzeigeerstatter im Einzelnen eingegangen worden sei, habe dies den jeweils anderen Anzeigeerstattern nicht vorenthalten werden können. Auch Schwärzungen oder Auslassungen in den Mitteilungen an die Anzeigeerstatter seien nicht angezeigt gewesen.

Die Begründung der Staatsanwaltschaft war für mich nicht nachvollziehbar. Ich habe zwar Verständnis dafür, dass die Staatsanwaltschaft weniger Aufwand betreiben muss, wenn sie die Anzeigeerstatter mit einem „Einheitsbescheid“ unterrichten kann. Rationalisierungszwang kann aber nicht jede Datenübermittlung rechtfertigen. § 171 Satz 1 StPO verpflichtet die Staatsanwaltschaft lediglich dazu, die Anzeige unter Angabe der Gründe zu bescheiden. Auch in den Richtlinien für das Straf- und Bußgeldverfahren wird hierzu nur ausgeführt, dass Begründungen aussagekräftig und für den rechtsunkundigen Antragsteller verständlich sein sollen beziehungsweise Mitteilungen nach § 171 Satz 1 StPO dem Anzeigeerstatter im Regelfall formlos zu übersenden sind. Diesen Anforderungen hätte Rechnung getragen werden können, ohne jeden Anzeigeerstatter über die Namen der jeweils anderen Anzeigeerstatter zu informieren. Diese Namen stellen weder einen Grund im Sinne des § 171 Satz 1 StPO beziehungsweise der genannten Vorschriften der Richtlinien für das Straf- und Bußgeldverfahren dar, noch machen sie die Begründung der Staatsanwaltschaft für die Anzeigeerstatter verständlicher. Auch ohne Namensnennung wäre es möglich gewesen, den Anzeigeerstattern sowohl das inhaltliche Vorbringen aller Anzeigeerstatter als auch die Gründe der Staatsanwaltschaft darzustellen, weshalb den Anzeigen nicht Folge gegeben wurde. Statt der Namen hätte die Staatsanwaltschaft genauso gut Buchstaben oder Ziffern im Text nennen und dem jeweiligen Anzeigeerstatter in einem Anschreiben mitteilen können, welcher Buchstabe oder welche Ziffer sich auf ihn bezieht.

In einer weiteren Stellungnahme hat die Staatsanwaltschaft ihre Vorgehensweise mit einem Beschluss des Bundesverfassungsgerichts (2 BvR 261/02) vom 27. Februar 2002 begründet. In diesem Beschluss geht es um Informationen über einen Beschuldigten, die dem Anzeigeerstatter, der zugleich Geschädigter war, von der Staatsanwaltschaft übermittelt worden waren. Das Bundesverfassungsgericht führt in dieser Entscheidung aus, dass der Anzeigeerstatter, der zugleich Geschädigter ist, umfassende Auskunftsansprüche habe, soweit er ein berechtigtes Interesse geltend machen könne und über den Abschluss des Verfahrens zu unterrichten sei. Die Übermittlung der entsprechenden, den Beschuldigten betreffenden Informationen stelle die einfach-rechtliche Ausformung des Anspruchs des Geschädigten auf rechtliches Gehör nach Artikel 103 Absatz 1 des Grundgesetzes dar. Der Geschädigte müsse in die Lage versetzt werden, in den gesetzlich vorgesehenen Fällen gegen die jeweilige Entscheidung der Staatsanwaltschaft – zum Beispiel mittels Klageerzwingungsverfahren gemäß § 172 StPO – vorgehen zu können. Dies sei jedoch nur möglich, wenn ihm die Entscheidung zuvor auch bekannt gemacht worden sei.

Diese Entscheidung entspricht datenschutzrechtlichen Grundsätzen. Sie kann meiner Ansicht nach jedoch nicht als Begründung für die Vorgehensweise der Staatsanwaltschaft in dem Ausgangsfall herhalten. Denn es liegt eine völlig andere Fallkonstellation vor. Hier geht es eben nicht um Informationen über den Beschuldigten, die der Geschädigte benötigt, um gegebenenfalls gegen die Entscheidung der Staatsanwaltschaft vorgehen zu können. Es geht vielmehr um die Übermittlung von Informationen über Anzeigeerstatter an andere Anzeigeerstatter, die nicht Geschädigte sind. Die Namen der Anzeigeerstatter sind unerheblich für die Entscheidung der Staatsanwaltschaft, keine Ermittlungen aufzunehmen, und damit auch für die Frage, ob der einzelne Anzeigeerstatter die Begründung der Staatsanwaltschaft nachvollziehen kann oder ob er es für aussichtsreich hält, hiergegen vorzugehen (wobei der Anzeigeerstatter, der nicht zugleich Geschädigter ist, anders als ein Geschädigter, auf die Rechtsbehelfe der Gegenvorstellung und Dienstaufsichtsbeschwerde beschränkt ist). Das vom Bundesverfassungsgericht angesprochene berechtigte Interesse an den übermittelten Informationen liegt in dem mir vorliegenden Fall im Verhältnis der Anzeigeerstatter untereinander daher gerade nicht vor.

Ich sehe daher weiterhin keine Rechtsgrundlage für die Vorgehensweise der Staatsanwaltschaft, jeden Anzeigeerstatter über die Namen der jeweils anderen Anzeigeerstatter zu informieren. Dementsprechend habe ich die Generalstaatsanwaltschaft über die Angelegenheit unterrichtet und darum gebeten, dafür Sorge zu tragen, dass die Staatsanwaltschaften künftig Mitteilungen nach § 171 StPO datenschutzkonform formulieren.

Wenige Tage vor Veröffentlichung dieses Tätigkeitsberichts teilte mir die Generalstaatsanwaltschaft mit, dass sie meine Ansicht grundsätzlich teile.

Mangels Rechtsgrundlage ist es nicht zulässig, dass Staatsanwaltschaften in Mitteilungen gemäß § 171 StPO einen Anzeigeerstatter über die Namen anderer Personen informieren, die in der gleichen Angelegenheit ebenfalls eine Anzeige erstattet haben.

3. Teil: Bildung und Forschung

1. Datenschutz an Schulen

1.1 Aktuelle Entwicklungen im Bereich der öffentlichen Schulen in Baden-Württemberg: Es tut sich etwas!

Im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 63 f.) hatte ich an verschiedenen Beispielen die datenschutzrechtliche Situation an öffentlichen Schulen des Landes Baden-Württemberg deutlich gemacht. Insbesondere hatte ich kritisiert, dass datenschutzrechtliches Fachwissen an Schulen oftmals kaum vorhanden sei, obwohl dort eine Vielzahl teilweise auch sensibler, personenbezogener Daten verarbeitet werden. Meine Kritik hatte ich nicht nur gegenüber den Schulen, sondern auch gegenüber dem Kultusministerium formuliert. In der Zwischenzeit hat das Kultusministerium erfreulicherweise Maßnahmen ergriffen, die zum Ziel haben, die datenschutzrechtliche Situation an öffentlichen Schulen zu verbessern:

So hat das Kultusministerium in den vergangenen Wochen und Monaten eine Konzeption zur Schulung von Schulleitern erarbeitet, bei der auch Mitarbeiter meines Amtes datenschutzrechtliche Belange einbringen konnten. Es ist danach geplant, Schulleitern in einem eintägigen Seminar datenschutzrechtliches Basiswissen und den behördlichen Datenschutzbeauftragten in einem zweitägigen Seminar ein tiefergehendes Wissen zu vermitteln. Dem Vernehmen nach ist auch angedacht, für weitere schulische Gruppen entsprechende Seminare anzubieten. Das Regierungspräsidium Stuttgart hat in seiner Funktion als Aufsichtsbehörde für seinen Zuständigkeitsbereich angeordnet, dass die Schulen einen behördlichen Datenschutzbeauftragten zu bestellen haben. Diese Entwicklung ist sicherlich zu begrüßen, obgleich fraglich ist, ob – zumindest in der nächsten Zeit – alle bestellten Datenschutzbeauftragten über das erforderliche Fachwissen auch tatsächlich verfügen. Dies wird wohl erst dann der Fall sein, wenn alle geschult sind. Weiterhin ist zu überlegen, ob diese dann nicht über regelmäßige regionale Arbeitskreise vernetzt werden und sich so über etwaige Probleme und entsprechende Lösungen austauschen können.

Auch in Sachen Verfahrensverzeichnis hat sich einiges getan: Ich hatte seinerzeit bemängelt, dass Verfahrensverzeichnisse oftmals fehlerhaft und unvollständig erstellt wurden. Das Kultusministerium hat nun veranlasst, dass für zentral zur Verfügung gestellte automatisierte Verfahren wie beispielsweise Moodle oder das pädagogische Netzwerk sowie von vielen Schulen eingesetzte Schulverwaltungssoftware Vorlagen für Verfahrensverzeichniseinträge erarbeitet werden. In diese Vorlagen werden alle zentral beziehungsweise systembedingt vorgegebenen Datenschutzmaßnahmen eingetragen. Es obliegt dann den einzelnen Stellen, ihre spezifischen Konfigurationen einzutragen. Ich halte dies für eine sinnvolle und notwendige Hilfestellung. Zudem beabsichtigt das Kultusministerium die Einführung eines webbasierten Werkzeugs für schulische Verfahrensverzeichnisse, in welches die zentral vorgegebenen automatisierten Verfahren bereits weitgehend eingetragen sind, damit auch hier die Schulen nur noch ihre eigenen Besonderheiten nachzutragen haben. Auf diese Weise kann das Kultusministerium als vorgesetzte Behörde die Qualität der Verfahrensverzeichniseintragungen in eigener Zuständigkeit prüfen. Aus meiner Sicht ist dies sehr zu begrüßen.

Erfreulicherweise hat das Kultusministerium auch meine Anregung, einen Lehrer an mein Amt zeitlich befristet abzuordnen, aufgegriffen. Ich erhoffe mir dadurch eine positive Wirkung hinsichtlich meiner Beratung der Schulen, verbunden mit der Hoffnung, dass Hemmschwellen abgebaut und datenschutzrechtliches Problembewusstsein geschaffen wird.

1.2 Sparsamkeit am falschen Platz: Datenschutz an einer Gesamtschule

Besorgte Eltern von Schülern einer Gesamtschule haben sich an mein Amt gewandt und mitgeteilt, eine Lehrkraft dieser Schule habe ihren Schülern Kopien des Lehrplans für Geschichte ausgeteilt. Sie habe der Klasse zuvor erklärt, dass sie für Kopien – aus Gründen der Sparsamkeit und des Umweltschutzes – stets bereits einseitig bedrucktes Papier aus dem Mülleimer des Kopierraums verwenden würde. Dabei habe sie betont, dass möglicherweise auch dem Datenschutz unterliegende Kopien dabei seien, die die Schüler wieder zurückgeben könnten. Und tatsächlich hat die Lehrerin Schreiben an Eltern über störendes Verhalten einzelner, namentlich genannter Schüler „wiederverwendet". Die Namen von Eltern und Schülern waren dabei so unzureichend geschwärzt, dass die Namen der Betroffenen ohne Weiteres zu lesen waren. Auf diese Weise seien, so teilten die Eltern mit, persönliche Mitteilungen der Schulleitung an einzelne Eltern zum Verhalten ihrer Kinder weitergegeben worden, wobei Name und Anschrift der Erziehungsberechtigten und der Kinder erkennbar gewesen seien.

Die Schule hat – nach mehrmaliger Nachfrage – den Sachverhalt bestätigt. Allerdings sei die Lehrerin der Auffassung gewesen, es sei ausreichend, die Adressen zu schwärzen; dabei habe sie versäumt, die Wirksamkeit des Schwärzens zu überprüfen. Zudem sei die Lehrkraft davon ausgegangen, es genüge, Oberstufenschüler darauf hinzuweisen, dass Blätter mit erkennbaren personenbezogenen Daten Dritter von den Schülern zurückzugeben seien. Ferner teilte die Schule mit, es sei im Kollegium üblich, dass personenbezogene Schreiben, die keine Verwendung mehr fänden, von der Person, die direkt mit dem Schriftstück zu tun hatte, zerrissen und weggeworfen würden. Im Sekretariat oder bei der Schulleitung anfallendes Schriftgut werde im Reißwolf vernichtet.

Den geschilderten Sachverhalt habe ich wie folgt bewertet:

Bei den Angaben auf den Elternbriefen handelte es sich um besonders sensible personenbezogene Daten, die unter anderem die Verhaltensauffälligkeiten einiger Schüler beschreiben. Der Umgang mit solchen Daten stellt hohe Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen. Die an der Schule getroffenen organisatorischen Regelungen waren ganz offensichtlich nicht ausreichend: Die Lehrkraft hatte nur unzureichende Maßnahmen zur Unkenntlichmachung personenbezogener Daten ergriffen. Es genügte auch nicht, die Schüler aufzufordern, Papier mit personenbezogenen Daten Dritter zurückzugeben. Ungeachtet der Frage, ob die Lehrerin davon ausgehen konnte, dass die Schüler ihrer Aufforderung, entsprechende Papiere zurückzugeben, nachkommen, nahm sie in Kauf, dass die Schüler – und damit Unbefugte – diese Daten einsehen konnten. Der Umstand, dass Unterlagen mit solch sensiblen personenbezogenen Daten in einem Papiermülleimer gelandet sind, belegt, dass auch anderen Lehrkräften der Schule ein korrekter Umgang mit Schriftgut nicht bekannt war. Auch die Darstellung der Schule, wonach es im Kollegium üblich sei, nicht mehr benötigtes Schriftgut mit personenbezogenen Daten unter anderem durch „Zerreißen" zu vernichten, zeigt grundsätzliche datenschutzrechtliche Defizite im Schulbetrieb auf. Allein durch das manuelle Zerreißen von Schriftstücken kann nicht wirksam verhindert werden, dass Unbefugte auf Daten zugreifen. Zwar hat die Schule mitgeteilt, dass die Vorgehensweise der Lehrkraft falsch gewesen und diese belehrt worden sei. Jedoch sind faktisch sensible personenbezogene Daten von Schülern durch mangelhafte organisatorische Kontrollen in die Hände unbefugter Dritter gelangt. Zudem hat die Schule nicht mitgeteilt, dass die bereits in der Vergangenheit im Rahmen von Gesamtlehrerkonferenzen durchgeführten Belehrungen erweitert oder konkretisiert worden seien. Insofern konnte an dieser Schule der datenschutzgerechte Umgang mit Schriftstücken, die personenbezogene Daten enthalten, offenbar nicht ausreichend gewährleistet werden. Eine Beanstandung war die zwangsläufige Folge.

2. Datenschutz im Hochschulbereich

2.1 Sicherheitsforschung – für welchen Zweck?

„Die Sicherheitsrisiken haben sich gewandelt: Versorgungsnetze als Lebensnerven der Gesellschaft können trotz robuster Technik schon durch kleine Störungen ausfallen, die globale Mobilität erleichtert die Verbreitung von Gefahren. Aber auch Großveranstaltungen können zur sicherheitstechnischen Herausforderung werden, kriminell motivierte Gruppen erheblichen Schaden anrichten. Was kann die Forschung tun, um Katastrophen zu verhindern? Wie kann die Sicherheit der Bürgerinnen und Bürger verbessert werden? Diesen Fragen widmet sich die Sicherheitsforschung in der Hightech-Strategie der Bundesregierung". So heißt es im Internet-Auftritt des Bundesministeriums für Bildung und Forschung zum Thema „Sicherheitsforschung – Forschung für die zivile Sicherheit".

Auch im breiten Themenspektrum der Forschung finden sich immer wieder auch für den Datenschutz interessante Vorhaben. Niemand wird bestreiten wollen, dass Forschung auch in Bereichen notwendig ist, in denen es um höchstpersönliche Rechte Betroffener gehen kann. Daher löste ein Pressebericht aus Tübingen im Juni 2010 bei mir großes Interesse aus: Es ging darin um ein Forschungsprojekt zur „intelligenten" Videoüberwachung, das unter Federführung eines Instituts der Universität Tübingen in Zusammenarbeit mit weiteren drei deutschen Universitäten als interdisziplinäres Projekt sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen zur Mustererkennung und zum Video Tracking erarbeiten und Lösungen anbieten soll. Dieses Projekt mit dem Namen MuViT wird vom Bundesministerium für Bildung und Forschung gefördert, ist aber nur eines von vielen Projekten der Sicherheitsforschung, für die das Ministerium seit dem Jahr 2007 immerhin 235 Millionen Euro bis Ende des Jahres 2013 bereitstellt.

Wie der Name schon sagt, geht es in dem Projekt darum, „auffällige" Verhaltensweisen (Muster) mit der Hilfe der Videotechnik (wieder) zu erkennen und die erkannten Personen im Bild weiter zu verfolgen („Tracking").

Die in dem Forschungsprojekt angelegte Verbindung zwischen der rein technischen Betrachtung von Mustererkennungs- und Video-Tracking-Techniken, der Prüfung sozialpsychologischer Auswirkungen auf die beobachteten Personen, dem gesellschaftlichen Aspekt des Themas Sicherheit aus der Sicht aller betroffenen Kreise und einer umfassenden rechtlichen Bewertung (einschließlich der Implementierung solcher Verfahren in die deutsche Rechtsordnung) stellt meines Erachtens ein positives Beispiel für derartige Vorhaben dar. Ich habe daher den Kontakt zum Institut gesucht und wurde, erfreulich offen, mit den Überlegungen des Instituts und ersten Ergebnissen vertraut gemacht. Ich gehe davon aus, dass mir noch Gelegenheit gegeben wird, die datenschutzrechtlichen Anforderungen einzubringen.

Denn wenn man einmal näher in das Thema „Sicherheitsforschung" einsteigt, wird man schon wegen der Vielfalt der vom Bundesministerium für Bildung und Forschung geförderten Vorhaben auf diesem Gebiet nachdenklich. Ich kann nur empfehlen, den Internet-Auftritt *www.bmbf.de* mit der Liste von immerhin acht bewilligten Verbundprojekten aus dem Themenfeld „Mustererkennung" näher anzuschauen. Es lohnt sich aber auch ein Blick über den nationalen Tellerrand hinaus, denn die BT-Drucksache 17/3940 vom November 2010 lässt erkennen, dass es nicht nur national, sondern vor allem in Europa Forschungsvorhaben gibt, die umfassend zu Eingriffen in die Bürgerrechte beitragen könnten: In diesem Zusammenhang ist vor allem das von der Europäischen Kommission im 7. Forschungsrahmenprogramm auf fünf Jahre angelegte Vorhaben INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment – Intelligentes Informationssystem zur Unterstützung von Überwachung, Suche und Erfassung für die Sicherheit von Bürgern in städtischer Umgebung) zu nennen, das mit allen denkbaren

technischen Überwachungsmitteln Terrorismus, schwere Verbrechen, auch im Internet, verhindern soll, um die Sicherheit der Bürger zu verbessern. Die Reaktionen auf dieses Projekt, die im Internet nachzulesen sind, erwecken den Eindruck, dass „1984“ von George Orwell im Vergleich zu INDECT harmlos wäre – wenn es denn Realität wird. INDECT könnte für die Zukunft eine völlige Überwachung der Bürgerinnen und Bürger ermöglichen und damit den Weg zum Polizeistaat ebnen. Ich finde es auch nicht wirklich beruhigend, dass nach der erwähnten Bundestags-Drucksache bisher keine mittelbaren oder unmittelbaren Verbindungen zwischen den Forschungsprojekten für die zivile Sicherheit in Deutschland und INDECT bestehen sollen, denn man fragt sich unwillkürlich, in welchem anderen europäischen Land die Forschungsergebnisse eines Tages eingesetzt werden sollen und welcher Wertekonsens in Europa eigentlich besteht. Immerhin werden die europäischen Forschungsprojekte auch von Deutschland über die EU mitfinanziert.

Ein anderes Projekt wurde mir Ende Juli 2011 durch Medienanfragen und Bürgereingaben bekannt. Bei einem Fußballspiel sollte im Karlsruher Wildparkstadion die Technik für das Projekt „Parallele Gesichtserkennung in Videoströmen (PaGeVi)“ getestet werden. Auch hier hatte, wie in LT-Drucksache 15/470 nachzulesen ist, nach Auskunft des federführenden Karlsruher Instituts für Technologie (KIT) das Bundesministerium für Bildung und Forschung eine Förderung bewilligt. Bei diesem Projekt sollte ein Verfahren zur Identifizierung gesuchter Personen bei Großveranstaltungen weiterentwickelt werden. Die Videokameras waren schon installiert. Allerdings hatte sich bis zu der Berichterstattung offenbar niemand darüber Gedanken gemacht, ob Aufnahmen von den nicht als Testpersonen vorgesehenen Zuschauern des Spiels denn überhaupt zulässig sind. Nach den ersten Medienberichten gingen zahlreiche Anfragen bei meiner Dienststelle ein. Meine Recherchen ergaben, dass das KIT mit einer interessierten Sicherheitsfirma zwar etwas überlegt hatte, aber angefangen von der Polizei, über die Vereinsspitze des Karlsruher SC, die Stadt bis hin zu den für die Beratung in Datenschutzfragen an der Universität zuständigen Stellen, ganz zu schweigen von meiner Dienststelle und den Fans des KSC niemand vorher (zumindest nicht offiziell) beteiligt worden war. Damit ergaben sich so viele Fragezeichen zu dem Vorhaben, dass das KIT von einer praktischen Umsetzung zunächst absah. Wie das Projekt weitergehen wird, bleibt abzuwarten. Zwar sind nach den Bestimmungen des Landesdatenschutzgesetzes Forschungsvorhaben hinsichtlich der Datenverarbeitung grundsätzlich privilegiert, jedoch sind auch dabei Mindestanforderungen zu beachten. Was mir bis zur vorläufigen Einstellung des Projekts unklar blieb: Warum hat sich niemand die Mühe gemacht, die gesellschaftliche Akzeptanz und rechtliche Zulässigkeit des Vorhabens vorab zu prüfen? Das etwas „blauäugige“ Hineinstolpern in absehbare Konflikte könnte zu dem Schluss verleiten, dass eher die Exportchancen für eine zweifelhafte Technik im Vordergrund standen.

Das Projekt „MuViT“ der Universität Tübingen stellt mit seinem interdisziplinären Ansatz aus meiner Sicht die entscheidenden Fragen. Denn wer will schon mit absoluter Sicherheit sagen, was unter welchen Rahmenbedingungen als „normales Verhalten“ anzusehen ist. Ich hoffe, dass dieses Projekt dem Schutz der Privatsphäre und damit auch dem Datenschutz hinreichende Aufmerksamkeit widmet.

2.2 Ohne nachzudenken ins Internet eingestellt und dann vergessen?

Ein Petent hat sich an unser Amt gewandt und darüber geklagt, dass im Zusammenhang mit einer Seminarpräsentation an einem Hochschulinstitut im Vorfeld an alle Teilnehmer eine Nachricht per E-Mail versendet worden sei. Dieser Nachricht sei eine Liste angefügt gewesen, die neben den Präsentationsterminen auch Vor- und Nachnamen sowie die zugehörigen Matrikelnummern von allen Teilnehmern enthalten habe. Insgesamt sei diese Liste an ca. 30 Personen geschickt worden. Kurze Zeit nach dem Versand dieser E-Mail sei noch eine zweite E-Mail an die Seminarteilnehmer versandt worden, die erneut die Namen und zu-

gehörigen Matrikelnummern im Anhang enthalten habe. Mit Hilfe dieser E-Mails sei es nun unter anderem möglich, die auf der Homepage des Instituts veröffentlichten Noten einzelnen Personen zuzuordnen. Eine Einwilligung der Betroffenen habe hierfür nicht vorgelegen.

Die Hochschule hat auf meine Nachfrage mitgeteilt, dass tatsächlich die genannte E-Mail zweimal versandt worden sei. Zudem sei aufgrund von Unwissenheit und Vergesslichkeit auf dem Web-Auftritt des Instituts die Liste mit Matrikelnummern und Noten veröffentlicht worden. Die Mitarbeiter des betroffenen Lehrstuhles seien unverzüglich nach Eingang der Beschwerde diesbezüglich belehrt worden. Die im Internet veröffentlichte Liste, in der Matrikelnummern und Noten aufgeführt waren, sei ebenfalls unmittelbar nach Bekanntwerden der Beschwerde entfernt worden.

Natürlich war die vorliegende Verarbeitung personenbezogener Daten – auch die Veröffentlichung von Matrikelnummern und Noten im Internet – nicht zulässig. Aufgrund des Umstandes, dass sofort nach dem Bekanntwerden die Verarbeitung beendet wurde und sämtliche Mitarbeiter des Lehrstuhls belehrt wurden, sah ich jedoch von einer förmlichen Beanstandung ab.

Auch an einer Pädagogischen Hochschule des Landes konnte ich eine solche Vergesslichkeit beobachten. Eine Studentin hatte sich an mein Amt gewandt und mitgeteilt, dass die Hochschule unverschlüsselte sog. Praktikalisten auf ihrer Homepage eingestellt habe. Dort abgelegte, personenbezogene Daten seien damit weltweit abrufbar gewesen. Auch diese Petentin gab an, dass sie keine Einwilligung für diese Art der Verarbeitung personenbezogener Daten erteilt habe. In einem Telefonat mit dem Prorektor der Pädagogischen Hochschule stellte sich heraus, dass das Dokument eigentlich schon längst hätte entfernt sein sollen, dies jedoch tatsächlich zunächst nicht geschehen war. Tatsächlich wurde nur der Link, nicht jedoch die Datei an sich entfernt. Man sicherte meinem Amt zu, dass das abrufbare Dokument umgehend aus dem Internet entfernt werde. Einige Tage darauf war dann tatsächlich das Dokument nicht mehr über das Internet abrufbar. Ein wirkliches Umdenken war damit offenbar nicht verbunden, denn die Pädagogische Hochschule erkundigte sich kurz darauf, ob das Verfahren in der bereits bekannten Weise wieder aufgenommen werden könne beziehungsweise welche Verfahrensänderung vorgenommen werden müsse.

Bei der Veröffentlichung personenbezogener Daten im Internet rate ich den öffentlichen Stellen des Landes zu großer Zurückhaltung. Die Erforderlichkeit für eine solche Veröffentlichung ist dabei in einem strengen Sinne zu prüfen.

4. Teil: Gesundheit und Soziales

1. Abschnitt: Gesundheit

1. Die Elektronische Gesundheitskarte – eine fast unendliche Geschichte

Nach vielen kontroversen politischen und fachlichen Diskussionen in der Vergangenheit hat mit knapp sechs Jahren Verzögerung schrittweise die bundesweite Auslieferung der neuen Elektronischen Gesundheitskarte (eGK) begonnen. Die Karte gilt ab dem 1. Oktober 2011 als Versicherungsnachweis.

Vielfältige Probleme, vor allem technischer Art, aber auch datenschutzrechtliche Bedenken, führten in der Vergangenheit immer wieder zu Verzögerungen; die Einführung stand zeitweise sogar auf der Kippe (vgl. 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910, 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650, 28. Tätigkeitsbericht für das Jahr 2007, LT-Drucksache 14/2050, 29. Tätigkeitsbericht 2009, LT-Drucksache 14/5500). Erst Ende 2010 entschied die Bundesregierung, dass die Karte doch 2011 eingeführt wird – allerdings in abgespeckter Form. Die Karte übernimmt in einem ersten Schritt die Funktionen der bisherigen Krankenversichertenkarte. Zur Grundausstattung der neuen Karte gehören – wie auf der bisherigen Krankenversichertenkarte – wichtige administrative Daten wie der Versichertenstammdatensatz, aber auch die schon länger eingeführte lebenslange Versichertennummer. Als zusätzliches Identifizierungsmerkmal kommt ein Foto des Karteninhabers hinzu. Das aufgebrachte Foto für Versicherte ab einem Alter von 15 Jahren soll dem Missbrauch der Karte vorbeugen.

Die Ausgabe der Karte gilt als erster Schritt zu einer vernetzten Telematik-Infrastruktur im Gesundheitswesen. Denn in weiteren Ausbaustufen sollen auf Wunsch des Versicherten auch Notfalldaten – etwa über bestehende Vorerkrankungen oder Allergien – aufgenommen werden. Schließlich soll der elektronische Arztbrief kommen, mit dem Ärzte untereinander Daten auf sicherem Weg austauschen können. Völlig unklar ist, ob und wann weitere Anwendungen wie die elektronische Patientenakte realisiert werden. Zunächst wurden jedenfalls alle zusätzlichen Funktionen zurückgestellt, bis praxistaugliche und sichere Lösungen vorgelegt werden. Das aber kann noch Jahre dauern. Aktuell wird auch die Aufnahme von Organspendeerklärungen diskutiert. Weitere Verfügungen etwa zur Gewebespende, zur Vorsorgevollmacht und ein Hinweis, wo die Patientenverfügung gespeichert ist, könnten folgen.

Momentan werden in Krankenhäusern und Praxen neue – Kartenlesegeräte, die für die elektronische Gesundheitskarte geeignet sind, installiert. Bis zum Ende des Jahres müssen die gesetzlichen Krankenkassen zehn Prozent ihrer Versicherten mit dieser Karte ausstatten, andernfalls drohen Kürzungen finanzieller Mittel.

Den weiteren Verlauf des Projektes werde ich aufmerksam verfolgen und darauf achten, dass die datenschutzrechtlichen Anforderungen, vor allem die Rechte der Betroffenen, gewahrt werden.

2. Datenschutz im Krankenhaus

2.1 Kontrollbesuch in einem Klinikum

Bei einem Krankenhausaufenthalt entstehen große Mengen an sensiblen Daten über Patienten, ihre persönliche Situation und ihren Gesundheitszustand. Nur wenn Patienten sicher sein können, dass sensible Informationen über sie mit größtmöglicher Vertraulichkeit behandelt werden, wird das Krankenhaus den an ein modernes Dienstleistungsunternehmen gestellten Anforderungen gerecht.

Gesundheitsdaten gelten als besonders sensibel und sind nach der EU-Datenschutzrichtlinie und den deutschen Datenschutzgesetzen besonders schützenswert und geheimhaltungsbedürftig. Sie werden sowohl

durch § 203 des Strafgesetzbuchs (berufsmäßige Verschwiegenheitspflicht der Ärzte und ihrer Gehilfen) wie auch durch besondere bereichspezifische Vorschriften (Landeskrankenhausgesetz, Sozialgesetzbuch, Bundes- und Landesdatenschutzgesetz, etc.) geschützt. Es ist daher von höchster Bedeutung, dass Krankenhausmitarbeiter und -verwaltung die vom Gesetzgeber vorgegebenen Grenzen für den Umgang mit Patientendaten sorgfältig beachten. Dass dies nicht immer einfach ist, zeigte einmal mehr ein im Berichtszeitraum durchgeführter Kontrollbesuch eines großen Klinikums in Baden-Württemberg.

Erfreulich war zu sehen, dass in wichtigen Bereichen des Klinikums, wie Patientenaufnahme, Verwaltung, Krankenhausapotheke, aber auch auf einer von uns besuchten Krankenstation, ein hohes Datenschutzbewusstsein herrscht. Namentlich in der Patientenaufnahme und in der Verwaltung konnte gegenüber einem früheren Kontrollbesuch eine deutliche Verbesserung festgestellt werden. Leider stießen meine Mitarbeiter aber auch auf zum Teil gravierende Datenschutzmängel, die von mir beanstandet wurden.

So waren in einigen Bereichen des Klinikums erhebliche Mengen von teilweise älteren Dokumenten mit personenbezogenen Daten auf Dateisystemen abgelegt, die dort nicht (mehr) benötigt wurden. Zudem war die Zugriffsberechtigung auf diese Dokumente viel zu großzügig vergeben worden. Von einer passgenauen Berechtigungsstruktur, bei der auch nur diejenigen auf die Dokumente zugreifen können, die diese zur Erfüllung ihrer dienstlichen Aufgaben benötigen, konnte nicht die Rede sein. Ferner waren die Berechtigungen auf die Systemsteuerung teilweise so weitreichend, dass es Benutzern möglich war, Sicherheitseinstellungen zu verändern (Deaktivierung des Virenschutzes, Anlegen neuer User u. a.).

Erhebliche datenschutzrechtliche Probleme bereiten vor allem das Krankenhausarchiv und die im Klinikum installierten Videoüberwachungsanlagen.

2.1.1 Das Krankenhausarchiv

Die Digitalisierung der Datenverarbeitung im Klinikum ist noch nicht so weit fortgeschritten, dass auf herkömmliche Archive verzichtet werden kann. Bei den im von meinen Mitarbeitern besuchten Zentralarchiv gelagerten Akten handelt es sich daher auch um Papierakten, die auf Rollfilmen bzw. Mikrofilmen gesichert wurden. Seit 2006 werden Patientenakten elektronisch archiviert.

Positiv anzumerken ist, dass das Klinikum eine Archivordnung eingeführt hat, die für alle Patientenakten, unabhängig von der Speicherungsform, Gültigkeit hat. Aus datenschutzrechtlicher Sicht bestand jedoch erheblicher Nachbesserungsbedarf (zum Beispiel Aufbewahrungsfristen, Löschungsregelungen, Zutritts- und Zugriffsregelungen, Dokumentation der Herausgabe und Rückgabe sowie Entsorgung der Akten).

Geradezu erschreckend war der recht sorglose Umgang der im Archiv Beschäftigten mit den Patientenakten. Diese schienen bei vielen tagtäglich praktizierten Arbeitsabläufen kaum oder gar nicht an die datenschutzrechtlichen Konsequenzen zu denken:

- Dass die zwar mangelhaften, aber dennoch existierenden archivrechtlichen Vorschriften offensichtlich gar nicht bekannt waren, zeigte sich bereits daran, dass eine Mitarbeiterin erst nach langer Suche eine ältere Fassung der Archivordnung, die längst nicht mehr galt, vorlegte.
- Obwohl die Archivordnung Aufbewahrungsfristen vorsah, war nicht gewährleistet, dass Patientenakten nach Ablauf dieser Fristen vernichtet beziehungsweise Patientendaten gelöscht werden. So existierten bei unserem Besuch Akten über Patienten, deren Entlassung mehr als 30 Jahre zurücklag. Auf Mikrofilm archivierte Akten reichten sogar bis in das Jahr 1971 zurück.

– Zutrittsberechtigt waren laut Archivordnung nur Beschäftigte des Klinikums, die über eine Anforderungsberechtigung verfügen. Allerdings mussten wir feststellen, dass die Berechtigung allenfalls hinsichtlich des Tragens eines Klinikausweises geprüft wurde. Ob der/die anfordernde Beschäftigte berechtigt war, die gewünschte Akte einzusehen, wurde gar nicht oder nur eingeschränkt überprüft. Nach einer gegebenenfalls erforderlichen Einwilligung des Patienten wurde ebenso wenig gefragt.

– Bestimmungen darüber, wer und unter welchen Voraussetzungen einen Schlüssel und damit Zugang außerhalb der regelmäßigen Öffnungszeiten zum Zentralarchiv erhält, fehlten. Mit Hilfe des Schlüssels konnten daher die Beschäftigten des Klinikums ohne weiteres Akten aus dem Archiv entnehmen, ohne dass dies in irgendeiner Weise kontrolliert worden wäre.

– Auf Patientenakten, die vom Archiv an Beschäftigte herausgegeben wurden, wurde lediglich handschriftlich vermerkt, an welchem Tag die Akte, Teile davon und/oder Aufnahmen entnommen wurden. An wen die Krankenakte herausgegeben wurde und wann sie durch wen zurückgegeben wurde, wurde nicht dokumentiert. Ein Überblick, welche Akten sich aktuell wo befinden, war nicht möglich.

Das Klinikum hat zwischenzeitlich die Archivordnung unter Berücksichtigung meiner Hinweise überarbeitet sowie ergänzend eine Verfahrensanweisung zur Durchführung der stationären Behandlungsdokumentation und des Aktenlaufs bis zur Archivierung erstellt. Die neue Archivordnung in Verbindung mit der Verfahrensanweisung bietet nunmehr eine gute Grundlage für den datenschutzgerechten Umgang mit Patientenakten. Klare und unmissverständliche Regelungen, insbesondere über Archivzugang, Anforderungsberechtigung, Dokumentation der Aktenherausgabe und Rückgabe stellen sicher, dass künftig jederzeit nachvollzogen werden kann, wer wann zu welchem Zweck welche Patientenakte/Fallakte aus dem Archiv erhalten und diese wieder zurückgegeben hat. Mindestens ebenso wichtig ist es nun, die Beschäftigten im Archiv in Sachen Datenschutz grundlegend und immer wieder zu schulen und dabei insbesondere sowohl die rechtlichen Grundlagen des Datenschutzes als auch die spezifischen Regelungen des Klinikums zu vermitteln. Eine erste Schulung für das Archiv hat bereits stattgefunden; dies gilt es nun intensiv fortzuführen. Nur so kann gewährleistet werden, dass der Umgang mit Patientenakten im Archiv datenschutzkonform erfolgt.

2.1.2 Die Videoüberwachung

Bereits im Frühsommer 2009 hatte ich aufgrund von Anfragen einzelner Bürger das Klinikum aufgefordert, zu Videoüberwachungsmaßnahmen in den verschiedenen Häusern Stellung zu nehmen. Obwohl, wie ich inzwischen weiß, 90 Überwachungsanlagen im Klinikum betrieben werden, hatte der Datenschutzbeauftragte des Klinikums bis zu diesem Zeitpunkt keinerlei Kenntnis davon, dass, wo, zu welchem Zweck und unter welchen Voraussetzungen Videoüberwachungsanlagen in der von ihm zu beaufsichtigenden Einrichtung betrieben werden. Nicht hinnehmbar war auch, dass dem Datenschutzbeauftragten die beabsichtigten Überwachungsmaßnahmen vor deren Inbetriebnahme nicht angezeigt wurden und keine datenschutzrechtliche Zulässigkeitsprüfung erfolgte.

Ende 2009 hat die Geschäftsleitung des Klinikums endlich beschlossen, sich dieser Problematik anzunehmen. Alle Abteilungen und Fachbereiche wurden aufgefordert, sowohl bereits installierte als auch alle künftigen Videoanlagen dem Datenschutzbeauftragten zu melden. Außerdem werden nunmehr mit Hilfe eines

Formulars alle für die Erstellung des Verfahrensverzeichnisses und für die Durchführung der Vorabkontrolle erforderlichen Daten erhoben.

Kein Verständnis kann ich dafür aufbringen, dass das Klinikum – trotz der getroffenen Maßnahmen – anlässlich eines weiteren Kontrollbesuchs die genaue Anzahl der Anlagen immer noch nicht zuverlässig angeben konnte (84 bis 120 Anlagen). Auch die nachträgliche datenschutzrechtliche Prüfung der einzelnen Anlagen erfolgte schleppend und – soweit ersichtlich – bis heute nur unzureichend. Mitte 2010 wurde mir zwar eine Aufstellung mit insgesamt 99 Anlagen vorgelegt. Alle Anlagen wurden jedoch als genehmigungsfähig bewertet, obwohl sich bereits beim ersten Blick auf die Liste ergab, dass bei der überwiegenden Anzahl der Anlagen die Einwilligung der Betroffenen fehlte, die Kennzeichnung ungeklärt war, Angaben zum Zweck fehlten, der Antrag unvollständig war oder ganz fehlte und/oder die Löschung ungeklärt war. Auf welcher Rechtsgrundlage und gegebenenfalls unter welchen Voraussetzungen die einzelnen Anlagen zulässigerweise betrieben werden dürfen, war ebenfalls nicht nachvollziehbar. Inzwischen steht zwar die Anzahl der betriebenen Videoanlagen fest. Nach wie vor sind aber erhebliche Defizite im Zusammenhang mit der Prüfung der Zulässigkeit des Betriebs der Videoanlagen festzustellen, weil insbesondere die Erforderlichkeit der einzelnen Anlagen vom Datenschutzbeauftragten allenfalls unzulänglich ge- beziehungsweise überprüft wurde. So konnte beispielsweise die Notwendigkeit des Betriebs zweier Kameras im Bereich von Personenaufzügen nicht dargelegt werden. Die eingesetzten Videoanlagen wurden zwischenzeitlich mit einem blauen Schild oder einem Aufkleber mit Kamerasymbol gekennzeichnet. Insoweit bestehen aber Bedenken, ob die markierten Bereiche den überwachten Raum tatsächlich umfassen. Dies bedeutet aus meiner Sicht, dass auch heute noch nicht feststeht, ob das Klinikum alle Videoanlagen betreiben darf. Ich werde daher weiterhin alle mir zur Verfügung stehenden aufsichtsrechtlichen Mittel ergreifen, um sicherzustellen, dass nur die den rechtlichen Anforderungen genügenden Anlagen eingesetzt werden. Dies könnte unter anderem auch die Aufforderung umfassen, einzelne Anlagen außer Betrieb zu nehmen.

2.1.3 Der Datenschutzbeauftragte im Klinikum

Nach § 51 Absatz 1 des Landeskrankenhausgesetzes (LKHG) hat der Krankenhausträger für das Krankenhaus einen Beauftragten für den Datenschutz zu bestellen. Dieser Verpflichtung ist das Klinikum nachgekommen. Dem zum Datenschutzbeauftragten bestellten Mitarbeiter wurden jedoch zusätzlich Zuständigkeiten im Bereich der Revision übertragen; Mitarbeiter zu seiner Unterstützung stehen ihm nicht zur Verfügung. Dass diese Personalkapazität in Anbetracht der Aufgabe hinten und vorne nicht reicht, mögen einige Zahlen belegen: Das Klinikum betreibt an mehreren Standorten insgesamt 52 Kliniken und Institute mit rund 2 300 Betten; rund 6 400 Mitarbeiterinnen und Mitarbeiter versorgen die Patienten oder sind in Verwaltung und Technik tätig. Angesichts der Größe des Klinikums, der zunehmenden Komplexität der datenschutzrechtlichen Fragestellungen sowie der Sensibilität von Patientendaten ist eine sachgerechte und umfassende Aufgabenerfüllung durch einen einzelnen Datenschutzbeauftragten – sei er noch so kompetent und engagiert – faktisch nicht leistbar. Die von mir festgestellten, teilweise schwerwiegenden Datenschutzverstöße haben sicherlich vielfältige Ursachen. Ein wesentlicher Grund liegt nach meiner Einschätzung gerade auch in der unzureichenden personellen Ausstattung des Datenschutzbeauftragten. Ich halte es daher für dringend geboten, dass dem innerbetrieblichen Datenschutz durch konkrete Veränderungen mehr Beachtung geschenkt wird.

In dieser Frage zeigt sich das Klinikum grundsätzlich aufgeschlossen. Von der von mir vorgeschlagenen Unterstützung des Datenschutzbeauftragten durch die im hausinternen Datenschutzleitfaden ohnehin bereits vorgesehene Möglichkeit, sogenannte Bereichsdatenschutzbeauftragte zu bestellen, soll künftig Gebrauch gemacht werden. Geplant ist danach, in den Organisationseinheiten die Aufgabe „ordnungsgemäße Datenschutzorganisation“ in Abstimmung mit dem Datenschutzbeauftragten an fachlich geeignete Mitarbeiter zu delegieren. Dies halte ich für eine sinnvolle und notwendige Maßnahme, die nicht nur den Datenschutzbeauftragten bei der Wahrnehmung seiner Aufgaben unterstützt, sondern auch dem Personal in den Organisationseinheiten und damit auch den Patientinnen und Patienten zugute kommt. Nicht zuletzt ist ein funktionierender Datenschutz Voraussetzung für eine positive Wahrnehmung in Politik und Öffentlichkeit.

2.2 Die neue Orientierungshilfe für Krankenhausinformationssysteme

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Unbestreitbar hat dies Vorteile sowohl für den Patienten als auch für das ärztliche und das Pflegepersonal. Nicht übersehen werden darf dabei, dass die schnelle, leichte und vollständige Verfügbarkeit der Patientendaten erhebliche Datenschutzrisiken birgt.

Nirgendwo sonst werden so viele hochpersönliche und sensible Daten über so viele schutzbedürftige Personen gespeichert, genutzt und verarbeitet wie in Krankenhäusern. Da dies inzwischen flächendeckend mit Hilfe von Krankenhausinformationssystemen geschieht, muss sichergestellt werden, dass nur das in die Patientenbehandlung eingebundene Personal Zugriff auf die entsprechenden Patientendaten erhält. Gleichzeitig müssen Patienten nachvollziehen können, wer auf ihre Daten zugegriffen hat. Die reale Krankenhauspraxis weist jedoch beträchtliche Defizite bei der Wahrnehmung des Datenschutzes und der ärztlichen Schweigepflicht im Zusammenhang mit der Nutzung von Krankenhausinformationssystemen auf. Probleme bestehen zum einen darin, die Datenschutzanforderungen im Klinikalltag sowohl praxisgerecht als auch rechtskonform abzubilden. Zum anderen sind die Möglichkeiten zur Umsetzung in Krankenhausinformationssystemen begrenzt. Die Hersteller der Softwaresysteme implementieren die datenschutzrechtlichen Anforderungen bisher nicht oder unzureichend beziehungsweise realisieren dies nur gegen Aufpreis.

Aus diesen Gründen hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zum Datenschutz bei der Verwendung von Krankenhausinformationssystemen erarbeitet, die als Richtschnur für alle beteiligten Aufsichtsbehörden, Krankenhausbetreiber und Softwareanbieter den Weg in eine datenschutzgerechte Zukunft in diesem wichtigen und hochsensiblen Bereich weisen soll. Einbezogen wurden in die Erstellung der Orientierungshilfe Krankenhäuser, Krankenhausgesellschaften, Hersteller von Krankenhausinformationssystemen, Anwendervereinigungen und Vertreter der Kirchen. Die sowohl von den Datenschutzbeauftragten des Bundes und der Länder mit Entschließung vom 16./17. März 2011 (vgl. Anhang 18) als auch den obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) mit Beschluss vom 4./5. Mai 2011 (vgl. Anhang 39) zustimmend zur Kenntnis genommene Orientierungshilfe umfasst in einem ersten Teil „Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus“, die die bereits jetzt bestehenden gesetzlichen Anforderungen konkretisieren. In einem zweiten Teil werden die „Technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“ dargestellt, also Maßnahmen, die

zur technischen Umsetzung der gesetzlichen Anforderungen erforderlich sind. Vorangestellt sind ein Begleitpapier mit einer kurzen Erläuterung der Ziele der Orientierungshilfe sowie ein umfassendes Glossar mit ihren zentralen Begriffen.

Auch wenn die Orientierungshilfe keinen Gesetzescharakter hat, so besteht aus datenschutzrechtlicher Sicht das dringende Bedürfnis, die darin formulierten Anforderungen in allen Krankenhäusern – unter Berücksichtigung einer angemessenen Übergangsfrist – umzusetzen. Für mich – und ebenso für die übrigen Datenschutzbehörden – wird die Orientierungshilfe als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen meiner Kontroll- und Beratungsfunktion dienen. Dabei bin ich mir bewusst, dass der Umsetzungsprozess nicht von heute auf morgen zu schaffen sein wird. Nicht nur die Tatsache, dass ein Teil der am Markt angebotenen Krankenhausinformationssysteme in technischer Hinsicht derzeit noch hinter den in der Orientierungshilfe genannten Anforderungen zurückbleibt, sondern auch wirtschaftliche Überlegungen und Notwendigkeiten der betroffenen Krankenhäuser werden nach meiner Einschätzung dazu führen, dass eine flächendeckende Umsetzung Zeit beansprucht, die ich den Krankenhäusern auch zugestehe. Das Ziel aller Beteiligten muss jedoch eine zügige Anpassung der Krankenhausinformationssysteme an die in der Orientierungshilfe geforderten Standards sein. Dazu habe ich bereits mit der Baden-Württembergischen Krankenhausgesellschaft e. V. Kontakt aufgenommen.

Krankenhausbetreiber sollten schnellstmöglich prüfen, welche Teile der Orientierungshilfe bereits jetzt umgesetzt werden können und ihre Verfahren entsprechend einrichten. Die Hersteller der Krankenhaussysteme sind ihrerseits aufgefordert, ihre Systeme nachzubessern, um einen praxisgerechten und rechtskonformen Einsatz im Krankenhaus zu ermöglichen.

2.3 Terminvereinbarung an der Krankenhauspforte

Die Erhebung sensibler Patientendaten durch Pförtner eines Krankenhauses zum Zwecke der Vereinbarung eines Arzttermins ist dann datenschutzrechtlich unbedenklich, wenn diese nach dem Verpflichtungsgesetz und auf das Datengeheimnis verpflichtet sind.

Die Frage, welche Krankenhausmitarbeiter welche personenbezogenen Daten zu welchem Zweck verarbeiten dürfen, stellte sich bei der Terminvergabe durch den Pförtner einer Universitätsklinik. Ein Bürger wollte telefonisch einen Arzttermin im Klinikum vereinbaren. Nach mehreren vergeblichen Versuchen wurde er schließlich an einen Pförtner der Klinik verwiesen. Dieser verlangte Angaben zu gesundheitlichen Beschwerden und bestehenden oder eventuellen Diagnosen. Da sich der Bürger nicht vorstellen konnte, dass Pförtner eines Krankenhauses berechtigt sind, derartige sensible Gesundheitsdaten zu erfragen, wandte er sich an das Beschwerdetelefon des Klinikums. Dort wurde ihm, ohne nähere Begründung und wenig überzeugend, lediglich mitgeteilt, Bedenken an der Rechtmäßigkeit des Verfahrens bestünden nicht. Der Vorgang, der mir zunächst höchst zweifelhaft erschien, entpuppte sich bei genauerem Hinsehen unter datenschutzrechtlichen Aspekten als zulässig, aber dennoch verbesserungswürdig.

Das Klinikum bestätigte, dass die eingesetzten Pförtner auch die Aufgaben der Telefonvermittlung wahrnehmen und in diesem Zusammenhang auch die für einen Arzttermin erforderlichen Angaben formulargestützt aufnehmen und an die eigentliche Terminvergabestelle weiterleiten würden, falls diese Stelle besetzt ist. Meine datenschutzrechtliche Prüfung ergab, dass dieses Vorgehen vor allem deshalb unbedenklich ist, da alle Pförtner des Klinikums bei Arbeitsaufnahme nach § 1 des Gesetzes über die förmliche Verpflichtung nicht beamteter Personen (Verpflichtungsgesetz) vom 2. März 1974 (BGBl. I S. 547) und nach § 6 LDSG zur Wahrung des Datengeheimnisses verpflichtet werden:

– Nach § 1 Absatz 1 Verpflichtungsgesetz soll, wer ohne Amtsträger zu sein, bei einer Behörde oder einer sonstigen Stelle, die Aufgaben der

öffentlichen Verwaltung wahrnimmt, beschäftigt oder sei es auch nur mittelbar für sie tätig ist, auf die gewissenhafte Erfüllung seiner Obliegenheiten verpflichtet werden. Mit Hilfe des Verpflichtungsgesetzes soll damit bei Personen, die nicht Amtsträger sind, eine den Amtsträgern annähernd vergleichbare strafrechtliche Verantwortlichkeit bei Korruption, Geheimnisverrat und Verwahrungsbruch herbeigeführt werden.

– Gemäß § 6 LDSG ist es den bei öffentlichen Stellen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden (Datengeheimnis). Einer besonderen Verpflichtung der Beschäftigten bedarf es daher an sich grundsätzlich nicht. Die Erfahrung zeigt allerdings, dass viele Beschäftigte diese Regelung nicht kennen. Es empfiehlt sich daher, im Rahmen der förmlichen Verpflichtung nach dem Verpflichtungsgesetz auch auf § 6 LDSG zu verweisen.

Auch die vom Pförtner zu erfragenden Informationen waren nicht zu beanstanden. Zwar sah das dazu vorgesehene Formular neben Patientenname und Adressdaten sensible personenbezogene Daten wie Krankheit und Krankenkasse vor. Insoweit wurde für mich aber nachvollziehbar dargelegt, dass diese Daten zur Vereinbarung eines Termins in der für den jeweiligen Patienten zuständigen Sprechstunde erforderlich waren. Denn bei der Terminvergabe war zu entscheiden, ob der Patient der allgemeinen Ambulanzsprechstunde oder der Fachsprechstunde für gesetzlich oder privat Versicherte zuzuweisen ist. Das Klinikum hat auf meine Anregung zugesagt, das Formular so abzuändern, dass für die Beschäftigten klar erkennbar ist, dass – wie in der täglichen Praxis auch üblich – nur die vorläufige Diagnose und ob der Patient gesetzlich oder privat versichert ist, nicht aber der Name der Krankenkasse, zu erheben ist.

Zu kritisieren war jedoch die Aufklärung des anfragenden Bürgers sowohl durch den Pförtner als auch die Mitarbeiter des Beschwerdetelefons. Ich habe daher dem Uniklinikum empfohlen, dafür Sorge zu tragen, dass Pförtner und Mitarbeiter des Beschwerdetelefons das Verfahren bei Terminanfragen erläutern und vor allem auf die beschriebene Verpflichtung der Pförtner hinweisen. Damit können Unklarheiten, aber auch Misstrauen hinsichtlich der datenschutzrechtlichen Sensibilität des Klinikums vermieden werden.

2.4 Akteneinsicht in Patientenakte einer verstorbenen Verwandten in einem Krankenhausarchiv

Patientenakten sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist (§ 23 Absatz 1 LDSG). Vor einer Löschung sind die Daten dem zuständigen Archiv nach Maßgabe des Landesarchivgesetzes (LArchG) zur Übernahme anzubieten (§ 23 Absatz 3 LDSG). Werden Patientenakten vom Archiv übernommen, prüft und entscheidet dieses nach pflichtgemäßem Ermessen über die Einsichtnahme durch Dritte.

Dass die Archivierung von und der Umgang mit Patientenakten längst verstorbener Patienten nicht immer reibungslos funktioniert, erfuhr ich von einem Bürger, der an einer Biografie seiner verstorbenen psychisch kranken Großtante arbeitete. Mit Hinweis auf die ärztliche Schweigepflicht und ethische Bedenken grundsätzlicher Art hatte eine Universitätsklinik für Psychiatrie und Psychotherapie seiner Bitte um Einsicht in eine Krankenakte, einen Aufenthalt seiner Großtante in einer Heilanstalt im Land von 1930 bis 1938 betreffend, nicht entsprochen.

Im Rahmen meiner sich äußerst mühsam gestalteten datenschutzrechtlichen Überprüfung des vorgetragenen Sachverhalts musste ich feststellen, dass die Patientenakte der bereits 1943 verstorbenen Großtante zwar gemäß § 23 Absatz 3 LDSG im Universitätsarchiv aufbewahrt wurde. Allerdings hatte das Universitätsklinikum die Akte zur Prüfung des Ansinnens des Bürgers beim Archiv angefordert und auch erhalten,

was in keiner Weise archivrechtlichen Regelungen entsprach: Das Universitätsarchiv nimmt im Bereich der Universität die Aufgaben eines öffentlichen Archivs nach dem Landesarchivgesetz wahr und hat damit nach § 8 Absatz 2 Satz 1 LArchG die entsprechenden archivrechtlichen Bestimmungen zu beachten. Auf Grundlage des Landesarchivgesetzes hat die Universität eine Benutzungsordnung für das Universitätsarchiv erlassen (§ 8 Absatz 2 Satz 2 LArchG). Danach ist der Benutzungsantrag schriftlich an das Universitätsarchiv zu richten; über den Benutzungsantrag befindet der Leiter des Universitätsarchivs. Vorliegend hätte also das Klinikum den Antrag des Bürgers an das Universitätsarchiv weiterleiten und das Archiv über den Antrag auf Akteneinsicht nach pflichtgemäßem Ermessen entscheiden müssen. Ich habe das Klinikum daher aufgefordert, den Antrag des Bürgers zur Prüfung und Entscheidung nach Maßgabe des Landesarchivgesetzes und der Benutzungsverordnung dem Universitätsarchiv zurückzugeben und dafür zu sorgen, dass in künftigen Fällen datenschutzkonform verfahren wird.

Das Universitätsarchiv hat bei seiner Entscheidung zu berücksichtigen, dass nach der Benutzungsordnung das Archiv der Forschung, der Lehre und dem Studium an der Universität und darüber hinaus der sonstigen wissenschaftlichen Arbeit und sachlichen Information dient. Die Benutzung ist jedem möglich, der ein berechtigtes Interesse, insbesondere ein rechtliches, wissenschaftliches oder heimat- und familiengeschichtliches Interesse glaubhaft macht. Allerdings ist die Benutzung einzuschränken oder zu versagen, soweit Grund zu der Annahme besteht, dass schutzwürdige Belange Dritter entgegenstehen (§ 6 Absatz 6 Satz 1 Nummer 2 LArchG). Personenbezogene Unterlagen wie Patientenakten unterliegen besonderen Bedingungen, denn Personen genießen bis zum Ablauf von zehn Jahren (§ 8 Absatz 1 Nummer 3 Benutzungsverordnung, § 6 Absatz 2 Satz 3 LArchG) über ihren Tod hinaus den Schutz ihrer Privat- und Intimsphäre (sogenannter postmortaler Persönlichkeitsschutz). Archivische Sperrfristen tragen dem postmortalen Persönlichkeitsrecht Rechnung, indem sie die Einsicht in personenbezogene Unterlagen im Archivgut erst nach einiger Zeit nach Abschluss der Unterlagen freigeben. Auch danach endet der Schutz nicht automatisch, sondern er ist mit dem berechtigten Interesse des potenziellen Nutzers abzuwägen. Generell gilt jedoch: Je länger der Zeitpunkt des Todes einer Person zurückliegt, desto größeres Gewicht kommt dem Recht auf freien Zugang zu Wissen und Information zu.

Im Rahmen der Abwägung ist zudem zu beachten, dass Patientenakten sensible personenbezogene Daten enthalten, die der ärztlichen Schweigepflicht unterfallen. Die ärztliche Schweigepflicht dient dem Schutz des persönlichen Lebens- und Geheimnisbereichs (Privatsphäre) einer Person, die sich einem Arzt bzw. anderen unter § 203 des Strafgesetzbuchs (StGB) fallenden Personen anvertraut (hat), und schützt das Recht auf informationelle Selbstbestimmung des Patienten. Das Landesarchivgesetz enthält besondere Rechtsvorschriften zum Schutz von Berufs- und besonderen Amtsgeheimnissen nach § 203 StGB. So sind nach § 3 Absatz 1 Satz 3 LArchG dem Landesarchiv auch Unterlagen anzubieten, die durch Rechtsvorschriften über Geheimhaltung geschützt sind, wenn die abgebende Stelle im Benehmen mit dem Landesarchiv festgestellt hat, dass schutzwürdige Belange des Betroffenen durch geeignete Maßnahmen unter Abwägung aller Umstände des Einzelfalls angemessen berücksichtigt werden. Die erforderlichen Maßnahmen müssen bereits vor der Übergabe durchgeführt oder festgelegt werden.

§ 6 Absatz 2 Satz 2 LArchG lässt eine Nutzung von Archivgut, das Rechtsvorschriften über die Geheimhaltung unterlag, frühestens 60 Jahre nach Entstehung der Unterlagen zu. Nach § 6 a Absatz 2 LArchG gelten für Archivgut, das Rechtsvorschriften des Bundes über die Geheimhaltung im Sinne der §§ 10 oder 11 des Bundesarchivgesetzes unterliegt und das von anderen als den in § 2 Absatz 1 des Bundesarchivgesetzes genannten Stellen öffentlichen Archiven übergeben worden ist, § 2 Absatz 4 Satz 2 sowie § 5 Absatz 1 bis 7 und 9 des Bundesarchivgesetzes entsprechend. Daraus ergibt sich, dass auch Patientenakten generell nicht auf Dauer einer Nutzung entzogen werden können. Andernfalls

hätte der Gesetzgeber eine Überführung solcher Akten in das Landesarchiv nicht zulassen dürfen. Dies hat er jedoch mit den genannten besonderen Schutzvorschriften getan.

3. Laborbeauftragung durch Arzt

Der Patient eines niedergelassenen Arztes wandte sich an die Aufsichtsbehörde, nachdem er von einem medizinischen Labor eine Rechnung für Laborleistungen erhalten hatte. Sein Arzt hatte ohne sein Wissen ein Labor mit der Analyse von patienteneigenem Untersuchungsmaterial beauftragt. Das Labor betraute ein weiteres Labor mittels eines Überweisungs- beziehungsweise Abrechungsscheins mit einem Teil der vom Arzt in Auftrag gegebenen Laborleistungen und übermittelte zu diesem Zweck neben Untersuchungsmaterial die Personalien des Patienten an das zweite Labor. Dieses sandte die Laborbefunde an das „überweisende“ Labor und stellte die Laborleistungen dem Patienten in Rechnung, welcher dadurch erstmals von dem Vorfall erfuhr.

Arztpraxen unterliegen als private Stellen den Vorschriften des Bundesdatenschutzgesetzes. Der Arzt und seine Mitarbeiter haben außerdem die berufliche Schweigepflicht (Patientengeheimnis) zu wahren (§ 203 Absatz 1 Nummer 1 und Absatz 3 Satz 2 des Strafgesetzbuchs). Die ärztliche Schweigepflicht ist in der Berufsordnung der Landesärztekammer (BO) besonders geregelt und gilt grundsätzlich auch bei der kollegialen Zusammenarbeit unter Ärzten. Ärzte, die gleichzeitig oder nacheinander denselben Patienten untersuchen und behandeln, sind gemäß § 9 Absatz 4 BO insoweit von der Schweigepflicht befreit, als das Einverständnis des Patienten besteht oder anzunehmen ist.

Dabei ist zu beachten, dass § 9 Absatz 4 BO – anders als § 4 a Absatz 1 Satz 3 BDSG für die datenschutzrechtliche Einwilligung – kein besonderes Formerfordernis aufstellt, der Patient sein Einverständnis im Sinne von § 9 Absatz 4 BO also auch mündlich und sogar stillschweigend erklären kann. Die Annahme des Einverständnisses des Patienten mit der Übermittlung von Patientendaten an ein externes Labor durch den Arzt setzt jedoch voraus, dass der Arzt den Patienten ausdrücklich auf die geplante Einschaltung eines Labors hinweist und der Patient dem nicht widerspricht. Zumindest auf Nachfrage muss dem Patienten auch mitgeteilt werden, welcher Laborarzt oder welches Labor mit welcher Untersuchung beziehungsweise in welchem Behandlungszusammenhang eingeschaltet werden soll. Die Erteilung von Unteraufträgen durch das Labor an Speziallabore ist nur dann vom Einverständnis des Patienten gedeckt, wenn dieser zuvor hinreichend deutlich auch auf diese Möglichkeit hingewiesen wurde und nicht widersprochen hat.

Beauftragt ein Arzt einen Laborarzt mit weiteren Untersuchungen, entsteht hierdurch nur dann ein Behandlungsvertrag zwischen dem Patienten und dem Laborarzt, wenn der Patient seinem behandelnden Arzt eine entsprechende Vollmacht erteilt hat. Von einer stillschweigenden Bevollmächtigung kann nur ausgegangen werden, wenn der Patient vom behandelnden Arzt über die beabsichtigte Laboruntersuchung unterrichtet wurde und nicht widersprochen hat.

In dem der Beschwerde zugrunde liegenden Fall hatte es der Arzt versäumt, den Patienten auf die vorgesehene Einschaltung eines Labors und die Möglichkeit der Beauftragung eines zweiten Labors hinzuweisen. Daher schied die Annahme eines (stillschweigenden) Einverständnisses im Sinne von § 9 Absatz 4 BO mit der Datenweitergabe aus. Da auch keine Einwilligung gemäß § 4 a BDSG vorlag und die Voraussetzungen der in Frage kommenden Übermittlungstatbestände des § 28 Absatz 6 und 7 BDSG ebenfalls nicht erfüllt waren, war die Übermittlung der Patientendaten vom Arzt an das zunächst beauftragte Labor ebenso rechtswidrig wie die Erhebung, Speicherung und Übermittlung der Patientendaten und Laborbefunde durch die beiden Labore. Mangels Bevollmächtigung des Arztes beziehungsweise des ersten Labors war kein Behandlungsvertrag zwischen den beiden Laboren und dem Patienten zustande gekommen. Die Datenverarbeitung durch die Labore war daher auch nicht dadurch gerechtfertigt, dass dies für die Geltendmachung rechtlicher Ansprüche gegen den Patienten erforderlich gewesen wäre (§ 28 Absatz 6 Nummer 3 BDSG).

Gemäß § 10 BO sind Ärzte verpflichtet, ihre Aufzeichnungen für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Dies gilt auch für laboratoriumsmedizinische Untersuchungen. Die Aufbewahrungs- und Dokumentationspflicht besteht auch in solchen Fällen, in denen es an einem (wirksamen) Behandlungsvertrag zwischen Arzt und Patient fehlt und/oder die Erhebung und Speicherung der personenbezogenen Daten des Patienten durch den Arzt mangels wirksamer Einwilligung des Patienten rechtswidrig war, solange tatsächlich eine Untersuchung oder Behandlung stattgefunden hat. Im Hinblick auf die Dokumentations- und Aufbewahrungspflicht des Labors waren die personenbezogenen Daten des Beschwerdeführers vom Labor daher zwar nicht zu löschen, aber immerhin zu sperren.

4. Datenschutzrechtliche Fragen bei einem überbetrieblichen Dienst von Betriebsärzten

Die Aufsichtsbehörde für den nicht-öffentlichen Bereich hatte sich bereits in ihrem Vierten Tätigkeitsbericht im Jahr 2007 (S. 175 ff.) mit dem Zugriff von Betriebsärzten eines überbetrieblichen Dienstes auf Gesundheitsdaten von Arbeitnehmern befasst. Weitere in diesem Zusammenhang aufgetretene datenschutzrechtliche Fragestellungen konnten nunmehr abschließend geklärt werden.

Nach § 8 Absatz 1 des Gesetzes über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) sind Betriebsärzte bei der Anwendung ihrer arbeitsmedizinischen Fachkunde weisungsfrei und nur ihrem ärztlichen Gewissen unterworfen. Außerdem haben sie die Regeln der ärztlichen Schweigepflicht zu beachten, § 8 Absatz 1 Satz 3 ASiG. Nähere Regelungen zu den arbeitsmedizinischen Vorsorgeuntersuchungen, die Pflicht-, Angebots- und Wunschuntersuchungen umfassen, finden sich in der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV). Bestimmte Tätigkeiten darf ein Arbeitgeber nur von Arbeitnehmern verrichten lassen, die sich einer Erst- und regelmäßigen Nachuntersuchungen unterzogen haben (sog. Pflichtuntersuchungen). Daneben muss ein Arbeitgeber bestimmten Beschäftigten regelmäßig bestimmte Untersuchungen anbieten (Angebots- und Wunschuntersuchungen). In diesen Fällen darf er den Arbeitnehmer auch weiter beschäftigen, wenn dieser nicht an der Untersuchung teilnimmt. Gemäß § 6 Absatz 3 ArbMedVV hat der Arzt den Untersuchungsbefund und das Untersuchungsergebnis bei allen Vorsorgeuntersuchungen schriftlich festzuhalten, die untersuchte Person darüber zu beraten und ihr eine Bescheinigung auszustellen, die Angaben über den Untersuchungsanlass und den Tag der Untersuchung sowie die ärztliche Beurteilung, ob und inwieweit bei Ausübung einer bestimmten Tätigkeit gesundheitliche Bedenken bestehen, enthält. Nur im Fall einer Pflichtuntersuchung erhält der Arbeitgeber eine Kopie dieser Bescheinigung, § 6 Absatz 3 Satz 3 ArbMedVV.

Mit der so umrissenen Tätigkeit von Betriebsärzten sind eine ganze Reihe datenschutzrechtlicher Fragestellungen verbunden, vor allem, wenn ein externer Dienstleister, in diesem Fall ein überbetrieblicher Dienst, zum Einsatz kommt:

a) Verantwortliche Stelle für die Tätigkeit eines Betriebsarztes

Ein von seinem Arbeitgeber zum Betriebsarzt bestellter Arbeitnehmer wird von der herrschenden Meinung in der datenschutzrechtlichen Literatur als Teil der verantwortlichen Stelle „Arbeitgeber“ angesehen. Gleichwohl gilt die ärztliche Schweigepflicht auch im Verhältnis zwischen dem Betriebsarzt und seinem Arbeitgeber. Dem Betriebsarzt ist es daher verwehrt, personenbezogene Daten von Arbeitnehmern, die er in seiner Eigenschaft als Betriebsarzt erhoben hat, an den Arbeitgeber weiterzugeben, soweit nicht eine gesetzliche Offenbarungsbefugnis oder -pflicht besteht oder der Betroffene den Betriebsarzt von seiner Schweigepflicht entbunden hat. Der ärztlichen Schweigepflicht ist auch dadurch Rechnung zu tragen, dass alle technisch-organisatorischen Maßnahmen getroffen werden, die erforderlich sind, um

einen unberechtigten Zugriff des Arbeitgebers auf die ärztliche Dokumentation des Betriebsarztes zu verhindern.

Bestellt ein Arbeitgeber dagegen einen überbetrieblichen Dienst als Betriebsarzt, ist der überbetriebliche Dienst und nicht der Arbeitgeber als verantwortliche Stelle im Sinn von § 3 Absatz 7 BDSG für die Tätigkeit des überbetrieblichen Dienstes als Betriebsarzt im Unternehmen des Arbeitgebers anzusehen. Der Annahme einer Auftragsdatenverarbeitung gemäß § 11 BDSG steht die in § 8 Absatz 1 ASiG vorgeschriebene Weisungsfreiheit des Betriebsarztes entgegen. Damit hat der überbetriebliche Dienst und nicht der Arbeitgeber einem betroffenen Arbeitnehmer Auskunft über die gespeicherten Daten zu erteilen und nach § 35 BDSG für die gebotene Löschung zu sorgen. Daten, die der überbetriebliche Dienst speichert, werden auf keinen Fall Bestandteil der vom Arbeitgeber über einen Mitarbeiter geführten Personalakte. Der von einem überbetrieblichen Dienst in ein Unternehmen entsandte Betriebsarzt unterliegt (nur) der Kontrolle des vom überbetrieblichen Dienst bestellten Datenschutzbeauftragten.

b) Benennung eines oder mehrerer Betriebsärzte gegenüber dem Arbeitgeber und den Arbeitnehmern

Der Arbeitgeber bestellt gemäß § 19 ASiG den überbetrieblichen Dienst als solchen und nicht einen oder mehrere der dort angestellten Ärzte. Der überbetriebliche Dienst kann deshalb grundsätzlich frei entscheiden, welcher Arzt für ein Unternehmen tätig wird. Allerdings sollte in der Bestellungsvereinbarung vorgesehen werden, dass der überbetriebliche Dienst dem Auftraggeber einen oder mehrere Betriebsärzte schriftlich benennt, der die betriebsärztlichen Aufgaben in dem Unternehmen wahrnimmt. Werden mehrere Betriebsärzte in dem Unternehmen tätig, sollte die Zuständigkeit jedes Betriebsarztes vorab schriftlich festgelegt werden, zum Beispiel nach Anfangsbuchstaben der Mitarbeiter, Art der Aufgabe, Betriebsstätte usw. Auch für den Vertretungsfall (Urlaub, Erkrankung) sollten Regelungen getroffen werden. Wird dem Arbeitgeber der (die) Name(n) des Betriebsarztes (der Betriebsärzte) mitgeteilt, bei mehreren Betriebsärzten unter Angabe der exakten Aufgaben-/Zuständigkeitsabgrenzung, sollte dieser die Information an seine Mitarbeiter weitergeben.

Aus dem Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG) folgt, dass jeder Betriebsarzt des überbetrieblichen Dienstes nur auf die Mitarbeiterdaten zugreifen darf, die er zur Erfüllung der ihm zugewiesenen Aufgaben tatsächlich benötigt. Sind beispielsweise zwei Betriebsärzte in einem Unternehmen tätig, ist die Zugriffsberechtigung auf eine elektronische Patientendokumentation des überbetrieblichen Dienstes entsprechend der Verteilung der Zuständigkeit einzuschränken. Ein Urlaubs- und Krankheitsvertreter darf den Zugriff auf Mitarbeiterdaten nur für die Dauer der Vertretung haben. Bei einem Wechsel des für ein Unternehmen oder bestimmte einzelne Mitarbeiter zuständigen Betriebsarztes eines überbetrieblichen Dienstes können die Daten der betroffenen Mitarbeiter ohne deren Einwilligung durch den neuen Betriebsarzt verarbeitet und genutzt werden.

c) Unterrichtung des Arbeitgebers über Untersuchungsergebnisse

Der Betriebsarzt darf den Arbeitgeber nur dann über die Ergebnisse einer von ihm durchgeführten Untersuchung unterrichten, wenn es dafür eine Rechtsgrundlage gibt oder der Arbeitnehmer ihn von seiner ärztlichen Schweigepflicht entbunden und in die Übermittlung seiner Daten rechtswirksam eingewilligt hat. Nach § 4 a Absatz 1 Satz 1 und Absatz 3 BDSG muss eine entsprechende Einwilligung auf der freien Entscheidung des Betroffenen beruhen und sich ausdrücklich auf besondere Arten personenbezogener Daten, wie Gesundheitsdaten, beziehen. Für Pflichtuntersuchungen findet sich eine gesetzliche Offenbarungs- und Übermittlungsbefugnis in § 6 Absatz 3 Satz 3 ArbMedVV. In Bezug auf Angebots- und Wunschuntersuchungen gibt es keine vergleichbare Regelung. Die Datenübermittlung an den Arbeitgeber ist daher nur auf der Grundlage einer (freiwilligen) Einwilligung des Betroffenen möglich.

d) Verbleib der Patientenakten bei einem Wechsel des überbetrieblichen Dienstes

Endet die Tätigkeit eines überbetrieblichen Dienstes für einen bestimmten Arbeitgeber, weil dieser eigene Arbeitnehmer oder einen anderen überbetrieblichen Dienst mit der Wahrnehmung der Aufgaben des Betriebsarztes betraut, gilt für den Verbleib der Patientenakten Folgendes:

Eine Übergabe der Patientendokumentation an den Arbeitgeber scheidet aus. Entweder verbleiben die Akten oder Daten mindestens für die Dauer der gültigen Dokumentations- und Aufbewahrungsfristen – soweit keine Sonderregelungen einschlägig sind, beträgt die Aufbewahrungsfrist gemäß § 10 Berufsordnung der Landesärztekammer Baden-Württemberg 10 Jahre nach Abschluss der Behandlung – beim bisherigen überbetrieblichen Dienst. Dieser übergibt dann einzelne Akten oder Datensätze auf Anforderung an den neuen Betriebsarzt, sofern der Betroffene in die Datenübermittlung schriftlich eingewilligt hat. Alternativ dazu können auch alle Akten sofort ohne Einwilligung der Betroffenen dem Nachfolgebetriebsarzt übergeben werden, wenn sie dort entsprechend dem zur Übergabe von Krankenunterlagen an einen Praxisnachfolger entwickelten „Zwei-Schränke-Modell“ separat und unzugänglich gelagert werden und ein Verwahrungsvertrag unter Androhung einer Vertragsstrafe geschlossen wird. Auch in diesem Fall darf der neue Betriebsarzt nur nach Einwilligung des Betroffenen auf die Patientendokumentation zugreifen. Die Betroffenen sollten über den Wechsel des überbetrieblichen Dienstes durch ihren Arbeitgeber informiert werden.

e) Personenbezogene Angaben in Abrechungen des überbetrieblichen Dienstes gegenüber dem Arbeitgeber

Bei der Vergütung der betriebsärztlichen Leistungen überbetrieblicher Dienste treten mehr und mehr Einzelabrechungen an die Stelle der früher verbreitet vereinbarten Pauschalhonorare. Um überprüfen zu können, ob in Rechnung gestellte Leistungen auch tatsächlich erbracht wurden und in dieser Form erforderlich waren, äußern öffentliche und private Arbeitgeber vereinzelt den Wunsch nach einer detaillierten Abrechung mit namentlicher Angabe der Patienten und der für diese erbrachten ärztlichen Leistungen. Dabei kann es sich um Angaben über die Gesundheit von Arbeitnehmern und damit um besonders geschützte Daten im Sinne von § 3 Absatz 9 BDSG handeln. Sowohl die Tatsache, dass jemand einen bestimmten (Betriebs-) Arzt aufgesucht hat als auch die erbrachten ärztlichen Leistungen unterliegen – auch gegenüber dem Arbeitgeber – der ärztlichen Schweigepflicht. Eine Mitteilung an den Arbeitgeber ist daher nur zulässig, wenn

- die Tatsache, dass ein Arbeitnehmer den Betriebsarzt aufgesucht hat, dem Arbeitgeber bereits bekannt ist (beispielsweise, weil er die Untersuchung veranlasst hat),
- eine Rechtsvorschrift die Übermittlung von Gesundheitsdaten an den Arbeitgeber zu Abrechungszwecken erlaubt oder
- der Betroffene freiwillig in die Übermittlung konkret bezeichneter gesundheitlicher Daten an den Arbeitgeber eingewilligt und den Arzt von der Schweigepflicht entbunden hat.

Außer § 6 Absatz 3 Satz 3 ArbMedVV, wonach der Arbeitgeber im Fall einer Pflichtuntersuchung eine Kopie der Untersuchungsbescheinigung erhält, sind keine weiteren gesetzlichen Übermittlungsbefugnisse ersichtlich. Zwar ist eine Übermittlung von Gesundheitsdaten gemäß § 28 Absatz 6 Nummer 3 BDSG zulässig, wenn dies zur Geltendmachung rechtlicher Ansprüche erforderlich ist. Eine personenbezogene Abrechnung könnte – je nach dem Inhalt des mit dem Arbeitgeber geschlossenen Vertrages – zur Geltendmachung von Honoraransprüchen des überbetrieblichen Dienstes auch erforderlich sein. Jedoch dürften die schutzwürdigen Belange der Arbeitnehmer einer Übermittlung entgegenstehen, da ansonsten die Vorschriften der ArbMedVV, die nur eine eingeschränkte Unterrichtung des Arbeitgebers über Untersuchungen und ihre Ergebnisse vorsehen, faktisch umgangen würden.

Eine datenschutzkonforme Auflösung des Widerspruchs zwischen dem Wunsch nach einer größtmöglichen Plausibilisierung der Abrechnungen einerseits und dem Erfordernis der Wahrung der ärztlichen Schweigepflicht andererseits könnte in der Pseudonymisierung der personenbezogenen Angaben in den Abrechnungen liegen. Es ist dann jedoch durch geeignete Vorkehrungen sicherzustellen, dass dem Arbeitgeber eine Rückführung der pseudonymisierten Daten auf konkrete Arbeitnehmer nur in einem vorab festgelegten Verfahren in bestimmten Fallgruppen (zum Beispiel bei konkreten Anhaltspunkten für Unregelmäßigkeiten oder unabhängig davon zur stichprobenweisen Kontrolle einer geringen Anzahl von Abrechnungen) und nach rechtswirksamer, § 4 a BDSG genügender Einwilligung der Patienten in die Datenübermittlung und Entbindung von der ärztlichen Schweigepflicht im Einzelfall möglich ist. Wenn Patienten in solchen Fällen den überbetrieblichen Dienst nicht von der ärztlichen Schweigepflicht entbinden, darf dieser die Zuordnung „Referenznummer/Mitarbeiter“ dem Arbeitgeber nicht mitteilen.

5. Korrektur psychiatrischer Verdachtsdiagnosen mittels des datenschutzrechtlichen Berichtigungsanspruchs?

Ein Patient eines niedergelassenen Neurologen und Psychiaters wandte sich an uns, weil er sich durch einen Arztbrief des Psychiaters in seinem allgemeinen Persönlichkeitsrecht verletzt sah. Er gab an, dass er an einer in dem Arztbrief als Verdachtsdiagnose diagnostizierten psychischen Krankheit objektiv nicht leide und bereits die Diagnose mit einem negativen Werturteil verbunden sei. Außerdem bemängelte er, dass der Arztbrief bestimmte andere psychische Krankheiten, die ein anderer Arzt zu einem früheren Zeitpunkt bei ihm diagnostiziert hatte, nicht enthalte und aus diesem Grund unvollständig und damit falsch sei. Der Patient war der Auffassung, mittels des Berichtigungsanspruchs gemäß § 35 Absatz 1 BDSG könne er von dem Arzt eine Korrektur des Arztbriefs in Form der Löschung der diagnostizierten Krankheit und der nachträglichen Aufnahme der von dem anderen Arzt getroffenen Diagnosen verlangen.

Nun sind personenbezogene Daten nach § 35 Absatz 1 Satz 1 BDSG zwar zu berichtigen, wenn sie unrichtig sind. Das gilt grundsätzlich auch für ärztliche Diagnosen und Behandlungsdokumentationen. Dabei gelten jedoch zwei Besonderheiten: Zum einen kommt eine Berichtigung nur in Betracht, soweit objektive Feststellungen über die körperliche Befindlichkeit des Patienten oder Aufzeichnungen über die ihm zuteil gewordene Behandlung, die einem Beweis zugänglich sind, in Rede stehen. Zum anderen können selbst nachweislich falsche tatsächliche Feststellungen nicht durch eine Löschung der ursprünglichen Feststellung oder Aufzeichnung berichtigt werden. Denn die ursprünglichen Daten sind in einem solchen Fall möglicherweise nicht unrichtig, weil sie die ärztliche Diagnose zum Zeitpunkt ihrer Erstellung durchaus richtig wiedergeben können. Außerdem steht die ärztliche Dokumentationspflicht einer Berichtigung entgegen, denn diese will gerade im Interesse des Patienten verhindern, dass mögliche Beweismittel für einen Arzthaftungsprozess verloren gehen. In einem solchen Fall kommt daher nur eine Präzisierung der fraglichen ärztlichen Aufzeichnung und ihre Erläuterung oder Fortschreibung in Betracht.

Darüber hinaus unterliegen ärztliche Diagnosen bezüglich psychischer Krankheiten dem Berichtigungsanspruch aus § 35 Absatz 1 BDSG ohnehin nicht, da sie – ebenso wie Verdachtsdiagnosen – lediglich die subjektive Einschätzung des behandelnden Arztes zum Zeitpunkt der Behandlung oder Aufzeichnung wiedergeben und somit Werturteile und keine Tatsachenangaben sind. Auch die Tatsache, dass der Arzt in seinem Arztbrief von seiner Verdachtsdiagnose abweichende Diagnosen eines anderen Psychiaters, bei dem sich der Patient zuvor über einen längeren Zeitraum in ärztlicher Behandlung befunden hatte, nicht mitaufgeführt hat, vermochte keinen Berichtigungsanspruch aus § 35 Absatz 1 BDSG zu begründen. Insoweit ist der Arztbrief weder unvollständig noch unrichtig, denn ein Arztbrief gibt lediglich wieder, was ein bestimmter Arzt zu einem bestimmten Zeitpunkt aufgrund seiner subjektiven Eindrücke und Wahrnehmungen des Patienten diagnostiziert hat und nicht, welche Krankheiten von anderen Ärzten zu früheren Zeitpunkten festgestellt wurden.

6. Aufzeichnung von Anrufen bei Integrierten Leitstellen

Unter anderem zum Nachweis der ordnungsgemäßen Ausführung von Einsatzaufträgen und zur Geltendmachung beziehungsweise Ausübung oder Verteidigung rechtlicher Ansprüche sowie zur Verfolgung von Straftaten werden Anrufe bei den Integrierten Leitstellen Feuerwehr und Rettungsdienst aufgezeichnet. Dies führt dann zu datenschutzrechtlichen Problemen, wenn in Integrierten Leitstellen verschiedene Hilfeersuchen abgewickelt werden.

Eine Rettungsdienstorganisation wickelt in ihrer Integrierten Leitstelle Anrufe unter anderem in den Bereichen Notfallrettung, Krankentransport und ärztlicher Notfalldienst ab. Sämtliche Anrufe, die auf der Telefonnummer für den Notruf (112), den Krankentransport (19222), den Ärztlichen Notdienst (19292) eingehen und interne Gespräche, die von den Rettungswachen eingehen, werden aufgezeichnet, auf einer Festplatte gespeichert und 90 Tage lang archiviert. Die Zulässigkeit dieses Vorgehens ist differenziert nach Art des Hilferufes zu sehen.

§ 31 Absatz 1 des Rettungsdienstgesetzes (RDG) erlaubt die Erhebung, Veränderung, Speicherung und Nutzung personenbezogener Daten, soweit sie zur Durchführung von Notfallrettung und Krankentransport, einschließlich der anschließenden Versorgung des Patienten, zum Nachweis der ordnungsgemäßen Ausführung des Einsatzauftrages und zur verwaltungsmäßigen Abwicklung des Einsatzauftrages, insbesondere der Abrechnung der erbrachten Leistung, erforderlich ist. Gegenstand der Notfallrettung ist es, bei Notfallpatienten Maßnahmen zur Erhaltung des Lebens und zur Vermeidung gesundheitlicher Schäden einzuleiten, sie transportfähig zu machen und unter fachgerechter Betreuung in eine für die Weiterversorgung geeignete Einrichtung zu befördern.

Leitstellen für den Rettungsdienst und für die Feuerwehr sind als Integrierte Leitstellen in gemeinsamer Trägerschaft zu betreiben (§ 4 Absatz 1 Satz 2 des Feuerwehrgesetzes [FwG]). § 37 Absatz 5 Satz 1 FwG erlaubt den Leitstellen die Aufzeichnung von Inhalts- und Verbindungsdaten von über die Rufnummer 112 eingehenden Anrufen, die die Feuerwehr oder den Rettungsdienst betreffen, ohne Kenntnis des Betroffenen. Die Aufgaben der Feuerwehr sind in § 2 FwG geregelt. Über andere Rufnummern eingehende Anrufe dürfen nur aufgezeichnet werden, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist und der Anrufer vor der Aufzeichnung hierauf hingewiesen wurde (§ 35 Absatz 5 Satz 2 FwG). Davon sind die Anrufe betroffen, die über reguläre Rufnummern der Feuerwehr eingehen. Die genannten Regelungen im Feuerwehrgesetz und Rettungsdienstgesetz stellen damit eine ausreichende Rechtsgrundlage für die Aufzeichnung und Speicherung der bei der Integrierten Leitstelle eingehenden Hilfeersuchen in den Bereichen Notfallrettung und Krankentransport auf den Telefonnummern 112 und 19222 dar.

Der Bereich des Ärzte-Notdienstes (19292) wird hingegen weder vom Rettungsdienstgesetz noch vom Feuerwehrgesetz erfasst. Die vertragsärztlichen Notdienste dienen der „Sicherstellung der vertragsärztlichen Versorgung“ in den sprechstundenfreien Zeiten. Die datenschutzrechtliche Zulässigkeit der Aufzeichnung beim ärztlichen Notfalldienst ist nach dem Bundesdatenschutzgesetz zu beurteilen. Da bei einem Anruf beim ärztlichen Notfalldienst Gesundheitsdaten und damit besonders sensible Daten im Sinne des § 3 Absatz 9 BDSG anfallen können, dürfen diese ohne Einwilligung des Betroffenen nur unter den engen Voraussetzungen des § 28 Absatz 6 bis 9 BDSG erhoben, verarbeitet und genutzt werden. Die dort genannten Voraussetzungen liegen bei der Aufzeichnung und Speicherung der im Bereich des ärztlichen Notfalldienstes eingehenden Anrufe gerade nicht vor, sodass es insoweit der Einwilligung der Betroffenen bedarf. Der Anruf beim ärztlichen Notfalldienst ist seinem Charakter nach einem Anruf in einer Arztpraxis gleichzustellen. Hier kann nicht davon ausgegangen werden, dass der Anrufer, wenn er gefragt würde, mit einer Aufzeichnung seines Anrufs einverstanden wäre. Eine konkludente Einwilligung kann allenfalls dann angenommen werden, wenn dem Anrufer bekannt ist, dass sein Gespräch aufgezeichnet wird, er aber dennoch anruft. Ich gehe davon aus, dass Anrufern bei einem ärztlichen Notfalldienst nicht generell bekannt sein

dürfte, dass dort Gespräche aufgezeichnet werden. Anrufe bei Leitstellen, die die Aufgaben des ärztlichen Notfalldienstes übernommen haben, dürfen daher nur dann aufgezeichnet werden, wenn der Anrufer zuvor – beispielsweise durch eine kurz gefasste Bandansage – hierauf hingewiesen wurde.

Zusammenfassend kann festgehalten werden, dass Anrufe in den Integrierten Leitstellen zu Notfallrettung und Krankentransport ohne vorherigen Hinweis aufgezeichnet werden dürfen, nicht aber Telefonate im Bereich des ärztlichen Notfalldienstes. Dem Datenschutz, der an sich eine ausdrückliche Einwilligung des Anrufers verlangt, ist damit zwar nicht in vollem Umfang Rechnung getragen. Es ist jedoch sichergestellt, dass der Anrufer in Kenntnis der Aufzeichnung das Gespräch fortsetzt und sich die Leitstellenmitarbeiter nicht strafbar machen (§ 201 Absatz 1 Nummer 1 des Strafgesetzbuchs).

7. Wie geht es weiter mit der Einschulungsuntersuchung?

„Die umfangreichen Datenerhebungen bei Eltern und Erzieherinnen für die Einschulungsuntersuchung sind weder aus fachlicher noch aus datenschutzrechtlicher Sicht erforderlich“, so lautete mein Fazit im letzten Tätigkeitsbericht. Für besonders begrüßenswert halte ich daher das Vorhaben des fachlich zuständigen Ministeriums für Arbeit und Sozialordnung, Familie, Frauen und Senioren (Sozialministerium), die Verwaltungsvorschrift des Ministeriums für Arbeit und Soziales zur Durchführung der Einschulungsuntersuchung (ESU-VwV) vom 28. November 2008 (GABl. S. 381) auch unter datenschutzrechtlichen Aspekten zu überarbeiten.

Bereits mein Amtsvorgänger hatte mehrfach grundsätzliche Bedenken hinsichtlich der neu konzipierten Einschulungsuntersuchung geäußert (vgl. 26. Tätigkeitsbericht für das Jahr 2005, LT-Drucksache 13/4910, 27. Tätigkeitsbericht für das Jahr 2006, LT-Drucksache 14/650). Die Kritik betraf vor allem die fehlende gesetzliche Grundlage der Datenerhebung durch die Gesundheitsämter und den fünfseitigen Elternfragebogen, mit dem nicht nur medizinische Informationen erhoben, sondern auch Fragen zum häuslichen Umfeld und zu auffälligen Verhaltensweisen des Kindes gestellt werden. Dass wir mit unserer datenschutzrechtlichen Beurteilung nicht völlig falsch lagen, bestätigten unsere Kontrollbesuche bei einem Gesundheitsamt und einem Kindergarten, die meine Mitarbeiter nach der flächendeckenden Einführung der Einschulungsuntersuchung durchführten (vgl. 29. Tätigkeitsbericht 2009, LT-Drucksache 14/5500).

Knapp drei Jahre nach Einführung der zunächst heftig unter Beschuss stehenden Einschulungsuntersuchung haben sich nach meinem Eindruck die Wogen geglättet. Eingaben, die besorgte Eltern an meine Dienststelle richten, zeigen jedoch, dass nach wie vor große Zweifel bestehen, ob die durch die Gesundheitsämter zu erhebenden personenbezogenen Daten tatsächlich erforderlich sind.

Erfreulicherweise hat das Sozialministerium meine Empfehlung, das Verfahren der Einschulungsuntersuchung nochmals kritisch zu hinterfragen, aufgegriffen und einen Arbeitskreis mit der Überarbeitung der ESU-VwV beauftragt. Mittlerweile liegt mir ein Entwurf einer Verwaltungsvorschrift zur Durchführung der Einschulungsuntersuchung und der Jugendzahnpflege (VwV ESU und Jugendzahnpflege) vor, der bereits zahlreiche Anregungen, die ich im Arbeitskreis vorbringen konnte, berücksichtigt.

Gleichwohl bin ich mit dieser Fassung der Verwaltungsvorschrift nicht einverstanden. Denn das Ministerium hat es bedauerlicherweise versäumt, die Überarbeitung der Verwaltungsvorschrift dazu zu nutzen, die Einschulungsuntersuchung auf eine tragfähige Rechtsgrundlage zu stützen. Die wesentlichen Bestimmungen zu Inhalt und Grenzen der Verarbeitung personenbezogener Daten müssen in einem Gesetz getroffen werden, aus dem klar und eindeutig die rechtliche Betroffenheit der Kinder und gegebenenfalls auch anderer Beteiligter unmittelbar erkennbar ist. Es ist mit dem Recht auf informationelle Selbstbestimmung und dem Prinzip des Vorbehalts des Gesetzes nicht zu vereinbaren, solche Bestimmungen einer Verwaltungsvorschrift vorzubehalten. Die Schuluntersuchungsverordnung – ebenso wenig

der ebenfalls vorgelegte Entwurf einer Verordnung zur Durchführung schulärztlicher Untersuchungen sowie zielgruppenspezifischer Untersuchungen und Maßnahmen in Kindertageseinrichtungen und Schulen – stellt keine hinreichende Rechtsgrundlage dar.

Beim Elternfragebogen steht für mich nach wie vor die Erforderlichkeit der abgefragten Daten im Vordergrund. Positiv hervorzuheben ist, dass von mir bislang als besonders kritisch eingeschätzte Fragen, wie die zur Geburt des Kindes (normale Geburt/Frühgeburt/Mehrlingsgeburt/Komplikationen) und zu Stärken und Schwächen des Kindes, gestrichen werden sollen.

Die Frage, ob sich Eltern Sorgen um die Entwicklung des Kindes machen, soll nicht mehr differenziert (Legasthenie in der Familie, familiäre Probleme, Verhaltensauffälligkeiten des Kindes), sondern lediglich mit ja oder nein beantwortet werden. Damit werden zwar weniger Informationen zu familiären Problemen eingeholt. Es bleibt aber die Frage, welchen Erkenntnisgewinn diese Angaben für die Beurteilung der Schulfähigkeit bringen und welche Rückschlüsse auf die Förderbedürftigkeit daraus gezogen werden sollen. Angaben zum Medienverhalten des Kindes sind weiterhin vorgesehen. Ein Zusammenhang dieser Angaben mit der Einordnung und Beurteilung von Befunden und Entwicklungsbesonderheiten des Kindes konnte bislang ebenfalls nicht überzeugend belegt werden; sie sind daher aus datenschutzrechtlicher Sicht weiterhin abzulehnen.

Soziodemografische Angaben zu den Bezugspersonen des Kindes (zum Beispiel: Elternbildung, Erwerbstätigkeit) sollen künftig lediglich zur anonymen statistischen Auswertung durch das Landesgesundheitsamt erfolgen. Um sicherzustellen, dass diese Daten ausschließlich zur statistischen Auswertung genutzt werden, halte ich allerdings deren Löschung für zwingend, sobald sie dem Landesgesundheitsamt anonymisiert übermittelt wurden.

Wenngleich der Entwurf der VwV ESU und Jugendzahnpflege immer noch die Erhebung personenbezogener Daten vorsieht, die zur Beurteilung der Schulreife und eines eventuellen Förderbedarfs nach meiner Auffassung nicht generell erforderlich sind, erkenne ich an, dass neben den personenbezogenen Daten des Kindes und der Eltern deutlich weniger sensible Daten erfragt werden. Meine Forderung, die im Rahmen der Einschulungsuntersuchung zu erhebenden Daten auf den notwendigen Umfang zu beschränken und auch erst dann zu erfragen, wenn feststeht, dass sie für Zwecke der Einschulungsuntersuchung benötigt werden, besteht weiterhin.

8. Pflegestützpunkte mit datenschutzrechtlichen Startproblemen

Die Landesregierung hat 2008 beschlossen, 50 Pflegestützpunkte in Baden-Württemberg einzurichten. Pflegestützpunkte sollen den Betroffenen und ihren Angehörigen als Anlaufstelle bei medizinischen und pflegerischen Versorgungsfragen dienen. Die Betroffenen sollen dort unabhängig und umfassend, das heißt ressortübergreifend, beraten werden. Darüber hinaus obliegt es den Pflegestützpunkten, vor Ort vorhandene Leistungsangebote zu koordinieren und zu vernetzen. Damit verbunden ist die Verarbeitung höchst sensibler personenbezogener Daten der Hilfesuchenden.

Aufgrund der absehbaren demographischen Entwicklung in der Bundesrepublik Deutschland wird der Anteil alter Menschen in der Gesellschaft in den kommenden Jahrzehnten stark zunehmen. Für das Jahr 2040 prognostiziert die Rürup-Kommission 3,4 Millionen pflegebedürftige Menschen. Somit wird unweigerlich auch der Bedarf an pflegerischen Leistungen steigen. Um der daraus resultierenden erhöhten Nachfrage nach Informationen zum pflegerischen Angebot gerecht zu werden, hat der Gesetzgeber mit dem am 1. Juli 2008 in Kraft getretenen Gesetz zur strukturellen Weiterentwicklung der Pflegeversicherung (Pflege-Weiterentwicklungsgesetz – PfWG), BGBl. I S. 874, Kranken- und Pflegekassen verpflichtet, zur wohnortnahen Beratung, Versorgung und Betreuung der Versicherten Pflegestützpunkte einzurichten, sofern das jeweilige Land dies bestimmt. Baden-Württemberg hat davon mit Allgemeinverfügung zur Errichtung von Pflegestützpunkten in Baden-Württemberg vom 22. Januar 2010, GABl. 2010 S. 117, Gebrauch gemacht. Unter Moderation des Ministeriums für Arbeit und Soziales haben

sich die Landesverbände der Pflege- und Krankenkassen und die Kommunalen Landesverbände auf die am 15. Dezember 2008 unterzeichnete Kooperationsvereinbarung über die Errichtung und den Betrieb von Pflegestützpunkten verständigt. Die Kooperationsvereinbarung sieht einen von den Pflege- und Krankenkassen gemeinsam mit den Kommunalen Landesverbänden ins Leben gerufenen Verein „Landesarbeitsgemeinschaft Pflegestützpunkte e. V." (LAG) vor, der vor allem über die Trägerschaft von Pflegestützpunkten in den Stadt- und Landkreisen entscheidet und Standards für die Arbeit der Pflegestützpunkte festlegen soll.

Mit den Pflegestützpunkten werden wohnortnah Anlaufstellen geschaffen, die alte und pflegebedürftige Menschen und deren Angehörige umfassend, unabhängig und unentgeltlich zu allen Fragen rund um die Pflege und ums Alter, zu diesbezüglichen Leistungen der Pflege- und der Krankenkassen, zu Sozialleistungen des Staates und zu sämtlichen Hilfsangeboten in der Pflege informieren und beraten. Darüber hinaus koordinieren die Stützpunkte sämtliche für die Versorgung und Betreuung im Einzelfall in Frage kommenden Angebote und unterstützen die Betroffenen bei deren Inanspruchnahme. Schließlich werden die regional oder bei den verschiedenen Trägern und Einrichtungen vorhandenen pflegerischen und sozialen Versorgungs- und Betreuungsangebote aufeinander abgestimmt und vernetzt, um auf diese Weise den Bürgerinnen und Bürgern möglichst das gesamte Angebot an Hilfeleistungen aufzuzeigen und zur Verfügung stellen zu können. Leistungsentscheidungen werden nicht im Pflegestützpunkt getroffen. Sie obliegen weiterhin den jeweils zuständigen Leistungsträgern.

Aufgrund der in den Pflegestützpunkten zu verarbeitenden sensitiven Daten der Hilfesuchenden (beispielsweise über gesundheitliche Probleme, Hilfebedarf) kommt dem Datenschutz in den Stützpunkten unstreitig eine hohe Bedeutung zu. Gleichwohl hat mich die LAG bedauerlicherweise zunächst nicht zu Rate gezogen. Und so musste ich, nachdem die ersten Pflegestützpunkte ihre Arbeit bereits aufgenommen hatten, leider feststellen, dass die LAG zwar umfangreiche Dokumente (Datenschutzvereinbarung, Datenschutzkonzept, Merkblatt für Hilfesuchende und Einwilligungserklärung), die den Umgang mit dem Datenschutz regeln, entwickelt hat, diese jedoch umfänglichen datenschutzrechtlichen Bedenken begegneten. Wenngleich sich die LAG einsichtig gezeigt hat und auch bereit war, die Dokumente im Sinne eines verbesserten Datenschutzes zu überarbeiten, so hat es doch über ein Jahr gedauert, Einvernehmen in wesentlichen und auch für den Inhalt zentraler Dokumente bedeutsamen Fragestellungen zu erzielen. Strittig war bis zuletzt vor allem die Frage, ob es (zusätzlich) einer gesonderten datenschutzrechtlichen Einwilligung der Hilfesuchenden in die Verarbeitung ihrer Daten bedarf.

Die LAG ging zunächst davon aus, dass eine Verarbeitung personenbezogener Daten der Hilfesuchenden in den Pflegestützpunkten nur und ausschließlich mit deren Einwilligung zulässig ist. Ob und in welchem Umfang eine Rechtsvorschrift die Datenverarbeitung erlaubt, war nach meinem Eindruck weder bekannt noch geprüft worden. Aber auch die von der LAG für die Pflegestützpunkte vorgesehene Einwilligungserklärung entsprach in keiner Weise den datenschutzrechtlichen Anforderungen. Da von den Pflegestützpunkten besonders sensible Daten der Hilfesuchenden verarbeitet werden, müssen die Rechtsgrundlage sowie Umfang, Zweck und Dauer der Datenverarbeitung klar und transparent sein. Das Merkblatt „Wichtige Informationen des Pflegestützpunktes" für die Hilfesuchenden erfüllte diese Voraussetzungen ebenfalls nicht. Mein beinahe gebetsmühlenhaft vorgetragener Hinweis, dass das Elfte Buch des Sozialgesetzbuchs (SGB XI) sehr wohl eine datenschutzrechtliche Erlaubnisnorm für die Datenverarbeitung in den Stützpunkten biete und damit eine Einwilligung der Hilfesuchenden nicht erforderlich sei, führte leider zu keinem Umdenken.

Gemäß § 92 c Absatz 7 SGB XI dürfen im Pflegestützpunkt tätige Personen Sozialdaten nur erheben, verarbeiten und nutzen, soweit dies zur Erfüllung der Aufgaben nach diesem Buch erforderlich oder durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist. Darüber hinaus sollen die Träger der Sozialhilfe nach § 4 des Zwölften Buchs des Sozialgesetzbuchs (SGB XII) gemeinsam mit den Beteiligten der Pflegestützpunkte

nach § 92 c SGB XI alle für die wohnortnahe Versorgung und Betreuung in Betracht kommenden Hilfe- und Unterstützungsangebote koordinieren. Und schließlich muss die Pflegeberatung durch die Pflegekassen nach § 7 a SGB XI bei Bedarf auch im Pflegestützpunkt angeboten werden.

Nach meiner Auffassung bieten die genannten Regelungen eine hinreichende Rechtsgrundlage für die Verarbeitung personenbezogener Daten in den Pflegestützpunkten; einer zusätzlichen gesonderten Einwilligung der Hilfesuchenden in die Verarbeitung ihrer Daten bedarf es nicht.

Die LAG hat demgegenüber immer wieder betont, die gesetzlichen Bestimmungen seien nicht ausreichend, eine Einwilligung der Betroffenen daher unverzichtbar. Gleichwohl sieht sich die LAG bis heute nicht in der Lage, konkret die Datenverarbeitungsvorgänge zu benennen, die mit einer Einwilligung vermeintlich abgedeckt werden sollen. Dies wiederum wäre zwingende Voraussetzung für eine wirksame Einwilligungserklärung. Denn aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, dass die vom Pflegestützpunkt vorgenommene Verarbeitung personenbezogener Daten für die Hilfesuchenden nachvollziehbar und transparent ist. Dies bedeutet, dass für die Betroffenen ersichtlich sein muss, welche personenbezogenen Daten Pflegestützpunkte aufgrund einer Rechtsvorschrift ohnehin und welche Daten diese zusätzlich mit Einverständnis der Hilfesuchenden verarbeiten dürfen.

Die LAG hat sich nunmehr bereit erklärt, bis auf Weiteres auf eine Einwilligungserklärung zu verzichten. Die Hilfesuchenden sollen durch ein Merkblatt verständlich und umfassend über die Datenverarbeitung im Pflegestützpunkt informiert werden. Sollten die Erfahrungen der Pflegestützpunkte in den kommenden Monaten zeigen, dass dort konkret benennbare Datenverarbeitungsvorgänge anfallen, die nur mit Einwilligung der Betroffenen rechtmäßig vorgenommen werden können, bin ich gerne bereit, meine Rechtsauffassung zu überprüfen. Wichtig wird dabei für mich auch künftig sein, den Hilfesuchenden nur das abzuverlangen, was datenschutzrechtlich notwendig, aber ausreichend ist.

Wenngleich die Diskussion mit der LAG schwierig und langwierig war, bin ich doch zuversichtlich, dass nunmehr zügig das Merkblatt für die Hilfesuchenden überarbeitet und den Pflegstützpunkten für ihre tägliche Arbeit zur Verfügung gestellt wird. Meine Mitarbeiter werden die Arbeit der Pflegestützpunkte begleiten und dafür Sorge tragen, dass die Rechte der Hilfesuchenden gewahrt werden.

2. Abschnitt: Soziales

1. ELENA gestoppt – ein Sieg der Vernunft und des Datenschutzes

Im 29. Tätigkeitsbericht (LT-Drucksache 14/5500) hatte ich das ELENA-Verfahren noch als eines der größten datenschutzrechtlichen Ärgernisse der letzten Jahre bezeichnet. Nun kam das Aus schon, bevor der Wirkbetrieb begann.

Seit Beginn des Jahres 2010 haben Arbeitgeber die Einkommensdaten ihrer Beschäftigten an eine Zentrale Speicherstelle gemeldet. Hierzu waren sie gesetzlich verpflichtet. Eine gigantische Datensammlung auf Vorrat entstand, denn der Regel-Betrieb im ELENA-Verfahren sollte erst ab Januar 2012 beginnen. Ab diesem Zeitpunkt sollten die für die Bewilligung von Anträgen auf Arbeitslosengeld, Wohngeld und Bundeselterngeld erforderlichen Daten unter Einsatz von Signaturkarten der Leistungsbezieher von den Sozialbehörden abgerufen werden.

Schnell zeigte sich, dass voraussichtlich auch erst dann die Infrastruktur zur Verfügung stehen würde, um den gesetzlich geregelten Auskunftsanspruch des Betroffenen über die zu seiner Person gespeicherten Daten realisieren zu können.

Im Frühjahr 2010 wurde beim Bundesverfassungsgericht eine Verfassungsbeschwerde gegen das ELENA-Verfahren eingereicht, die von über 22 000 Bürgern unterstützt wurde. In der Beschwerde wurde die Verletzung von

Grundrechten, insbesondere des Rechts auf informationelle Selbstbestimmung, gerügt.

Anfang Juli 2010 trat der damalige Bundeswirtschaftsminister mit der Botschaft an die Öffentlichkeit, das ELENA-Verfahren auf unbestimmte Zeit aussetzen zu wollen. Er begründete dies damit, dass die öffentlichen Haushalte durch das Verfahren nicht zu sehr belastet werden dürfen und dass noch nicht klar sei, ob bei Teilen des Mittelstands tatsächlich eine Entlastung stattfinde.

Im September 2010 übergab der Nationale Normenkontrollrat dem Bundeswirtschaftsminister ein ausführliches Gutachten zu den Auswirkungen des ELENA-Verfahrens[8], wonach die Einsparungen durch das ELENA-Verfahren äußerst bescheiden ausfallen würden: Während die Wirtschaft mit etwas mehr als 90 Millionen Euro entlastet werde, führe das ELENA-Verfahren in der Verwaltung zu einem Mehraufwand in Höhe von 82 Millionen Euro. Außerdem komme es bei Unternehmen mit weniger als 10 Mitarbeitern (sog. Kleinstunternehmen) zu einer Mehrbelastung gegenüber dem bisherigen papiergebundenen Verfahren; solche Kleinstunternehmen machen rund 90 Prozent aller Unternehmen in Deutschland aus. Diese Aussage in dem Gutachten ist schon deswegen bemerkenswert, weil nach der Begründung zum Gesetzentwurf Anlass für das ELENA-Verfahren neben Effizienzverlusten in der Verwaltung hohe Kosten für die Arbeitgeber waren (BT-Drucksache 16/10492, S. 15). Die Kommunalen Spitzenverbände gingen sogar von weitaus höheren Kosten für die Verwaltung aus. Offenbar war den Akteuren erst allmählich bewusst geworden, dass die zur Datenfreigabe einzusetzende Signaturkarte samt Lesegerät nicht ganz billig werden würde und die Kosten hierfür nicht von den Leistungsempfängern, sondern eher von den Sozialleistungsträgern aufzubringen sind. Sie forderten den Bundeswirtschaftsminister im Oktober 2010 auf, das ELENA-Verfahrensgesetz in seiner gegenwärtigen Fassung aufzuheben.

Im November 2010 ging der „Tod auf Raten“ weiter: Zunächst verschob die Koalition die Einführung des Regel-Betriebs im ELENA-Verfahren; danach sollten die Datenabrufe nun erst im Januar 2014, das heißt zwei Jahre später als geplant, beginnen.

Am 18. Juli 2011 verkündeten schließlich das Bundesministerium für Wirtschaft (BMWi) und das Bundesministerium für Arbeit und Soziales (BMAS) das endgültige Aus für ELENA[9]. Die Einstellung des Verfahrens wurde mit der fehlenden Verbreitung der qualifizierten elektronischen Signatur begründet. Die Bundesregierung erklärte allerdings, dass das Bundeswirtschaftsministerium in Kürze einen Gesetzentwurf vorlegen werde, in dem die unverzügliche Löschung der bisher gespeicherten Daten und die Entlastung der Arbeitgeber von den bestehenden elektronischen Meldepflichten geregelt werden. Außerdem werde das Bundesarbeitsministerium ein Konzept erarbeiten, wie die bereits bestehende Infrastruktur des ELENA-Verfahrens und das erworbene Know-how für „ein einfacheres und unbürokratisches Meldeverfahren in der Sozialversicherung“ genutzt werden können. Diese Ankündigung macht mich nach den Erfahrungen der Vergangenheit aber eher hellhörig und misstrauisch.

Den in der Pressemitteilung angekündigten Gesetzentwurf des Bundeswirtschaftsministerium verabschiedete die Bundesregierung im September 2011. Parallel zu der Aufhebungsinitiative beschloss das Kabinett Eckpunkte für ein ELENA-Nachfolgeverfahren. Auch wenn diesem Papier zufolge der Datenschutz Priorität haben soll, wird sich erst, wenn – wie im Eckpunktepapier angekündigt – das Bundesarbeitsministerium Ende des Jahres 2011 eine abgestimmte Konzeption des Projekts vorlegen wird, Näheres zu dem Nachfolgeverfahren sagen lassen.

---

[8] Das Gutachten kann im Internet nachgelesen werden unter http://www.normenkontrollrat.bund.de/Webs/NKR/Content/DE/Artikel/2010-09-13-elena-gutachten.html

[9] Die Pressemitteilung kann im Internet nachgelesen werden unter http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=424742.html?view=renderPrint

Der Bundestag hat das Gesetz zur Aufhebung von Vorschriften zum ELENA-Verfahren Ende September beschlossen. Anfang November 2011 billigte auch der Bundesrat das Gesetz. Dieses tritt am Tag nach seiner Verkündung in Kraft.

Im Rahmen einer begleitenden Entschließung hat der Bundesrat die Bundesregierung aufgefordert zu prüfen, welche Daten auch nach Inkrafttreten des Gesetzes noch einer Löschung bedürfen, und hierzu die erforderlichen Gesetzentwürfe vorzulegen. Hintergrund dieser Aufforderung ist der Umstand, dass das Gesetz zur Aufhebung von Vorschriften zum ELENA-Verfahren (lediglich) vorsieht, dass von der *Zentralen Speicherstelle und der Registratur Fachverfahren* alle im Zusammenhang mit dem ELENA-Verfahren gespeicherten Daten unverzüglich zu löschen sind. Allerdings sind im Rahmen des ELENA-Verfahrens auch von den Rentenversicherungsträgern und gegebenenfalls anderen Behörden Daten gespeichert worden, die nun nicht mehr benötigt werden.

Und das Fazit aus Sicht eines Datenschutzbeauftragten?

Auch wenn der Hauptgrund für die Einstellung des ELENA-Verfahrens wohl die hohen Kosten beziehungsweise das schlechte Kosten-Nutzen-Verhältnis waren, hoffe ich, dass auch die vielfältigen Mahnungen der Datenschützer nicht ungehört blieben. Die strukturellen Mängel waren von vornherein erkennbar; sie lagen darin, dass das Verfahren zu einem riesigen zentralen Datenspeicher führte, obwohl ein großer Anteil der Betroffenen die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals geltend machen wird. Eine solche Vorratsdatenspeicherung ist aus verfassungsrechtlichen Gründen äußerst problematisch.

Bei dem angekündigten neuen Meldeverfahren gilt es darauf zu achten, dass ein solches nicht – zum Beispiel aus Kostengründen – noch weniger datenschutzrechtliche Anforderungen als das ELENA-Verfahren erfüllt. Insofern ist das Aus für ELENA lediglich ein Etappensieg. Die neuen Planungen der Bundesregierung führen zwar zu Recht den Datenschutz als bestimmend für das Nachfolgeverfahren an. Ob die am Gesetzentwurf beteiligten Ministerien sowie Bundestag und Bundesrat aber nicht eher geneigt sind, ein „ELENA light“ zu schaffen und zu diesem Zweck etwa die hohe Hürde einer elektronischen Signatur einzureißen, bleibt abzuwarten. Die Datenschutzbeauftragten des Bundes und der Länder werden die Planungen jedenfalls wie bisher wachsam und kritisch begleiten.

2. Grundsicherung für Arbeitsuchende neu geregelt

Das Bundesverfassungsgericht hatte schon Ende 2007 entschieden, dass die Arbeitsgemeinschaften als Gemeinschaftseinrichtung von Bundesagentur für Arbeit und kommunalen Trägern mit dem Grundgesetz nicht vereinbar sind[10] und die Arbeitsgemeinschaften deshalb nur noch während einer – meines Erachtens großzügig bemessenen – Übergangszeit längstens bis zum 31. Dezember 2010 tätig werden dürfen.

Um den lang andauernden Streit um die Zukunft der Jobcenter zu beenden, wurde daraufhin eine interfraktionelle Bund-Länder-Arbeitsgruppe eingesetzt, die sich im März 2010 darauf verständigte, die Zusammenarbeit von Bundesagentur für Arbeit und kommunalen Trägern fortzusetzen. Argumente hierfür waren, dass sich die Durchführung der Grundsicherung für Arbeitsuchende in den Arbeitsgemeinschaften grundsätzlich bewährt habe und die Zusammenarbeit von Arbeitsagenturen und Kommunen gewährleiste, dass die Hilfebedürftigen aus einer Hand betreut werden und Leistungen aus einer Hand erhalten. Für die Fortführung der Zusammenarbeit musste das Grundgesetz geändert und eine Ausnahme vom Verbot der Mischverwaltung aufgenommen werden. Artikel 91 e des Grundgesetzes, nach dessen Absatz 1 bei der Ausführung von Bundesgesetzen auf dem Gebiet der Grundsicherung für Arbeitsuchende Bund und Länder oder die nach Landesrecht zuständigen Gemeinden und Gemeindeverbände in der Regel in

[10] Die Entscheidung kann im Internet nachgelesen werden unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20071220_2bvr243304.html

gemeinsamen Einrichtungen zusammenwirken, wurde am 17. Juni 2010 mit der notwendigen Zweidrittelmehrheit vom Bundestag beschlossen und trat im Juli 2010 in Kraft.

Zusätzlich zur Grundgesetzänderung wurde das Zweite Buch des Sozialgesetzbuchs novelliert. Neben Änderungen im Zusammenhang mit den gemeinsamen Einrichtungen wurde auch die Forderung der Datenschutzbeauftragten erfüllt, die datenschutzrechtliche Aufsichtszuständigkeit *eindeutig* zu regeln. Dies war bislang nicht der Fall. § 50 des Zweiten Buchs des Sozialgesetzbuchs bestimmt nun, dass die Datenschutzkontrolle und die Kontrolle der Einhaltung der Vorschriften über die Informationsfreiheit bei den gemeinsamen Einrichtungen sowie für die zentralen Verfahren der Informationstechnik nach § 24 BDSG dem *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* obliegen.

Außerdem sieht das geänderte Gesetz eine begrenzte Erweiterung der Anzahl der zugelassenen kommunalen Träger – dies sind Stadt- und Landkreise, die die Aufgaben nach dem Zweiten Buch des Sozialgesetzbuchs in alleiniger Verantwortung erfüllen – vor. Für die Datenschutzkontrolle bei den zugelassenen kommunalen Trägern in Baden-Württemberg ist meine Dienststelle zuständig. Mit Wirkung zum 1. Januar 2012 wurden (zusätzlich zu den schon bestehenden fünf zugelassenen kommunalen Trägern) die folgenden Stadt- und Landkreise neu zugelassen: Der Enzkreis, der Landkreis Ludwigsburg, der Ostalbkreis, die Stadt Pforzheim, der Landkreis Ravensburg sowie die Landeshauptstadt Stuttgart.

In dem wichtigen Bereich der Grundsicherung für Arbeitsuchende ist meine Dienststelle ab 1. Januar 2012 zuständig für die folgenden Stadt- und Landkreise: Landkreis Biberach, Bodenseekreis, Enzkreis, Landkreis Ludwigsburg, Ortenaukreis, Ostalbkreis, Stadt Pforzheim, Landkreis Ravensburg, Landeshauptstadt Stuttgart, Landkreis Tuttlingen und Landkreis Waldshut.[11]

3. Einzelfälle

3.1 Auskunftspflicht von Unterhaltspflichtigen

Eine Bürgerin hatte sich an meine Dienststelle gewandt und Folgendes vorgetragen: Ihr sei vom Sozialamt mitgeteilt worden, dass ihr Vater in einem Pflegeheim untergebracht sei und sie zur Feststellung ihrer Unterhaltspflicht ihre Vermögensverhältnisse anzugeben habe. Die Petentin war der Ansicht, dass eine Unterhaltspflicht wegen „unbilliger Härte“ nicht bestehe, da sie seit ihrer Kindheit keinen Kontakt mehr zu ihrem Vater hatte und dieser ihr damals nur unregelmäßig oder gar nicht Unterhalt gezahlt habe. Daher sei sie bezüglich ihrer Vermögensverhältnisse auch nicht auskunftspflichtig.

Die Prüfung durch meine Dienststelle ergab jedoch, dass die Datenerhebung des Sozialamts nicht zu beanstanden war:

Gemäß § 117 Absatz 1 Satz 1 des Zwölften Buchs des Sozialgesetzbuchs (SGB XII) haben die Unterhaltspflichtigen, ihre nicht getrennt lebenden Ehegatten oder Lebenspartner und die Kostenersatzpflichtigen dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben, soweit die Durchführung dieses Buchs es erfordert. Hintergrund dieser Regelung ist, dass zivilrechtliche Unterhaltsansprüche von sozialhilfeberechtigten Personen bis zur Höhe der geleisteten Aufwendungen auf den Träger der Sozialhilfe übergehen. Hierdurch soll der vom Gesetzgeber gewollte Nachrang der Sozialhilfe nachträglich wieder hergestellt werden.

Die Verpflichtung von potenziell Unterhaltspflichtigen zur Auskunft ist nicht davon abhängig, ob im konkreten Fall tatsächlich ein Unterhalts-

[11] Bis Ende des Jahres 2011 ist meine Dienststelle zuständig für den Landkreis Biberach, den Bodenseekreis, den Ortenaukreis, den Landkreis Tuttlingen, den Landkreis Waldshut und in den Stadt- und Landkreisen, in denen die Aufgaben der Grundsicherung für Arbeitsuchende noch getrennt wahrgenommen werden, für den jeweiligen kommunalen Träger.

anspruch besteht, denn erst nach erfolgter Auskunft kann der Sozialhilfeträger beurteilen, ob und in welchem Umfang er den Nachranggrundsatz des Sozialhilferechts durch die Inanspruchnahme eines Dritten wiederherstellen kann. Aufgrund der Vorschrift können alle Personen als Unterhaltspflichtige im Sinne der sozialhilferechtlichen Vorschriften gelten, die als Unterhaltsschuldner in Betracht kommen und nicht offensichtlich (sog. Negativevidenz) ausscheiden. Von einer solchen Evidenz war vorliegend insbesondere deshalb nicht auszugehen, da gemäß § 94 Absatz 3 Satz 1 Nummer 2 SGB XII der Unterhaltanspruch nicht auf den Träger der Sozialhilfe übergeht, soweit dies eine unbillige Härte bedeuten würde. Bei der Auslegung dieser Härteklausel kommt es neben der sozialen Lage aber gerade auch auf die *wirtschaftlichen Verhältnisse* der Beteiligten an.

3.2 Datenerhebung beim Vermieter

Ein Bürger teilte meiner Dienststelle mit, dass er Leistungen der Sozialhilfe erhalte. Aufgrund einer Erkrankung sei er nicht in der Lage, sein Auto – welches er für Arztbesuche benötige – im Winter von Schnee und Eis zu befreien. Daher habe er beim Sozialamt des Landratsamts die Übernahme der Mietkosten für seine Garage beantragt; die Garage sei Bestandteil des Mietvertrags über seine Wohnung. Das Sozialamt habe sich daraufhin an seinen Vermieter gewandt und gefragt, ob eine Weitervermietung der Garage an Dritte möglich sei. Der Petent hielt die Nachfrage bei seinem Vermieter für unzulässig.

Das Sozialamt erklärte meiner Dienststelle gegenüber, dass es beim Gesundheitsamt des Landratsamts angefragt habe, ob der Petent aufgrund seiner Erkrankung überhaupt in der Lage sei, ein Kraftfahrzeug zu steuern. Das Gesundheitsamt habe geantwortet, dass nach den Begutachtungsleitlinien zur Kraftfahreignung Bedenken hinsichtlich der Fahrtauglichkeit bestünden. Aufgrund dieser Äußerung des Gesundheitsamts sei das Sozialamt der Auffassung gewesen, dass der Petent nicht auf ein Kraftfahrzeug angewiesen und daher die Garagenmiete nicht als sozialhilferechtlicher Bedarf anzuerkennen sei. Sollte eine Weitervermietung der Garage mangels Zustimmung des Vermieters nicht zulässig sein, müsse die Garage aber dennoch als – nicht von der Wohnung zu trennender – sozialhilferechtlicher Bedarf anerkannt werden. Das Sozialamt habe zunächst den Petenten gebeten, eine schriftliche Erklärung seines Vermieters vorzulegen, ob die Garage von diesem an Dritte weitervermietet werden dürfe. Nachdem der Petent die angeforderte Erklärung des Vermieters nicht vorgelegt habe, habe sich das Sozialamt direkt an den Vermieter gewandt.

Auch wenn es ausnahmsweise zulässig sein kann, Daten über den Betroffenen bei Dritten einzuholen, beispielsweise wenn der Betroffene selbst nichts sagen will, halte ich die Datenerhebung bei dem Vermieter des Petenten im vorliegenden Fall *nicht* für erforderlich: Die Entziehung der Fahrerlaubnis durch die Fahrerlaubnisbehörde ist nach § 46 Absatz 1 der Fahrerlaubnis-Verordnung zulässig, wenn sich der Inhaber einer Fahrerlaubnis als ungeeignet zum Führen von Kraftfahrzeugen *erweist.* Bedenken allein sind nicht ausreichend, um einem Inhaber einer Fahrerlaubnis diese zu entziehen. Vielmehr ist in einem solchen Fall – gegebenenfalls mit Hilfe eines ärztlichen Gutachtens – eine Klärung bezüglich des Vorliegens der Eignung herbeizuführen. Der Schluss, allein aufgrund von *Bedenken des Gesundheitsamts bezüglich der Fahrtauglichkeit* davon auszugehen, dass der Petent zum Führen von Kraftfahrzeugen ungeeignet und die Garage aus diesem Grund nicht als sozialhilferechtlicher Bedarf anzuerkennen ist, war daher so nicht nachvollziehbar: Erstens kam das Gesundheitsamt vorliegend gerade nicht zu dem Ergebnis, dass der Petent zum Führen von Kraftfahrzeugen ungeeignet ist. Zweitens stellt sich die Frage, ob es überhaupt zulässig ist, dass das Sozialamt im Rahmen des Sozialhilferechts anstelle der Fahrerlaubnisbehörde über die Eignung zum Führen eines Kraftfahrzeugs entscheidet.

Aufgrund des Umstands, dass zum Zeitpunkt der Anfrage bei dem Vermieter gar nicht feststand, dass der Petent *mangels Fahrtauglichkeit*

nicht auf ein Kraftfahrzeug und folglich nicht auf eine Garage angewiesen ist und die Garagenmiete daher nicht als sozialhilferechtlicher Bedarf anzuerkennen ist, hielt ich eine Involvierung des Vermieters jedenfalls zu diesem Zeitpunkt für nicht zulässig.

Das Sozialamt ist in diesem Fall über das Ziel hinausgeschossen und hat bei seinem Vorgehen wohl seinen eigentlichen Zuständigkeitsbereich – Sozialhilferecht – zu Lasten des Petenten überdehnt. Das Sozialamt hat zu Recht eingeräumt, dass sein Vorgehen nicht in allen Punkten den gesetzlichen Regelungen entsprochen hat.

3.3 Verstoß gegen die Unterstützungspflicht öffentlicher Stellen

Ein Bezieher von Leistungen der Grundsicherung für Arbeitsuchende vermutete, dass sich das für ihn zuständige Landratsamt als Grundsicherungsträger an seinen ehemaligen Arbeitgeber gewandt hatte, um dort nachzufragen, weswegen er entlassen worden war. Das Landratsamt räumte meiner Dienststelle gegenüber zwar ein, sich in der Tat an den früheren Arbeitgeber des Petenten gewandt zu haben. Dies sei aufgrund eines Sozialdatenabgleichs erfolgt, wonach der Petent bei dem Arbeitgeber aktuell versicherungspflichtig beschäftigt sein sollte. Hierzu muss man wissen, dass mit einem solchen Datenabgleich der unberechtigte Bezug von Leistungen der Grundsicherung für Arbeitsuchende, die einkommens- und vermögensabhängig sind, aufgedeckt werden soll. Dabei seien aber keine Informationen hinsichtlich des Kündigungsgrunds bei dem Arbeitgeber erfragt worden. Der ehemalige Arbeitgeber habe vielmehr lediglich bestätigt, dass der Petent – wie von diesem selbst vorgetragen – zwar früher dort gearbeitet habe, aber aktuell nicht mehr bei ihm beschäftigt sei. Ich teilte dem Petenten daraufhin mit, dass sich seine Vermutung, dass der Grundsicherungsträger sich bei seinem ehemaligen Arbeitgeber Informationen über den Kündigungsgrund beschafft habe, aufgrund der Stellungnahme des Landratsamts nicht bestätigt habe. Zur Überprüfung der Angaben des Landratsamts habe ich dieses noch aufgefordert, das Anschreiben an den Arbeitgeber in Kopie vorzulegen. Aus der daraufhin vorgelegten Kopie des Schreibens an den Arbeitgeber hat sich – im Widerspruch zu den Ausführungen des Landratsamts meiner Dienststelle gegenüber – ergeben, dass durchaus gefragt wurde, weswegen der Petent entlassen worden war. Dass dem Landratsamt nicht bekannt wurde, aus welchem Grund das Arbeitsverhältnis mit dem Petenten endete, war lediglich dem Verhalten des Arbeitgebers zu verdanken, der diese Frage trotz entsprechender Aufforderung des Grundsicherungsträgers, der sogar auf eine angebliche Auskunftspflicht hingewiesen hatte, nicht beantwortet hat.

Um es auf den Punkt zu bringen: Die Frage nach dem Kündigungsgrund war – zumal das Beschäftigungsverhältnis mit dem Petenten schon mehr als eineinhalb Jahre vor der Anfrage geendet hatte – nicht zulässig. Zudem hat das Landratsamt meiner Dienststelle gegenüber falsche Auskünfte erteilt. Aufgrund dessen habe ich das Verhalten des Landratsamts als Verstoß gegen § 29 Absatz 1 LDSG förmlich beanstandet. Nach dieser Vorschrift ist mir und meinen Mitarbeitern im Rahmen der Kontrollbefugnis nach § 28 LDSG Auskunft zu unseren Fragen zu gewähren. Die Auskünfte der verpflichteten öffentlichen Stelle müssen selbstverständlich der Wahrheit entsprechen. Der Fall ist nicht nur ein schlechtes Beispiel für den Umgang mit Sozialdaten durch das Landratsamt, sondern auch für dessen Verständnis über seine Pflichten gegenüber der Aufsichtsbehörde.

Meine Dienststelle kann die ihr gesetzlich zugewiesenen Aufgaben nur erfüllen, wenn die zu beaufsichtigenden öffentlichen Stellen auch ihrer gesetzlich vorgeschriebenen Unterstützungspflicht nachkommen. Hierbei ist meine Dienststelle insbesondere darauf angewiesen, dass ihr keine unrichtigen Auskünfte erteilt werden. Nach meinen Erfahrungen handelt es sich vorliegend zum Glück um einen Einzelfall. Die allermeisten öffentlichen Stellen erfüllen ihre Mitwirkungspflichten ordnungsgemäß und geben inhaltlich richtige Auskünfte.

5. Teil: Datenschutz in anderen Verwaltungsbereichen

1. Kommunales

1.1 Fertigung von Luftbildaufnahmen zur Ermittlung von kommunalen Abwassergebühren

Das Thema „Fertigung von Luftbildaufnahmen zur Ermittlung kommunaler Abwassergebühren“ hat mich während des Berichtzeitraumes längere Zeit beschäftigt. Mich erreichten hierzu eine Vielzahl von Anfragen und Eingaben. Auch die Presse und die Politik zeigten großes Interesse an diesem Thema. Im Ergebnis halte ich die zum Zweck der Einführung der gesplitteten Abwassergebühr von zahlreichen Gemeinden vorgenommene Erhebung von Daten durch den Erwerb von Luftbildaufnahmen beim Landesamt für Geoinformation und Landentwicklung oder durch Beauftragung privater Unternehmen mit der Herstellung entsprechender Aufnahmen ohne Einwilligung der Betroffenen mangels Rechtsgrundlage für unzulässig. Das Innenministerium des Landes sieht dies bis heute anders. Doch der Reihe nach:

Auslöser war das Urteil des Verwaltungsgerichtshofs Baden-Württemberg (VGH) vom 11. März 2010, 2 S 2938/08, mit dem ein Abwassergebührenbescheid aufgehoben wurde, der auf dem sog. Frischwassermaßstab beruhte. Der Verwaltungsgerichtshof hielt es nämlich nicht mehr für vertretbar, wenn die Abwassergebühr nur aufgrund der Menge des bezogenen Frischwassers berechnet wird, weil die Kanalisation einer Gemeinde auch im Hinblick auf die Menge des abzuleitenden Niederschlagswassers zu dimensionieren ist. Diese Menge hängt wiederum stark von der Bodenversiegelung ab. Satzungen, die keine getrennte Erfassung und Veranlagung des Niederschlagswassers vorsehen, seien daher nichtig und die darauf gestützten Bescheide rechtswidrig. Viele Gemeinden in Baden-Württemberg beschlossen daraufhin, zur Ermittlung der kommunalen Abwassergebühren Luftbilder zu verwenden, um feststellen zu können, welche Flächen in welchem Grad versiegelt sind.

Wegen der grundsätzlichen und landesweiten Bedeutung der Thematik, von der zahlreiche Gemeinden in Baden-Württemberg betroffen sind, habe ich mich zunächst unter anderem an das Innenministerium gewandt; eine übereinstimmende Bewertung der komplexen Rechtsfragen konnte im Ergebnis aber nicht erreicht werden. Luftbildaufnahmen von privaten Grundstücken, die im Zusammenhang mit der Berechnung der Abwassergebühr verwendet werden sollen, lassen – zumindest in Verbindung mit weiteren Informationen – Rückschlüsse auf persönliche oder sachliche Verhältnisse von bestimmbaren Personen, etwa der Eigentümer oder Bewohner der abgebildeten Grundstücke oder Objekte, zu. Es handelt sich somit um personenbezogene oder zumindest personenbeziehbare Daten. Gemäß § 4 Absatz 1 LDSG ist die Verarbeitung entsprechender Daten durch Behörden nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Eine Einwilligung wird regelmäßig nicht vorliegen, aber auch eine passende Rechtsvorschrift ist für mich nicht ersichtlich. In diesem Zusammenhang ist aus Sicht des Datenschutzes ausschlaggebend, dass auch in Bezug auf die Erhebung von Kommunalabgaben der Grundsatz der Direkterhebung von Informationen beim Betroffenen Vorrang genießt. Näheres kann meiner Stellungnahme „Fertigung von Luftbildaufnahmen zur Ermittlung von kommunalen Abwassergebühren“ vom 12. August 2011 entnommen werden, die diesem Tätigkeitsbericht als Anhang 44 angeschlossen ist.

Ergänzend ist darauf hinzuweisen, dass durch die Erhebung und Nutzung von Luftbildaufnahmen in der Regel keine abschließende Berechnung der gesplitteten Abwassergebühr möglich ist und eine Befragung der Betroffenen erforderlich ist, um die den Luftbildaufnahmen zu entnehmenden Informationen zu ergänzen beziehungsweise zu korrigieren. Dieser Umstand wirft allerdings auch die Frage auf, warum die Luftbildaufnahmen dann überhaupt noch erforderlich sind. Immerhin ist be-

merkenswert, dass entsprechende Satzungen jüngeren Datums aus anderen Ländern häufig ausschließlich den Grundstückseigentümer in die Pflicht nehmen, Angaben zu den angeschlossenen Grundstücksflächen zu machen. Auch ist in diesem Zusammenhang interessant, dass es durchaus Kommunen in Baden-Württemberg gibt, die auf die Verwendung von Luftbildaufnahmen verzichtet haben, weil sie dies für nicht erforderlich halten.

Von einer Beanstandung entsprechender kommunaler Erhebungen habe ich bislang abgesehen, weil das Innenministerium die beschriebene Vorgehensweise für rechtmäßig hält und die Gemeinden bereits zu einem frühen Verfahrenszeitpunkt – als zumindest ich noch die Hoffnung auf eine Einigung hatte – entsprechend informiert hatte. Ob damit dem Datenschutz ein Gefallen getan wurde, wird sich spätestens dann zeigen, wenn es zu der von einigen Betroffenen angekündigten verwaltungsgerichtlichen Überprüfung der Abgabenbescheide kommen sollte.

Der Grundsatz der Direkterhebung gilt auch im kommunalen Abgabenrecht. Personenbezogene Daten sollten daher nach Möglichkeit immer beim Betroffenen direkt erhoben werden. Auf andere Erhebungsmethoden sollten die Kommunen erst zurückgreifen, wenn ihnen der Betroffene nicht die notwendigen Angaben zur Verfügung stellt.

1.2 So kommt der Datenschutz auf den Hund

Bereits in früheren Tätigkeitsberichten meiner Dienststelle (11. Tätigkeitsbericht, LT-Drucksache 10/4540, S.105, 12. Tätigkeitsbericht, LT-Drucksache 10/6470, S. 68 und 17. Tätigkeitsbericht, LT-Drucksache 12/750, S. 62) wurde die Frage aufgeworfen, ob eine Stadt entweder eigene Mitarbeiter oder Mitarbeiter einer beauftragten Firma von Haus zu Haus schicken und in jedem Haushalt nachfragen lassen darf, ob ein Hund gehalten wird, um so nicht angemeldete Hunde aufzuspüren.

Nachdem dieses Thema einige Jahre nicht mehr an meine Dienststelle herangetragen worden war, habe ich in den letzten Monaten von mehreren Städten erfahren, die eine solche Hundebestandskontrolle im Berichtszeitraum durchgeführt oder eine derartige Kontrolle geplant haben. Wie meine Vorgänger im Amt, kam auch ich im Zusammenhang mit den aktuellen Vorgängen zu dem Ergebnis, dass derartige Hundebestandskontrollen nicht zulässig sind:

Selbstverständlich müssen Städte und Gemeinden ihre Steuern und Abgaben, und damit auch die Hundesteuer, gleichmäßig erheben. Dazu gehört auch, diejenigen Hundehalter zu ermitteln, die ihren Anzeigepflichten nach der Hundesteuersatzung nicht nachgekommen sind und sie zur Hundesteuer heranzuziehen. Obwohl sich durch Haus-zu-Haus-Befragungen unter Umständen eine erhebliche Zahl bislang nicht angemeldeter Hunde aufspüren lässt, ist diese Art der Sachaufklärung nicht rechtmäßig. Liegen konkrete Anhaltspunkte dafür vor, dass eine Person einen Hund hält, ohne diesen angemeldet zu haben, darf eine Stadt selbstverständlich der Angelegenheit nachgehen und aufklären, ob eine unangemeldete Hundehaltung vorliegt. Die von Haus-zu-Haus-Befragungen, die sich auf alle Haushalte in allen Gebäuden einer Stadt erstrecken, sind jedoch von völlig anderer Qualität. Diese Befragungen erfolgen, ohne dass im Einzelfall irgendwelche Anhaltspunkte für eine nicht angemeldete Hundehaltung vorliegen. Die Ermittlungen sollen vielmehr erst dazu dienen, Anhaltspunkte für eine Verletzung von Pflichten nach der Hundesteuersatzung zu gewinnen. Von derartigen Ermittlungen sind ganz überwiegend solche Personen betroffen, die entweder gar keinen Hund halten oder die ihre Hundehaltung ordnungsgemäß gemeldet haben. Solche Ermittlungen bedeuten eine flächendeckende Totalerhebung, bei der ohne jeden konkreten Verdacht ungezielt alle Haushalte „durchgerastert“ werden mit dem Ziel, diejenigen „herauszufiltern“, die ihren steuerlichen Pflichten nicht nachgekommen sind. Hinzu kommt, dass die Bewohner jeweils in ihrem häuslichen, also einem vom Grundgesetz besonders geschützten Bereich, aufgesucht werden. Eine derartig umfassende behördliche Kontrolle der Bevölkerung steht außer Verhältnis zu dem damit verfolgten Ziel, einige

„Steuersünder“ aufzuspüren. Solche Hundebestandserfassungen sind auch nicht mit § 99 Absatz 2 der Abgabenordnung vereinbar. Nach dieser Vorschrift darf das Betreten von Grundstücken und Räumen nicht zu dem Zweck angeordnet werden, nach „unbekannten Gegenständen“ – also beispielsweise nach nicht angemeldeten Hunden – zu forschen.

Die Durchführung von Hundebestandskontrollen ist – unabhängig davon, ob sie von eigenen Mitarbeitern der Städte und Gemeinden oder von externen Unternehmen durchgeführt werden – aus datenschutzrechtlicher Sicht unzulässig.

1.3 Kommunale Veröffentlichungen im Internet

Inzwischen ist es selbstverständlich, dass Kommunen einen eigenen Internet-Auftritt haben. Auf diversen kommunalen Internet-Seiten ist eine Vielzahl von interessanten und hilfreichen Informationen zu finden. Die entsprechenden Angebote können einfach, unkompliziert und in Sekundenschnelle rund um die Uhr abgerufen werden. Die Beweggründe der Kommunen für ein solches Internet-Angebot sind für mich gut nachzuvollziehen. Jedoch wirft die Veröffentlichung von personenbezogenen Daten durch Kommunen im Internet eine Vielzahl von datenschutzrechtlichen Fragen auf, denn die Veröffentlichungen sind in der Regel einfach recherchierbar, unterliegen keinen Zweckbindungen oder sonstigen Beschränkungen, können von einem unübersehbar großen Nutzerkreis global abgerufen werden und sind meist ohne Einschränkungen mit anderen Daten verknüpfbar. Deshalb sind mit einer Einstellung von personenbezogenen Daten in das Internet besonders hohe Risiken verbunden.

Wie bei jeder Datenverarbeitung, so ist auch eine Veröffentlichung von personenbezogenen Daten im Internet ohne Einwilligung des Betroffenen nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene einwilligt. Für eine Veröffentlichung im Internet ist zudem erforderlich, dass eine normenklare Rechtsvorschrift nicht nur allgemein eine Veröffentlichung erlaubt, sie muss sich vielmehr auch ausdrücklich auf eine Veröffentlichung im Internet beziehen. Es versteht sich von selbst, dass unabhängig davon auch bei der Gestaltung von kommunalen Internet-Auftritten die Grundsätze der Datensparsamkeit und Datenvermeidung gelten.

Bei Fehlen einer Rechtsgrundlage ist es erforderlich, dass die Betroffenen wirksam in eine Veröffentlichung ihrer Daten mit Personenbezug im Internet einwilligen. Eine wirksame Einwilligung des Betroffenen zur Datenverarbeitung setzt voraus, dass dieser über die beabsichtigte Datenverarbeitung und den konkreten Zweck der Datenverarbeitung aufgeklärt wird (vgl. § 4 Absatz 2 Satz 1 LDSG und § 14 LDSG). Die Einwilligungserklärung muss bei einer Veröffentlichung im Internet auch diese besondere Veröffentlichungsform umfassen. Die Einwilligung bedarf grundsätzlich der Schriftform (§ 4 Absatz 3 Satz 1 LDSG). Mutmaßliche, stillschweigende oder auch konkludente Erklärungen scheiden aus. Bei Minderjährigen, denen die datenschutzrechtliche Einsicht fehlt, sind Einwilligungserklärungen von den jeweiligen Erziehungsberechtigten abzugeben. Eine Einwilligung ist ferner nur wirksam, wenn sie freiwillig erfolgt. Wenn beispielsweise eine Drucksituation innerhalb einer sozialen Gruppe gegeben ist, kann es aus Sicht des Datenschutzes unter Umständen bereits aus diesem Grund an der Freiwilligkeit fehlen. Erklärungen, die nicht den Anforderungen des § 4 LDSG entsprechen, sind nichtig. Bei von einer Kommune vorbereiteten Einwilligungserklärungen (Vordruck/Formular) für Betroffene ist unter anderem auf die Freiwilligkeit der Erteilung der Einwilligung, die Widerrufsmöglichkeit der Einwilligung und bei Veröffentlichungen im Internet auf die damit verbundenen Gefahren (unter anderem weltweite Abrufbarkeit, Gefahr der Nutzung zu anderen Zwecken durch Dritte) hinzuweisen. Wenn eine Einwilligung zusammen mit anderen Erklärungen erteilt werden soll, ist sie deutlich hervorzuheben. Im Ergebnis kann festgehalten werden, dass aus Sicht des Datenschutzes an eine wirksame Einwilligung des Betroffenen zur Veröffentlichung von per-

sonenbezogenen Daten im Internet sehr hohe Anforderungen zu stellen sind.

Im Berichtszeitraum ging es für uns schwerpunktmäßig um die Übertragung von Gemeinderatssitzungen im Internet, um die Veröffentlichung von Alters- und Ehejubiläen sowie von Fotos und Videoaufnahmen.

1.3.1 Die Übertragung von Gemeinderatssitzungen im Internet

Eine Großstadt hat mich um Mitteilung gebeten, wie ich die Zulässigkeit von Übertragungen von Gemeinderatssitzungen im Internet beurteile.

Zunächst ist aus datenschutzrechtlicher Sicht festzustellen, dass keine Rechtsgrundlage ersichtlich ist, die eine solche Vorgehensweise erlauben würde. Insbesondere stellt der kommunalrechtliche Grundsatz der Öffentlichkeit von Gemeinderatssitzungen (vgl. § 35 der Gemeindeordnung – GemO –) keine geeignete Rechtsgrundlage dar. Demnach sind Gemeinderatssitzungen zwar grundsätzlich öffentlich und jedermann muss Zutritt haben. Dabei können auch Ortsfremde und Minderjährige nicht ausgeschlossen werden. Der Öffentlichkeitsgrundsatz ist jedoch bereits hinreichend beachtet, wenn die Sitzungen an einem Ort stattfinden, der allgemein zugänglich ist und Platz für interessierte Bevölkerungskreise bietet (sog. „Saalöffentlichkeit“). Eine weitere Ausdehnung der Öffentlichkeit ist nach § 35 GemO nicht erforderlich. Auch hilft der Vergleich mit einer Fernsehübertragung aus einem Parlament nicht weiter. Der Gemeinderat als Kollegialorgan ist ein Verwaltungsorgan der Gemeinde und kein Parlament im staatsrechtlichen Sinne (vgl. § 23 GemO). Das Verwaltungshandeln überwiegt bei der Aufgabenwahrnehmung, da selbst bei größeren Gemeinden regelmäßig kommunalpolitische Sachthemen im Vordergrund stehen.

Von maßgeblicher Bedeutung bei der Übertragung beziehungsweise Aufzeichnung von Gemeinderatssitzungen ist noch immer das Urteil des Bundesverwaltungsgerichts vom 3. August 1990 (7 C 14/90), in dem es um Tonaufzeichnungen durch Journalisten in einer Gemeinderatssitzung ging, gegen die sich ein Gemeinderatsmitglied zur Wehr setzte. Das Gericht führte hierzu aus, „eine von psychologischen Hemmnissen möglichst unbeeinträchtigte Atmosphäre“ gehöre „zu den notwendigen Voraussetzungen eines geordneten Sitzungsbetriebs“, den der Vorsitzende zu gewährleisten habe. Tonbandaufzeichnungen hätten erhebliche Wirkungen auf das Verhalten der Betroffenen, „weil sie jede Nuance der Rede, einschließlich der rhetorischen Fehlleistungen, der sprachlichen Unzulänglichkeiten und der Gemütsbewegungen des Redners, dauerhaft und ständig reproduzierbar“ konserviere. Was für reine Tonbandaufzeichnungen gilt, dürfte erst recht für Bild- und Tonaufnahmen gelten, und ganz besonders für die Übertragungen derartiger Aufnahmen in das Internet. Immerhin gibt es bereits eine Vielzahl von Fällen, bei denen sich Betroffene ohne ihre Einwilligung oder gar ohne ihr Wissen mit Videoaufnahmen im Internet auf Portalen wie „Youtube“ wiedergefunden haben.

Da keine Rechtsgrundlage für diese Form der Datenverarbeitung ersichtlich ist, stellt sich die Frage nach einer datenschutzrechtlich wirksamen Einwilligung durch die Betroffenen. Der Einzelne muss sich völlig frei und ohne jeglichen Druck von außen entscheiden können. Nicht nur objektive Kriterien, sondern auch das subjektive Empfinden des Einzelnen spielt hierbei eine Rolle. Dabei ist für öffentliche Gemeinderatssitzungen zumindest nach den beteiligten Gruppen zu differenzieren:

– Gemeinderäte:

Die einzelnen Gemeinderäte sind nach der Gemeindeordnung ehrenamtlich tätig (vgl. § 32 GemO) und wegen des beschränk-

ten Wirkungskreises des Kollegialorgans in aller Regel keine Personen der relativen Zeitgeschichte. Auf ihre sachorientierte Arbeit kann es sich nachteilig auswirken, wenn Wortbeiträge vollständig in Bild und Ton im Internet live wiedergegeben und unter Umständen beliebig oft als Aufzeichnung abgerufen werden könnten. Es besteht dann die Gefahr, dass einzelne Gemeinderäte sich bei entsprechenden Übertragungen nicht mehr oder nicht mehr unbefangen zu Wort melden. Auch verfügen die Gemeinderäte nicht über Immunität oder Indemnität wie Parlamentarier. Das Recht der freien Meinungsäußerung steht ihnen „lediglich“ im Rahmen des Artikels 5 des Grundgesetzes zu. Teilweise wird deshalb die Auffassung vertreten, eine Internet-Übertragung von Gemeinderatssitzungen könne nicht auf eine ausdrückliche Einwilligung der Gremiumsmitglieder gestützt werden. Begründet wird dies unter anderem damit, der Entscheidungsdruck auf einzelne Gemeinderäte könne unter Umständen so groß sein, dass von einer freiwilligen Einwilligung nicht mehr die Rede sein könne. Ich halte diese Auffassung für zu eng. Allerdings sind alle Gemeinderatsmitglieder im Vorfeld über die damit verbundenen Folgen für das informationelle Selbstbestimmungsrecht umfassend schriftlich zu informieren.

– Mitarbeiter der Gemeindeverwaltung, externe Gutachter, Sachverständige, Berater etc.:

  Anders verhält es sich nach meiner Auffassung hingegen bei Mitarbeitern der Gemeindeverwaltung. Im Hinblick auf das besondere Verhältnis zum Arbeitgeber beziehungsweise Dienstherrn kann nicht ohne Weiteres davon ausgegangen werden, dass eine Entscheidung, ob eine Einwilligung erteilt werden soll, frei von jeglichem (zumindest subjektiv empfundenem) Zwang erfolgen kann. Soweit es sich – insbesondere bei größeren Stadtverwaltungen – um besonders hervorgehobene Führungskräfte handelt, wie beispielsweise Beigeordnete, ist eine Einwilligungslösung nach meinem Empfinden hinnehmbar. Beim übrigen Personal ist mangels Einwilligungsmöglichkeit zu gewährleisten, dass im Zusammenhang mit Internet-Übertragungen keine personenbezogenen Daten verarbeitet werden. Dies gilt entsprechend für nicht der Verwaltung angehörende Personen, die in einer Gemeinderatssitzung zum Beispiel als externe Gutachter, Sachverständige oder Berater auftreten. Auch hier wird aufgrund des bestehenden oder angestrebten Vertragsverhältnisses nicht ohne Weiteres eine wirkliche Entscheidungsfreiheit hinsichtlich des Auftritts vor dem Gemeinderat und der Übertragung dieses Vorgangs ins Internet anzunehmen sein.

– Saalöffentlichkeit:

  Aus Sicht des Datenschutzes ist es aufgrund der erheblichen Eingriffstiefe in das informationelle Selbstbestimmungsrecht des Einzelnen problematisch, wenn bei Internet-Übertragungen die sog. Saalöffentlichkeit aufgenommen wird. Es kann hier nicht ausgeschlossen werden, dass der subjektiv empfundene Druck, in die Verarbeitung von personenbezogenen Daten einzuwilligen, zu groß wird, als dass eine wirklich freie Entscheidung getroffen werden kann. Es besteht vielmehr die Gefahr, dass Einzelne – entgegen ihrer eigentlichen Auffassung – nicht von ihrem Recht Gebrauch machen, eine Einwilligung abzulehnen, beziehungsweise erst gar nicht zur Sitzung erscheinen, um sich dieser (Ablehnungs-)Situation nicht aussetzen zu müssen. Eine Einwilligungslösung ist deshalb selbst bei „passiv“ Anwesenden aus meiner Sicht nicht darstellbar. Im besonderen Maße gilt dies jedoch dann, wenn Bürger sich aktiv an einer Gemeinderatssitzung, zum Beispiel im Rahmen

einer sog. Fragestunde, beteiligen möchten. Im Ergebnis sollten bei Aufnahmen über Gemeinderatssitzungen daher der Zuschauerbereich ausgeblendet oder allenfalls so aufgenommen werden, dass einzelne Personen nicht zu erkennen sind.

– Sonstige Betroffene (Nicht-Anwesende):

  Eine Schwierigkeit stellt auch dar, dass bei Internet-Übertragungen nicht ausgeschlossen werden kann, dass personenbezogene Daten von nicht anwesenden Dritten zur Sprache kommen, beispielsweise durch Ausführungen eines Mitglieds des Gemeinderats oder durch Beiträge von frageberechtigten Bürgern. Die Gemeinde müsste bei Live-Übertragungen insofern gewährleisten, dass diese gegebenenfalls umgehend unterbrochen und bei Aufzeichnungen die entsprechenden Passagen herausgeschnitten werden.

Soweit Einwilligungen möglich sind, sind bei einer Übertragung von Gemeinderatssitzungen im Internet aus meiner Sicht zumindest noch folgende Punkte zu beachten:

– Live-Übertragungen sind sofort zu unterbrechen oder beenden, wenn dies aus datenschutzrechtlichen Gründen erforderlich ist. Dies kann beispielsweise unter anderem dadurch erreicht werden, dass die Sitzungen nicht unmittelbar, sondern mit wenigen Minuten Zeitverzögerung übertragen werden.

– Alle Teilnehmer einer Sitzung (nicht nur die Mitglieder des Gemeinderates) sind vorher, umfassend und ausdrücklich über die Art und den Umfang von Bild- und Tonaufzeichnungen und deren Abrufbarkeit im Internet (einschließlich Löschfristen) zu informieren. Das umfasst auch die Möglichkeit, dass Dritte die im Internet abrufbaren Aufzeichnungen, auch wenn das technisch erschwert ist, kopieren und speichern sowie – ungeachtet der Löschfristen – zum Abruf im Internet zur Verfügung stellen oder in sonstiger Weise verarbeiten können.

– Jeder Gemeinderat hat im Vorfeld seine ausdrückliche Einwilligung zu einer Internet-Übertragung schriftlich zu erklären. Soweit ein Gemeinderatsmitglied nicht einwilligt, erfolgt keine Internet-Übertragung („Vetorecht“).

– Mitarbeiter der Gemeindeverwaltung, die eine besonders herausgehobene Position haben, müssen im Vorfeld ihre ausdrückliche Einwilligung in eine Internet-Übertragung schriftlich erteilen. Dabei darf keinerlei Druck auf sie ausgeübt werden. Vielmehr ist darauf hinzuweisen, dass die Einwilligung freiwillig und eine Nichteinwilligung mit keinerlei Nachteilen verbunden ist. Bei anderen Mitarbeitern kommt eine Einwilligung nicht in Betracht.

– Eine erteilte Einwilligung ist jederzeit ohne Angabe von Gründen (bei Aufzeichnungen auch nachträglich) widerruflich. Die Betroffenen sind entsprechend zu unterrichten.

– Soweit Betroffene nachträglich ihre bereits erteilte Einwilligung zurückziehen, sind (leicht zeitversetzte) Übertragungen sofort zu unterbrechen oder zu beenden. Bei Aufzeichnung sind die entsprechenden Passagen umgehend zu löschen.

– Die Kamera und das Mikrophon sind so auszurichten, dass nach Möglichkeit nur der jeweilige Redner aufgenommen wird. Es ist zu gewährleisten, dass dabei Personen, die nicht ausdrücklich in die Datenverarbeitung eingewilligt haben (zum Beispiel weil dies mangels echter Entscheidungsfreiheit nicht möglich ist), nicht aufgenommen werden können (weder durch Bild noch durch Ton).

– Die Bereitstellung von Aufzeichnungen sollte derart erfolgen, dass Internet-Nutzern nicht ohne Weiteres die Anfertigung einer Kopie ermöglicht wird.

– Eingestellte Aufzeichnungen sind spätestens nach der nächsten Gemeinderatssitzung aus dem Internet zu entfernen.

1.3.2 Die Veröffentlichung von Alters- und Ehejubiläen im Internet

Bei Internetveröffentlichungen reicht es nicht aus, wenn eine entsprechende Rechtsvorschrift allgemein eine Veröffentlichung erlaubt, sie muss sich vielmehr auch ausdrücklich auf diese besondere Veröffentlichungsform „Internet“ beziehen. Als Beispiel kann hier auf § 34 Absatz 2 des Meldegesetzes (MG) verwiesen werden. Zwar regelt diese Vorschrift die Befugnis der Meldebehörde, Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums von Alters- und Ehejubilaren zu veröffentlichen und an Presse und Rundfunk zum Zwecke der Veröffentlichung zu übermitteln, jedoch bezieht sich die Erlaubnis zur Veröffentlichung nach § 34 Absatz 2 MG nicht explizit auf Veröffentlichungen im Internet. Im Ergebnis dürfen deshalb, wenn die entsprechenden Voraussetzungen erfüllt sind, Alters- und Ehejubilare im kommunalen Amtsblatt in Papierform, jedoch nicht elektronisch im Internet veröffentlicht werden. Dies scheint allerdings nicht allen Kommunen geläufig zu sein, da ich immer wieder Eingaben von Betroffenen erhalte, deren Alters- und Ehejubiläen ohne Einwilligung im Internet veröffentlicht wurden.

So hatte sich eine Petentin an mich gewandt, da ihr ein ehemaliger Kollege, der in Australien lebt, zum Geburtstag gratulierte und diesem auch ihre neue Adresse bekannt war. Die entsprechenden Informationen hatte der Gratulant dem Internet entnommen. Die Petentin war hierüber sehr besorgt, weil sie ihre frühere Wohnung wegen polizeibekannter Vorgänge aufgeben musste und unter Geheimhaltung ihrer neuen Adresse umgezogen sei. Selbst in ihrem Bekanntenkreis habe niemand die neue Adresse gekannt, sie sei lediglich unter ihrer E-Mail-Adresse erreichbar gewesen. Auch sei bereits vor dem Umzug ihre Adresse und Telefonnummer aufgrund ihrer früheren beruflichen Tätigkeit nur sehr wenigen Personen bekannt gewesen. Der Gratulant aus Australien konnte nun ganz einfach und bequem die entsprechenden Informationen dem Internet-Auftritt der Wohnortgemeinde der Petentin entnehmen, die die Adressdaten der Petentin anlässlich eines Alterjubiläums ohne deren Kenntnis und Einwilligung sowie ohne Rechtsgrundlage veröffentlicht hatte. Und bis die Gemeinde aufgrund meiner Hinweise die entsprechenden Adressdaten aus ihrem Internet-Angebot herausgenommen hat, waren die Daten weltweit abrufbar. Leider kann man nicht davon ausgehen, dass jeder, der die Möglichkeit hat, Adressdaten (und damit unter Umständen auch noch weitere personenbezogene Daten) über das Internet in Erfahrung zu bringen, ein harmloser Geburtstagsgratulant ist.

1.3.3 Die Einstellung von Fotos in das Internet

Es kommt häufig vor, dass Gemeinden ihr Amtsblatt auch in das Internet einstellen. Oft enthalten auf diese Weise eingestellte Ausgaben der Amtsblätter personenbezogene Daten in Form von Fotos. Fotos (oder Videos), auf denen eindeutig Personen zu erkennen sind, haben einen Personenbezug. Dies scheint sich im kommunalen Bereich, wie verschiedene Eingaben zeigen, immer noch nicht überall herum gesprochen zu haben. Wenn eine Gemeinde als datenschutzrechtlich verantwortliche Stelle personenbezogene Daten, zum Beispiel in Form eines Fotos, in ihrem Amtsblatt veröffentlicht, benötigt sie auch hierfür entweder eine wirksame Einwilligung des Betroffenen oder es muss eine Rechtsvorschrift geben, die ihr konkret diese Form der Datenver-

arbeitung erlaubt. Dies gilt übrigens unabhängig davon, ob die Veröffentlichung ausschließlich in Papierform oder auch elektronisch im Internet erfolgt. Jedoch ist die Gefahr von Missbrauch bei Internet-Veröffentlichungen wesentlich höher.

In einem Fall wandte sich eine Petentin an mich und teilte mir mit, dass ihre Wohnortgemeinde das Amtsblatt auch in das Internet einstelle. Im Internet könnten alle Ausgaben des Amtsblattes ab dem Jahr 2002 eingesehen werden. Durch die Einstellung des Amtblattes in das Internet seien auch von ihr Daten mit Personbezug, teilweise in Form von Bildern, ohne ihre Einwilligung veröffentlicht worden. Die Gemeinde hatte sich laut Mitteilung der Petentin zunächst auf den Standpunkt gestellt, die Betroffenen müssten einer Internet-Veröffentlichung im Voraus widersprechen. Dies habe sie nicht getan, die entsprechenden Daten würden deshalb nicht gelöscht werden. Selbstverständlich irrte sich die Gemeinde hier gewaltig. Für eine entsprechende Datenverarbeitung gibt es keine Rechtsgrundlage, eine Einwilligung der Petentin lag nicht vor, die Internet-Veröffentlichung war somit schlichtweg rechtswidrig.

Ein Beweggrund der Petentin, sich an mich zu wenden, war, dass sie in der Vergangenheit von einem sog. Stalker verfolgt wurde und nun befürchtete, dass dieser durch entsprechende Veröffentlichungen im Internet angeregt werden könnte, wieder Kontakt zu ihr aufzunehmen. Ich kann solche Befürchtungen durchaus nachvollziehen. Nachdem ich der Gemeinde mitteilte, wie Veröffentlichungen im Internet datenschutzrechtlich zu bewerten sind, hat diese von sich aus alle Ausgaben des Amtsblattes aus ihrem Internet-Auftritt entfernt.

1.3.4 Videoaufnahmen von Kindergartenkindern im Internet

In einem anderen Fall war ein Vater erstaunt, als er beim Surfen im Internet Videoaufnahmen seines Kindes fand, aufgenommen im Kindergarten. Wie kam es dazu? Die Gemeinde hatte es einem Unternehmer ermöglicht, Aufnahmen aus einem kommunalen Kindergarten in einen sog. Image-Film über die Gemeinde einzuarbeiten. Die abgebildeten Kinder waren auf den Videoaufnahmen gut erkennbar. Der Image-Film, unter anderem mit Sequenzen aus dem Kindergarten, wurde in das Internet eingestellt. Mangels Rechtsgrundlage kann sich die Zulässigkeit der Veröffentlichung von Filmsequenzen im Internet nur aus der Einwilligung der Betroffenen ergeben. Für Kindergartenkinder ist eine solche Einwilligung von den Erziehungsberechtigten abzugeben. Zwar hatte die Gemeinde die Eltern eine Art von Einwilligungserklärung unterschreiben lassen. Die von der Gemeinde vorgelegten Einwilligungsvordrucke genügten dem datenschutzrechtlichen Bestimmtheitserfordernis jedoch in keiner Weise, da sie sich nur ganz allgemein auf Veröffentlichungen von Aufnahmen im Kindergarten selber und in der Presse bezogen. Dass auch Internet-Veröffentlichungen vorgesehen und diese mit besonderen Risiken verbunden sind, wurde nicht angesprochen. Es fehlten außerdem Hinweise auf die Freiwilligkeit sowie auf die Widerrufsmöglichkeit. Da die Gemeinde nicht von sich aus Abhilfe schaffte, waren eine förmliche Beanstandung und die Unterrichtung der Aufsichtsbehörde die unvermeidliche Folge.

Kleine Prüfliste für die Veröffentlichung von personenbezogenen Daten im Internet:

1. *Ist eine Veröffentlichung ohne Personenbezug möglich (reine Sachinformation)?*
2. *Sind alle personenbezogenen Angaben erforderlich oder können einzelne weggelassen werden?*
3. *Gibt es eine Rechtsgrundlange, die eine Veröffentlichung im Internet erlaubt?*

4. Liegt eine wirksame Einwilligung des Betroffenen für eine Veröffentlichung im Internet vor?

5. Wann können/müssen die personenbezogenen Daten wieder gelöscht werden?

1.4 Das neue Bundesmeldegesetz kommt – ohne zentrales Bundesmelderegister

Im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 26) hatte ich auf einen Referentenentwurf des Bundesinnenministeriums für ein Bundesmeldegesetz hingewiesen, der die Einrichtung eines zentralen Bundesmelderegisters auf Bundesebene vorsah. Die Verwirklichung dieser Pläne hätte zur Folge gehabt, dass die Einwohnerdaten künftig auf zwei oder gar drei Ebenen parallel gespeichert werden, nämlich bei den originär zuständigen Meldebehörden (Gemeinden), beim Bund und zusätzlich noch (wie zum Teil schon bisher) auf Landesebene.

Hiergegen waren von Seiten der Datenschutzbeauftragten des Bundes und der Länder massive rechtliche Bedenken vorgetragen worden. So bestanden erhebliche Zweifel hinsichtlich der Notwendigkeit und der verfassungsrechtlichen Zulässigkeit eines inhaltlich umfänglichen, zentralen Bundesmelderegisters, da es nach der ständigen Rechtsprechung des Bundesverfassungsgerichts keine Datenspeicherung auf Vorrat für unbestimmte Zwecke geben darf und die Ziele, die als Begründung für ein zentrales Bundesmelderegister genannt worden waren, möglicherweise auch durch eine Vernetzung vorhandener Melderegister erreicht werden können.

Der genannte Referentenentwurf des Bundesinnenministeriums hatte in der 16. Wahlperiode des Deutschen Bundestags keine Gesetzesreife mehr erlangt. Meine im 29. Tätigkeitsbericht zum Ausdruck gebrachte Hoffnung, dass in nachfolgenden Entwürfen eine datenschutzfreundlichere Lösung gefunden wird, hat sich erfüllt.

In dem am 31. August 2011 vom Bundeskabinett beschlossenen und dem Bundesrat zugeleiteten Entwurf für ein Bundesmeldegesetz (Gesetz zur Fortentwicklung des Meldewesens, BR-Drucksache 524/11) wird auf die Einrichtung eines zentralen Bundesmelderegisters verzichtet. Der Bundesrat hat den Entwurf im Wesentlichen befürwortet. Bis zum Inkrafttreten werden aber noch einige Jahre ins Land gehen.

1.5 Meldewesen – Fehler im Meldeverfahren MeldIT

„Mit MeldIT steht für Behörden und Polizei, Bürger und Wirtschaft ein hochmoderner Auskunftsservice über Meldedaten zur Verfügung. Hierbei handelt es sich um eine serviceorientierte Lösung, basierend auf Internet-Technologie und einer selbsterklärenden Web-Oberfläche.“ So lautet die Werbebotschaft der Datenzentrale Baden-Württemberg für das bei den Meldebehörden und anderen Dienststellen weitverbreitete Verfahren MeldIT. Im Berichtszeitraum haben wir aufgrund mehrerer Einzelfälle erfahren müssen, dass das Verfahren nicht ganz fehlerfrei funktioniert:

Fall 1: Das unbekannte, nichteheliche Kind

Welche Überraschungen ein Verfahren wie MeldIT bieten kann, musste die kinderlose Ehefrau eines Bürgers zweimal kurz hintereinander erleben. Denn sie wurde Ende 2010 und Anfang 2011 damit konfrontiert, dass ein nichteheliches Kind des Ehemanns existierte. Das Melderecht sieht grundsätzlich vor, dass dieses Kind beim Vater gespeichert wird. Aber das Melderecht enthält auch weitere Regelungen – zum Beispiel für Zwecke der Steuererhebung oder der Rentenzahlung – und bei deren Umsetzung in das elektronische Verfahren MeldIT kamen die Persönlichkeitsrechte des Vaters, aber auch die des Kindes und seiner Mutter zu kurz. Zwar stellt die Vielzahl höchst unterschiedlicher Behördenbedürfnisse unstreitig erhöhte Anforderungen an die Software und deren Entwickler. Dennoch müssen diese bzw. deren Auftraggeber präzise

festlegen, wer welche Daten über wen benötigt. Das musste ich der betroffenen Großstadt als datenschutzrechtlich verantwortlicher Stelle in den beiden erwähnten Vorgängen ins Stammbuch schreiben.

Wie kam es nun zu den überraschenden Erkenntnissen der Ehefrau? Ausgangspunkt war die Erfassung des nichtehelichen Kindes auch in dem entsprechenden Datensatz der Ehefrau, die eben nicht die Mutter dieses Kindes ist. Grund dafür ist das Steuerrecht. Damit auf den seinerzeit noch üblichen Lohnsteuerkarten ggf. die Berücksichtigung eines Kindes vermerkt werden konnte, war dieses in dem Meldedatensatz der Ehefrau zu vermerken. D. h. bei einer Lohnsteuerkarte hätte die Ehefrau, wenn für den Ehemann keine erstellt werden müsste, in der entsprechenden Rubrik den Hinweis auf ein zu berücksichtigendes Kind finden müssen. Im November 2009 trat eine Gesetzesänderung in Kraft, nach der auch Kindererziehungszeiten bei einem Ehegatten im Rahmen der Rentenversicherung berücksichtigt werden können. Und damit begannen die Probleme im Meldeprogramm, denn die Ehefrau wurde von der Deutschen Rentenversicherung über die mit dem Gesetz verbundenen Vorteile für die Anerkennungszeiten wegen der Kindererziehung informiert. Ursächlich war das Meldeprogramm, das diese steuerrechtlich zulässige Information auch für diesen anderen Zweck verwendete. Dafür war aber im Melderecht keine gesetzliche Stütze zu finden. Diese unerfreuliche Begleiterscheinung wurde nach den Angaben der Stadt bis Ende Januar 2010 beseitigt.

Allerdings stellte das Programm auch an einer anderen Stelle die Information über das Kind des Ehemannes zur Verfügung. Als die Ehefrau in einer Februarnacht 2010 in eine Verkehrskontrolle geriet und sich nicht ausweisen konnte, bedienten sich die Polizeibeamten des Meldeportals und stellten der Betroffenen auch die Frage nach dem Namen ihres Kindes, woraufhin die überraschte Ehefrau erklärte, sie habe kein Kind. Immerhin verzichteten dann die Polizeibeamten reaktionsschnell auf weitere Fragen. Festzuhalten ist, dass es keine Rechtsgrundlage gab, das steuerrechtlich relevante Merkmal (nichteheliches Kind des Ehemannes) online der Polizei beim Meldedatenabruf zur Verfügung zu stellen. Damit war das von der Stadt eingesetzte Meldeprogramm auch insoweit datenschutzrechtlich fehlerbehaftet, was ich mit Nachdruck beanstandete, da ich den Eindruck gewinnen musste, dass sich die Verantwortlichen für den Einsatz dieses Programms auf den Softwareentwickler ohne eine eigene gründliche Prüfung verlassen hatten.

Parallel zu dem Schriftverkehr mit der Stadt hatte ich das Innenministerium als Aufsichtsbehörde des Softwareentwicklers auf die Programmlücken hingewiesen. Dieses ließ mich dann wenige Monate später wissen, dass der Programmfehler in der Bereitstellung der Information über nichteheliche Kinder eines Ehegatten im Meldedatensatz des anderen Ehegatten beseitigt worden sei.

Ich hoffe, dass sich jede verantwortliche Stelle bewusst ist, dass sie ihre Verantwortung für die Verarbeitung personenbezogener Daten nicht abgeben kann. Auch die Auswahl eines noch so erfahrenen Softwareentwicklers entbindet nicht von der Verpflichtung, ein Programm zur automatisierten Verarbeitung solcher Daten einer Vorabkontrolle zu unterziehen.

Fälle 2 und 3: Falsche Auskünfte durch MeldIT

Auch in zwei weiteren Fällen taten sich Probleme bei der Verarbeitung personenbezogener Daten aufgrund des Verfahrens MeldIT auf. In einem Fall erklärte ein Petent, dass Auskünfte aus MeldIT über ihn erteilt würden, die unrichtig seien. Im zweiten Fall teilte eine Petentin mit, dass gegen sie zwei Vollstreckungsankündigungen erlassen wurden, obwohl sie nicht die Person sei, gegenüber der die Ankündigungen hätten abgegeben werden müssen. Ihre fälschlicherweise mitgeteilte Adresse sei das Ergebnis einer Behördenanfrage an MeldIT gewesen. Kurze Zeit später legte mir die Petentin einen Schriftwechsel vor, wonach ein Energiekonzern über ein Rechtsanwaltsbüro ihr gegenüber fälschlicherweise eine Forderung erhob. Auch in diesem Fall hatte die

Kanzlei die Adressdaten über ein auf Adressauskünfte spezialisiertes Unternehmen erhalten, das die Daten vom Meldeportal MeldIT bezogen hatte. Glücklicherweise gelang es der Petentin, das Unternehmen beziehungsweise die Anwaltskanzlei davon zu überzeugen, dass eine Verwechslung vorlag.

Da es sich in beiden Fällen um Meldedaten aus dem Melderegister derselben Großstadt handelte, haben meine Mitarbeiter das städtische Melderegister kontrolliert, um die Fehlerquelle zu finden. Beim Zugriff auf das Melderegister, in dem über die Historie der Einträge gesucht werden kann, stellte sich heraus, dass der Petent nicht in der angegebenen Straße der Stadt gewohnt hat, wohl aber eine namensgleiche Person. Die Stelle, die eine Melderegisterauskunft zu dem Petenten aus MeldIT eingeholt hat, hatte mit dem Vor- und Familiennamen, Geburtsdatum und weiteren vier Kriterien gesucht, weshalb eine Verwechslung schon deshalb nicht hätte auftreten dürfen, weil die Geburtsdaten des Petenten und der gefundenen Person nicht identisch waren. Der strukturelle Fehler lag nun darin, dass das Verfahren offenbar nicht alle Kriterien abprüfte, sondern bereits einen „Treffer“ vermeldete, wenn einige Suchkriterien zutrafen, obwohl andere Merkmale voneinander abwichen.

Auch hinsichtlich der Petentin ergab sich ein überraschender Befund. Bei der Suche mit den eingegebenen Kriterien war festzustellen, dass eine „fast“ namensgleiche Person zwar in der gleichen Straße, aber unter einer anderen Hausnummer gemeldet war. Der Unterschied der Namen bestand darin, dass die Petentin zwei Rufnamen hat, wovon einer mit dem Rufnamen der gesuchten Person identisch ist. Anscheinend wurde bei der Suche in MeldIT über die angegebenen Suchkriterien variiert, indem Kriterien weggelassen und umgestaltet wurden.

In § 29 a Absatz 3 des Meldegesetzes wird die einfache Behördenauskunft aus dem Meldeportal MeldIT geregelt. Für eine Suche in MeldIT müssen neben Vor- und Familiennamen sowie früheren, gegenwärtigen oder künftigen Anschriften des Betroffenen so viele Kriterien angegeben werden, dass die Identität des Betroffenen durch einen automatisierten Abgleich der im Auskunftsantrag angegebenen Daten mit den im Datenbestand von MeldIT gespeicherten Daten eindeutig festgestellt werden kann. Zwar wird dort nicht geregelt, wie zu verfahren ist, wenn mehr Suchkriterien angegeben werden, als für eine eindeutige Feststellung notwendig sind, aber deshalb überzählige Kriterien bei der Suche wegzulassen, wenn bei deren Einbeziehung kein Treffer gefunden werden kann, halte ich insbesondere bei dem wichtigen Kriterium Geburtsdatum für ungeeignet. Ebenso ungeeignet ist die Ergänzung um weitere Rufnamen unter gleichzeitiger Nichtbeachtung der Hausnummer der Anschrift im Auskunftsantrag. Mein Fazit lautete daher: Die Suche im Meldeportal MeldIT lieferte falsche Ergebnisse. Ich habe der Stadt deshalb aufgegeben, beim Betreiber des Meldeportals eine Korrektur der Suchmethode zu veranlassen und mir das Ergebnis mitzuteilen.

Diese Fälle zeigen erneut auf, welche unwägbaren Risiken bei einer zentralen Datenhaltung von Einwohnermeldedaten auftreten können. Nicht ohne Grund treffen zentrale Datenspeicherungen bei den Datenschutzbeauftragten des Bundes und der Länder regelmäßig auf Bedenken. Zu groß ist die Gefahr, dass es bei zentraler Verarbeitung zu Verwechslungen kommt, die bei dezentraler Verarbeitung wesentlich unwahrscheinlicher oder ausgeschlossen sind.

1.6 Der neue elektronische Personalausweis – Kontrollbesuch bei drei Kommunen

Seit dem 1. November 2010 ist der neue elektronische Personalausweis im Scheckkartenformat eingeführt. Wie bereits im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 26 f.) dargestellt, bietet er über die klassische Ausweisfunktion hinaus verschiedene Zusatzfunktionen. So kann er als elektronischer Identitätsnachweis im Internet gegenüber Behörden, aber auch für Rechtsgeschäfte mit der Privatwirtschaft eingesetzt werden. Diese Funktion, die bei über 16-Jährigen bei Ausgabe aktiviert ist, kann auf Wunsch von der Personalausweisbehörde jeder-

zeit deaktiviert und bei Bedarf wieder aktiviert werden. Nach Angaben des Bundesinnenministeriums ist die Funktion bei einem Drittel der bislang ausgegebenen neuen Personalausweise eingeschaltet.

Darüber hinaus erfolgt – erfreulicherweise auf freiwilliger Basis – eine elektronische Speicherung der Fingerabdrücke. Auslesbar sind diese Fingerabdrücke ausschließlich für bestimmte hoheitliche Stellen, die mit speziell zertifizierten Lesegeräten ausgestattet sind, wie zum Beispiel die Polizei, die Zollverwaltung oder die Pass- und Personalausweisbehörden.

Schließlich kann eine qualifizierte elektronische Signatur auf dem neuen Personalausweis aufgebracht werden. Der Ausweisinhaber kann damit Dokumente, zum Beispiel Verträge, rechtsverbindlich „unterschreiben“. Die qualifizierte elektronische Signatur muss bei einem privaten Anbieter beantragt und kann von diesem auf den Chip des Ausweises geladen werden. Das Aufspielen der Signatur und ihre Nutzung sind aber kostenpflichtig. Diese Zusatzfunktion ist dem Vernehmen nach bislang nur selten akzeptiert worden. Das mag mit gewissen Vorbehalten der Nutzer zusammenhängen, denn nach Umfragen des Branchenverbands BITKOM steht die Mehrheit der Bevölkerung dem neuen Personalausweis ablehnend oder unsicher gegenüber. Offenbar hat die anfängliche Diskussion von unsicheren Basislesegeräten Spuren hinterlassen. Kein Wunder, dass Branchenvertreter Politik und Wirtschaft immer wieder auffordern, weiter aktiv um Vertrauen in die neue Karte zu werben.

Aufgrund der neuen Funktionen des elektronischen Personalausweises enthält das Personalausweisgesetz umfangreiche Informationspflichten, die es den Bürgern ermöglichen sollen, in Kenntnis der Sach- und Rechtslage über die Nutzung der optionalen Funktionen des neuen Personalausweises und den damit verbundenen Datenverarbeitungsvorgängen entscheiden zu können.

Bereits vor Einführung des neuen Personalausweises am 1. November 2010 und auch in den Wochen danach häuften sich die Meldungen über Pannen. Berichte über fehlerhafte Software, defekte Terminals und lange Wartezeiten für die Bürger machten die Runde. Um uns selbst ein Bild machen zu können, führten Mitarbeiter meiner Dienststelle bereits im November 2010, also kurz nach Einführung des neuen Personalausweises, bei Personalausweisbehörden verschiedener Gemeinden unangemeldete Kontrollbesuche durch. Meine Mitarbeiter hatten dabei Gelegenheit, sich in Gesprächen mit Beschäftigten der Personalausweisbehörden, aber auch durch die Möglichkeit, Antragstellungen – mit Einverständnis der jeweiligen Antragsteller – „live“ zu verfolgen, ein Bild über die Verarbeitung personenbezogener Daten, die EDV-gestützten Abläufe sowie über die Handhabung der Informationspflichten bezüglich der neuen Funktionen des Personalausweises zu machen.

Positiv aufgefallen ist dabei, dass die Beschäftigten der Personalausweisbehörden sowohl über die Abläufe im Antrags- und Ausgabeverfahren als auch über die neuen Funktionen des Personalausweises gut informiert waren und die zum Schutz des informationellen Selbstbestimmungsrechts bestehenden Informationspflichten gegenüber den Antragstellern erfüllen konnten.

1.7 Bewerbungen für den Migrationsbeirat

Dürfen Gemeinderatsmitglieder Bewerberdaten, von denen sie aufgrund ihrer Tätigkeit im Gemeinderat Kenntnis erlangt haben, für die Fraktionsarbeit nutzen?

Der Gemeinderat einer Stadt hatte beschlossen, einen neuen Migrationsbeirat zu bestellen. Hierzu wurde eine Kommission gebildet, der unter anderem je ein Vertreter der vier Fraktionen des amtierenden Gemeinderats angehörte. Den Mitgliedern dieser Kommission wurden alle Bewerbungen – inklusive Lebensläufe und Anschriften – ausgehändigt. Die stellvertretende Vorsitzende einer Gemeinderatsfraktion, die als Vertreterin ihrer Fraktion Mitglied der Berufungskommission war,

nutzte diese Daten, um in ihrer Funktion als stellvertretende Fraktionsvorsitzende alle Bewerber zu einem Umtrunk einzuladen, um so das ehrenamtliche Engagement dieser Personen zu würdigen.

Die Einladung sämtlicher Bewerber für die Mitgliedschaft im Migrationsbeirat durch die stellvertretende Fraktionsvorsitzende, die diese Bewerberdaten als gemeinderätliches Mitglied der Berufungskommission erhalten hatte, stellt eine Verarbeitung personenbezogener Daten durch eine öffentliche Stelle dar, nämlich ein Nutzen personenbezogener Daten nach § 3 Absatz 2 Sätze 1 und 2 Nr. 5 LDSG. Nach § 4 Absatz 1 LDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat.

Eine Rechtsvorschrift, auf die die Datennutzung hätte gestützt werden können, existiert nicht. Auch entsprechende Einwilligungen der betroffenen Bewerber lagen nicht vor.

Die Nutzung der Bewerberdaten durch ein Gemeinderatsmitglied für die Fraktionsarbeit stellt daher einen Datenschutzverstoß dar. Hieran ändert auch der Umstand nichts, dass ehrenamtliches Engagement Anerkennung verdient und die Nutzung der Daten in bester Absicht erfolgte.

1.8 Auskünfte aus Bauakten an Dritte

1.8.1 Grundlegendes

Dritte begehren, wie sich im Rahmen meiner Tätigkeit immer wieder zeigt, häufig Auskünfte aus Bauakten. Dies können beispielsweise Architekten sein, die Ansichten und Schnitte eines Gebäudes anfordern, weil sie ein Nachbargrundstück beplanen, oder Mieter, die im Zusammenhang mit einem Rechtsstreit über eine Mieterhöhung die exakte Wohnfläche wissen wollen. Der folgende Beitrag gibt einen Überblick über die rechtlichen Voraussetzungen, unter denen eine Baurechtsbehörde Dritten Auskünfte aus einer Bauakte erteilen darf.

Zunächst hat das Baurechtsamt zu prüfen, ob es sich bei den Unterlagen oder Auskünften aus der Bauakte, auf die sich der Antrag des Dritten bezieht, um personenbezogene Daten handelt. Nur dann fällt die Angelegenheit in den Anwendungsbereich des Landesdatenschutzgesetzes. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 3 Absatz 1 LDSG). Da diese gesetzliche Definition auch Angaben über sachliche Verhältnisse einbezieht, betrachtet meine Dienststelle regelmäßig auch Informationen über die baulichen Verhältnisse eines Objekts, das sich einer natürlichen Person (z. B. dem Grundstückseigentümer) zuordnen lässt, als personenbezogen.

Die Weitergabe von Unterlagen oder Auskünften mit Personenbezug an Dritte unterliegt datenschutzrechtlichen Einschränkungen. Soweit der Betroffene nicht in die Übermittlung eingewilligt hat, ist eine solche nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt. Findet sich, wie in den geschilderten Fällen, keine bereichsspezifische Regelung im Baurecht, so kommt eine Übermittlung nach § 18 LDSG in Betracht, wenn der Empfänger, an den die Daten übermittelt werden sollen, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Unter dem vom Gesetzgeber geforderten „berechtigten Interesse“ des Übermittlungsadressaten ist ein sich aus vernünftigen Erwägungen ergebendes, durch die Sachlage gerechtfertigtes Interesse zu verstehen, das auch wirtschaftlicher oder ideeller Art sein kann. Dieses Auskunftsinteresse ist gegenüber der Behörde darzulegen, und die dargelegten Tatsachen sind glaubhaft zu machen. Das Glaubhaftmachen ist eine einfachere Form des Be-

weises: Die Tatsachen brauchen nicht mit an Sicherheit grenzender Wahrscheinlichkeit festzustehen; vielmehr genügt es, dass die übermittelnde Stelle von ihrem Vorliegen mit überwiegender Wahrscheinlichkeit überzeugt wird[12].

Dieses berechtigte Empfängerinteresse ist mit den datenschutzrechtlichen Belangen des Betroffenen abzuwägen. Zu diesem Zweck gilt es zunächst festzustellen, welche schutzwürdigen Interessen des Betroffenen durch die Datenübermittlung beeinträchtigt würden. Dies muss das Baurechtsamt von Amts wegen und gegebenenfalls unter Einbeziehung des Betroffenen ermitteln. Die Intensität der Aufklärung richtet sich unter anderem danach, wie gravierend die Folgen einer Ablehnung für den Empfänger und die einer Übermittlung für den Betroffenen sind[13].

Soweit das Baurechtsamt nach Prüfung der genannten Voraussetzungen zu dem Schluss kommt, dass eine Übermittlung zulässig ist, knüpft das Gesetz an die Weitergabe der Daten noch bestimmte Folgepflichten, die von der übermittelnden Stelle zu beachten sind. So ist der Betroffene von der Übermittlung seiner Daten zu unterrichten, soweit nicht eine Ausnahme des § 18 Absatz 3 Satz 2 LDSG greift. Außerdem hat die übermittelnde Stelle den Empfänger der Daten darauf hinzuweisen, dass er die Daten nur zu dem Zweck verarbeiten darf, zu dessen Erfüllung sie ihm übermittelt worden sind. Schlussendlich hat das Baurechtsamt zu prüfen, ob Auflagen oder Vereinbarungen mit dem Dritten zur Sicherstellung des Datenschutzes erforderlich sind.

1.8.2 Datenübermittlung an einen Mieter

In einem von meiner Dienststelle zu prüfenden Fall hatte ein Mieter beim städtischen Bauamt seines Wohnorts nachgefragt, ob ein an seine Mietwohnung angrenzender Raum zur Wohnung gehöre oder nicht. Hintergrund der Anfrage war, dass die Vermieterin diese Fläche in die Berechnung der Miete einbeziehen wollte.

Das Bauamt hat dem Mieter daraufhin Einsichtnahme in den Grundrissplan des von ihm bewohnten Dachgeschosses gewährt und eine Kopie der Wohnflächenberechnung ausgehändigt. Diese Kopie enthielt allerdings nicht nur eine Berechnung der Wohnfläche des von dem Mieter gemieteten Dachgeschosses, sondern auch eine Berechnung der Wohnflächen im Erdgeschoss und im 1. Obergeschoss. Schwärzungen wurden auf der Kopie nicht vorgenommen.

Eine Weitergabe der Kopie der gesamten Wohnflächenberechnung war aus folgendem Grund nicht zulässig: Bei der Prüfung, ob dem Mieter vorliegend Auskünfte aus der Bauakte erteilt werden durften, hatte das Bauamt wie oben beschrieben vorzugehen. Bei der Wohnflächenberechnung handelt es sich um personenbezogene Daten der Vermieterin – die auch Eigentümerin des Mehrfamilienhauses war –, da es sich um Informationen über die baulichen Verhältnisse eines Objekts handelte, welches sich der Eigentümerin zuordnen ließ. Im Rahmen der Prüfung des § 18 LDSG hatte das Bauamt nicht beachtet, dass ein berechtigtes Interesse des Mieters an der Kenntnis der Wohnfläche der anderen Geschosse nicht dargelegt worden war und daher die Voraussetzungen des § 18 LDSG zumindest insoweit nicht vorlagen. Daher hätte eine Übermittlung der Wohnflächenberechnung bezüglich der anderen beiden Geschosse nicht erfolgen dürfen. Als geeignetes Mittel, um dem Auskunftsersuchen des Mieters Rechnung zu tragen und zugleich die personenbezogenen Daten der Vermiete-

[12] Dammann in Simitis, Kommentar zum Bundesdatenschutzgesetz, 7. Auflage § 16 Rn. 27.

[13] Dammann, a. a. O., § 16 Rn. 29.

rin zu schützen, wäre gegebenenfalls in Betracht gekommen, die den Mieter nicht betreffenden Passagen unkenntlich zu machen. Meine datenschutzrechtliche Bewertung habe ich der Stadt und der Vermieterin, die sich in der Angelegenheit an meine Dienststelle gewandt hatte, mitgeteilt.

Der Fall zeigt einmal mehr, dass viele Behörden für die Belange des Datenschutzes sensibilisiert werden müssen, um die von § 18 LDSG vorgegebene Abwägungssituation überhaupt zu erkennen. Nur dann lassen sich im Einzelfall korrekte und sachgerechte Lösungen finden.

1.9 Das Ende des Subventionsprangers – der EuGH hat ein Einsehen

Mit Urteil vom 9. November 2010 (C-92/09 und C-93/09) hat der Europäische Gerichtshof die Verordnungen (EG) Nr. 1290/2005 und 259/2008, durch welche die Mitgliedsstaaten verpflichtet worden waren, personenbezogene Daten von Agrarbeihilfenempfängern im Internet zu veröffentlichen, in Teilen für nichtig erklärt.

Im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500) hatte ich darüber berichtet, dass Landwirte, die finanzielle Beihilfen aus den großen europäischen Agrartöpfen EGFL und ELER beziehen, sich als Subventionsempfänger bis auf Weiteres damit abfinden müssten, dass ihr Name, ihr Wohnort und die Höhe der bezogenen Mittel auf der Website *www.agrar-fischerei-zahlungen.de* im Internet veröffentlicht werden. Da in Gestalt verschiedener europarechtlicher Verordnungen (auf nationaler Ebene umgesetzt durch das „Agrar- und Fischereifonds-Informationengesetz“ und einer dazugehörigen „Agrar- und Fischereifonds-Informationen-Verordnung“) eine eindeutige Rechtsgrundlage bestand, welche die Mitgliedsstaaten im Rahmen der sogenannten Transparenzinitiative zu dieser Maßnahme verpflichtete, waren mir weitgehend die Hände gebunden.

Anlass zu einiger Hoffnung, dass das letzte Wort in dieser Angelegenheit noch nicht gesprochen sein könnte, gab lediglich das Verwaltungsgericht Wiesbaden, das Zweifel an der Europarechtskonformität der Veröffentlichungspflicht hegte und sich deshalb an den Europäischen Gerichtshof gewandt hatte. Allerdings teilten die übrigen mit der Materie befassten deutschen Gerichte, darunter auch der Verwaltungsgerichtshof Baden-Württemberg, die Bedenken ihrer hessischen Kollegen keinesfalls; deswegen erschien der Ausgang des Verfahrens in Luxemburg zumindest ungewiss.

Fast wider Erwarten hat die Große Kammer des Europäischen Gerichtshofs mit Urteil vom 9. November 2010 das einschlägige EU-Verordnungsrecht (die grundlegende Verordnung Nr. 1290/2005 sowie die Ausführungs-Verordnung (EG) 259/2008) jedoch tatsächlich in Teilen für ungültig erklärt.

Zwar hat der Europäische Gerichtshof das grundsätzliche Anliegen Brüssels, die Verwendung der Mittel aus den Agrarfördertöpfen transparenter zu gestalten, an sich nicht in Frage gestellt. Unverhältnismäßig sei indes, so das Verdikt der Luxemburger Richter, die Maßgabe an die Mitgliedsstaaten, auch die personenbezogenen Daten natürlicher Personen zu veröffentlichen, ohne dabei nach einschlägigen Kriterien wie den Zeiträumen, während derer sie Beihilfen bezogen haben, der Häufigkeit oder auch Art und Umfang dieser Beihilfen zu differenzieren. In einer demokratischen Gesellschaft hätten die Steuerzahler zwar einen Anspruch darauf, über die Verwendung ihrer Steuergelder informiert zu werden; dieser müsse aber mit dem durch die Charta der Grundrechte der Europäischen Union gewährleisteten Recht der Empfänger auf Achtung ihres Privatlebens und dem Schutz ihrer personenbezogenen Informationen abgewogen werden, was hier versäumt worden sei.

Die Kommission hat unterdessen reagiert und die Verordnung (EG) Nr. 259/2008 entsprechend den Vorgaben des Europäischen Gerichtshofs geändert. Die Verpflichtung der Mitgliedsstaaten, Informationen über die Subventionsempfänger zu veröffentlichen, ist nur für juris-

tische Personen bestehen geblieben; Angaben zu natürlichen Personen sind hingegen nicht mehr ins Netz zu stellen.

Ein datenschutzrechtliches „Happy End“ also – mit einem Wermutstropfen: Denn die Luxemburger Richter haben auch entschieden, dass die bereits in das Netz gestellten Daten nachträglich nicht mehr gelöscht werden müssen. Dies sei nämlich in Anbetracht der „großen Zahl von Veröffentlichungen, die in den Mitgliedsstaaten auf der Grundlage von Rechtsvorschriften erfolgt sind“, nicht zumutbar.

Dennoch wird man die Bedeutung des Urteils des Europäischen Gerichtshofs nicht gering veranschlagen dürfen. Immerhin hat das Gericht dem europäischen Verordnungsgeber vor Augen geführt, dass auch er das Recht des Bürgers auf informationelle Selbstbestimmung nicht pauschal zugunsten anderer, vermeintlich vorrangiger politischer Ziele, wie vorliegend der Transparenz der Mittelvergabe, hintanstellen darf.

1.10 Personenbezug bei Webcams – wo fängt er an, wo hört er auf?

Der Einsatz von Webcams berührt immer wieder datenschutzrechtliche Grenzfragen. Im 29. Tätigkeitsbericht 2009 (LT-Drucksache 14/5500, S. 126) ging es zum Beispiel um Webcams an Autobahnen oder Lichtsignalanlagen. Diesmal kam eine anders gelagerte Beschwerde auf meinen Tisch. Ein Ehepaar, das in einer Großen Kreisstadt im südlichen Teil des Landes lebt, trug Folgendes vor: Im Anschluss an einen Fastnachtsumzug, von dem die Stadt Bilder einer von ihr betriebenen Webcam auf ihrem WWW-Server zum Abruf anbot, wurde die Kamera gegenüber dem von den Eheleuten bewohnten Gebäude nicht etwa von der Stadt stillgelegt und abgebaut, sondern weiter betrieben. Lediglich die Ausrichtung wurde verändert. Nicht mehr Narren, sondern eine Straßenbaustelle wurde fortan aufgenommen, um die Bürger über den Baufortschritt zu informieren und auf mögliche Stausituationen frühzeitig aufmerksam zu machen. Dazu stellte die Stadt jede Minute ein Bild der Kamera auf ihrem WWW-Server zum Abruf ein. Das Paar wies darauf hin, dass nicht nur die Baustelle, sondern auch die Fenster der von ihm bewohnten Wohnung auf den Aufnahmen zu sehen seien. Schon mehrfach sei in Gesprächen mit Verwandten und Bekannten geäußert worden, man habe an der Zimmerbeleuchtung gesehen, dass die Eheleute sich nicht in ihrer Wohnung aufhielten, oder dass ein angekündigter Urlaub doch nicht angetreten wurde, da die Zimmer beleuchtet waren. Spontane Telefonanrufe von Bekannten wurden damit erklärt, man habe eben im Internet gesehen, das Licht brenne und dies als günstige Gelegenheit zu einem kleinen Plausch gesehen.

Aus datenschutzrechtlicher Sicht ist dazu Folgendes zu bemerken:

Ob ein Datum personenbezogen ist, lässt sich nach § 3 Absatz 1 LDSG beurteilen. Danach sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Die eingeschaltete Zimmerbeleuchtung in unterschiedlichen Räumen als sachliche Verhältnisse aufzufassen, dürfte unstreitig sein. Aber ob dieses einer bestimmten Person zugeordnet werden kann, scheint fraglich. Wie viele Personen sich in einer Wohnung aufhalten, ergibt sich nicht aus der Beleuchtung, selbst wenn in mehreren Zimmern das Licht eingeschaltet ist. Ebenso kann nicht zweifelsfrei festgestellt werden, ob überhaupt jemand oder welche Person sich in der Wohnung aufhält. Vielleicht wurde vergessen, das Licht auszuschalten. Es gibt auch elektronische Geräte, die zur Vortäuschung der Abwesenheit das Licht ein- und ausschalten. Damit lässt sich das Geschehen nicht präzise einer Person zuordnen. So weit, die im Internet veröffentlichten Bilder im vorliegenden Fall als personenbezogenes Datum zu beurteilen, wollte ich daher nicht gehen. Gleichwohl sah ich in der Veröffentlichung der Bilder eine mögliche Beeinträchtigung, die aufgrund datenschutzrechtlicher Erwägungen zu beseitigen war. Deshalb bat ich die Eheleute, nachdem ich der Stadt meine Auffassung dargelegt hatte, sich mit der Stadt ins Benehmen zu setzen und gegebenenfalls auf zivilrechtliche Weise die Beeinträchtigung aus der Welt zu schaffen.

Nachzutragen ist, dass die Eingabe beschieden wurde, bevor in Deutschland Hausfassaden durch Kamerawagen erfasst und die Bilder im Internet zum Abruf bereitgestellt wurden. Wenn nunmehr das Abfahren deutscher Städte mit Kamerawagen in mehrjährigen Intervallen und die Veröffentlichung der dabei gewonnenen zeitlich punktuellen Abbildungen von Hausfassaden im Internet datenschutzrechtlich problematisiert wird, ergibt sich fast zwangsläufig die Frage, ob angesichts der hier dargestellten permanenten „Webcam-Überwachung" einer Hausfassade unter „nahezu" Echtzeitbedingungen die datenschutzrechtlichen Grenzen des Personenbezugs nicht neu zu definieren sind.

2. Steuerverwaltung

2.1 Datenschutzpanne beim elektronischen Lastschriftverfahren für die Kfz-Steuer

Beim elektronischen Einzug der Kraftfahrzeugsteuer hat es im Juni 2011 eine gravierende Datenschutzpanne gegeben, wovon besorgte Bürger nach einem Blick auf ihre Kontoauszüge umgehend mein Amt in Kenntnis setzten. Neben dem Namen des Steuerpflichtigen, dem Kfz-Kennzeichen und dem Betrag der gezahlten Kfz-Steuer wurden dort weitere Steuerdaten, unter anderem Steuernummern und Umsatzsteuern von anderen Bürgern und Unternehmen, sowie Angaben zur Religionszugehörigkeit der Betroffenen genannt und damit den Banken übermittelt. Tatsächlich stellte sich bei näherer Betrachtung heraus, dass Steuerdaten von Dritten – offenkundig ohne Rechtsgrundlage – unbeteiligten Bürgern zur Kenntnis gebracht wurden. Ich vermutete einen Softwarefehler als Ursache für die peinliche Panne.

Die sofort eingeschaltete Finanzverwaltung bestätigte dies rasch und brachte somit Licht in das Dunkel: Im Rahmen einer Aktualisierung der Zahlungsverkehrssoftware seien am 14. Juni 2011 neue Funktionalitäten zur Verfügung gestellt worden, die einen Softwarefehler in einem nicht von der Erweiterung betroffenen Bereich des Programms verursacht hätten. Der Fehler sei zuvor weder von der Herstellerfirma noch von der Landesoberkasse im Rahmen der durchgeführten Tests erkannt worden. Erst aufgrund von Rückmeldungen einzelner Steuerzahler über die Finanzämter beziehungsweise das Rechenzentrum der Finanzverwaltung sei der Fehler am Freitag, den 17. Juni 2011, bemerkt und die weitere Verarbeitung der Zahlungsverkehrsdaten umgehend gestoppt worden. Der Softwarehersteller habe drei Tage später ein bereinigtes Programm zur Verfügung gestellt, das nach erfolgreich bestandenen Tests produktiv gesetzt worden sei. In den wenigen Tagen bis zum Bekanntwerden des Fehlers seien aber schon fehlerhafte Buchungsinformationen in rund 283 000 Fällen verarbeitet worden. Die Oberfinanzdirektion Karlsruhe teilte mir abschließend mit, dass zur künftigen Vermeidung derartiger Pannen die Testszenarien und die Testfälle der Landesoberkasse, aber auch die internen Tests des Softwareherstellers erweitert worden seien; der aufgetretene Fehler könne sich nicht mehr wiederholen.

Die Finanzverwaltung hat erfreulich rasch reagiert und die richtigen Gegenmaßnahmen ergriffen. Der Vorfall zeigt aber wieder überdeutlich die Notwendigkeit auf, neue Software einschließlich Updates vor ihrem Einsatz in jedem Fall gründlich und gewissenhaft zu testen. Die Freigabe neuer Software darf zudem nur im Mehr-Augen-Prinzip erfolgen. Dies gilt ganz besonders bei sensiblen Daten, wie sie nun einmal im Steuerbereich unvermeidlich anfallen.

2.2 Auch Steuerpflichtige haben ein Recht auf Auskunft!

Das Recht auf Auskunft ist eine grundlegende Ausprägung des Datenschutzes. Nur wer überhaupt weiß, was Behörden an Daten über ihn speichern, kann sich unter Umständen in weiteren Schritten darum kümmern, dass etwa falsche Daten berichtigt oder gelöscht werden. Es ist daher schlicht unakzeptabel, dass ausgerechnet im Besteuerungsverfahren, wo regelmäßig eine Vielzahl teilweise höchst sensibler Daten verarbeitet wird, das gesetzliche Auskunftsrecht von der Finanzverwal-

tung seit Jahren missachtet wird. Die Quelle des Übels ist eine schlichte Verwaltungsanweisung des Bundesministeriums der Finanzen (BMF) aus dem Jahr 2008, das ohne gesetzliche Grundlage den Auskunftsanspruch einschränkt, indem es die Auskunftserteilung von einem „berechtigten Interesse“ abhängig macht. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung vom 26./27. März 2009 klar Stellung bezogen:

> *Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.*

(Der vollständige Wortlaut der Entschließung ist dem Anhang 15 des 29. Tätigkeitsberichts 2009, LT-Drucksache 14/5500, zu entnehmen.)

Leider hat sich seither nichts Entscheidendes verbessert. Der Regierungswechsel im Frühjahr 2011 wirkte sich jedenfalls noch nicht auf den Auskunftsanspruch im Besteuerungsverfahren aus, obwohl die Koalition eine Stärkung des Datenschutzes in Aussicht stellte. Auf mein Schreiben an den Minister für Finanzen und Wirtschaft äußerte dieser Ende Juni 2011 zwar Verständnis, sah sich aber bis auf Weiteres an die Verwaltungsanweisung des BMF gebunden. Immerhin trat auch der Minister für eine „zeitnahe“ gesetzliche Regelung des Auskunftsanspruchs in der Abgabenordnung ein. Mittlerweile gibt es erste Zeichen der Hoffnung: Im Oktober 2011 wurde auf Bundesebene eine vernünftige Lösung im Interesse der Betroffenen in Aussicht gestellt. Dabei ist insbesondere darauf zu achten, dass überzogene Anforderungen an die Geltendmachung des Auskunftsanspruchs vermieden werden.

3. Volkszählung Zensus 2011: Ohne wesentliche Datenschutzmängel

Nach jahrelangen Vorarbeiten hat zum Stichtag 9. Mai 2011 die eigentliche und auch für die Bevölkerung wahrnehmbare Volkszählung stattgefunden. Es handelte sich um den ersten Zensus im wiedervereinigten Deutschland überhaupt, sowie den ersten auf dem Gebiet der „alten“ Bundesrepublik seit 1987, auf dem Gebiet der ehemaligen DDR seit 1981. Auch wenn diese Volkszählung nicht mehr wie 1987 als Direkterhebung bei allen Bürgerinnen und Bürgern, sondern im Wesentlichen unter Auswertung vorhandener Verwaltungsregister stattfindet, werden dabei massenhaft höchst sensible personenbezogene Daten verarbeitet. Bei der Haushaltebefragung auf Stichprobenbasis werden beispielsweise zwingend Angaben zur rechtlichen Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft erhoben. Daher war bei der Vorbereitung, insbesondere bei den für den Zensus maßgeschneiderten Bundesgesetzen, und vor allem bei der Durchführung des Zensus zum Schutz des Grundrechts auf informationelle Selbstbestimmung ganz besondere Sorgfalt angebracht. Die behördlichen Akteure, die meiner Kontrolle unterliegen, sind insbesondere das Statistische Landesamt Baden-Württemberg und knapp 90 sog. örtliche Erhebungsstellen bei den Kommunen.

Auch nach mehreren Informations- und Kontrollbesuchen beim Statistischen Landesamt und bei örtlichen Erhebungsstellen, einigen eingehenden Dienstbesprechungen sowie nach der Bearbeitung zahlreicher Eingaben gibt es erfreulicherweise keinen Grund zur datenschutzrechtlichen Beanstandung. Ich konnte im Wesentlichen feststellen, dass die beteiligten Statistikbehörden des Landes nicht nur das Statistikgeheimnis, sondern auch dem Datenschutz Aufmerksamkeit widmeten. Dies dürfte zu einem gewissen Teil darauf zurückzuführen sein, dass schon frühzeitig vor dem Zensus-Stichtag die datenschutzrechtlichen Aspekte, unter anderem zur Ausstattung

der örtlichen Erhebungsstellen, intensiv mit dem Statistischen Landesamt, mit dem Finanzministerium Baden-Württemberg als der für die Volkszählung zuständigen obersten Landesbehörde und mit dem Innenministerium Baden-Württemberg (hinsichtlich melderechtlicher Fragen) erörtert wurden. Im Kreis der Datenschutzbeauftragten des Bundes und der Länder wurden ebenfalls die relevanten Fragen intensiv abgestimmt. Der Zensus führte zwar zu einem merklichen Anstieg der Anzahl von Eingaben und Beschwerden, allerdings in einem überschaubaren Rahmen, verglichen mit den Verhältnissen während der Volkszählung 1987. Die Kritik vieler Bürgerinnen und Bürger zielte auf grundlegende Weichenstellungen durch bundesgesetzliche Regelungen, etwa auf die in § 18 des Zensusgesetzes 2011 (ZensG 2011) statuierte Auskunftspflicht insgesamt oder die sich aus § 6 Absatz 3 Nr. 3 ZensG 2011 in Verbindung mit § 18 ZensG 2011 ergebende Pflicht von Eigentümern und Verwaltern, bei der Gebäude- und Wohnungszählung Namen und Vornamen von bis zu zwei Wohnungsnutzern je Wohnung anzugeben. Soweit sich die baden-württembergischen Statistikbehörden im Rahmen dieser Vorschriften bewegen, was nach meinen Feststellungen der Fall ist, gibt dies keinen Anlass zur Kritik.

Im Zusammenhang mit der Gebäude- und Wohnungszählung haben sich wiederholt Bürger an mein Amt gewandt und vorgetragen, dass in dem ihnen zugegangenen Umschlag nicht nur der für sie bestimmte Fragebogen, sondern zusätzlich noch ein Fragebogen für ein weiteres Objekt, das allerdings einem anderen Eigentümer gehört, enthalten gewesen sei. Das Statistische Landesamt hat mir auf Nachfrage mitgeteilt, dass ihm solche Probleme auch über die dortige Telefonhotline bekannt geworden seien. Sofort durchgeführte Recherchen hätten ergeben, dass hauptsächlich in einer bestimmten Versandtranche eines einzigen Tages bei einem vom Statistischen Landesamt beauftragten Dienstleister Fehler beim maschinellen Kuvertieren der Unterlagen aufgetreten seien. Diese Tranche habe insgesamt ca. 250.000 Erhebungsunterlagen der Gebäude- und Wohnungszählung umfasst und sich auf einen umgrenzten Postleitzahlenbereich bezogen. Zwar seien die Kuvertiervorgänge stichprobenweise überprüft worden, zudem sei eine automatische Kontrolle durch die Dickenmessung der Briefsendungen erfolgt. Leider seien dennoch in einzelnen Fällen innerhalb dieser einen Tranche solche Fehler geschehen. Die Hotline hätte den Betroffenen mitgeteilt, dass sie die für sie bestimmten Fragebögen ausfüllen und zusammen mit den anderen, fehlerhaft versandten Fragebögen portofrei an das Statistische Landesamt zurücksenden könnten.

Aus datenschutzrechtlicher Sicht ist dazu zu sagen, dass öffentliche Stellen, die personenbezogene Daten verarbeiten, durch geeignete Maßnahmen sicherstellen müssen, dass personenbezogene Daten nicht in die Hände von Unbefugten gelangen können. Diese Anforderung wurde ganz offensichtlich nicht vollumfänglich erfüllt. Ich habe jedoch von einer förmlichen Beanstandung abgesehen, weil das Statistische Landesamt den Fehler bereits selbst erkannt und behoben hatte. Das Statistische Landesamt habe ich aber aufgefordert, durch geeignete Maßnahmen sicherzustellen, dass derartige Fehler zukünftig nicht mehr geschehen können. Insbesondere habe ich geraten, die Stichprobenhäufigkeit bei der maschinellen Kuvertierung zu erhöhen.

Einige Bürgerinnen und Bürger, die im Jahr 2011 auch zur Teilnahme am sog. Mikrozensus, einer stichprobenweisen „kleinen“ Variante der eigentlichen „großen“ Volkszählung ausgewählt worden waren, äußerten ihr Unverständnis, dass sie in diesem Jahr somit zweifach zur Auskunft herangezogen wurden. Diese Kritik kann ich ohne weiteres nachvollziehen. Umgekehrt ist für mich unerfindlich, warum Bürgerinnen und Bürger, die beim eigentlichen, „großen“ Zensus erfasst sind, zugleich auch noch den Anforderungen des Mikrozensus genügen müssen. Dabei wäre es ein Leichtes gewesen, diese Doppelarbeit zu vermeiden. Nach § 13 Absatz 1 des Mikrozensusgesetzes 2005 ist das Bundesministerium des Innern unter anderem dazu ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Erhebung einzelner Erhebungsmerkmale auszusetzen, die Periodizität zu verlängern und Erhebungszeitpunkte zu verschieben. Es ist aus meiner Sicht sehr zu bedauern, allerdings nicht datenschutzrechtlich zu beanstanden, dass von dieser Möglichkeit kein Gebrauch gemacht wurde.

6. Teil: Datenschutz in der Arbeitswelt

1. Abschnitt: Gesundheitsdaten im Arbeitsverhältnis

1. Erhebung von Gesundheitsdaten bei Arbeitnehmern anlässlich der Einstellung

Viele Arbeitgeber lassen ihre künftigen Mitarbeiter vor der Einstellung ärztlich untersuchen. Teilweise ist dies in gesetzlichen Vorschriften ausdrücklich vorgeschrieben, teilweise interessiert sich der Arbeitgeber dafür, ob der Betroffene gesund und den körperlichen Anforderungen, die auf ihn zukommen, gewachsen ist. Bei einem Großunternehmen der Automobilbranche wurden zusammen mit diesen Untersuchungen, aber auch Vorsorgeuntersuchungen im Interesse der Mitarbeiter vorgenommen, um diese rechtzeitig auf zu erwartende Krankheiten aufmerksam zu machen.

Diese Automobilfirma unterhält einen werksärztlichen Dienst, der organisatorisch von den sonstigen Bereichen des Unternehmens, insbesondere von der Personalverwaltung, getrennt ist. Im Berichtszeitraum führte der werksärztliche Dienst bei Bewerbern, die vorbehaltlich ihrer medizinischen Tauglichkeit eingestellt werden sollten, in einem Untersuchungstermin sowohl Einstellungsuntersuchungen als auch solche medizinischen Untersuchungen durch, die aufgrund der Verordnung zur arbeitsmedizinischen Vorsorge gesetzlich vorgeschrieben waren. Daneben gab es aber auch Vorsorgeuntersuchungen „im Interesse des Arbeitnehmers“, durch die herausgefunden werden sollte, ob bei den Mitarbeitern langfristig mit einer Erkrankung, die gegenwärtig für die eigentliche Einstellungsuntersuchung ohne Bedeutung ist, gerechnet werden muss. Vor der Untersuchung mussten die Bewerber um einen Ausbildungsplatz einen Fragebogen ausfüllen, in dem unter anderem nach deren Alkohol- und Drogenkonsum, aber auch nach Krankheiten von Familienangehörigen gefragt wurde. Zu Beginn der Untersuchung wurden die Betroffenen zwar über deren Ablauf, nicht aber darüber belehrt, welchen Zwecken die einzelnen Untersuchungsmaßnahmen und -auswertungen dienen. Was im Zusammenhang mit der Feststellung der Tauglichkeit für eine Beschäftigung, also bei der eigentlichen Einstellungsuntersuchung, im Einzelnen untersucht werden soll, haben die Werksärzte differenziert für den gewerblichen-technischen und den kaufmännischen Bereich festgelegt. Innerhalb des gewerblichen-technischen Bereichs wurde noch einmal unterschieden zwischen reinen Montagetätigkeiten und sonstigen Tätigkeiten. Für Betätigungen mit gesteigerten gesundheitlichen Anforderungen – etwa für den Dienst bei der Werksfeuerwehr – gab es spezielle Untersuchungsprogramme. Doch wurden in der Vergangenheit Blut- und Urinuntersuchungen stets vorgenommen. Das Blut wurde in erster Linie auf Stoffwechsel- und Herzerkrankungen, nicht aber im Hinblick auf HIV-Infektionen und Schwangerschaften ausgewertet. Auch erfolgten keine Genomanalysen. Über die gesundheitliche Tauglichkeit des Bewerbers entschied ausschließlich der Werksarzt, bei dem auch die Befunde verblieben. Die Personalabteilung erfuhr nur, ob „keine gesundheitliche Bedenken“, „keine gesundheitliche Bedenken unter bestimmten Voraussetzungen“ oder „befristete/dauernde gesundheitliche Bedenken“ gegen den Bewerber bestehen. Zeigten sich bei der Gesundheitsvorsorgeuntersuchung Auffälligkeiten, die die Tauglichkeit für eine Beschäftigung nicht in Frage stellen, wurden davon zwar die Bewerber, nicht aber die Personalverwaltung informiert.

Bei dieser Vorgehensweise hat die Aufsichtsbehörde folgende datenschutzrechtliche Mängel festgestellt:

– Dadurch, dass der werksärztliche Dienst in einem Termin nicht nur Eignungs- und Pflichtuntersuchungen, sondern auch weitere, ausschließlich im Interesse des Betroffenen vorzunehmende Vorsorgeuntersuchungen durchführte, verstieß er gegen das gesetzliche Trennungsgebot, nach dem Untersuchungen, über deren Ergebnis der Arbeitgeber zu unterrichten ist, und solche, bei denen die Unterrichtung zu unterbleiben hat, grundsätzlich nicht zusammen durchgeführt werden dürfen.

– Der werksärztliche Dienst unterließ es datenschutzrechtswidrig, die Bewerber in der gebotenen Weise über die verschiedenartigen Untersuchungen, deren Zweck und Inhalt, etwaige Mitwirkungspflichten und die Folgen der Verweigerung zu informieren.

– Die Firma verwendete bei der Einstellungsuntersuchung von Auszubildenden Fragebögen, in denen auch nach persönlichen Umständen des zu Untersuchenden und seiner Familie gefragt wurde, die zur Beurteilung seiner Eignung für eine bestimmte Tätigkeit als künftiger Mitarbeiter dieser Firma nicht erforderlich waren.

– Ein weiterer Verstoß gegen den Erforderlichkeitsgrundsatz war darin zu sehen, dass sich Art und Umfang der Datenerhebung bei den Einstellungsuntersuchungen nicht strikt an den Anforderungen des jeweiligen Arbeitsplatzes orientierte. Insbesondere Blut- und Urinuntersuchungen dürfen auch nach der Rechtsprechung der Arbeitsgerichte nur vorgenommen werden, um Gefahren auszuschließen, die mit der Tätigkeit, die der Betroffene anstrebt, verbunden sind und ihm oder anderen drohen können.

Die Aufsichtsbehörde hat die festgestellten Datenschutzverstöße beanstandet und die Firma aufgefordert, künftig datenschutzkonform zu verfahren.

Die Firma erarbeitet derzeit im Zusammenwirken mit dem Landesbeauftragten für den Datenschutz eine Konzeption, wie Einstellungsuntersuchungen datenschutzgerecht durchgeführt werden können. Urin- und Blutuntersuchungen bei solchen Personen, bei denen diese aus Sicherheitsgründen unter keinen Umständen erforderlich sind, etwa für reine Bürotätigkeiten, sind bereits seit längerem abgestellt worden.

Der Arbeitgeber ist berechtigt, ärztlich feststellen zu lassen, ob ein Arbeitnehmer für eine bestimmte Zeit den Anforderungen der angestrebten Tätigkeiten gewachsen ist, ob von ihm Gefahren für ihn und andere Mitarbeiter ausgehen und ob er den gesundheitlichen Vorgaben genügt, die gesetzlich vorgeschrieben sind. Darüberhinausgehende Untersuchungen dürfen nur mit dem Einverständnis des Betroffenen vorgenommen werden. In jedem Fall muss die medizinische Datenerhebung transparent gemacht werden. Der Umfang der Gesundheitsdatenerhebung ist auf das Unabdingbare zu beschränken.

2. Erhebung von Gesundheitsdaten im Rahmen von Krankenrückkehrgesprächen

Mehrfach hat sich die Aufsichtsbehörde im Berichtszeitraum mit der datenschutzrechtlichen Zulässigkeit der Erhebung von Gesundheitsdaten bei Krankenrückkehrgesprächen im Rahmen eines sog. Fehlzeitenmanagements befasst (vgl. bereits B 1.6 des Fünften Tätigkeitsberichts des Innenministeriums 2009).

In einem Fall hatte ein Unternehmen in einer „Richtlinie Fehlzeitenmanagement“ ein dreistufiges System für Krankenrückkehrgespräche vorgesehen. Dabei sollte nach jeder krankheitsbedingten Abwesenheit – unabhängig von deren Dauer und Häufigkeit – zunächst der jeweilige Vorgesetzte oder Meister ein informelles Rückkehrgespräch mit dem Mitarbeiter führen. Die Richtlinie nannte als Ziel dieses Gesprächs, den Mitarbeiter zu motivieren und ihm zu verstehen zu geben, dass seine Abwesenheit bemerkt wurde und er gefehlt hat. Weitere Vorgaben, etwa zur Reichweite des Fragerechts oder zur Dokumentation des Gesprächs, enthielt die Richtlinie nicht. Ab drei Fehlzeiten oder zwanzig Fehltagen innerhalb von zwölf Monaten sollte ein weiteres Gespräch mit dem Ziel stattfinden, dem Mitarbeiter die Folgen seines Fehlens zu verdeutlichen, die Ursachen des Fehlens zu ergründen und mögliche Konsequenzen aufzuzeigen. Hierüber sollte eine Gesprächsnotiz angefertigt werden. Wurde der Mitarbeiter innerhalb von drei Monaten nach einem solchen Gespräch erneut krank, sollte sein Fehlzeitenverhalten mit ihm in einem disziplinarischen Fehlzeitengespräch unter Beteiligung der Personalabteilung sowie eines Mitglieds des Betriebsrats erörtert und er über mögliche arbeitsrechtliche Konsequenzen informiert werden.

Die Richtlinie sah außerdem vor, durch monatliche Aushänge an allen Schwarzen Brettern des Unternehmens die aktuelle Fehlzeitenquote sowie

die Zahl der Mitarbeiter ohne Fehltage, mit ein bis drei Fehltagen usw. bekanntzugeben.

Bei unserer datenschutzrechtlichen Überprüfung gingen wir von folgenden Grundsätzen aus:

Ein Arbeitgeber, der mit seinen Mitarbeitern nach der Rückkehr aus dem Krankenstand ein Rückkehrgespräch führt, beziehungsweise führen lässt, darf dabei personenbezogene Daten – insbesondere Gesundheitsdaten – nur in dem Maße erheben, wie dies nach § 32 Absatz 1 und § 28 Absatz 6 Nr. 3 BDSG zulässig ist. Diese gesetzlichen Befugnisse des Arbeitgebers können nicht durch eine Einwilligung des Arbeitnehmers erweitert werden, da sich dieser wegen der existenziellen Bedeutung seines Arbeitsverhältnisses gegenüber dem Arbeitgeber in einer schwächeren Position befindet und es deshalb an der nötigen Freiwilligkeit für eine solche Erklärung fehlt. Auch im Wege von Betriebsvereinbarungen können keine weitergehenden Eingriffe in das Persönlichkeitsrecht der Beschäftigten vorgesehen werden, als dies bereits aufgrund Gesetzes möglich ist. Maßnahmen des betrieblichen Eingliederungsmanagements nach § 84 Absatz 2 des Neunten Buchs des Sozialgesetzbuchs (SGB IX) einschließlich der dafür erforderlichen Datenverarbeitung bedürfen dagegen der Einwilligung des Mitarbeiters.

Der Arbeitgeber darf sich bei Krankenrückkehrgesprächen nur insoweit nach der Ursache der Erkrankung erkundigen, als dieser eine betriebliche oder ersatzleistungsrechtliche Relevanz zukommt. Der Vorgesetzte darf in Krankenrückkehrgesprächen deshalb danach fragen, wann der Mitarbeiter wieder voll einsatzfähig ist und welche Einschränkungen in der Person des Mitarbeiters vorliegen, bis er wieder voll einsatzfähig ist. Der Vorgesetze darf sich zudem danach erkundigen, ob von dem Mitarbeiter eine Ansteckungsgefahr ausgeht und ob der Erkrankung ein Unfall beziehungsweise ein schädigendes Ereignis durch einen Dritten zugrunde liegt. Außerdem ist der Arbeitgeber berechtigt, danach zu fragen, ob es Gründe gibt, derentwegen der Arbeitnehmer die Leistung, zu der er sich in seinem Arbeitsvertrag verpflichtet hat, auf Dauer nicht mehr erbringen kann. In allen diesen Fällen besteht eine Verpflichtung des Arbeitnehmers, die Fragen wahrheitsgemäß zu beantworten. Hierauf ist der Arbeitnehmer vor Durchführung des Gesprächs hinzuweisen.

Darüber hinaus darf der Vorgesetzte sich danach erkundigen, ob die Erkrankung betriebliche Ursachen hat. Der Vorgesetzte darf weiter ansprechen, welche Veränderungen am Arbeitsplatz des Betroffenen vorgenommen werden müssen, um seinem Gesundheitszustand Rechnung zu tragen. Schließlich darf der Vorgesetzte sich auch danach erkundigen, ob der Mitarbeiter bei der Verrichtung seiner Arbeit gefährdet ist, weil er noch Medikamente einnimmt, die seine Reaktionsfähigkeit verzögern.

Die letztgenannten drei Fragen darf der Arbeitgeber zwar stellen. Sie müssen aber vom Arbeitnehmer mangels einer durchsetzbaren Verpflichtung nicht beantwortet werden. Hierauf ist der Arbeitnehmer vom Arbeitgeber vor Durchführung des Gesprächs hinzuweisen. Beantwortet der Arbeitnehmer die letztgenannten Fragen nicht, kann dies zur Folge haben, dass der Arbeitgeber nichts zugunsten des Arbeitnehmers unternehmen muss.

Nach konkreten medizinischen Diagnosen darf auf keinen Fall gefragt werden.

Zu Beginn der Krankenrückkehrgespräche müssen die Mitarbeiter durch die verantwortliche Stelle umfassend im Sinne des § 4 Absatz 3 BDSG belehrt werden. Dabei müssen sie zumindest darauf hingewiesen werden, zu welchem Zweck welche Erhebung dient, zu welchen Angaben sie verpflichtet sind beziehungsweise welche Nachteile ihnen drohen, wenn sie sonstige Fragen nicht beantworten, für welchen Zweck die Daten verarbeitet und genutzt werden und welche Daten an die Rechts- oder die Personalabteilung aus welchem Grund weitergegeben werden. Auch sollte den Beschäftigten mitgeteilt werden, ob eine Niederschrift über das Gespräch angefertigt und zur Personalakte genommen wird und wer von den darin niedergeschriebenen Angaben Kenntnis nehmen kann.

Über das Gespräch können Niederschriften gefertigt werden, soweit dies zu Dokumentationszwecken erforderlich ist und die Datenerhebung zulässig

war. Ungefragte Angaben des Betroffenen zu seinem Gesundheitszustand dürfen dabei nur festgehalten werden, soweit dies zur Wahrnehmung von Rechten und zur Erfüllung von Pflichten des Arbeitgebers erforderlich ist und keine schutzwürdigen Interessen des Arbeitnehmers entgegenstehen. In den allermeisten Fällen dürfte eine personenbezogene Speicherung von Krankheitsdaten nicht erforderlich und damit auch nicht zulässig sein. Insbesondere ist eine Speicherung von Krankheitsdaten in den Personalakten regelmäßig unzulässig.

Bei den Krankenrückkehrgesprächen werden Gesundheitsdaten erhoben und genutzt, die zugleich Personaldaten sind und in die Personalakte gehören. Bereits die reinen Fehlzeiten eines Erkrankten sind sensible (Gesundheits-)Daten im Sinne von § 3 Absatz 9 BDSG, weil sie aus dem Kontext heraus etwas über die Schwere der Krankheit aussagen. Bei solchen Daten ist der Kreis der Personen, die davon Kenntnis erhalten dürfen, zur Wahrung des Persönlichkeitsschutzes der Betroffenen so eng wie irgend möglich zu halten. Das hat zur Folge, dass an den Krankenrückkehrgesprächen nur teilnehmen darf, wer die dabei offenbar werdenden personenbezogenen Daten nach den für Personalakten geltenden Grundsätzen auch erhalten darf. Dies sind in der Regel nur die Vorgesetzten des Betroffenen sowie solche Angehörigen der Personalabteilung, die für die Betreuung des Mitarbeiters zuständig sind beziehungsweise an den diesen betreffenden Personalentscheidungen mitwirken dürfen.

Diesen Vorgaben genügte die zur Überprüfung stehende Richtlinie nicht. Denn sie überließ es letztlich dem jeweiligen Vorgesetzten, was er im Einzelnen fragen wollte. Der Vorgesetzte wurde außerdem im Unklaren darüber gelassen, welche Angaben auf keinen Fall erhoben werden dürfen.

Wir haben das Unternehmen daher aufgefordert, in die Richtlinie als schriftliche Handreichung für die Vorgesetzten, die Rückkehrgespräche durchführen müssen, die zulässigen Fragen – differenziert danach, welche Fragen der Arbeitnehmer wahrheitsgemäß beantworten muss und bei welchen Fragen ihm eine Antwort freisteht – sowie die Vorgabe, dass nach konkreten medizinischen Diagnosen in keinem Fall gefragt werden darf und diese, wenn sie ungefragt offenbart werden, im Regelfall nicht schriftlich festgehalten werden dürfen, aufzunehmen. Zudem musste die Richtlinie um klare Vorgaben in Bezug auf die Reichweite der notwendigen Belehrungen des Arbeitnehmers durch den Vorgesetzten vor Durchführung des Rückkehrgesprächs ergänzt werden. Das Unternehmen ist dem nachgekommen und hat unsere Vorgaben in einer Betriebsvereinbarung über das betriebliche Eingliederungsmanagement umgesetzt.

Die in der Richtlinie vorgesehene Veröffentlichung statistischer Daten zum Krankheitsstand im Betrieb über einen Aushang an einem Schwarzen Brett war datenschutzrechtlich dagegen nicht zu beanstanden. Denn da die mitgeteilten Daten keiner bestimmten Person zugeordnet werden konnten, handelte es sich nicht um personenbezogene Daten.

3. Krank im Kalender? Gesundheitsdaten in elektronischen Abwesenheitsmanagementsystemen

Durch die Beschwerde des Betriebsrats eines Unternehmens wurde die Aufsichtsbehörde auf folgenden Sachverhalt aufmerksam:

In einem Werk des Unternehmens kam ein elektronisches Abwesenheitsmanagementsystem zum Einsatz. In diesem waren die Abwesenheitstage aller Mitarbeiter der betreffenden Organisationseinheit mit einem Kürzel für den Abwesenheitsgrund eingetragen. Die Mitarbeiter einer Organisationseinheit konnten die Abwesenheitsliste aller übrigen Mitarbeiter der Organisationseinheit einschließlich der Kürzel GL (Gleitzeit), U (Urlaub) und SO (Sonderurlaub) einsehen. Diese Informationen waren für die Mitarbeiter erforderlich, damit sie sich mit ihren Kollegen bezüglich der Urlaubsplanung oder eines Tauschs von Schichtdiensten abstimmen konnten. Dieser Abstimmung dienten auch zusätzliche Freitextfelder, in denen zwar nur der jeweilige Vorgesetzte Eintragungen vornehmen konnte, die jedoch für alle Mitarbeiter zur Einsicht freigeschaltet waren. In den Schulungsunterlagen

für die Vorgesetzten zum Einsatz des Abwesenheitsmanagements fand sich der Hinweis, dass in die Freitextfelder keine „persönlichen Informationen“ eingetragen werden dürfen.

Ein Vorgesetzter verstieß gegen diese Vorgabe, indem er bei vier Arbeitnehmern Eintragungen zum Grund der krankheitsbedingten Abwesenheit im Freitextfeld vornahm. Auf diese Weise konnten sich andere Angehörige der Organisationseinheit darüber informieren, dass ihr Kollege beziehungsweise ihre Kollegin sich an einem bestimmten Tag einer Behandlung der Weisheitszähne, einem Allergietest für Wespenstiche oder einer Operation am Fuß unterziehen musste. Der Werksleitung war diese Praxis des Vorgesetzten nicht bekannt.

Datenschutzrechtlich war sie nicht in Ordnung, denn durch die Eintragungen wurden personenbezogene Gesundheitsdaten von Beschäftigten gespeichert. Soweit Kollegen des Betroffenen die Daten tatsächlich zur Kenntnis genommen haben, lag daneben auch eine Übermittlung an einen Dritten in Form der Einsichtnahme durch den Dritten gemäß § 3 Absatz 4 Satz 2 Nr. 3 b BDSG vor. Diese Datenverarbeitung war weder durch eine Einwilligung des Betroffenen gedeckt noch lagen die Voraussetzungen des § 32 Absatz 1 Satz 1 BDSG oder des § 28 Absatz 6 BDSG vor. Das Unternehmen hat umgehend die Löschung aller Einträge in den Freitextfeldern des elektronischen Abwesenheitsmanagements veranlasst, die Rückschlüsse auf Krankheitsgründe zulassen. Um zu gewährleisten, dass in Zukunft in die Freitextfelder bei krankheitsbedingter Abwesenheit keine Kommentare mehr eingetragen werden, wird bei jedem Öffnen des entsprechenden Eingabefeldes ein Warnhinweis ausgegeben, der daran erinnert, dass in das Freitextfeld keine persönlichen oder privaten Inhalte, insbesondere keine Krankheitsgründe eingegeben werden dürfen.

4. Erhebung der Schwerbehinderteneigenschaft von Bewerbern und Arbeitnehmern

Die Aufsichtsbehörde hatte sich im Berichtszeitraum wiederholt mit der Frage zu befassen, ob und unter welchen Voraussetzungen Arbeitgeber in Bewerbungsverfahren und bestehenden Beschäftigungsverhältnissen nach einer anerkannten Schwerbehinderung fragen dürfen.

Ein Arbeitgeber darf sich danach erkundigen, ob ein Bewerber an bestimmten körperlichen Gebrechen leidet, die der angestrebten Beschäftigung entgegenstehen.

Darüber hinaus kann in bestimmten Fällen auch eine sog. tätigkeitsneutrale Frage des Arbeitgebers nach der Schwerbehinderteneigenschaft zulässig sein. Tätigkeitsneutral ist die Frage dann, wenn sie keinen Bezug zur vorgesehenen Beschäftigung hat, sondern nur darauf abzielt zu erfahren, ob eine Schwerbehinderung festgestellt ist oder objektiv vorliegt und ihre Feststellung beantragt wird. Bezüglich der Zulässigkeit einer tätigkeitsneutralen Frage nach einer Schwerbehinderung ist zwischen dem Bewerbungsverhältnis und dem bestehenden Arbeitsverhältnis zu unterscheiden:

Im *Bewerbungsverfahren* ist die tätigkeitsneutrale Frage des Arbeitgebers nach einer anerkannten Schwerbehinderung oder Gleichstellung von Bewerbern grundsätzlich unzulässig. Auch der Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (BT-Drucksache 17/4230) schließt in § 32 Absatz 3 jegliche Frage nach einer Schwerbehinderung oder Gleichstellung vor Begründung eines Beschäftigungsverhältnisses aus. Eine tätigkeitsneutrale Frage nach dem Status der Schwerbehinderung oder einem laufenden Feststellungsverfahren im Anbahnungsverhältnis ist nach geltendem Recht – zumindest bis zum Inkrafttreten des o. g. Gesetzes – jedoch ausnahmsweise zulässig, wenn der Arbeitgeber deutlich macht und beweisen kann, dass das Ziel der Frage eine positive Maßnahme im Sinne von § 5 des Allgemeinen Gleichbehandlungsgesetzes (AGG), insbesondere die Eingliederung von Behinderten oder die Steigerung des Ist-Satzes der Beschäftigungspflicht nach § 71 Absatz 1 des Neunten Buchs des Sozialgesetzbuchs (SGB IX) ist. In solchen Fällen muss dem Bewerber allerdings ein Selbstbestimmungsrecht hinsichtlich der Offenbarung der Schwerbehinderteneigen-

schaft verbleiben, das heißt ob der Bewerber eine diesbezügliche Frage des Arbeitgebers wahrheitsgemäß beantwortet oder hierzu keine Angaben macht, muss ihm, ohne rechtliche Folgen fürchten zu müssen, freigestellt sein. Während ein Vortäuschen der Anerkennung als arglistige Täuschung anzusehen wäre, ist es dem Bewerber freigestellt, den ihm gewährten Schutz bereits im Anbahnungsverhältnis in Anspruch zu nehmen, das heißt im Personalfragebogen muss die Beantwortung dieser Frage ausdrücklich als freiwillig gekennzeichnet sein.

Im bestehenden Arbeitsverhältnis ist die tätigkeitsneutrale Frage nach der Schwerbehinderteneigenschaft ohne Einschränkungen zulässig, da der Arbeitgeber im Hinblick auf die von ihm gemäß § 71 Absatz 1 SGB IX zu erfüllende Beschäftigungsquote ein berechtigtes Interesse an der Kenntnis der Schwerbehinderteneigenschaft seiner Mitarbeiter hat. In diesem Stadium muss die Frage vom Arbeitnehmer auch wahrheitsgemäß beantwortet werden.

5. Mehr Datenschutz beim Voranerkennungsverfahren für die Beihilfefähigkeit einer ambulanten psychotherapeutischen Behandlung

Beim Voranerkennungsverfahren, das auch Gegenstand des 8. Tätigkeitsberichts 1987 war (LT-Drucksache 9/5230, S. 78 f.), geht es um die Kosten einer ambulanten psychotherapeutischen Behandlung eines Beamten, Richters oder berücksichtigungsfähigen Angehörigen. Das Landesamt für Besoldung und Versorgung Baden-Württemberg erstattet diese Kosten nur dann, wenn es deren Beihilfefähigkeit zuvor anerkannt hat. Dazu erstellt der behandelnde Arzt einen ärztlichen Bericht für einen Gutachter, den das Landesamt bestimmt. Dieser erstattet ein „Psychotherapie-Gutachten“, anhand dessen das Landesamt entscheidet, ob die Kosten beihilfefähig sind. In dem ärztlichen Bericht sind unter anderem die Psychogenese und Psychodynamik der neurotischen oder psychotischen Entwicklung dargestellt sowie Geschlecht, Familienstand und Beruf aufgeführt. Damals wurde von Seiten des Datenschutzes bemängelt, dass dort auch Name und Geburtsdatum des Patienten genannt wurden, anstatt diese durch eine Chiffre und das Alter zu ersetzen, ähnlich wie bei der gesetzlichen Krankenversicherung. Das soll eine Bestimmbarkeit des Patienten möglichst ausschließen, zumindest jedoch verringern; das Alter (oder das damit insoweit vergleichbare Geburtsjahr) ist allgemeiner als das Geburtsdatum.

Inzwischen sieht das Landesamt beim Voranerkennungsverfahren vor, dass der Name durch einen „Anonymisierungscode“ ersetzt wird. Allerdings wird weiterhin das Geburtsdatum genannt. Dagegen regelt die allgemeine Verwaltungsvorschrift zur Bundesbeihilfeverordnung, dass im Bericht des Therapeuten an den Gutachter sowohl der „Anonymisierungscode“ anstatt des Namens als auch das Alter anstatt des Geburtsdatums genannt wird.

Ich habe gegenüber dem Landesamt nochmals die (Rechts-)Grundlage für die Nennung des Geburtsdatums in Zweifel gezogen und das Ministerium für Finanzen und Wirtschaft Baden-Württemberg davon unterrichtet. Nachdem der größte Stein des Anstoßes, die Nennung des Namens aus der Welt geschafft wurde, sollte auch noch der Rest bereinigt werden.

6. Verwaltungsvorschrift zur Beihilfeverordnung – Beihilfe für berücksichtigungsfähige Angehörige

Der auch aus meiner Sicht unhaltbare Zustand ist schon im 21. Tätigkeitsbericht 2000 (LT-Drucksache 12/5740, S. 75) unter dem Titel „Kein Datenschutz in der Familie?“ beschrieben worden: Es geht um Beihilfe für Aufwendungen bei Krankheit, die einem Angehörigen eines Beamten oder Richters entstanden sind. Während bei der gesetzlichen Krankenversicherung jedes Familienmitglied einen eigenen Anspruch auf Versicherungsleistungen hat, hat auf Beihilfe auch für seine Angehörigen (soweit sie überhaupt berücksichtigt werden können) nur der beihilfeberechtigte Beamte selbst einen Anspruch; nur er kann die Aufwendungen geltend machen. Dem Antrag sind Kopien der Rechnungen oder Rezepte beizufügen. Auf diesen steht unter anderem, wann der Patient bei welchem Arzt war, was

dieser diagnostiziert hat und was der Arzt verschrieben hat. Das gilt natürlich dann auch für den Ehepartner oder volljährige Kinder.

Das Finanzministerium Baden-Württemberg hatte auf die wiederholte Intervention meiner Vorgänger damals mitgeteilt, die Konferenz der Finanzministerinnen und Finanzminister der Länder habe ein eigenes Antragsrecht für berücksichtigungsfähige Angehörige einstimmig abgelehnt.

Fairerweise muss man ergänzen, dass es im Land zwei Möglichkeiten gibt, im Beihilfeverfahren die Daten der Angehörigen vor dem Beihilfeberechtigten ein wenig zu schützen: So können die Belege der Angehörigen in einem verschlossenen Umschlag unmittelbar der Beihilfestelle vorgelegt werden, wenn der Beihilfeberechtigte die Beihilfe beantragt. Außerdem kann der Beihilfeberechtigte seinen von ihm getrennt lebenden oder von ihm rechtskräftig geschiedenen Ehegatten für dessen Beihilfeangelegenheiten sowie die der Kinder des Beihilfeberechtigten, die bei diesem Ehegatten leben, bevollmächtigen; auf dem entsprechenden Vordruck des Landesamts für Besoldung und Versorgung Baden-Württemberg hat der Bevollmächtigte das Konto anzugeben, auf das die Beihilfe überwiesen werden soll.

Inzwischen wurde die Beihilfeverordnung des Bundes geändert. Danach kann die Festsetzungsstelle zur Vermeidung unbilliger Härten nach vorheriger Anhörung des Beihilfeberechtigten zulassen, dass Angehörige oder deren gesetzliche Vertreter ohne Zustimmung des Beihilfeberechtigten die Beihilfe selbst beantragen; es ist dann also entbehrlich, dass der Beihilfeberechtigte den Angehörigen bevollmächtigt. Was auf Bundesebene klappt, bereitet auf Landesebene aber offenbar immer noch Probleme. Auf meine Anfragen dazu hat das Ministerium für Finanzen und Wirtschaft zuletzt im Zusammenhang mit einer neuen Verwaltungsvorschrift zur Beihilfeverordnung mitgeteilt, es werde anlässlich einer künftigen Änderung der Beihilfeverordnung nochmals prüfen, ob und gegebenenfalls wie die Regelung des Bundes zur Antragstellung durch berücksichtigungsfähige Angehörige für das Land sachgerecht übernommen werden könne; eine Regelung durch Verwaltungsvorschrift sei, anders als zunächst angenommen, aber nicht möglich. Derzeit würden Zahlungen auf Grundlage einer Vollmacht des Beihilfeberechtigten an den von diesem getrennt lebenden oder geschiedenen berücksichtigungsfähigen Ehegatten und deren berücksichtigungsfähige Kinder überwiesen; diese Praxis sei bisher auf keine nennenswerten Probleme gestoßen. Bereits zuvor hatte das Finanzministerium angemerkt, dass die genannte Bundesregelung für innerfamiliäre Konflikte die Tür in die Beihilfeabrechnung geöffnet habe; jedoch seien diese nicht in der Beihilfeabrechnung zu lösen, sondern gegebenenfalls familienrechtlich beziehungsweise unterhaltsrechtlich. Auch das spricht meines Erachtens dafür, einen eigenen Beihilfeanspruch für die berücksichtigungsfähigen Angehörigen zu schaffen. Ohne einen solchen Anspruch dürfte die Angelegenheit aus Sicht des Datenschutzes unbefriedigend bleiben.

2. Abschnitt: Weitere Fragen des Arbeitnehmerdatenschutzes

1. Speicherung und Nutzung der bei Personaleinkäufen anfallenden Daten

Eine Drogeriemarktkette speichert und nutzt die bei Personaleinkäufen anfallenden Daten. Es fragt sich, in welchem Umfang sie das tun darf.

Wie in anderen Betrieben auch, erhielten die Beschäftigten einer Drogeriemarktkette bei einem Einkauf in einer der Filialen einen Rabatt. Auf Antrag bekamen sie dazu einen Einkaufsausweis, der an der Kasse vorgelegt werden musste. Nach einer internen Vorgabe durfte generell nur in den Pausenzeiten und in der Freizeit eingekauft werden. Beim Bezahlen wurden neben dem Einzel- und dem Gesamtkaufpreis unter anderem die Mitarbeiterkennung, die Anzahl der erworbenen Warenartikel, deren Nummer und der gewährte Rabatt festgehalten. In diesem Zusammenhang ist zu erwähnen, dass der steuerliche Jahresfreibetrag für Personalrabatte gemäß § 8 Absatz 3 Satz 2 des Einkommensteuergesetzes (EStG) zurzeit 1.080 EUR beträgt. Wird darüber hinaus Rabatt gewährt, muss das Unternehmen für diesen „geldwerten Vorteil zugunsten seiner Beschäftigten“ Lohnsteuer abführen.

Ein Beschäftigter der Drogeriemarktkette hatte mir gegenüber Zweifel geäußert, ob sich die Kontrollen der Personaleinkäufe durch die Drogeriemarktkette im datenschutzrechtlich zulässigen Rahmen bewegten. Neben der Kontrolle, inwieweit der Rahmen des steuerlichen Freibetrags eingehalten wird, seien die Filialleiter angeblich auch angehalten, beim Erwerb von Ware durch die Beschäftigten nach bestimmten sonstigen Auffälligkeiten zu suchen, wie zum Beispiel Einkäufen innerhalb der Arbeitszeit oder privatem Weiterverkauf.

Die Drogeriemarktkette teilte auf Anfrage mit, dass die bei Personaleinkäufen anfallenden Daten in erster Linie für Auswertungen zur Einhaltung der Steuerfreibetragsgrenze genutzt würden. Die Beschäftigten, die mit ihrem Personalrabatt im Jahresdurchschnitt über dem anteiligen Steuerfreibetrag von aktuell 1.080 EUR lägen, erhielten darüber im Abstand von drei Monaten eine schriftliche Information.

Des Weiteren zeigte sich, dass bei der Firma auch Auswertungen der anlässlich der Personaleinkäufe erhobenen Daten zu Missbrauchs- und Manipulationsrecherchen vorgenommen wurden. Dabei habe es kein einheitliches, strukturiertes Vorgehen gegeben. Vielmehr hätten mal das Controlling, mal die Revision, mal die Personalverwaltung, mal die Verkaufsleiter sporadische Auswertungen durchgeführt. Auf diese Weise hatten alle möglichen Stellen Zugriff auf die besagten Beschäftigtendaten, obwohl es sich dabei um besonders sensible Informationen handelte. Diese Maßnahmen wurden inzwischen ausgesetzt.

Die Erhebung, Speicherung, Nutzung und Übermittlung der Mitarbeiterkennung und der gegebenenfalls zu versteuernden Rabatte halte ich im Übrigen datenschutzrechtlich für zulässig, wenn die Beschäftigten nach § 33 Absatz 1 Satz 1 BDSG darüber aufgeklärt werden, um welche Daten es sich dabei konkret handelt und was mit diesen geschieht. Die Notwendigkeit, weitere Informationen, etwa die Warenartikelnummer oder die Häufigkeit von Einkäufen, zu erheben, erschließt sich mir allerdings nicht so ohne Weiteres. Ich habe daher das Unternehmen aufgefordert, ein Gesamtkonzept für die Datenverarbeitung bei der Rabattgewährung einschließlich eventueller Kontrollmaßnahmen zu erarbeiten und meiner Dienststelle zur Prüfung vorzulegen. Soweit erforderlich, muss auch das Finanzamt beteiligt werden.

Die Großzügigkeit gegenüber den Beschäftigten bei der Gewährung von materiellen Vorteilen erlaubt dem Chef noch lange nicht, auch entsprechend großzügig mit deren persönlichen Daten umzugehen.

2. Fragerecht des Arbeitgebers im Bewerbungsverfahren: Bewerberfragebogen

Der Umfang des Fragerechts von Arbeitgebern gegenüber Bewerbern in Bewerbungsverfahren hat uns auch im Berichtszeitraum immer wieder beschäftigt (vgl. dazu bereits B 1.8 des Fünften Tätigkeitsberichts des Innenministeriums 2009).

In mehreren Fällen waren Arbeitgeber der Ansicht, die Grenzen ihres in weiten Teilen durch die arbeitsgerichtliche Rechtsprechung abgesteckten Fragerechts ließen sich durch den Hinweis auf die Freiwilligkeit bestimmter Angaben oder die Einholung einer Einwilligung des Bewerbers erweitern. Das trifft nicht zu. Das Fragerecht eines Arbeitgebers im Personalauswahlverfahren kann nicht durch die Einholung einer Einwilligung des Bewerbers erweitert werden, da dies dazu führen würde, dass die arbeitsrechtlichen Beschränkungen des Fragerechts unterlaufen würden. Gleiches gilt – von wenigen Ausnahmen abgesehen (vgl. hierzu 6. Teil, 1. Abschnitt, Nr. 4) – auch für den Hinweis auf die Freiwilligkeit bestimmter Angaben.

Nach der Rechtsprechung des Bundesarbeitsgerichts wird dem Arbeitgeber ein Fragerecht zugestanden, soweit er für die Auswahlentscheidung ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Beantwortung seiner Fragen im Hinblick auf den konkreten Arbeitsplatz und die zu leistende Arbeit hat. Die Antwort muss folglich für die Eingehung des Beschäftigungsverhältnisses von Bedeutung sein und dabei einen unmittelbaren Sachzusammenhang zur auszuübenden Tätigkeit aufweisen. Betrifft

eine Frage lediglich die Privatsphäre eines Bewerbers und liefert ihre Beantwortung keine Informationen, die für die Eingehung des Beschäftigungsverhältnisses von Bedeutung sind, ist sie unzulässig.

Ein Arbeitgeber erkundigte sich in seinen Bewerberfragebögen danach, ob der Bewerber Kinder habe und, falls dies zutreffe, nach deren Zahl und Alter. Außerdem wollte er wissen, ob der Bewerber bei der Aufsicht und Erziehung der Kinder Unterstützung erhalte und ob er alleinerziehend sei. Fragen nach dem Familienstand und den Familienverhältnissen des Bewerbers (zum Beispiel Zahl und Alter seiner Kinder oder wie deren Betreuung geregelt ist oder ob der Bewerber alleinerziehend ist) betreffen Daten aus der Privatsphäre des Bewerbers, die im Regelfall in keinem notwendigen Zusammenhang mit dem Arbeitsverhältnis stehen und daher in Bewerberfragebögen grundsätzlich unzulässig sind. Wegen ihrer steuerrechtlichen Relevanz darf der Arbeitgeber diese Daten zwar nach der Eingehung eines Arbeitsverhältnisses erfragen. Im Bewerbungsgespräch können derartige Fragen dagegen nur unter besonderen Umständen ausnahmsweise zulässig sein. Solche Umstände können etwa dann gegeben sein, wenn die Position, für die sich der Arbeitnehmer bewirbt, regelmäßig mit unvorhersehbaren Einsätzen zu ungewöhnlichen Zeiten verbunden ist, die einem alleinerziehenden Elternteil minderjähriger Kinder nicht oder nur schwer möglich sind. In welcher Form alleinerziehende Arbeitnehmer die Betreuung ihrer Kinder während der regulären Arbeitszeit organisieren, ist allein ihre Sache.

Die Frage, ob ein Bewerber einer Nebentätigkeit nachgeht und, wenn ja, welcher, ist in dieser Form zu weitgehend und daher unzulässig. Gefragt werden darf nur nach solchen Nebentätigkeiten, die Einfluss auf die Erfüllung der arbeitsvertraglichen Pflichten haben können. Darunter fallen solche bei Konkurrenzunternehmen, Nachtarbeit oder sonstige Tätigkeiten, die zu einer Überarbeitung des Bewerbers führen können.

Auch für Fragen nach privaten, nicht arbeitsplatzbezogenen Lebensgewohnheiten, wie z. B. dem Rauchen, besteht regelmäßig kein legitimes Informationsinteresse des Arbeitgebers. Der Arbeitgeber muss im Hinblick auf die Arbeitsstättenverordnung (§ 5) Regelungen zum Rauchen im Betrieb treffen und deren Einhaltung überprüfen. Er kann in Bewerbungsgesprächen auf Rauchverbote im Unternehmen hinweisen, darf aber Bewerber nicht danach fragen, ob sie Raucher oder Nichtraucher sind. Ob jemand raucht oder Nichtraucher ist, ist grundsätzlich der privaten Lebensgestaltung zuzurechnen. Mithin darf die Frage nach der „Rauchereigenschaft“ im Vorstellungsgespräch regelmäßig keine Rolle spielen.

Allgemeine Fragen nach dem Gesundheitszustand, Behinderungen, Beschwerden und chronischen oder wiederkehrenden Krankheiten oder Leiden sind grundsätzlich unzulässig. Stattdessen kann sich der Arbeitgeber danach erkundigen, ob es gesundheitliche Beeinträchtigungen gibt, die die Eignung des Bewerbers bei der Verrichtung der angestrebten Tätigkeiten auf Dauer oder in periodisch wiederkehrenden Abständen einschränken. Zudem darf gefragt werden, ob ansteckende Krankheiten vorliegen, die zwar nicht die Leistungsfähigkeit beeinträchtigen, jedoch die zukünftigen Kollegen oder Kunden gefährden. Legitim ist schließlich auch die Frage, ob zum Zeitpunkt des Dienstantritts beziehungsweise in absehbarer Zeit mit einer Arbeitsunfähigkeit zu rechnen ist, zum Beispiel durch eine geplante Operation, eine bewilligte Kur oder auch durch eine zurzeit bestehende akute Erkrankung. Fragen nach Körperbehinderungen sind nur insoweit zulässig, als sie auf eine durch die Körperbehinderung mögliche Beeinträchtigung der zu verrichtenden Arbeit gerichtet sind. Das heißt es darf nur nach solchen Körperbehinderungen gefragt werden, die erfahrungsgemäß geeignet sind, die Arbeitsfähigkeit des Bewerbers für die ihm zugedachte Arbeit zu beeinträchtigen.

Ein berechtigtes Interesse des Arbeitgebers an Angaben, die über die vorgenannten Auskünfte zum Gesundheitszustand hinausgehen, besteht nicht. Unzulässig ist beispielsweise die Frage „Gibt es gesundheitliche Einschränkungen aktuell und/oder wiederkehrend? Wenn ja, welche?“, da die Frage in dieser Form unabhängig von einer Einschränkung der Eignung des Bewerbers zur Verrichtung der angestrebten Tätigkeit gestellt wird. Ebenfalls unzulässig ist die Frage, ob eine medizinische Operation geplant ist, denn bestimmte medizinische Operationen können auch außerhalb der Arbeits-

zeit und ohne Beeinträchtigung der Arbeitsfähigkeit durchgeführt werden. Der Präzisierung bedarf die Frage „Wurde Ihnen eine Kur bewilligt oder von Ihnen beantragt?“. In dieser Form ist die Frage nämlich insofern missverständlich, als auch Bewerber, die in der Vergangenheit eine Kur beantragt und durchgeführt haben, sich verpflichtet fühlen könnten, die Frage mit „Ja“ zu beantworten.

3. Verarbeitung personenbezogener Daten für Auslandseinsätze von Mitarbeitern durch eine Wirtschaftsprüfungsgesellschaft im Auftrag des Arbeitgebers

Ein großes Unternehmen in Baden-Württemberg ließ sich bei der Erfüllung der ihm obliegenden steuerrechtlichen Pflichten im Zusammenhang mit der Entsendung von Mitarbeitern ins Ausland – insbesondere der Ermittlung des korrekten Lohnsteuereinbehalts – von einer externen Wirtschaftsprüfungsgesellschaft (im Folgenden: WPG) unterstützen. Diese unterstützte die betreffenden Mitarbeiter zudem auf Wunsch auch kostenlos bei der Erstellung ihrer Steuererklärungen im In- und Ausland. Die WPG erhob für diese Zwecke personenbezogene Daten des Mitarbeiters und seiner Angehörigen in zwei Gesprächen. Dabei wurde den Mitarbeitern eine „Einverständniserklärung für die Verarbeitung und Weitergabe von personenbezogenen Daten für Human Capital Services“ zur Unterschrift vorgelegt. Darin hieß es unter anderem:

> *„Im Rahmen der Erbringung von Dienstleistungen für Sie und Ihren Arbeitgeber kann es zur Verarbeitung Ihrer personenbezogenen Daten durch WPG kommen. In Verbindung mit der ordnungsgemäßen Erstellung von Steuererklärungen kann dies auch sensible personenbezogene Daten umfassen, wie etwa rassische oder ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, physische oder geistige Gesundheit, Sexualleben, Strafverfahren, Sozialversicherungsnummer oder andere vom Staat zugewiesene Identifikationsnummern sowie Informationen zu Bankkonten.“*

Ein betroffener Mitarbeiter vermisste in der Einverständniserklärung hinreichend konkrete Angaben dazu, welche seiner sensiblen Daten im Einzelnen erhoben und verarbeitet werden und bat die Aufsichtsbehörde um eine Überprüfung.

Wir stellten fest, dass die verwendete „Einverständniserklärung“ nicht den inhaltlichen Anforderungen des § 4 a Absatz 1 Satz 2 sowie Absatz 3 BDSG für eine informierte Einwilligung entsprach. Danach ist der Betroffene vor Erteilung seiner Einwilligung auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen. Soweit besondere Arten personenbezogener Daten erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen. Aus der „Einverständniserklärung“ wurde für die Betroffenen nicht hinreichend deutlich, welche Daten zu ihrer Person, mit welchem Ziel und zu welchem Zweck verarbeitet werden und welche Folgen dies für sie hat. Unabdingbar ist dabei, dass die von § 4 a Absatz 1 Satz 2 und Absatz 3 BDSG vorgeschriebenen Informationen dem Betroffenen vollständig vor Unterzeichnung der Einwilligungserklärung zur Verfügung gestellt werden. Außerdem wurde das Unternehmen und die WPG darauf hingewiesen, dass es im Hinblick auf das Freiwilligkeitserfordernis der Einwilligung dem betroffenen Mitarbeiter freistehen müsse, seine Steuererklärung selbst zu erstellen bzw. eine Person oder Stelle seiner eigenen Wahl damit zu beauftragen oder das Angebot der Erstellung durch die WPG anzunehmen. In Bezug auf die zur Erfüllung der steuerrechtlichen Verpflichtungen des Unternehmens erforderlichen Daten des Arbeitnehmers muss diesem zudem die Möglichkeit eingeräumt werden, diese Daten dem Unternehmen auch unmittelbar zur Verfügung zu stellen beziehungsweise stellen zu lassen.

Die WPG hat ihr Verfahren daraufhin geändert. In einem Beratungsgespräch erläutern Mitarbeiter der WPG dem ausreisewilligen Mitarbeiter des Unternehmens zunächst, welche Daten zu welchem Zweck erhoben werden

und mit welchen Stellen diese Daten ausgetauscht werden sollen. Nach Unterzeichnung einer Einwilligungserklärung werden die benötigten Daten sodann im Gespräch erhoben. Auf Wunsch des Beschäftigten werden ihm vor Unterzeichnung der Einwilligungserklärung Informationsblätter ausgehändigt, in denen die Datenerhebung und der Datenaustausch bei der steuerlichen Beratung ausführlich dargestellt werden. Dort wird unter anderem auch erläutert, aus welchen Gründen besondere Arten personenbezogener Daten für die Erbringung der steuerlichen Beratungsleistungen erforderlich sein können und um welche Daten es dabei im Einzelnen geht. So kann die Abfrage der Staatsangehörigkeit (rassische und ethnische Herkunft) zur Feststellung des anzuwendenden Besteuerungsrechts erforderlich sein. Ebenso können Mitgliedsbeiträge und Spenden an politische Parteien (politische Meinungen) sowie die Zugehörigkeit zu einer Kirche (religiöse und philosophische Überzeugungen) oder Spenden an Gewerkschaftsorganisationen (Gewerkschaftszugehörigkeit) und Krankheitskosten (Gesundheitsdaten) – letztere wegen ihrer möglichen Absetzbarkeit als außergewöhnliche Belastungen – für die Erstellung einer Steuererklärung bedeutsam sein.

4. Datenübermittlung in die USA zur Vorbereitung einer Mitarbeiterbefragung

Ein Unternehmen in unserem Zuständigkeitsbereich teilte uns mit, dass seine nach „Safe Harbor“ (siehe dazu den Beitrag im 1. Teil, Nr. 3.3.3) zertifizierte Konzernmutter in den USA durch einen externen Dienstleister (ebenfalls mit Sitz in den USA) eine konzernweite Mitarbeiterbefragung zur Messung der Zufriedenheit der Mitarbeiter am Arbeitsplatz durchführen lassen wolle. Die Teilnahme an der Befragung sollte für die Mitarbeiter freiwillig sein. Zur Vorbereitung der Umfrage hatte das Mutterunternehmen („A“) das deutsche Tochterunternehmen („B“) aufgefordert, Personaldaten aller Mitarbeiter zu übermitteln. Diese Daten wollte das Mutterunternehmen an den mit der Durchführung der Umfrage beauftragten Dienstleister weitergeben, welcher sodann den Mitarbeitern über ihre geschäftliche E-Mail-Adresse einen persönlichen Zugangscode zukommen lassen sollte. Mit Hilfe dieses Zugangscodes konnten die Mitarbeiter online einen Fragebogen ausfüllen. Dem die Befragung durchführenden Dienstleister sollte bei der Auswertung der ausgefüllten Online-Fragebögen die Identität des jeweiligen Teilnehmers bekannt sein. Vor der Weitergabe an die Konzernmutter sollten die Ergebnisse der Befragung jedoch in der Weise aufbereitet werden, dass lediglich Gruppenergebnisse ab einer Mindestzahl von fünf Personen pro Gruppe dargestellt werden.

Zur Übermittlung personenbezogener Beschäftigtendaten an die Konzernmutter existierte in dem Unternehmen eine „Regelungsabrede“ zwischen der Geschäftsleitung und dem Betriebsrat. Diese enthielt nach einem Verweis auf die Bestimmungen des Bundesdatenschutzgesetzes sowie des Safe Harbor-Abkommens folgende Regelung:

> *„Die personenbezogenen Daten, welche an „A“ übermittelt werden, dienen allein der Erfüllung von geschäftlichen Zwecken zwischen „B“ und „A“. Es dürfen keine Daten übermittelt werden, die über die Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen hinausgehen. Die der Übermittlung an „A“ zugänglichen personenbezogenen Daten sind: …“*

Sodann wurden ca. 40 personenbezogene Datenkategorien (z. B. Vor- und Nachname, Personalnummer, betriebliche Position und E-Mail-Adresse, Kostenstelle, Organisationseinheit, Familienstand, Kinderanzahl, Urlaubszeiten) aufgezählt. Darauf folgte folgender Hinweis:

> *„Falls weitere personenbezogenen Daten zur Übermittlung von „A“ bei „B“ angefragt werden, wird die Geschäftsleitung einen vom Betriebsrat benannten Beauftragten umgehend und unaufgefordert über den Inhalt der angefragten Daten vorab informieren. Mit dessen Einverständnis kann eine Übermittlung der Daten stattfinden.“*

Das Unternehmen fragte bei uns an, unter welchen Voraussetzungen nunmehr eine Übermittlung von Beschäftigtendaten an das Mutterunternehmen zur Vorbereitung der Mitarbeiterbefragung erfolgen könne.

Da das deutsche Datenschutzrecht kein Konzernprivileg kennt, ist der Austausch von Arbeitnehmerdaten zwischen verschiedenen konzernangehörigen Unternehmen oder zwischen der Konzernmutter und konzernangehörigen Firmen als Übermittlung anzusehen, die gemäß § 4 Absatz 1 BDSG nur zulässig ist, wenn das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift es erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Betriebs- und Dienstvereinbarungen können zwar als vorrangige Erlaubnisnormen im Sinne von § 4 Absatz 1 BDSG angesehen werden. Betriebsvereinbarungen können jedoch den Datenschutz gegenüber dem Bundesdatenschutzgesetz nicht einschränken. Sie können davon nur soweit abweichen, wie sie dem dort festgeschriebenen Datenschutzniveau im Ergebnis entsprechen, allerdings mindestens so weitreichend sind. Daraus folgt, dass eine Betriebsvereinbarung nicht dazu dienen kann, eine Datenübermittlung zu rechtfertigen, die aufgrund der gesetzlichen Erlaubnistatbestände des Bundesdatenschutzgesetzes nicht zulässig ist. Würde eine Betriebsvereinbarung im Interesse eines einheitlichen konzerninternen Datenverkehrs mehr gestatten als das Bundesdatenschutzgesetz, so wären diese Regelungen regelmäßig unwirksam.

Gemäß § 32 Absatz 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Ein konzerninterner Personaldatenfluss ist nur dann für die Durchführung eines Beschäftigungsverhältnisses erforderlich, wenn dieses Konzernbezug aufweist, etwa weil der Mitarbeiter sich zu einem konzernweiten Einsatz bereiterklärt oder verpflichtet hat. Darüber hinaus kann die Übermittlung von Arbeitnehmerdaten an die Konzernmuttergesellschaft zulässig sein, soweit sie zur Wahrung berechtigter Interessen der Tochtergesellschaft (§ 28 Absatz 1 Nr. 2 BDSG) oder der Konzernmuttergesellschaft (§ 28 Absatz 2 Nr. 2 BDSG) erforderlich ist. Dabei ist jedoch zu berücksichtigen, dass das Streben nach einem einheitlichen Personalmanagement innerhalb eines Konzerns und der Wunsch nach einer konzernweiten Personalsteuerung für sich genommen die konzerninterne Übermittlung von Personaldaten nicht rechtfertigen können, da dies auf eine Einführung des vom Gesetzgeber gerade nicht gewollten Konzernprivilegs hinauslaufen würde. Grundsätzlich muss jedes einem Konzern angehörende, rechtlich selbstständige Unternehmen sein Personal selbst verwalten. Unabhängig davon, welche Rechtsgrundlage man anwendet, ist dem Grundsatz der Erforderlichkeit stets Rechnung zu tragen.

Davon ausgehend konnten wir nicht feststellen, dass die Übermittlung der Daten sämtlicher Arbeitnehmer an die Muttergesellschaft zur Vorbereitung der freiwilligen Mitarbeiterbefragung tatsächlich erforderlich war. Vielmehr wäre eine Information der Mitarbeiter über die Möglichkeit der Teilnahme an der freiwilligen Online-Befragung verbunden mit der Aufforderung, bei Interesse den erforderlichen Zugangscode anzufordern, ausreichend gewesen. Auf diese Weise hätten das Mutterunternehmen und der die Befragung durchführende Dienstleister zumindest von den Mitarbeitern, die sich nicht zu der Teilnahme an der Befragung entschlossen hätten, keine personenbezogenen Daten erhalten.

Hinzu kommt, dass eine arbeitsrechtliche Nebenpflicht zur Teilnahme an Mitarbeiterbefragungen zur Feststellung der Zufriedenheit der Mitarbeiter grundsätzlich nicht besteht. Somit kann ein Arbeitgeber die Erhebung personenbezogener Daten seiner Mitarbeiter im Rahmen einer Mitarbeiterbefragung grundsätzlich nicht auf § 32 und § 28 Absatz 1 Nr. 2 bzw. § 28 Absatz 2 Nr. 2 a BDSG, sondern nur auf eine Einwilligung der Mitarbeiter stützen.

Eine Einwilligung gemäß § 4 a BDSG als Rechtfertigungsgrundlage ist in dem Fall, in dem die Daten bei der Befragung durch einen Dritten im Auftrag des Arbeitgebers erhoben werden sollen, dann unproblematisch, wenn die Freiwilligkeit der Teilnahme gewährleistet ist, also wenn die Mitarbeiter von der Teilnahme absehen können, ohne Nachteile seitens ihres Arbeitge-

bers befürchten zu müssen. Davon kann zumindest immer dann ausgegangen werden, wenn der Arbeitgeber nicht erfährt, welche Mitarbeiter an der Befragung teilgenommen haben und welche nicht. Daraus folgt, dass dem Arbeitgeber das Ergebnis der Mitarbeiterbefragung nur in einer Form zur Verfügung gestellt werden darf, die keine Rückschlüsse auf die Teilnahme bestimmter Arbeitnehmer oder die von diesen gemachten Angaben zulässt.

Der in der Regelungsabrede vorgesehene Übermittlungsausschluss für alle Daten, „die über die Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen hinausgehen“, war in unseren Augen zu unbestimmt. Wir haben das Unternehmen daher um eine Konkretisierung gebeten. Die Regelung, wonach weitere Mitarbeiterdaten mit Einverständnis einer vom Betriebsrat beauftragten Person übermittelt werden können, war zumindest insoweit missverständlich, als der Eindruck entstehen könnte, die Erklärung des Beauftragten des Betriebsrats erweitere die von §§ 32 und 28 BDSG gezogenen Grenzen der zulässigen Übermittlung von Mitarbeiterdaten an das Mutterunternehmen.

5. Dürfen Mitarbeiterdaten mit „Antiterrorlisten“ abgeglichen werden?

Vermutlich will kein Arbeitgeber gerne einen Terroristen oder jemanden beschäftigen, der unter Terrorverdacht steht. Kein Wunder, dass nach den Anschlägen vom 11. September 2001 verstärkte Anstrengungen unternommen wurden, um verdächtigen „Schläfern“ auch in der Arbeitswelt auf die Spur zu kommen. Als Instrument sollen dabei die sogenannten Antiterrorlisten der EU und der Vereinten Nationen zum Einsatz kommen. Ob diese tatsächlich einen nennenswerten Beitrag zur Verhinderung einschlägiger Straftaten leisten können, ist nach wie vor umstritten. Immerhin müssen die Betroffenen mittlerweile aufgrund der Verordnung (EU) 1286/2009 von der EU-Kommission über ihre Aufnahme in die Liste unterrichtet werden und können hierzu auch eine Gegenäußerung abgeben, die dann dem Sanktionsausschuss der Vereinten Nationen zugeleitet wird. Was dort damit geschieht, ist von hier aus ebenso schwer zu beurteilen wie die Frage, wie man überhaupt auf die Liste geraten kann. In der Praxis besteht unabhängig davon eine erhebliche Unsicherheit, wer unter welchen Voraussetzungen einen Datenabgleich mit den Antiterrorlisten vornehmen darf oder gar muss. In Bezug auf die Arbeitswelt halten die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) einen Abgleich von Mitarbeiterdaten mit „Antiterrorlisten“ durch Unternehmen auf Grundlage von Artikel 2 der Verordnung (EG) Nummer 881/2002 und Artikel 2 der Verordnung (EG) Nummer 2580/2001 für unzulässig. In ihrem Beschluss vom 24. April 2009 begründen sie dies damit, dass Unternehmen für einen automatisierten Abgleich ihrer Mitarbeiter mit Listen, die terrorverdächtige Personen und Organisationen enthalten, nur solche Listen verwenden dürfen, für die eine Rechtsgrundlage vorliegt. Die genannten Verordnungen würden aber dem rechtsstaatlichen Bestimmtheitsgebot nicht genügen. Soweit es auf eine Interessenabwägung ankomme, würden die schutzwürdigen Interessen der von einem Datenabgleich betroffenen Mitarbeiter überwiegen. Nicht zuletzt bestünden Zweifel an der Rechtsstaatlichkeit des Zustandekommens der Listen und unzureichende Rechtschutzmöglichkeiten. Nach einer mit den übrigen Bundesressorts abgestimmten Mitteilung des Auswärtigen Amts gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind Unternehmen und andere Wirtschaftsbeteiligte rechtlich nicht zu einem systematischen, anlassunabhängigen Abgleich ihrer Kunden- und Mitarbeiterdaten verpflichtet. Aufgrund des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes bestehe diese Pflicht ausschließlich nach Maßgabe von Sorgfaltspflichten.

Leider sind die sich aus dieser Auskunft ergebenden Konsequenzen für die Praxis weiterhin unklar. Unzulässig dürfte es auf jeden Fall sein, systematisch, flächendeckend und anlassunabhängig die Daten aller Mitarbeiter mit den „Antiterrorlisten“ abzugleichen. Ein Abgleich ist allenfalls dann zulässig, wenn der Dienstherr oder Arbeitgeber im Einzelfall einen konkreten Verdacht hat, dass ein Mitarbeiter zu dem Personenkreis gehört, der in den „Antiterrorlisten“ aufgeführt ist. Soweit Sorgfaltspflichten einen Abgleich gebieten, ist das zu beachten.

6. Compliance-Ermittlungen

Große Unternehmen sind der Gefahr der Werksspionage ausgesetzt. Aber auch in ihren eigenen Reihen kann es Mitarbeiter geben, die dem Unternehmen Schaden zufügen. Es ist das gute Recht eines Unternehmens, sich gegen solche Bestrebungen zur Wehr zu setzen. Soweit dabei sensible personenbezogene Daten der Mitarbeiter oder Dritter erhoben, verarbeitet und genutzt werden, sind strenge datenschutzrechtliche Vorgaben und der Grundsatz der Verhältnismäßigkeit zu beachten. Um diesen Anforderungen Rechnung zu tragen und um die jeweilige Prozedur für die Beschäftigten transparent zu machen, erlassen große Unternehmen sog. Compliance-Richtlinien.

Ein Großkonzern hatte ein solche Richtlinie, mit deren Hilfe bei den einzelnen Konzerngesellschaften erhebliche Verstöße gegen arbeitsvertragliche Pflichten und Straftaten von Mitarbeitern aufgeklärt werden sollen, erarbeitet und der Datenschutzbehörde zur Überprüfung und Beratung vorgelegt. Nach diesem Konzept sollen auf der Konzernebene, aber auch bei den Einzelgesellschaften Institutionen geschaffen werden, die über speziellen kriminalistischen Sachverstand und entsprechende Aufklärungsmöglichkeiten verfügen. Teilweise sollen diese Stellen auch Ermittlungsaufgaben in anderen Konzerngesellschaften wahrnehmen.

Nach § 33 Absatz 1 Satz 1 BDSG und nach der arbeitsgerichtlichen Rechtsprechung ist der Arbeitgeber berechtigt, Arbeitnehmerdaten zu erheben, zu verarbeiten und zu nutzen, soweit dies erforderlich ist, um ein vertragswidriges Verhalten des Mitarbeiters aufzuklären und zu sanktionieren, wenn der Verdacht einer nicht unerheblichen Arbeitsvertragsverletzung besteht. Für die Abklärung von Straftaten lässt dies § 32 Absatz 1 Satz 2 BDSG zu, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat und die Ermittlungsmaßnahmen nicht unverhältnismäßig sind. Stichprobenweise, verdachtsunabhängige prophylaktische Kontrollmaßnahmen ohne Wissen des Arbeitnehmers – etwa in Bereichen, wo Großaufträge vergeben oder mit Betriebsgeheimnissen umgegangen wird – sind jedoch nicht zulässig und sollen auch durch das zu erwartende Arbeitnehmerdatenschutzgesetz künftig nicht ermöglicht werden.

Grundsätzlich dürfen Personaldaten nur von den Mitarbeitern eines Unternehmens erhoben, verarbeitet und genutzt werden, die gegenüber dem betroffenen Arbeitnehmer aufsichtspflichtig oder weisungsberechtigt sind oder die für diesen Personalentscheidungen vorzubereiten oder zu treffen haben. Zur Gewährleistung der Vertraulichkeit von Personalangelegenheiten sollte die Zahl dieser Personen so begrenzt wie möglich gehalten werden. Das gilt insbesondere für die in Rede stehenden sensiblen Aufklärungsmaßnahmen.

Mit derartigen Compliance-Ermittlungen kann aber auch eine dafür besonders befähigte und zuverlässige Stelle außerhalb der jeweiligen Gesellschaft, bei der der Verdächtige beschäftigt ist, beauftragt werden. Datenschutzrechtlich handelt es sich dabei um eine sogenannte Funktionsübertragung, da diese Stellen eigenständige Entscheidungen über das Vorgehen bei den Ermittlungen, wohl aber immer im Auftrag und nach Absprache mit der Beschäftigungsstelle, treffen. Das bedeutet, dass die jeweilige Beschäftigungsgesellschaft mit allen Stellen, die außerhalb ihres Unternehmens angesiedelt und an der Compliance-Prozedur beteiligt sind, vertragliche Absprachen treffen muss, die einen an § 11 BDSG orientierten Datenschutzstandard gewährleisten. Dies gilt selbst dann, wenn es sich bei der beauftragten Stelle um eine andere Gesellschaft des Konzerns, zu dem auch die Beschäftigungsgesellschaft des Betroffenen gehört, handelt. Jede Konzerngesellschaft und die Konzernmutter sind datenschutzrechtlich im Verhältnis zueinander „Dritte“. Die maßgeblichen Entscheidungen, ob ein Compliance-Verfahren eingeleitet bzw. fortgeführt wird und ob nach dessen Beendigung Personalmaßnahmen gegenüber dem Betroffenen ergriffen werden, dürfen nur dessen Vorgesetzte treffen. Die Compliance-Ermittler können daran allenfalls beratend mitwirken. Hat sich ein Verdacht nicht bestätigt, muss der Betroffene im Nachhinein von den Ermittlungen informiert werden.

Problematisch ist die Beteiligung von Betriebsratsmitgliedern in den Gremien, die in dem Compliance-Verfahren vorgesehen sind. Betriebsratsmitglieder sollten grundsätzlich nicht in Ermittlungsmaßnahmen des Arbeitgebers gegen einen Arbeitnehmer hineingezogen werden, jedenfalls nicht von vornherein. Der Betriebsrat hat in erster Linie die Interessen der Beschäftigten zu vertreten, also diese sozusagen zu verteidigen. Das bedeutet, dass ein Betriebsratsmitglied nur dann am Compliance-Verfahren mitwirken darf, wenn es vom Betroffenen ausdrücklich darum gebeten wird. Dagegen sollte der betriebliche Datenschutzbeauftragte stets in das Verfahren mit eingebunden werden, nicht zuletzt um sicherzustellen, dass die einzelnen Ermittlungsschritte dem Grundsatz der Verhältnismäßigkeit genügen. So darf etwa die Kontrolle des E-Mail-Verkehrs eines Mitarbeiters nicht erfolgen, wenn sich der Verdacht auch in einem Gespräch mit dem Betroffenen abklären lässt.

Für jede Stelle, die an dem Compliance-Verfahren beteiligt ist, muss es zudem eine Datenlöschkonzeption geben, in der geregelt wird, wie lange die dort angefallenen personenbezogenen Daten zu welchem Zweck vorgehalten werden dürfen beziehungsweise wann sie gelöscht werden müssen.

Das Unternehmen wird sein mit meiner Dienststelle abgestimmtes Compliance-Verfahren ein halbes Jahr lang testen. Dann wird geprüft werden, ob gegebenenfalls Änderungen erforderlich sind.

Compliance-Konzeptionen müssen sowohl den Interessen des Betriebes, nicht ausspioniert oder in sonstiger Weise geschädigt zu werden, als auch den schutzwürdigen Belangen der Arbeitnehmer, nicht zu Unrecht beziehungsweise mit unverhältnismäßigen Mitteln am Arbeitsplatz überwacht zu werden, gerecht werden.

7. Erhebung und Speicherung der Standortdaten von Dienstfahrzeugen mittels Ortungssystemen

Für eine Firma mag es praktisch sein, immer zu wissen, wo sich ihre Mitarbeiter im Außendienst gerade aufhalten. Allerdings ist dies datenschutzrechtlich nur unter engen Voraussetzungen zulässig.

Durch die Beschwerde eines Betroffenen wurde die Aufsichtsbehörde im Sommer 2010 auf ein Unternehmen mit mehreren Niederlassungen in ganz Deutschland aufmerksam, das seinen Service-Technikern sowie den Mitarbeitern des Vertriebs mit überwiegender Tätigkeit im Außendienst (Verkäufern) Dienstwagen zur Verfügung stellte. Während die Fahrzeuge den Service-Technikern nur für Außendiensteinsätze zur Verfügung gestellt wurden, war den Verkäufern und ihren Ehepartnern oder Lebensgefährten auch die private Nutzung der Dienstwagen gestattet. In jedem Dienstwagen war neben einem Navigationsgerät auch eine Telematik-Rechnereinheit mit GPS-Empfänger und Mobilfunkmodul zur Übertragung der Positionsdaten in Echtzeit an ein webbasiertes Portal eingebaut. Das webbasierte Portal wurde von einem EDV-Dienstleister im Auftrag des Unternehmens betrieben. In dem Portal konnte der jeweilige Standort der Fahrzeuge von allen Vorgesetzten des betreffenden Fahrers sowie dem örtlichen Betriebsrat eingesehen werden (sog. Life-Ortung). Außerdem wurden dort Datum, Uhrzeit und Aufenthaltsort zu Beginn und am Ende jeder Einzelfahrt (mit Ausnahme des ersten und letzten täglichen Aufenthaltsorts) sowie der jeweilige Kilometerstand des Fahrzeugs gespeichert (sog. Fahrtenbuch). Die Eintragungen im Fahrtenbuch wurden 90 Tage gespeichert und konnten in dieser Zeit vom jeweiligen Fahrer eingesehen werden. Die Fahrtenbücher von Service-Technikern konnten bei Kundenreklamationen, beim Bestehen konkreter Anhaltspunkte für missbräuchliches Verhalten sowie für eine Stichprobenkontrolle auch vom jeweiligen Vorgesetzten eingesehen werden. All dies war in einer Konzernbetriebsvereinbarung geregelt.

Das Unternehmen erhob die Daten, um dispositive Entscheidungen auf Basis aktueller Positionsdaten treffen und den Nachweis abrechnungsfähiger Fahrten und der alleinigen dienstlichen Nutzung der von Service-Technikern genutzten Fahrzeuge führen zu können. Verkäufer sollten außerdem in die Lage versetzt werden, ihre private Steuerlast zu optimieren. Daneben

diente die Datenerhebung auch der Verhaltens- und Missbrauchskontrolle der Service-Techniker. Beim Vorliegen konkreter Anhaltspunkte dafür, dass ein Mitarbeiter das in ihn gesetzte Vertrauen missbraucht oder eine Straftat begangen hatte, sollte der jeweilige Vorgesetzte im Beisein des Betriebsrats das Fahrtenbuch auswerten dürfen. Zudem war eine Stichprobenkontrolle in der Form vorgesehen, dass durch das Los quartalsweise ein Untersuchungszeitraum von maximal 72 Stunden festgelegt werden sollte, für den die Fahrtenbucheinträge aller Außendienstmitarbeiter durch ihre jeweiligen Vorgesetzten auf Unregelmäßigkeiten in Bezug auf die Angaben zur Arbeitszeit oder eine außergewöhnliche Höhe der zurückgelegten Kilometer durchgesehen werden sollten.

Das in den Fahrzeugen befindliche Navigationsgerät bot für Privatfahrten die Möglichkeit, einen Privatmodus einzustellen. Allerdings wurden auch im Privatmodus Positionsdaten, Zeiten und Kilometerstände an den Server übertragen und im Fahrtenbuch gespeichert. Die im Privatmodus übertragenen Echtzeit-Positionsdaten wurden im webbasierten Portal jedoch nicht angezeigt und die entsprechenden Fahrtenbucheinträge waren ausschließlich für den jeweiligen Fahrer einsehbar.

Der im 1. Teil, Nr. 2.3.2 erwähnte Gesetzentwurf der Bundesregierung (BR-Drucksache 535/10) sieht in § 32 g BDSG-E vor, dass Arbeitgeber Beschäftigtendaten mittels Ortungssystemen nur in drei Fallgruppen erheben, verarbeiten und nutzen dürfen: Der Einsatz von Ortungssystemen ist danach zulässig, soweit dies aus betrieblichen Gründen zur Sicherheit des Beschäftigten oder zur Koordinierung des Einsatzes des Beschäftigten erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interesse des Beschäftigten am Ausschluss der Datenerhebung, -verarbeitung oder -nutzung überwiegen. Eine Erhebung ist allerdings nur während der Arbeitszeit des Beschäftigten zulässig. Außerdem muss der Arbeitgeber den Einsatz des Ortungssystems für den Beschäftigten erkennbar machen und ihn über den Umfang der Aufzeichnungen und deren regelmäßige oder im Einzelfall vorgesehene Auswertung informieren. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks der Speicherung nicht mehr erforderlich sind oder schutzwürdige Interessen des Beschäftigten einer weiteren Speicherung entgegenstehen. § 32 g BDSG-E gestattet außerdem den Einsatz von Ortungssystemen durch Arbeitgeber zum Schutz beweglicher Sachen. Eine Ortung des Beschäftigten darf in diesem Fall nicht erfolgen, solange der Beschäftigte die bewegliche Sache erlaubterweise nutzt oder diese sich erlaubterweise in seiner Obhut befindet.

Auf der Grundlage des geltenden Rechts war der Vorgang datenschutzrechtlich so zu bewerten:

Datum, Uhrzeit und genaue Position zu Beginn und Ende der mit den Dienstfahrzeugen zurückgelegten Einzelfahrten sowie der entsprechende Kilometerstand sind personenbezogene Daten der jeweiligen Fahrer. Da dem Unternehmen bekannt war, welcher ihrer Mitarbeiter den jeweiligen Dienstwagen benutzt hat, konnte es die erhobenen Informationen einzelnen Mitarbeitern zuordnen. Indem die in den Fahrzeugen installierte GPS-Einheit Positions- und Zeitangaben an einen Server übertrug und die Daten dort gespeichert wurden, erhob und speicherte das Unternehmen diese Daten. Dies galt unabhängig davon, ob oder in welchem Umfang das Unternehmen sich von dem Dienstleister, der den Server im Auftrag des Unternehmens betrieb, Zugriffsrechte auf die Daten hatte einräumen lassen. Denn das Unternehmen musste sich das Wissen und Verhalten des Dienstleisters – seines Auftragsdatenverarbeiters – wie eigenes Verhalten zurechnen lassen.

Der Einsatz des Ortungssystems war an §§ 32 und 28 Absatz 1 Satz 1 Nr. 2 BDSG zu messen. Gemäß § 32 Absatz 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Durchführung eines Beschäftigungsverhältnisses erforderlich sind alle Daten, die der Arbeitgeber zur Erfüllung seiner Pflichten und zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt.

Gemäß § 28 Absatz 1 Satz 1 Nr. 2 BDSG ist das Erheben, Speichern oder Nutzen personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrnehmung 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. § 28 Absatz 1 Satz 1 Nr. 2 BDSG ist neben § 32 BDSG anwendbar, wenn ein Arbeitgeber Beschäftigtendaten erhebt, die er nicht zur Erfüllung seiner Pflichten oder zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer benötigt.

Neben § 32 und § 28 BDSG waren § 4 Absatz 2 BDSG sowie § 3 a BDSG zu beachten. Gemäß § 4 Absatz 2 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Gemäß § 3 a BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Davon ausgehend sah die Aufsichtsbehörde die Übertragung von Echtzeitpositionsdaten („Life-Ortung“) der Fahrzeuge von Service-Technikern als zulässig an. Arbeitgeber, die Mitarbeiter im Außendienst einsetzen, haben ein berechtigtes Interesse daran, jederzeit erfahren zu können, wo sich ihre Außendienstmitarbeiter während der Arbeitszeit befinden, um deren Einsatz dirigieren zu können. Die Übermittlung der Positionsdaten von Firmenfahrzeugen während der Arbeitszeit der Fahrzeugführer mittels eines GPS-Systems an den Arbeitgeber ist ein geeignetes Mittel zu diesem Zweck (vgl. hierzu den Fünften Tätigkeitsbericht des Innenministeriums, Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, 2009, B 1.9). Eine Speicherung der Standortdaten lässt sich damit aber allenfalls für kurze Zeit begründen. Denn nach Erhalt neuer aktueller Standortdaten wird die frühere Position des Dienstfahrzeugs nicht mehr benötigt, um den Einsatz des Außendienstmitarbeiters zu dirigieren. Spätestens zu diesem Zeitpunkt sind die alten Positionsdaten daher umgehend zu löschen. Die aktuellen Positionsdaten der von Außendienstmitarbeitern eingesetzten Dienstfahrzeuge dürfen im Betrieb des Arbeitgebers allen Stellen zugänglich gemacht werden, die diese zur ordnungsgemäßen Wahrnehmung ihrer Funktion benötigen. Der Betriebsrat zählt hierzu nicht.

Für zulässig erachtete die Aufsichtsbehörde auch die Speicherung der Wegezeiten von Service-Technikern zum Nachweis abrechnungsfähiger Fahrten, um bei Kundenreklamationen eine Überprüfung zu ermöglichen. Ist ein Arbeitgeber berechtigt, An- und Abfahrtszeiten seiner Mitarbeiter den Kunden, bei denen der Mitarbeiter tätig ist, nicht nur in Form einer Pauschale, sondern nach tatsächlichem Aufwand in Rechnung zu stellen, kann er dies zwar auch auf der Grundlage mündlicher oder schriftlicher Auskünfte des Mitarbeiters zu den Fahrzeiten tun. Bestreitet der Kunde die Angaben des Mitarbeiters, ist der Arbeitgeber aber unter Umständen gezwungen, seinen Mitarbeiter in einem Zivilprozess als Zeugen zu benennen. Um dem Arbeitgeber in solchen Fällen einen einfachen und sicheren Nachweis der Fahrzeiten zu ermöglichen, ist es gerechtfertigt, wenn der Arbeitgeber Datum, Uhrzeit, Kilometerstand und Position zu Beginn und Ende abrechnungsfähiger Fahrten seiner Mitarbeiter erhebt und speichert, solange mit Reklamationen und Rückfragen des Kunden zur Berechnung der Fahrten normalerweise zu rechnen ist (vgl. hierzu den Fünften Tätigkeitsbericht des Innenministeriums 2009, S. 69 bis 71). Eine Frist von 90 Tagen dürfte noch als angemessen anzusehen sein.

Die Erhebung und Speicherung von Positionsdaten zum Nachweis der dienstlichen Nutzung der Dienstfahrzeuge gegenüber Finanzbehörden wurde hingegen nicht als zulässig angesehen. Abgesehen davon, dass die vorgesehene Speicherfrist von 90 Tagen für diesen Zweck viel zu kurz war, da die Kontrollen von Finanzbehörden sich nur im Ausnahmefall auf die letzten 90 Tage beschränken dürften, ist zum Nachweis der alleinigen dienstlichen Nutzung von Dienstfahrzeugen gegenüber Finanzbehörden ein von jedem Fahrer auszufüllendes herkömmliches Fahrtenbuch ausreichend. Zeiten und Positionsdaten aller Fahrten müssen zu diesem Zweck nicht mittels GPS erhoben und auf einem Server gespeichert werden.

Als unzulässig wurde ferner die von dem Unternehmen vorgesehene Verhaltens- und Missbrauchskontrolle seiner Service-Techniker angesehen, weil einer Nutzung der Daten für diesen Zweck ohne konkrete Anhaltspunkte für ein Fehlverhalten im Einzelfall überwiegende Interessen des betroffenen Mitarbeiters entgegenstehen und § 32 Absatz 1 Satz 1 BDSG aus diesem Grund als Rechtsgrundlage für die Datenerhebung, -speicherung und -nutzung ausscheidet. Anhand der Eintragungen des elektronischen Fahrtenbuchs konnte ein Bewegungsprofil der Dienstwagen erstellt und ermittelt werden, wann und wo die jeweiligen Außendienstmitarbeiter mit dem Fahrzeug unterwegs waren. Damit war unter Umständen der Nachweis möglich, dass ein Mitarbeiter das Fahrzeug während der Arbeitszeit zu Privatfahrten benutzt, eine dienstliche Fahrt nicht oder anders als vorgegeben durchgeführt oder seine Arbeitszeit falsch abgerechnet hatte.

Ein Arbeitgeber ist zwar berechtigt, seine Mitarbeiter in angemessener Weise zu überwachen. Die abstrakte Möglichkeit, dass einzelne Mitarbeiter das in sie gesetzte Vertrauen missbrauchen, rechtfertigt jedoch keine dauerhafte Totalüberwachung sämtlicher Mitarbeiter. Die Erhebung und Speicherung von Zeit- und Positionsdaten aller mit einem Dienstfahrzeug unternommenen Einzelfahrten zum alleinigen Zwecke der Aufdeckung oder des Nachweises einer missbräuchlichen Verwendung des Fahrzeuges oder sonstigen Fehlverhaltens von Mitarbeitern ist daher allenfalls vorübergehend zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass der Fahrer des Dienstfahrzeugs bei seiner beruflichen Tätigkeit Straftaten oder vergleichbare Verfehlungen begangen hat oder begehen wird, die Datenerhebung und Speicherung zu deren Verhinderung oder Aufklärung unabdingbar erforderlich ist und das schutzwürdige Interesse des Beschäftigten am Unterbleiben der Datenerhebung nicht überwiegt, etwa weil die damit verbundene Verletzung des Persönlichkeitsrechts des Betroffenen in keinem Verhältnis zu dem angerichteten oder zu erwartenden Schaden steht. Nur wenn im Einzelfall tatsächliche Anhaltspunkte dafür bestehen, dass ein bestimmter Außendienstmitarbeiter das in ihn gesetzte Vertrauen missbraucht (hat) und die Erhebung von Zeit- und Positionsdaten einzelner Fahrten eines Dienstfahrzeugs geeignet ist, den Verdacht auszuräumen oder zu bestätigen, darf der Arbeitgeber entsprechende Daten erheben, nutzen und bis zur endgültigen Klärung des Verdachts speichern. Das von dem Unternehmen vorgesehene Stichprobenkontrollverfahren genügte diesen Vorgaben nicht und war daher einzustellen. In diesem Zusammenhang wurde das Unternehmen auf § 32 d Absatz 3 des Entwurfs eines Gesetzes zur Regelung des Beschäftigtendatenschutzes verwiesen. Danach sind Arbeitgeber künftig ohne konkreten Anfangsverdacht im Einzelfall lediglich zu einem automatisierten Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form befugt. Allenfalls in dieser Form hätte man sich die von dem Unternehmen beabsichtigte Stichprobenkontrolle vorstellen können.

Auf die Fahrtenbücher von Fahrzeugen, die Verkäufern und deren Ehepartnern zur dienstlichen und privaten Nutzung überlassen wurden, hatte das Unternehmen keinen Zugriff. Diese Daten konnten nur vom jeweiligen Fahrer und dem Betreiber des Servers eingesehen werden. Die Erhebung und Speicherung der Wegezeiten der Verkäufer im Fahrtenbuch hatte ausschließlich den Zweck, es den Verkäufern zu ermöglichen, diese Daten bei Bedarf für ihre Einkommenssteuererklärungen zu verwenden. Die Voraussetzungen der §§ 32 und 28 Absatz 1 Nr. 2 BDSG sahen wir für diese Datenerhebung zwar nicht als gegeben an. Denn die Optimierung der privaten Steuerlast ihrer Mitarbeiter ist kein eigenes Interesse des Unternehmens und für die Durchführung der Arbeitsverhältnisse nicht erforderlich. Insoweit

konnte die Datenerhebung und -verarbeitung jedoch durch eine den Anforderungen des § 4 a genügende Einwilligung des jeweiligen Verkäufers gerechtfertigt werden.

Gemäß § 4 a BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Da die Entscheidungsfreiheit eines Arbeitnehmers wegen der für ihn existentiellen Bedeutung eines Arbeitsverhältnisses faktisch eingeschränkt sein kann, scheidet eine Einwilligung als Rechtsgrundlage für eine Erhebung von Mitarbeiterdaten durch den Arbeitgeber mangels Freiwilligkeit in der Regel aus. Freiwillig ist eine Einwilligung nur dann, wenn der Arbeitnehmer seine Zustimmung zur Verarbeitung seiner Daten, ohne Sanktionen oder ungerechtfertigte Nachteile befürchten zu müssen, auch versagen beziehungsweise später wieder zurücknehmen kann. Unter der Voraussetzung, dass die Fahrtenbuchfunktion von den Verkäufern nach Belieben ein- und abgestellt werden kann – wofür ein entsprechender Schalter oder eine vergleichbare Funktion eingerichtet werden musste – handelte es sich um ein Angebot des Unternehmens an seine Mitarbeiter, das diese freiwillig in Anspruch nehmen oder auch nicht nutzen konnten. Dass den Verkäufern Nachteile seitens des Unternehmens gedroht hätten, wenn sie die Fahrtenbuchfunktion nicht nutzten, war nicht ersichtlich, zumal das Unternehmen kein Zugriffsrecht auf diese Daten besaß und daran offenkundig auch kein Interesse hatte.

Die Erhebung und Speicherung von Daten, die bei der zulässigen Nutzung eines Dienstwagens zu privaten Zwecken anfallen, konnte danach durch eine Einwilligung gemäß § 4 a BDSG gerechtfertigt werden, weil die Datenerhebung und -speicherung ausschließlich im Interesse des Arbeitnehmers erfolgte und der Arbeitgeber keinen Zugriff auf die Daten hatte. Für diejenigen Mitarbeiter, die diese Einwilligung nicht erteilten, musste die eingesetzte Hard- oder Software noch um eine Funktion ergänzt werden, die es dem Fahrer ermöglicht, jegliche Datenübertragung an das webbasierte Portal bei Privatfahrten zu unterbinden. Der bislang im Navigationsgerät wählbare Fahrttyp „Privatfahrt“ genügte dieser Vorgabe nicht, da auch im Privatmodus Positionsdaten, Zeiten und Kilometer an den Server übertragen wurden. Das ist ohne eine Einwilligung des Fahrers auch dann unzulässig, wenn das Unternehmen auf diese Daten keinen Zugriff hat, weil bereits die Übertragung und Speicherung der Daten einer Rechtsgrundlage bedarf.

Ergänzend wurde das Unternehmen darauf hingewiesen, dass eine Erhebung von Beschäftigtendaten mittels Ortungssystemen nach geltendem Recht auch in folgenden Fallgruppen zulässig sein kann:

Um die Position eines Dienstfahrzeuges nach einem Diebstahl oder Unfall ermitteln zu können, ist es ausreichend, wenn im Fahrzeug ein GPS-Sender installiert wird, der in einem solchen Fall aktiviert werden kann und dann die Position des Fahrzeugs übermittelt. Die ständige Übertragung der Fahrzeugposition an ein Web-Portal oder die Speicherung von Daten zu einzelnen Fahrten ist für diesen Zweck nicht erforderlich.

Im Außendienst tätige Mitarbeiter müssen ihren Arbeitgeber wahrheitsgemäß über den Beginn und das Ende ihrer Arbeitszeit sowie eingelegte Pausen unterrichten. Hierzu ist zwar grundsätzlich ein Selbstaufschrieb der Arbeitnehmer ausreichend. Wenn Beginn oder Ende der Arbeitszeit mit dem Beginn oder Ende einer Fahrt mit einem Dienst-Pkw zusammenfallen, ist nach geltendem Recht nichts dagegen einzuwenden, wenn der Arbeitgeber wie bei einer elektronischen Zeiterfassung das betreffende Datum mittels technischer Vorkehrungen erhebt und speichert, um die Arbeitszeiten zu dokumentieren.

8. Bei der Videobeobachtung kleine Brötchen backen!

In mehreren Fällen sah sich die Aufsichtsbehörde im nicht-öffentlichen Bereich mit der Videoüberwachung in Bäckereien konfrontiert.

Es begann im ersten Fall mit der alarmierenden Zeitungsschlagzeile im Juli 2009: „Big Brother in der Bäckerei“. Im Mittelpunkt stand die Mitarbeiterüberwachung in einer Großbäckerei. In 32 von 144 Filialen des Unternehmens waren verdeckt Kameras ohne Aufzeichnungsgerät installiert, um in

einem konkreten Verdachtsfall eine Videoüberwachung zur Aufklärung von Straftaten von Mitarbeitern durchführen zu können. Im Verkaufsbereich waren die Kameras so angebracht, dass sie die Verkaufstheken und die dort aufgestellten Kassen, nicht jedoch die Kundschaft im Blick hatten. In rückwärtigen Räumlichkeiten waren Kameras auf den Platz gerichtet, an dem die Mitarbeiter üblicherweise die Kassenabrechnungen vornehmen, sich aber auch umziehen. Wurden der Unternehmensleitung Inventur- und Abrechnungsdefizite bekannt, beauftragte sie Sicherheitsunternehmen, die in der jeweiligen Filiale konkrete Überwachungsmaßnahmen vornahmen, um so Diebstähle, Unterschlagungen und dergleichen aufzuklären. In acht Fällen erfolgten deshalb heimlich Videoaufzeichnungen.

Die Aufsichtsbehörde, die eine Überprüfung vor Ort durchführte, konnte in diesen acht konkreten Fällen, in denen Mitarbeiter mittels Videokameras heimlich überwacht wurden, keinen Verstoß gegen den Datenschutz feststellen. Erhebliche Kassen- oder Warendefizite über einen längeren Zeitraum hatten Anlass für die heimliche Überwachung gegeben, sodass anzunehmen war, dass die Anforderungen der arbeitsgerichtlichen Rechtsprechung an eine Mitarbeiterüberwachung (vgl. unten) erfüllt waren. Ferner ließ sich nicht feststellen, dass Mitarbeiter beim Umkleiden gefilmt wurden. Die Aufsichtsbehörde rügte jedoch die fehlende Durchführung einer Vorabkontrolle vor Beginn der Überwachungsmaßnahmen, die fehlende schriftliche Beauftragung der Sicherheitsunternehmen, die fehlende nachträgliche Unterrichtung der Mitarbeiter nach Abschluss der Überwachungsmaßnahmen sowie die fehlende Bestellung eines Datenschutzbeauftragten. Wegen des letzten Punktes wurde gegen das Unternehmen ein Bußgeld verhängt. Das Unternehmen hat sich kooperativ gezeigt und die festgestellten Datenschutzmängel abgestellt. Ein von dem Unternehmen vorgelegtes Konzept für künftige Videoüberwachungsmaßnahmen zur Aufdeckung von Straftaten hat die Aufsichtsbehörde im Sommer 2010 akzeptiert.

In zwei weiteren Fällen, welche die Aufsichtsbehörde zu untersuchen hatte, wurden die Filialen kleinerer Bäckereiketten offen videoüberwacht. In jeder Filiale waren im Verkaufsraum Kameras angebracht, welche die Verkaufstheke sowie den Kassenbereich erfassten. Dabei gerieten nicht nur die Mitarbeiter, sondern auch die Kunden in den Erfassungsbereich der Kameras. Als Grund für die Videoüberwachung gab eines der Bäckereiunternehmen die Kontrolle der einheitlichen Warenpräsentation in den Theken der Filialen an. Außerdem sollte etwaigen Einbruchsversuchen oder anderen Übergriffen wie Vandalismus oder Belästigungen entgegengewirkt werden. Die andere Bäckerei führte ebenfalls (versuchte) Einbrüche und Belästigungen von Mitarbeitern an. Ferner solle kontrolliert werden, ob die Mitarbeiter unerlaubterweise Backwaren mitnehmen und verkaufte Ware in der Kasse richtig verbuchen. Schließlich wurden Überfälle anderer Geschäfte im Umkreis geltend gemacht.

Die Aufsichtsbehörde hielt die Videoüberwachung in beiden Fällen nicht für zulässig. Hinsichtlich der Überwachung der Mitarbeiter ist zu sagen, dass nach der Rechtsprechung des Bundesarbeitsgerichts die Anfertigung von Videoaufnahmen eines Arbeitnehmers nur zulässig ist, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die Videoüberwachung praktisch die einzig verbleibende Möglichkeit zur Aufklärung oder zur Verhinderung des Missstandes darstellt und insbesondere im Hinblick auf den angerichteten oder zu verhindernden Schaden nicht unverhältnismäßig ist (BAG, Urteil v. 27. März 2003, 2 AZR 51/02). Sämtliche Mitarbeiter ständig unter Generalverdacht zu stellen und deshalb permanent zu überwachen, kann unter keinen Umständen akzeptiert werden. Das Persönlichkeitsrecht schützt den Arbeitnehmer ferner vor einer lückenlosen Überwachung am Arbeitsplatz durch Videoaufnahmen, die ihn einem ständigen Überwachungsdruck aussetzen, dem er sich nicht entziehen kann.

Bei der Beurteilung der Zulässigkeit der Kundenüberwachung ist ebenfalls eine Interessenabwägung zwischen den berechtigten Interessen des Unternehmens und dem informationellen Selbstbestimmungsrecht der Kunden erforderlich. Zu verlangen sind Tatsachen, etwa in der Vergangenheit began-

gene Straftaten, die belegen, dass eine Videoüberwachung erforderlich ist, um beispielsweise solche Straftaten zu verhindern oder aufzuklären. Der pauschale Einsatz von Videoüberwachungstechnik zur Abschreckung potenzieller Täter ist nicht zulässig. Zu fordern ist eine konkrete Gefahrenlage sowie die Vornahme einer Einzelfallprüfung für jede einzelne Filiale. Die betreffenden Bäckereiunternehmen konnten keine Tatsachen vorbringen, die eine Videoüberwachung in dem vorgenommenen Ausmaß gerechtfertigt hätte. Insbesondere die Videobeobachtung des gesamten Verkaufsraumes zur Kontrolle der einheitlichen Warenpräsentation der Auslagen in allen Filialen ist unverhältnismäßig, da eine persönliche Überprüfung vor Ort ein weniger einschneidendes Mittel darstellt, um das Interesse der Bäckerei zu wahren. Unbenommen bleiben den Unternehmen selbstverständlich eine Videoüberwachung außerhalb der Geschäftszeiten, wenn sich niemand in den Ladengeschäften aufhält, sowie eine reine Aufnahme der Waren, ohne dass Kunden oder Mitarbeiter erfasst werden.

Der Videoüberwachung in Ladengeschäften sind enge Grenzen gesetzt. Vor der Installation von Videoüberwachungsanlagen sind die gesetzlichen Voraussetzungen umfassend zu prüfen. In vielen Fällen dürfte eine Vorabkontrolle und damit die Bestellung eines betrieblichen Datenschutzbeauftragten erforderlich sein. Ich gebe jedem Unternehmen den Rat, sich nicht allein auf die Beurteilungen der Sicherheitsunternehmen zu verlassen, die meiner Erfahrung nach häufig viel zu kurz greifen. In Zweifelsfällen besteht auch die Möglichkeit, sich an meine Dienststelle zu wenden.

9. Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung beim konzernweiten Datentransfer

Durch eine Beschwerde wurde die Aufsichtsbehörde auf eine Drogeriemarktkette mit Sitz in Baden-Württemberg aufmerksam, die aus zwölf eigenständigen Gesellschaften besteht. Abgesehen von einer GmbH & Co. KG und einer Ltd. & Co. KG hatten alle Gesellschaften die Rechtsform einer GmbH. Bei der Ltd. & Co. KG waren für die gesamte Unternehmensgruppe tätige zentrale Rechts- und Personalabteilungen angesiedelt. Die Rechtsabteilung erledigte die arbeitsrechtlichen Angelegenheiten der Mitarbeiter der Einzelgesellschaften, machte Regressansprüche gegenüber Dritten im Falle der Schädigung eines Mitarbeiters geltend und verlangte von den Beschäftigten zu viel bezahlte Bezüge für die Zeit zurück, in der die Einzelfirmen nach dem Entgeltfortzahlungsgesetz keine Arbeitsvergütung leisten müssen. Die dafür notwendigen rechtlichen Bewertungen und Entscheidungen traf die Rechtsabteilung eigenständig. Die Personalabteilung führte in elektronischer Form die Personalakten für alle Beschäftigten der Unternehmensgruppe. Auf Anforderung stellte sie den Einzelunternehmen und der Rechtsabteilung der Ltd. & Co. KG die gespeicherten Personaldaten zur Verfügung. Ferner bezahlte sie die Löhne und Gehälter für die gesamte Unternehmensgruppe aus. Auch wurde die Personalabteilung von den Krankenkassen informiert, wenn diese an einen Arbeitnehmer der Unternehmensgruppe Krankengeld leisteten. Die Personalentscheidungen für die Mitarbeiter trafen die jeweiligen Einzelunternehmen.

Für die Mitarbeiter der Ltd. & Co. KG sowie einzelne Führungskräfte einer der GmbHs – dabei handelte es sich um den mit Abstand größten Arbeitgeber der Firmengruppe – gehörte die E-Mail-Nutzung zur Standardausstattung der Büroarbeitsplätze. Der hierfür erforderliche Mail-Server wurde von der Ltd. & Co. KG betrieben. In den Arbeitsverträgen aller Mitarbeiter der Unternehmensgruppe war geregelt, dass das betriebliche EDV-System ausschließlich für dienstliche Zwecke genutzt werden darf. Der Geschäftsführer der Ltd. und Co. KG überprüfte mit Hilfe seines Sekretariats in regelmäßigen Abständen strichprobenweise E-Mails von Beschäftigten der Ltd. & Co. KG und der GmbH auf dem Mail-Server. Damit sollte zum einen die Beachtung des Verbots der privaten E-Mail-Nutzung kontrolliert werden. Außerdem wollte der Geschäftsführer auf diese Weise Informationen darüber gewinnen, ob die Bediensteten der Unternehmensgruppe ihre Aufgaben ordnungsgemäß erledigen.

Schriftliche Vereinbarungen zwischen den Einzelunternehmen und der Ltd. & Co. KG über die Zusammenarbeit mit deren Rechts- und Personalabtei-

lung oder die Bereitstellung der E-Mail-Postfächer gab es nicht. In den Arbeitsverträgen der Beschäftigten mit den Einzelunternehmen war zur Datenverarbeitung durch andere Unternehmen der Firmengruppe nichts geregelt. Auch hatten die Mitarbeiter keine Einwilligungen für die Verarbeitung ihrer personenbezogenen Daten durch ein anderes Unternehmen erteilt.

In datenschutzrechtlicher Hinsicht hat die Aufsichtsbehörde diesen Sachverhalt wie folgt bewertet:

Da es sich bei den zwölf Einzelunternehmen der Unternehmensgruppe um rechtlich selbstständige Gesellschaften und damit jeweils um für die Rechtmäßigkeit der Verarbeitung der Daten ihrer Mitarbeiter selbst verantwortliche Stellen im Sinne des § 3 Absatz 7 BDSG handelte, waren sie im Verhältnis zueinander datenschutzrechtlich „Dritte“, also nicht als Einheit anzusehen. Dabei war es unerheblich, ob die Gesellschaften demselben Konzern angehören beziehungsweise ob eine von ihnen so viele Anteile an einer anderen innehatte, dass sie auf deren Geschäftsführung Einfluss nehmen konnte. Eine Weitergabe personenbezogener Daten von der einen Gesellschaft an eine andere war damit nur zulässig, wenn entweder eine Auftragsdatenvereinbarung vereinbart worden war oder die Voraussetzungen der für die Datenübermittlung geltenden Vorschriften erfüllt waren.

Bei der Auftragsdatenverarbeitung im Sinne des § 11 BDSG müssen die maßgeblichen Entscheidungen über den Umgang mit den personenbezogenen Daten bei der beauftragenden Stelle verbleiben. Die beauftragte Stelle verfährt lediglich entsprechend den Weisungen des Auftraggebers mit den von ihm überlassenen und für ihn zu verarbeitenden Daten. Das Serviceunternehmen fungiert gleichsam als ausgelagerte Abteilung des weiterhin datenschutzrechtlich verantwortlichen Auftraggebers, der als „Herr der Daten“ die volle Verfügungsgewalt behält und damit auch allein über die Erhebung, Verarbeitung oder Nutzung der Daten bestimmt.

Soweit die zentrale Personalabteilung der Ltd. & Co. KG die Personalakten für alle Einzelunternehmen führte, kamen ihr keine maßgeblichen Entscheidungsbefugnisse in den Personalangelegenheiten der Einzelunternehmen zu. Die Personalentscheidungen einschließlich der gebotenen Fürsorgemaßnahmen für ihre Mitarbeiter trafen jene vielmehr selbst. Die Tätigkeit der Personalabteilung für die elf anderen Unternehmen war darauf beschränkt, deren Personaldatenbestand zu speichern und den Einzelunternehmen beziehungsweise der Rechtsabteilung der Ltd. & Co. KG auf Anforderung zur Verfügung zu stellen. Die Personalabteilung wurde somit als Auftragsdatenverarbeiter für die anderen Einzelunternehmen tätig. Auch soweit sie prüfte, ob die Rechtsabteilung darauf aufmerksam gemacht werden sollte, dass möglicherweise von einem Mitarbeiter im Krankheitsfall zu Unrecht bezahlte Vergütung zurückverlangt werden kann, handelte es sich nicht um eine so wesentliche Entscheidung, dass dies der Annahme eines Auftragsdatenverarbeitungsverhältnisses zwischen den Einzelunternehmen und der Personalabteilung entgegenstehen würde. Denn diese Prüfung orientiert sich an engen gesetzlichen Vorgaben und bedarf lediglich einer schematischen Auswertung von Fehlzeiten, Abrechnungsunterlagen und Mitteilungen der Krankenkassen.

Unternehmen können sich anderer Stellen als Auftragsdatenverarbeiter bedienen, es sei denn, dem stehen Rechtsvorschriften oder arbeitsvertragliche Regelungen ausdrücklich entgegen, was hier nicht der Fall war. Nach § 11 Absatz 2 Satz 2 BDSG sind derartige Aufträge stets schriftlich zu erteilen, wobei in dem Auftrag die Datenerhebung, -verarbeitung oder -nutzung sowie die technischen und organisatorischen Maßnahmen detailliert festzulegen sind. Die bloße Wiederholung der diesbezüglichen gesetzlichen Vorgaben (Anlage zu § 9 Satz 1 BDSG) ist in keinem Fall ausreichend. Auch muss unter anderem festgelegt sein, zu welchem Zweck die Datenverarbeitung bei dem Auftragnehmer erfolgt, bei welchen Stellen (zum Beispiel Krankenkassen) der Auftragnehmer welche Daten anzufordern hat, an welche Stellen (zum Beispiel Rechtsabteilung) er diese weitergeben kann, wann der Verarbeitungszweck erreicht ist (zum Beispiel bei Ausscheiden des Mitarbeiters, bei Ablehnung einer Bewerbung) und nach welcher sich daran anschließenden Dokumentationsfrist, während der erfahrungsgemäß noch mit Rückfragen oder rechtlichen Auseinandersetzungen zu rechnen ist, die Daten gelöscht werden sollen (sog. Datenlöschkonzeption). § 11 Absatz 2

Satz 4 und 5 BDSG schreiben außerdem vor, dass sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat und das Ergebnis dieser Überprüfungen dokumentieren muss.

Der zentralen Rechtsabteilung der Ltd. & Co. KG oblag die Entscheidung, ob im Falle der Schädigung eines Mitarbeiters durch einen Dritten bei diesem Regress genommen wird, ob von einem Beschäftigten während der Krankheit zu Unrecht bezahlte Bezüge zurückgefordert werden und welche Erfolgsaussichten dafür bestehen, gegenüber einem Arbeitnehmer arbeitsrechtliche Maßnahmen zu ergreifen. Diese Verfahren führte die Rechtsabteilung eigenständig. Soweit sie dabei personenbezogene Daten erhob, verarbeitete oder nutzte, handelte es sich – abgesehen vom Tätigwerden für die Ltd. & Co. KG selbst – im Hinblick auf die Einzelunternehmen datenschutzrechtlich um eine Funktionsübertragung. Denn die Rechtsabteilung nahm diese Tätigkeiten an Stelle der Einzelunternehmen als eigene Aufgabe wahr, auch wenn die Einzelunternehmen sich das (Letzt-)Entscheidungsrecht in Einzelfragen vorbehalten hatten. Eine Rechtsabteilung als Auftragsdatenverarbeiter anzusehen und damit auf eine Stufe mit Telefon-Beratungszentren, Werbeagenturen, Rechenzentren und Katalogversendern zu stellen, würde deren Stellung nicht gerecht. Die Rechtsabteilung trug daher im Rahmen der ihr von den Einzelunternehmen erteilten Aufträge die datenschutzrechtliche Verantwortung.

Um zu gewährleisten, dass die personenbezogenen Daten bei der Stelle, auf die Datenverarbeitungskompetenz im Wege der Funktionsübertragung übergeleitet worden ist, zu keinem anderen Zweck als zu dem, zu dem sie die eigentlich zuständige Stelle verarbeiten dürfte, genutzt und verarbeitet werden, muss der Verarbeitungszweck ähnlich wie im Falle der Auftragsdatenverarbeitung in einem Vertrag zwischen den Beteiligten festgelegt werden. Auch muss sichergestellt sein, dass bei der Stelle, die die Funktion nunmehr wahrnimmt, eine datenschutzgerechte Organisation der Datenverarbeitung gewährleistet ist. Das gilt insbesondere dann, wenn dabei sensible Informationen wie Personaldaten verarbeitet werden. Deshalb müssen die beteiligten Stellen eine schriftliche Vereinbarung schließen, in der Absprachen wie sie in § 11 Absatz 2 Satz 2 Nummern 1 bis 6 und 10 BDSG vorgesehen sind, getroffen werden.

Bezüglich der Kontrolle von E-Mail-Postfächern von Mitarbeitern der Einzelunternehmen durch das Sekretariat der Geschäftsleitung der Ltd. & Co. KG war zu beachten, dass dem Geschäftsführer der Ltd. & Co. KG kein Aufsichtsrecht über die Beschäftigten der Einzelunternehmen zustand. Datenschutzrechtlich war die Ltd. & Co. KG im Verhältnis zu den Einzelunternehmen der Firmengruppe als Dritter anzusehen. Soweit die Kontrollen der Überprüfung des Ausschlusses der privaten Nutzung dienten, war diese als Auftragsdatenverarbeitung anzusehen, da die Unterscheidung dienstlich/privat bei E-Mails von Ausnahmefällen abgesehen einfach ist und ohne Beurteilungsspielraum erfolgen kann. Soweit die stichprobenweise ausgewählten E-Mails von der Geschäftsleitung der Ltd. & Co. KG dagegen zur Ausübung der allgemeinen Dienstaufsicht überprüft wurden, das heißt mit dem Ziel festzustellen, ob die betrieblichen Aufgaben im Einzelfall so erledigt wurden, wie die Geschäftsführung der Ltd. & Co. KG dies für geboten hielt, handelte es sich angesichts der dort vorbehaltenen Entscheidungskompetenz auch über andere Konzerngesellschaften nicht mehr um eine Auftragsdatenverarbeitung, sondern um eine Funktionsübertragung. Das Vorliegen der Voraussetzungen von § 32 Absatz 1 und § 28 Absatz 1 und 2 BDSG für eine Datenübermittlung und -erhebung lag in diesen Fällen nicht mehr vor.

Um unseren Beanstandungen abzuhelfen, hat das Unternehmen die E-Mail-Kontrolle durch den Geschäftsführer der Ltd. & Co. KG bei Tochterunternehmen zum Zwecke der Dienstaufsicht eingestellt und ein Konzept zur firmengruppenweiten Auftragsdatenverarbeitung und Funktionsübertragung entwickelt. Darin wurden die von § 11 BDSG vorgegebenen Regelungen auf mehreren Hierarchieebenen umgesetzt. Die Grundsätze der Auftragsdatenverarbeitung und Funktionsübertragung wurden in einer „Vereinbarung Datenschutz“ beschrieben; auf einer tieferen Hierarchieebene wurden zudem in gesonderten Anlagen die für die Auftragsdatenverarbeitung einer-

seits und für die Funktionsübertragung andererseits gültigen spezielleren Regelungen getroffen. Die Einzelheiten zu jedem Verfahren finden sich in einem Verfahrensverzeichnis und dessen Anlagen. Insgesamt wurden die Voraussetzungen geschaffen, um künftig in diesem Konzern mit den Daten der Mitarbeiter korrekt umzugehen.

10. Unbefugte Auskünfte aus dem Personalverwaltungssystem einer Stadt

Soziologisch gesehen bilden die Mitarbeiter einer Stadtverwaltung eine lernende Organisation. Dabei kommt es auch vor, dass einzelne Mitarbeiter ganz besonders viel über ihre Kollegen lernen wollen. So war es wohl im Berichtszeitraum auch bei einer Großstadt des Landes, denn dort – so wurde mir zugetragen – wurden bei einer bestimmten Stelle innerhalb der Stadtverwaltung Auskünfte an besonders verbundene Kollegen ohne langes Federlesen erteilt, zum Beispiel über das Alter von Kolleginnen oder die letzte Beförderung eines Kollegen, die Höhe des Gehalts oder die Kinderzahl.

Meine Mitarbeiter haben im Rahmen einer Kontrolle Folgendes herausgefunden: Bei der Stadt wurde für die Personalverwaltung die Software des Marktführers SAP eingesetzt. Bei der fraglichen Stelle der Stadtverwaltung wurden die Verfahren Familiengeld, Familienzuschlag und Lohnpfändung mit Hilfe dieser Software abgewickelt, wobei die fünf Mitarbeiter auf alle Daten zugreifen konnten. Zwar war eine organisatorische Aufgabentrennung anhand einer alphabetischen Aufteilung gegeben, aber sie wurde nicht durch entsprechende Zugriffsrechte im EDV-System umgesetzt. Das sei nicht möglich, da aufgrund der Größe der Stelle im Vertretungsfall der Zugriff möglich sein müsse, wurde meinen Mitarbeitern erklärt. Aus meiner Sicht war dieses Argument nicht überzeugend. Das mächtige Zugriffsrechtesystem der Software jedenfalls konnte im vorliegenden Fall seine datenschutzrechtliche Wirkung nicht entfalten. Erschwerend kommt hinzu, dass lesende Zugriffe von der Software nicht protokolliert werden. Es war deshalb im Nachhinein nicht möglich festzustellen, ob und, wenn ja, welche Mitarbeiter es an der erforderlichen datenschutzrechtlichen Sorgfalt fehlen ließen und Daten zur Kenntnis nahmen beziehungsweise weiterleiteten, die sie oder andere für ihre Arbeit gar nicht benötigten. In diesem Zusammenhang ist daran zu erinnern, dass verantwortliche Stellen im öffentlichen Bereich ihre Mitarbeiter regelmäßig auf § 6 LDSG hinweisen sollten, wonach den bei öffentlichen Stellen beschäftigten Personen der unbefugte Umgang mit personbezogenen Daten untersagt ist. Schließlich begeht derjenige, der zum Beispiel Personaldaten an einen Dritten ohne Erlaubnis weiterreicht, eine Ordnungswidrigkeit.

Auf meine Empfehlung hin hat die Stadt das System geändert, indem eine alphabetische Einteilung vorgenommen und durch entsprechende Zugriffsrechte im System abgebildet wurde. Meinem Vorschlag, den Zugriff auf die personenbezogenen Daten der eigenen Mitarbeiter der Stelle auf ihre Leitung zu beschränken, ist die Stadt auch gefolgt. Glücklicherweise muss es damit nicht sein Bewenden haben: Das Software-Unternehmen bietet neuerdings ein Zusatzprodukt namens „Business Objects GRC Solutions“ mit „SAP Security Monitor“ an, mit dem die Protokollierung lesender Zugriffe möglich ist. Ich habe der Stadt empfohlen zu prüfen, ob der Einsatz dieses Produkts in ihrer EDV-Umgebung möglich ist. Dieser Empfehlung will die Stadt folgen. Auch den bei der Kontrolle erkannten Mangel bei der Löschung personenbezogener Daten und der Verarbeitung nicht erforderlicher personenbezogener Daten wird die Stadt beseitigen.

Sofern personenbezogene Daten mit der Software der Firma SAP verarbeitet werden, empfehle ich den verantwortlichen Stellen den Einsatz des oben genannten Protokollierungsprodukts zu prüfen. Insbesondere in großen Einsatzbereichen könnte eine Protokollierung aller lesenden Zugriffe in dem System aber nicht zielführend sein. Die verantwortlichen Stellen müssen dann – etwa aufgrund einer Risikoanalyse – abwägen, welche lesenden Zugriffe auf personenbezogene Daten protokolliert werden sollten.

11. Datenschutzrechtliche Fallstricke einer Mitarbeiterbefragung

Eine Mitarbeiterbefragung war datenschutzrechtlich zu beanstanden: Die Stadt hatte ihre befragten Mitarbeiter nicht darauf hingewiesen, dass ihre Teilnahme freiwillig war, und die von den Mitarbeitern beurteilten Vorgesetzten nicht gefragt, ob sie einwilligen.

Soweit Mitarbeiterbefragungen anonym ablaufen, gibt es in der Regel keine datenschutzrechtlichen Probleme. Diese können jedoch – wie in diesem Fall – dann entstehen, wenn Fragen zur Person in den Fragebogen so genau sind, dass die Antworten darauf jedenfalls in einigen Fällen bestimmten befragten Mitarbeitern zuzuordnen waren und damit auch die jeweils ausgefüllten Fragebogen; die dortigen Antworten waren damit personenbezogen. Daran änderte es nichts, dass die Stadt eine Universität eingeschaltet hatte, welche die ausgefüllten Fragebogen erhielt und der Stadt lediglich zusammengefasste Ergebnisse zuleiten sollte. Auch wenn insoweit die Universität nur die ausgefüllten Fragebogen hatte und die Stadt nur die Informationen, die notwendig waren, um die Antworten auf die Fragen zur Person bestimmten Mitarbeitern zuzuordnen, beseitigte das den Personenbezug in den genannten Fällen nicht. Würde bei dieser Fallgestaltung ein Personenbezug verneint, wäre konsequenterweise insoweit auch auf Maßnahmen zum Datenschutz zu verzichten, etwa auf die Anforderung, dass die Universität die einzelnen (nicht zusammengefassten) ausgefüllten Fragebogen nicht der Stadt zuleiten und nicht veröffentlichen darf.

Die befragten Mitarbeiter waren auf die Freiwilligkeit ihrer Teilnahme an der Mitarbeiterbefragung hinzuweisen. Das hätte auf dem Fragebogen selbst geschehen müssen, was hier nicht der Fall war. Ein Hinweis in anderen Unterlagen oder in Veranstaltungen reicht dafür grundsätzlich nicht aus.

Zudem waren Antworten der befragten Mitarbeiter auf die Fragen zu ihren Vorgesetzten (im Rahmen einer Vorgesetztenbeurteilung) den Vorgesetzten zuzuordnen und deswegen hinsichtlich dieser personenbezogen. Die Vorgesetzten waren vor der Mitarbeiterbefragung zu fragen, ob Sie hinsichtlich der Vorgesetztenbeurteilung einwilligen. Das war ebenfalls nicht geschehen.

Außerdem war der Gemeinde die Möglichkeit der Zuordnung eines Mitarbeiters zur Befragung anhand der IP-Adresse eröffnet, wenn der Mitarbeiter von seinem Arbeitsplatz-PC bei der Gemeinde im Online-Verfahren an der Befragung teilnahm. Diese Möglichkeit hätte ausgeschlossen werden müssen.

Nachzutragen ist noch, dass die Stadt aufgrund der mehrmonatigen Auseinandersetzungen mit meiner Dienststelle schließlich das Interesse an einer Auswertung der Umfrageergebnisse verlor und die eingeschaltete Universität zur Löschung der erhobenen Daten veranlasste. Hiergegen bestanden von mir aus natürlich keine Bedenken mehr.

12. Der überwachungsbedürftige Wachmann

Die Gewerbeordnung schreibt vor, dass ein Bewachungsunternehmer nur solche Mitarbeiter beschäftigen darf, bei denen keine Tatsachen die Annahme rechtfertigen, dass sie die für eine Überwachungstätigkeit erforderliche Zuverlässigkeit nicht besitzen. Was aber darf der Unternehmer über seine Mitarbeiter in Erfahrung bringen, um deren Zuverlässigkeit zu beurteilen?

Grundsätzlich muss sich ein Unternehmer im Bewachungsgewerbe sowie in der Wert- und Geldtransportbranche regelmäßig davon überzeugen, ob seine Beschäftigten in strafrechtlicher und wirtschaftlicher Hinsicht zuverlässig sind. Haben sie Straftaten begangen, die befürchten lassen, dass sie sich an den in ihrer Obhut befindlichen Sachen vergreifen, scheidet für sie eine Tätigkeit in diesem Bereich grundsätzlich aus. Sie dürfen also nicht wegen Vermögensdelikten und dergleichen vorbestraft sein. Dies gilt für Straftaten gegen das Leben, die Freiheit und die körperliche Unversehrtheit sowie für den Verrat von Geschäfts- und Betriebsgeheimnissen der Kunden ihres Arbeitgebers entsprechend. Wer aufgrund derartiger, in der Vergangenheit begangener Straftaten Zweifel an seiner Zuverlässigkeit weckt, darf von einem Bewachungsunternehmen grundsätzlich nicht mit Bewachungs- und Sicherungsaufgaben betraut werden.

Allerdings ist es dem Arbeitgeber von Wachleuten verwehrt, Selbstauskünfte aus dem Bundeszentralregister zum Zwecke der Zuverlässigkeitsüberprüfung seiner Mitarbeiter einzuholen oder sich solche von seinen Mitarbeitern vorlegen zu lassen. Eine derartige Selbstauskunft beinhaltet nämlich alle Verurteilungen des Betroffenen, durch die auf Geldstrafen von mehr als 90 Tagessätzen und auf Freiheitsstrafen von mehr als drei Monaten unabhängig von dem konkreten Straftatbestand erkannt worden ist. Bei der Offenbarung derartiger Selbstauskünfte gegenüber dem Bewachungsunternehmer würde dieser auch von solchen Straftaten erfahren, die keine Rückschlüsse auf die Zuverlässigkeit für die Beschäftigung im Bewachungsgewerbe zulassen. Doch kann sich der Arbeitgeber einmal jährlich bei der für ihn zuständigen Gewerbebehörde erkundigen, ob dort entsprechende Umstände bekannt sind. Die Gewerbebehörde hat nämlich regelmäßig eine Auskunft aus dem Bundeszentralregister über die in ihrem Zuständigkeitsbereich im Überwachungsgewerbe Beschäftigten einzuholen, um von sich aus deren Zuverlässigkeit zu überprüfen. Richtet der Arbeitgeber eine solche Anfrage an die Behörde, darf ihm diese nur über diejenigen Straftaten informieren, die für die Tätigkeit des Arbeitnehmers relevant sind.

Um die wirtschaftliche Zuverlässigkeit seiner Mitarbeiter, die ebenfalls bei den im Bewachungsgewerbe Beschäftigten gegeben sein muss, zu klären, muss der Arbeitgeber grundsätzlich auch hierzu jährlich entsprechende Auskünfte einholen. Allerdings setzt der Grundsatz der Erforderlichkeit und der Verhältnismäßigkeit auch hier Grenzen. Der Arbeitgeber darf zum Beispiel keineswegs eine „umfassende“ Selbstauskunft der Schufa von seinen Mitarbeitern verlangen. Denn eine solche Auskunft vermag die wirtschaftliche Situation einer Person zumindest insoweit darzustellen, als dass mitgeteilt wird, ob nicht erfüllte Verbindlichkeiten gegenüber Dritten bestehen. Wer eine Selbstauskunft bei der Schufa anfordert, erhält eine sogenannte Teil 1-Schufa-Bonitätsauskunft. Diese beinhaltet sämtliche bei der Schufa eingemeldeten, vom Betroffenen nicht erfüllten Forderungen. Müssten die Beschäftigten eine solche Auskunft beibringen, so würde der Arbeitgeber auch hier personenbezogene Informationen erhalten, die über das für seine Zuverlässigkeitsprüfung Erforderliche hinausgehen. Ihm würde zum Beispiel auch die Nichtbegleichung kleiner Forderungen, die in der Regel keinen Anlass für die Annahme besagter Unzuverlässigkeit geben, bekannt. Die Auskunft der Schufa muss sich somit auf solche Informationen beschränken, die nach der allgemeinen Lebenserfahrung erwarten lassen, dass sich der Betroffene wegen seiner wirtschaftlichen Notlage an dem ihm anvertrauten Gut vergreift. Inwieweit dieses Risiko besteht, hängt entscheidend von der Höhe der bei der Schufa eingemeldeten Forderung ab, ob also diese den Schluss zulässt, dass der Betroffene in ernsthaften finanziellen Schwierigkeiten steckt. Von Letzterem kann in der Regel erst bei einer Überschuldung von 5.000 Euro und mehr ausgegangen werden. Darüber hinaus hat der Bewachungsunternehmer ein berechtigtes Interesse, von Umständen wie Insolvenzeröffnung oder Aufnahme in das Schuldnerverzeichnis der Amtsgerichte (sog. „harte Merkmale“) bezüglich seiner Mitarbeiter informiert zu werden.

Die Schufa bietet unter dem Stichwort „Schufa-webCode“ ein Verfahren an, bei dem jeder mündlich, per Telefon, E-Mail oder SMS eine andere Person ermächtigen kann, bei der Schufa eine Kurzinformation zur Bonität des Ermächtigenden zu erfragen. Der Ermächtigende bestimmt gegenüber der Schufa, in welchem von ihm selbst bestimmten Umfang dort gegebenenfalls gespeicherte Daten zu seiner Person dem Dritten offenbart werden sollen. Datenschutzrechtlich spricht nichts dagegen, wenn die Arbeitnehmer im Bewachungsgewerbe ihren Arbeitgeber ermächtigen, dass ihm die Schufa mitteilen darf, ob der Arbeitnehmer Forderungen von 5.000 Euro und mehr nicht beglichen hat beziehungsweise ob besagte „harte Merkmale“ bei ihm vorliegen. Selbstverständlich kann die wirtschaftliche Zuverlässigkeit gegenüber dem Arbeitgeber auch anderweitig belegt werden, soweit sich die jeweilige Auskunft auf den datenschutzrechtlich zulässigen Umfang beschränkt.

Zuverlässigkeitsüberprüfen sind bei Beschäftigten, bei denen dies in ihrem eigenen Interesse oder im Interesse des Arbeitgebers und der Allgemeinheit geboten ist, durchaus zulässig. Die Erhebung des dafür erforderlichen Datenmaterials muss sich aber auf das Notwendigste beschränken.

13. Löschkonzeption für elektronische Personalakten

Anlässlich eines Kontrollbesuchs bei der Personalabteilung eines großen Unternehmens stellten wir fest, dass in den dort über jeden Mitarbeiter geführten elektronischen Personalakten zahlreiche, teilweise schon sehr lange zurückliegende Abmahnungen gespeichert waren. Insgesamt handelte es sich nach Systemangaben um über 17 000 gespeicherte Abmahnungen. In den Personalakten wurden teilweise auch Führungszeugnisse gespeichert. Auch insoweit waren keine Löschungsfristen vorgesehen.

Bezüglich der Speicherung von Abmahnungen in den Personalakten ist Folgendes zu beachten: Nach der Rechtsprechung des Bundesarbeitsgerichts besteht grundsätzlich ein legitimes Anliegen des Arbeitgebers, dass die von ihm geführten Personalakten vollständig sind. Sie sollen möglichst lückenlos über die Person des Beschäftigten und seine berufliche Entwicklung Aufschluss geben. Der Arbeitgeber hat grundsätzlich ein überwiegendes Interesse, die für das Arbeitsverhältnis maßgeblichen Informationen über die Persönlichkeit des Arbeitnehmers zum Zwecke späterer Personalentscheidungen zu sammeln. Diesem berechtigten Interesse werden jedoch Grenzen durch den Schutz des Persönlichkeitsrechts des Mitarbeiters gesetzt. Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers – solche liegen vor, wenn über ihn personenbezogene Erkenntnisse gesammelt werden – können grundsätzlich nur durch die Wahrnehmung überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein. Im Einzelfall bedarf es zur Konkretisierung der Rechte und Pflichten beider Seiten im Einzelfall stets einer Güter- und Interessenabwägung. Verletzt der Arbeitgeber das Persönlichkeitsrecht des Arbeitnehmers etwa dadurch, dass er in den Personalakten Informationen speichert, ohne dass dies durch eigene überwiegende Interessen gerechtfertigt ist, liegt darin sowohl ein datenschutzrechtlicher Verstoß, wie auch ein solcher gegen die arbeitsvertraglichen Pflichten des Arbeitgebers.

Bei Abmahnungen entfällt das schutzwürdige Interesse des Arbeitgebers an der weiteren Aufbewahrung einer entsprechenden Niederschrift in den Personalakten beziehungsweise in Form von elektronischer Speicherung, wenn eine Wiederholung des berechtigt abgemahnten Verhaltens aufgrund der zwischenzeitlichen „Bewährung“ des Arbeitnehmers nicht mehr zu besorgen ist. Das ist auch dann der Fall, wenn diese Abmahnung in einem Arbeitszeugnis wegen Zeitablaufs nicht mehr berücksichtigt werden darf oder wenn ein so langer Zeitraum seit dem abgemahnten Ereignis ins Land gegangen ist, dass selbst bei arbeitsrechtlichen Maßnahmen wegen neuerlicher Verfehlungen das gespeicherte Vorkommnis nicht mehr berücksichtigt werden dürfte. Auch sind die Art der Verfehlung des Arbeitnehmers sowie sein weiteres Verhalten und seine Einstellung im Anschluss an die Abmahnung sowie das Gewicht der erhobenen Vorwürfe zu berücksichtigen. Zwar können angesichts der Relativität dieser Voraussetzungen keine konkreten Zeiträume vorgegeben werden, wann die Löschung erfolgen muss. Doch wird in der arbeitsrechtlichen Literatur davon ausgegangen, dass Abmahnungen, die länger als zwei bis drei Jahre zurückliegen, sich im Regelfall durch Zeitablauf erledigt haben und zu tilgen sind.

Sollen Führungszeugnisse mit Eintragungen zur Personalakte genommen werden, ist die Löschfrist hierfür im Hinblick auf das Verwertungsverbot des § 51 des Bundeszentralregistergesetzes (BZRG) an der Länge der Tilgungsfristen des § 46 BZRG auszurichten.

Nach alledem war die Praxis, sämtliche Abmahnungen ohne zeitliche Begrenzung zu speichern, datenschutzwidrig. Wir haben das Unternehmen daher aufgefordert, unter Beachtung der obigen Vorgaben eine Datenlöschkonzeption für die elektronisch gespeicherten Personalakten zu erstellen, aus der sich ersehen lässt, nach welchem Zeitraum bei welchem Schweregrad der Verfehlung des Arbeitnehmers eine Abmahnung zu löschen ist und unter welchen Voraussetzungen dies unterbleiben kann, wenn spätere Verfehlungen bekannt werden. Außerdem mussten die vorhandenen elektronischen Personalakten auf nicht mehr erforderliche Speicherungen hin durchforstet und gegebenenfalls Löschungen vorgenommen werden.

Die von dem Unternehmen erstellte Löschkonzeption sieht nunmehr vor, dass Abmahnungen zwei Jahre nach dem Einscannen der originalen Papierunterlagen zu löschen sind, wenn es in dieser Zeit keine neuen Vorfälle gab.

7. Teil: Datenschutz in der Wirtschaft

1. Abschnitt: Der Betriebliche Datenschutzbeauftragte

1. Grundsätzliche Anforderungen

Die betrieblichen Datenschutzbeauftragten bilden die tragende Säule des Datenschutzes in der Privatwirtschaft. Mit ihrer Qualität steht und fällt der Datenschutz in den Unternehmen. Die Aufsichtsbehörden haben deshalb Mindestanforderungen an ihre Fachkunde und Unabhängigkeit aufgestellt.

Nach § 4 f Absatz 1 BDSG haben nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz zu bestellen. Eine Ausnahme besteht dann, wenn in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen haben nicht-öffentliche Stellen stets einen Beauftragten für den Datenschutz zu bestellen, soweit sie automatisierte Verarbeitungen vornehmen, die besondere Risiken für die Rechte und die Freiheiten der Betroffenen aufweisen und daher im Wege der Vorabkontrolle zu überprüfen sind, oder personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeitet werden.

Zum Beauftragten für den Datenschutz darf gemäß § 4 f Absatz 2 Satz 1 BDSG nur bestellt werden, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Datenschutzbeauftragten in den verantwortlichen Stellen angesichts der zunehmenden Komplexität automatisierter Verfahren nicht durchgängig den Anforderungen des Bundesdatenschutzgesetzes genügen. Der Düsseldorfer Kreis, der Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, hat deswegen in seiner Sitzung vom 24./25. November 2010 Mindestanforderungen an Fachkunde und Unabhängigkeit des Betrieblichen Beauftragten für den Datenschutz in einem Beschluss (vgl. Anhang 35) formuliert:

Unabhängig von Branche und Größe der verantwortlichen Stelle müssen die Datenschutzbeauftragten über Grundkenntnisse zu den verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Beschäftigten der verantwortlichen Stelle sowie umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des Bundesdatenschutzgesetzes verfügen. Darüber hinaus sind Kenntnisse des Anwendungsbereiches datenschutzrechtlicher sowie einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG erforderlich. Branchenspezifisch sind des Weiteren umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit, betriebswirtschaftliche Grundkompetenz, Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle ebenso wie Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle notwendig. Die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse müssen grundsätzlich bereits zum Zeitpunkt der Bestellung zum Betrieblichen Datenschutzbeauftragten im ausreichenden Maße vorliegen.

Neben der Fachkunde spielt die Unabhängigkeit der Beauftragten für den Datenschutz eine große Rolle. Um sie zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich. Die Datenschutzbeauftragten sind der Leitung der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen, ihnen ist ein unmittelbares Vortragsrecht bei der Leitung einzuräumen und sie müssen in der Lage sein, ihre Verpflichtungen ohne lnteressenkonflikte erfüllen zu können. Des Weiteren dürfen die Be-

auftragten für den Datenschutz wegen der Erfüllung ihrer Aufgaben im Hinblick auf ihr sonstiges Beschäftigungsverhältnis nicht benachteiligt werden. Sie sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden.

Die Prüfpflichten der Beauftragten für den Datenschutz setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden. Sie müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden sein und haben die für die Aufgabenerfüllung erforderlichen Unterlagen zu erhalten. Zur Sicherung der zur Erfüllung der Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Ihnen muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Die verantwortlichen Stellen haben die Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben insbesondere dadurch zu unterstützen, dass sie ihnen Personal, Räume, Einrichtungen, Geräte und Mittel zur Verfügung stellen.

Schließlich ist zu bemerken, dass mit der Aufgabe des Beauftragten für den Datenschutz auch eine Person außerhalb der verantwortlichen Stelle betraut werden kann (externer Datenschutzbeauftragter). Der Dienstvertrag muss dabei so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. Grundsätzlich empfehle ich eine Mindestvertragslaufzeit von vier Jahren, bei Erstverträgen eine Vertragslaufzeit von ein bis zwei Jahren. Die Fortbildung kann Bestandteil der vereinbarten Vergütung sein. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt werden.

Die Nichtbestellung eines betrieblichen Datenschutzbeauftragten stellt übrigens eine Ordnungswidrigkeit dar, die mit einem empfindlichen Bußgeld geahndet werden kann. Die Aufsichtsbehörde hat davon in der Vergangenheit regelmäßig Gebrauch gemacht und wird auch in Zukunft keine Scheu davor haben, festgestellte Mängel dem nunmehr zuständigen Regierungspräsidium Karlsruhe weiterzumelden.

2. Ist Personal mit gelegentlichem Lesezugriff auf den Kundenadressbestand ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt?

Durch eine Beschwerde wurde die Aufsichtsbehörde auf einen Fachhändler mit Sitz in Baden-Württemberg aufmerksam, der zehn rechtlich unselbstständige Filialen im ganzen Bundesgebiet betrieb. Er hatte bislang keinen betrieblichen Datenschutzbeauftragten bestellt, weil er der Ansicht war, hierzu nicht verpflichtet zu sein.

In jeder der Filialen stand der Kundenadressbestand in elektronischer Form zur Verfügung. Bei jeder Rechnungsstellung wird die postalische Adresse des betreffenden Kunden aus dem EDV-System aufgerufen und in das Rechnungsschreiben eingesetzt. Das Unternehmen war der Auffassung, dass diese Tätigkeit keine Datenverarbeitung darstellt und wies außerdem darauf hin, dass hierdurch nicht einmal 1 % der Arbeitszeit der Kassenkräfte ausgefüllt werde. Mit der Neuanlage von Adressen und der Verwendung der Daten für Werbeaktionen seien dagegen lediglich ein bis zwei Mitarbeiter in der Hauptniederlassung beschäftigt.

Nach § 4 f Absatz 1 Satz 1 BDSG sind nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, verpflichtet, einen Beauftragten für den Datenschutz schriftlich zu bestellen. Dies gilt für nicht-öffentliche Stellen nicht, wenn sie in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. „Ständig“ beschäftigt ist ein Mitarbeiter, wenn er für diese Aufgabe, die nicht seine Hauptaufgabe zu sein braucht, auf unbestimmte, zumindest aber längere Zeit vorgesehen ist und sie entsprechend wahrnimmt. Das Tat-

bestandsmerkmal „ständig“ ist mithin auch erfüllt, wenn die Aufgabe selbst nur gelegentlich anfällt, der Arbeitnehmer sie aber stets wahrzunehmen hat. Auf den Anteil dieser Arbeit kommt es nicht an. Bei der Zählung der Mitarbeiter, die mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, sind auch die Personen relevant, die nur Zugriff zu gespeicherten Daten zum Zwecke der Nutzung haben. Da das Kassenpersonal in jeder der zehn Filialen für die Erstellung von Rechnungen auf den zentral verwalteten Adressdatenbestand zugriff, beschäftigte das Unternehmen in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten im Sinne von § 4 f Absatz 1 Satz 4 BDSG und war daher zur Bestellung eines Beauftragten für den Datenschutz verpflichtet.

2. Abschnitt: Werbung und Adresshandel

1. Neue datenschutzrechtliche Regelungen für die Werbung und den Adresshandel

Im Jahr 2009 sind die Vorschriften über die Verarbeitung und Nutzung personenbezogener Daten zum Zwecke der Werbung und der Werbewirtschaft in den Absätzen 3 bis 3 b des § 28 BDSG grundlegend neu gefasst worden. Obwohl zugleich die Datenverarbeitung zu Zwecken der Markt- und Meinungsforschung aus dem Regelungsgefüge des § 28 BDSG herausgenommen wurde und nunmehr in einer eigenen Norm (§ 30 a BDSG) behandelt wird, hat § 28 BDSG gegenüber seiner vorherigen Fassung erkennbar an Umfang und Komplexität zugenommen. Seit dem 1. September 2009 ist das neue Recht in Kraft, für personenbezogene Daten, die vor diesem Datum erhoben worden sind, gilt allerdings eine Übergangsregelung (§ 47 BDSG), für Zwecke der Werbung noch bis zum 31. August 2012.

Leider muss die Neuregelung als insgesamt wenig geglückt bezeichnet werden. Hatte der Gesetzgeber unter dem Eindruck diverser Datenschutzskandale ursprünglich eine strikte Einwilligungslösung realisieren wollen, so ist dieser datenschutzfreundliche Ansatz im Laufe des Gesetzgebungsverfahrens alsbald aufgeweicht worden. Herausgekommen ist eine überkomplexe Regelung, in deren Rahmen das bisherige sogenannte „Listenprivileg“ in veränderter Gestalt Urständ feiern durfte und deren richtiges Verständnis selbst Juristen vom Fach einiges Kopfzerbrechen bereiten kann.

Im Detail lässt sich der Regelungsgehalt des maßgeblichen § 28 Absatz 3 BDSG wie folgt skizzieren:

Nach § 28 Absatz 3 Satz 1 BDSG ist die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung zulässig, soweit der Betroffene eingewilligt hat. Für die Einwilligung gelten dabei nach Maßgabe der Absätze 3a und 3b besondere, über die allgemeine Regelung des § 4 a BDSG hinausgehende Wirksamkeitsvoraussetzungen. So weit, so gut.

Abweichend von diesem Grundsatz dürfen jedoch bestimmte, in § 28 Absatz 3 Satz 2 BDSG aufgeführte „listenmäßig oder sonst zusammengefasste“ Daten über Angehörige einer Personengruppe auch ohne Einwilligung des Betroffenen verarbeitet oder genutzt werden, und zwar in erster Linie für Zwecke der Werbung für eigene Angebote (§ 28 Absatz 3 Satz 2 Nr. 1 BDSG). Diese Listendaten muss die werbende Stelle entweder bei den Betroffenen selbst oder aus öffentlichen Verzeichnissen erhoben haben, darf zu diesen Listendaten jedoch „weitere Daten hinzuspeichern“. Nicht auf bestimmte Datenquellen, aber ohne Zuspeicherungsoption strikt auf die erlaubten Listendaten beschränkt ist demgegenüber die Werbung „im Hinblick auf die berufliche Tätigkeit des Betroffenen“, die nach § 28 Absatz 3 Satz 2 Nr. 2 BDSG statthaft ist, soweit sie unter dessen beruflicher Anschrift erfolgt. Dieselbe Beschränkung auf Listendaten gilt für die gleichfalls privilegierte Spendenwerbung (§ 28 Absatz 3 Satz 2 Nr. 3 BDSG).

Doch das „Listenprivileg“ reicht noch weiter: Gemäß § 28 Absatz 3 Satz 4 BDSG ist auch die sogenannte „transparente Übermittlung“ erlaubt, das heißt sog. Listeigner dürfen ihre Listendaten an dritte Stellen für deren eigene Werbezwecke weitergeben. Freilich sind in diesem Falle sowohl die über-

mittelnde Stelle als auch die Adressatin der Übermittlung verpflichtet, die Herkunft der Daten sowie die jeweils andere an dem Übermittlungsvorgang beteiligte Stelle zwei Jahre lang zu speichern (§ 28 Absatz 3 Satz 4 in Verbindung mit § 34 Absatz 1 a BDSG); zudem muss die Stelle, welche die Daten erstmals erhoben hat, aus der Werbung eindeutig hervorgehen. Dies soll den Betroffenen gegebenenfalls in die Lage versetzen, mittels seines Auskunftsanspruchs die Herkunft seiner Daten bis zu deren Quelle zurückzuverfolgen.

Schließlich autorisiert § 28 Absatz 3 Satz 5 BDSG auch noch die einwilligungsfreie „transparente Nutzung" personenbezogener Daten für Zwecke der Werbung für fremde Angebote, sofern für den Betroffenen „bei der Ansprache zum Zweck der Werbung die für die Nutzung der Daten verantwortliche Stelle", das heißt die Eigentümerin der Adressdaten, „eindeutig erkennbar" ist. Die Bedeutung dieser Regelung erschließt sich, wenn man weiß, dass Adressdaten in der Praxis der Werbewirtschaft häufig für den Versand fremder Werbepost eingesetzt werden – sei es, dass ein Unternehmen eigenen Werbe- und Warensendungen Werbematerial dritter Anbieter beifügt („Beipack- und Empfehlungswerbung"), sei es, dass ein Unternehmen, das über keine geeigneten eigenen Adressbestände verfügt, einen spezialisierten sog. Listbroker damit beauftragt, geeignete Adressdaten von dritten Listeignern anzumieten. Es ist im Übrigen strittig, ob die „transparente Nutzung" nach § 28 Absatz 3 Satz 5 BDSG ebenfalls noch einen Unterfall des „Listenprivilegs" darstellt. Vermutlich war dies die Intention des Gesetzgebers, doch nach dem reinen Wortlaut der Norm würde sich die „transparente Nutzung" keinesfalls auf Listendaten beschränken.

In allen vorgenannten Fällen gilt allerdings, dass die Verarbeitung und Nutzung der personenbezogenen Daten für Werbezwecke nur zulässig ist, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen (§ 28 Absatz 3 Satz 6 BDSG). Zudem haben die Betroffenen – wie schon nach alter Rechtslage – weiterhin das Recht, der Verarbeitung und Nutzung ihrer Daten für Werbezwecke gegenüber der werbenden Stelle jederzeit zu widersprechen (§ 28 Absatz 4 BDSG).

Und der Adresshandel? Dieser unterliegt, wie schon bisher, grundsätzlich den Bestimmungen des § 29 BDSG über die geschäftsmäßige Erhebung und Speicherung personenbezogener Daten zum Zweck der Übermittlung. Zwei unscheinbare Verweise, der eine in Absatz 1 Satz 2 der Norm, der andere in Absatz 2 Satz 2, erklären indessen nunmehr unter anderem § 28 Absätze 3 bis 3 b BDSG für anwendbar. Dient das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen der Daten daher den Zwecken der Werbung, so ist dies grundsätzlich nur noch mit der Einwilligung des Betroffenen zulässig. Ob darüber hinaus auch aufgrund einer gesetzlichen Ermächtigung mit Adressen gehandelt werden darf, ist zweifelhaft. Während das prinzipielle Einwilligungserfordernis § 28 Absatz 3 Satz 1 BDSG nämlich ausdrücklich Geltungsanspruch für Adresshandel und Werbung erhebt, ist ab § 28 Absatz 3 Satz 2 BDSG nur vom „Zweck der Werbung" die Rede. Einige gängige Kommentare zum Bundesdatenschutzgesetz ziehen daraus den Schluss, dass der Gesetzgeber den Adresshandel von der gesetzlichen Datenverarbeitungsnorm des „Listenprivilegs" habe ausnehmen wollen; doch auch die gegenteilige Auffassung wird in der Literatur vertreten. Eine abschließende Klärung dieser Streitfrage steht noch aus.

Alles in allem hat die Novelle der Vorschriften des Bundesdatenschutzgesetzes über die Werbung und den Adresshandel also viele Fragen aufgeworfen und die Rechtslage zumindest nicht vereinfacht. Dies könnte man nur hinnehmen, wenn die neuen Regelungen ungeachtet aller Zugeständnisse an die Werbewirtschaft mittelfristig dazu beitragen würden, den Schutz des informationellen Selbstbestimmungsrechts der Bürgerinnen und Bürger nachhaltig zu verbessern. Ein klares Bild zeichnet sich diesbezüglich in der Praxis bislang noch nicht ab.

Die Praxis wird zeigen, ob die Neufassung der Regelungen über die Verarbeitung und Nutzung personenbezogener Daten zu Zwecken der Werbung und des Adresshandels die Bürgerinnen und Bürger besser als bislang vor manchen Exzessen der Werbewirtschaft schützt. Angesichts der Komplexität der Regelungen und der Schlupflöcher, die der Gesetzgeber offen gelassen hat, ist jedoch Skepsis angebracht.

2. Moderne Zeiten – Wahlwerbung per E-Mail und SMS

Die Werbekampagne einer politischen Partei, die im Vorfeld der Bundestagswahl 2009 den Kontakt zu ihren potenziellen Wählern per E-Mail und SMS suchte, warf datenschutzrechtliche Fragen auf.

Eine Partei, die im Vorfeld der Bundestagswahl 2009 im Wahlkampf neue Wege beschritt, indem sie ihre Wahlbotschaften mit griffigen E-Mail- und SMS-Kurznachrichten („Wählen Sie klare Verhältnisse und eine stabile Regierung, die Probleme löst …“) an den potenziellen Wähler brachte, musste die Erfahrung machen, dass Wahlwerbung selten überall willkommen ist. Mehrere Betroffene, die sich durch die unerwartete Wahlwerbung belästigt fühlten, erkundigten sich bei den Aufsichtsbehörden ihrer Bundesländer, ob das Vorgehen der Partei rechtens gewesen sei.

Da die Partei (beziehungsweise ein parteieigener Presseverlag) einen großen baden-württembergischen Adresshändler damit beauftragt hatte, ihr die für ihre Werbekampagne benötigten E-Mail- und SMS-Adressen zu beschaffen, schaltete sich auch die Aufsichtsbehörde ein. Der Adresshändler erklärte, dass er einen Großteil der für die Werbekampagne genutzten E-Mail-Adressen aus eigenen Beständen bereitstellen könne, während die übrigen E-Mail-Anschriften sowie sämtliche SMS-Adressen von insgesamt fünf im In- sowie im europäischen Ausland ansässigen Partner- und Tochterunternehmen des Adresshändlers – der sich insoweit nur als Vermittler des Auftrags betrachtete – „angemietet“ seien. Da die an der Werbekampagne beteiligten Unternehmen den Versand des Werbetextes der Auftraggeberin an „ihre“ Anschriften jeweils selbst übernahmen, mussten sie Adressdaten von Betroffenen weder untereinander austauschen, noch der Auftraggeberin übermitteln.

Bei dieser Sachlage stellte sich zunächst die Frage, welche Stelle die datenschutzrechtliche Verantwortung für die Werbekampagne trug. Die Nutznießerin der Werbeaktion, also die wahlkämpfende Partei, war aus rein datenschutzrechtlicher Warte von vorneherein exkulpiert, da sie selbst (beziehungsweise ihr parteieigener Verlag), soweit ersichtlich, keinerlei personenbezogene Daten erhoben, verarbeitet oder genutzt hatte. Zwischen dem baden-württembergischen Adresshändler und den übrigen beteiligten Unternehmen bestanden zwar vertragliche Absprachen, aber ersichtlich kein Auftragsdatenverarbeitungsverhältnis im Sinne des § 11 BDSG, in dessen Rahmen die datenschutzrechtliche Verantwortung beim Adresshändler verblieben wäre. Demnach hatte jedes der Unternehmen für den eigenen Anteil an der Werbeaktion selbst einzustehen. Dies bedeutete freilich, dass die Aufsichtsbehörde ihre Kontrolle auf einen Adresshändler beschränken musste, da nur dieser der baden-württembergischen Datenschutzaufsicht unterlag. War dem Adresshändler aber überhaupt ein datenschutzrechtlicher Vorwurf zu machen?

Außer Diskussion stand, dass der Versand der Werbenachricht nur insoweit datenschutzrechtskonform hatte erfolgen können, als die betroffenen Adressaten sich zuvor rechtswirksam damit einverstanden erklärt hatten, dass ihre E-Mail- beziehungsweise SMS-Adressen zu Zwecken der (Wahl-)Werbung genutzt werden. Hierfür meinte der Adresshändler im Hinblick auf die eigenen Adressbestände einstehen zu können: Jedenfalls die von ihm selbst generierten, für die E-Mail-Kampagne verwendeten Datensätze seien mit schriftlicher Einwilligung der Betroffenen datenschutzrechtskonform erhoben, verarbeitet und genutzt worden. Dies ließ die Aufsichtsbehörde letztlich gelten.

Wie aber verhielt es sich mit den E-Mail- und SMS-Adressen, die von dritter Seite bereitgestellt worden waren? Die übrigen an der Werbeaktion mitwirkenden Unternehmen hatten dem Adresshändler zwar ihrerseits zugesichert, zur Abwicklung des Auftrags nur Datensätze solcher Betroffener zu verwenden, die in die Nutzung ihrer Daten zum Zweck der E-Mail- beziehungsweise SMS-Werbung per „Double Opt-In“ eingewilligt hatten. Der Adresshändler hatte es jedoch unterlassen, sich durch geeignete Stichproben davon zu überzeugen, ob diese Zusagen tatsächlich eingehalten wurden. Freilich hatte er sich zu derartigen Kontrollen gegenüber der Auftraggeberin auch nicht verpflichtet.

Hier setzte die Kritik der Aufsichtsbehörde an: Sie sah ein Manko der vertraglichen Absprache zwischen der Auftraggeberin und dem Adresshändler darin, dass diese die datenschutzrechtlichen Verantwortlichkeiten im „Dreiecks-Verhältnis“ zwischen dem Adresshändler, den eingebundenen Unternehmen und der Auftraggeberin nicht eindeutig regelte und insbesondere die Frage unbeantwortet ließ, welcher Vertragspartner sich durch Stichproben davon zu überzeugen hatte, dass für die vom Adresshändler als Makler vermittelten Adressbestände tatsächlich wirksame Einwilligungen der Betroffenen vorlagen. Möglicherweise sei, so das Fazit der Aufsichtsbehörde, die Auftraggeberin deshalb im Unklaren darüber geblieben, weil sie womöglich selbst entsprechende Überprüfungen hätte durchführen müssen.

Die Aufsichtsbehörde forderte den Adresshändler daher dazu auf, für künftige Fälle Musterverträge auszuarbeiten, die diesen Bedenken Rechnung tragen. Dies sagte der Adresshändler der Aufsichtsbehörde zu. Unterdessen hat er entsprechende Entwürfe vorgelegt.

Sind an einer Direktmarketing-Kampagne mehrere Stellen in unterschiedlichen Rollen beteiligt, so bedarf es klarer vertraglicher Absprachen, wer für welche Datenverarbeitung die datenschutzrechtliche Verantwortung trägt. Zumindest stichprobenweise ist zu überwachen, dass nur datenschutzrechtskonform generierte Datensätze genutzt werden.

3. Die Freundschaftswerbung

Gelegentlich fordern Firmen ihre Kunden auf, auf Bestellformularen den Namen und die Adresse anderer Personen anzugeben, damit die Firma, an die sich die Bestellung richtet, auch dem „Freund“ des Bestellers Werbematerial zusenden kann.

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich musste im Berichtszeitraum einen Fall bearbeiten, bei dem eine Firma für Sportartikel ihre Kunden bat, anlässlich von Bestellungen auf dem Bestellformular den Namen und die Anschrift von Bekannten und Freunden anzugeben, damit auch diesen Werbematerial zugesandt werden könne. Da diese Praxis weit verbreitet ist, lohnen sich hierzu einige grundlegende Bemerkungen.

Grundsätzlich ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, soweit dies das jeweilige Datenschutzgesetz oder eine andere Rechtsvorschrift erlaubt oder wenn der Betroffenen eingewilligt hat. Hat der Betroffene nicht eingewilligt, was sicher der Fall ist, wenn eine Firma Adressen bei Dritten ohne Wissen der Betroffenen erhebt, richtete sich die Zulässigkeit der Datenerhebung für Werbezwecke in dem konkreten Fall nach § 28 BDSG. Danach mussten auch personenbezogene Daten, die zu Werbezwecken genutzt werden sollten, grundsätzlich beim Betroffenen selbst mit seinem Wissen erhoben werden. Immerhin hat – wie schon das Bundesverfassungsgericht im Volkszählungsurteil von 1983 betont hat – jeder das Recht zu wissen, wer was wann und zu welchem Zweck über ihn an Daten sammelt, speichert und verarbeitet. Nur so ist es dem Betroffenen möglich, der Nutzung seiner Daten zu Werbezwecken zu widersprechen. Zwar ist die Erhebung, Speicherung und Nutzung von Adressdaten potenzieller Interessenten durchaus ein berechtigtes Anliegen der Firmen. Schließlich lebt die Wirtschaft von zielorientierter und einfallsreicher Werbung. Allerdings ist die Verwendung von Adressdaten für Werbezwecke nicht zulässig, wenn es Grund zu der Annahme gibt, dass das schutzwürdige Interesse des Betroffenen am Unterbleiben der Verarbeitung seiner Daten überwiegt. Letzteres ist sicher dann der Fall, wenn sich ein Unternehmen die Adressdaten ohne Wissen des Betroffenen und unter Ausnutzung der Gutmütigkeit eines Bekannten oder Freundes verschafft hat und der Betroffene somit keine Möglichkeit hatte, von seinem Widerspruchsrecht Gebrauch zu machen. Die Aufsichtsbehörde hat das Vorgehen dieser Firma beanstandet. Diese hat die rechtswidrig gewonnenen Daten inzwischen gelöscht und davon abgesehen, künftig noch Kunden aufzufordern, bei Bestellungen Adressen von anderen Personen zu Werbezwecken anzugeben.

Nach der seit dem 1. September 2009 geltenden gesetzlichen Regelung dürfen personenbezogene Daten grundsätzlich nur mit Einwilligung des Be-

troffenen zu Zwecken der Werbung und des Adresshandels weitergegeben werden. Von diesem Grundsatz gibt es allerdings gravierende Ausnahmen: So ist die Weitergabe zum Beispiel auch dann zulässig, wenn der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weitergegeben hat. Diese Stelle muss dem Betroffenen dann auf Nachfrage mitteilen, an wen sie seine Adressdaten zu Werbezwecken in den letzten zwei Jahren übermittelt hat. Ebenfalls ohne Einwilligung ist die Nutzung von Daten für Werbezwecke zulässig, wenn das Unternehmen seine eigene Kunden bewirbt. Aber auch in diesen Fällen hat der Betroffene das Recht, der Zusendung von Werbung zu widersprechen. Auf dieses Recht muss er ausdrücklich hingewiesen werden, wenn er Werbung zugesandt erhält.

Auch wenn es aufgrund der jetzt geltenden Datenschutzgesetze in bestimmten Fällen zulässig ist, Name und Anschrift zu Werbezwecken ohne Wissen des Betroffenen zu erheben und zu nutzen, wird doch dem Daten- und Verbraucherschutz teilweise dadurch Rechnung getragen, dass der Betroffene nachträglich widersprechen kann. Ein Verbot mit Erlaubnisvorbehalt wäre auch hier datenschutzgerechter.

3. Abschnitt: Auskunfteien und Inkassounternehmen

1. Allwissend und auskunftsfreudig – die Auskunfteien

Immer wieder wenden sich Bürger Hilfe suchend an mich, weil ihnen ein Unternehmen den Abschluss eines Vertrages verweigert hat, nachdem dieses von einer Auskunftei über eine angeblich von ihm nicht beglichene Forderung informiert worden war. Das zeigt, dass vielen Bürgern die Arbeitsweise einer Auskunftei und deren rechtliche Möglichkeiten oftmals nicht bekannt sind und dass die Auskunfteien datenschutzrechtliche Vorschriften nicht immer hinreichend beachten.

Bei Auskunfteien handelt es sich um Privatfirmen, die geschäftsmäßig Informationen über säumige Schuldner sammeln und ihre Vertragspartner – insbesondere Wirtschaftsunternehmen wie Telefongesellschaften und Versandwarenhäuser – auf Anfrage über ihre Erkenntnisse informieren, um diese Unternehmen vor Zahlungsausfällen zu schützen. Das Bundesdatenschutzgesetz erkennt diese Funktion im Interesse der Wirtschaft ausdrücklich an, hat aber auch die Risiken für Betroffene im Auge, die zu Unrecht in einer Schuldnerdatei gespeichert sind und dadurch vom Kreditverkehr, von einer Bestellung in einem Versandgeschäft oder vom Abschluss eines Telefonvertrags ausgeschlossen sind.

Im Einzelnen sieht das Bundessdatenschutzgesetz dazu Folgendes vor:

– Nach § 28 a Absatz 1 BDSG darf ein Gläubiger beziehungsweise ein von ihm beauftragter Rechtsanwalt oder ein Inkassoinstitut die Daten eines Schuldners einschließlich der Höhe der von ihm nicht beglichenen Forderung an eine Auskunftei übermitteln, wenn die Forderung durch ein vollstreckbares Urteil oder einen rechtskräftigen gerichtlichen Mahnbescheid festgestellt worden ist, oder wenn der Gläubiger das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos kündigen kann. Dasselbe gilt, wenn der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist, wobei zwischen der ersten Mahnung und der Übermittlung an die Auskunftei mindestens vier Wochen liegen müssen, der Schuldner rechtzeitig auf die beabsichtigte Übermittlung aufmerksam gemacht worden ist und er die Forderung nicht bestritten hat. Wurde eine Forderung bestritten, darf die Übermittlung an die Auskunftei erst erfolgen, wenn der Schuldner die Forderung nachträglich, etwa durch Leistung des geschuldeten Betrages, anerkennt oder wenn die Berechtigung der Forderung gerichtlich festgestellt worden ist und der Schuldner daraufhin nicht innerhalb einer angemessenen Frist bezahlt hat. Dem Bestreiten kommt nur ausnahmsweise keine „hemmende“ Wirkung zu, wenn es rechtsmissbräuchlich ist, also nur dazu dienen soll, dem Schuldner einen

ihm nicht zustehenden Zahlungsaufschub zu verschaffen. Neben diesen „weichen“ Negativmerkmalen (Daten aus vorgerichtlichen Inkassoverfahren) und „mittleren“ Merkmalen (Daten aus gerichtlichen Verfahren) beschaffen sich die Auskunfteien „harte“ Merkmale (Daten über Insolvenzeröffnungen und aus den gerichtlichen Schuldnerverzeichnissen), die sie bei den Amtsgerichten anfordern können.

– Die solchermaßen rechtmäßig einer Auskunftei übermittelten Daten darf diese speichern. Die Auskunftei betreibt dabei ein eigenes Geschäft, handelt also nicht im Auftrag oder Interesse der einmeldenden Stelle. Damit ist sie für die bei ihr gespeicherten Daten verantwortliche Stelle und kann sich nicht ohne Weiteres darauf berufen, sie habe nur gespeichert, was ihr von Dritten übermittelt worden ist, ohne für die inhaltliche Richtigkeit einstehen zu müssen. Zwar muss die Auskunftei nicht unbedingt bei jeder Einmeldung prüfen, ob die gesetzlichen Voraussetzungen für eine Speicherung vorliegen und ob die angemeldete Forderung besteht und fällig ist oder ob dagegen berechtigte Einwendungen bestehen. Doch muss eine Auskunftei zur Gewährleistung des Schuldnerschutzes durch Absprachen mit den einmeldenden Unternehmen sicherstellen, dass diese nur „berechtigte“ Forderungen übermitteln. Ob sich diese Unternehmen daran halten, hat die Auskunftei durch Stichproben zu überprüfen. Auch trifft die Auskunftei die Pflicht, nachträglichen Änderungen Rechnung zu tragen und Datensätze zu berichtigen, gegebenenfalls sogar zu löschen. Letzteres ist erforderlich, wenn der Schuldner gegenüber dem Gläubiger, dessen Vertretern oder gegenüber der Auskunftei die Forderung in beachtlicher Weise nachträglich bestreitet. Dem Bestreiten gleichzusetzen ist es, wenn der Schuldner gegen einen Mahnbescheid einen Widerspruch erhebt oder in einem Klageverfahren der angeblichen Forderung entgegentritt. Zu einer wesentlichen Änderung kann auch der nachträgliche Abschluss eines Vergleiches führen. Tritt der Vergleich an die Stelle einer umstrittenen Forderung, darf dieser nur dann gespeichert werden, wenn er nach seinem Abschluss nicht innerhalb einer angemessenen Frist erfüllt wird. Er tritt sozusagen an die Stelle der bislang nicht akzeptierten Forderung. Dagegen darf die ursprüngliche Forderung gespeichert bleiben, wenn dem Schuldner lediglich kulanzhalber ein Teil von ihr erlassen wird oder wenn ihm im Wege einer Zahlungsvereinbarung nachträglich Ratenzahlung gewährt wird. Die Auskunftei muss die Stellen, die bei ihr Einmeldungen vornehmen können, anhalten, alle relevanten Änderungen mitzuteilen. Ferner müssen Speicherungen gelöscht werden, wenn der Betroffene deren Unrichtigkeit schlüssig darlegt und die Auskunftei nicht in der Lage ist, die Richtigkeit der Speicherung zu beweisen.

– Die Auskunftei darf die zu einem Schuldner gespeicherten Erkenntnisse an anfragende Dritte übermitteln beziehungsweise zum Abruf bereit halten, soweit dies mit der Zielsetzung der Auskunftei in Einklang steht. Eine Auskunftei, die Unternehmen vor finanziellen Ausfallrisiken bewahren will, darf somit keine Adressdaten zum Zwecke des Auffindens einer gesuchten Person weitergeben. Der Anfragende muss ein berechtigtes Interesse an der Auskunft darlegen. Andererseits dürfen der Beauskunftung keine höherwertigen schutzwürdigen Interessen des Betroffenen gegenüberstehen. Allerdings kann sich die Auskunftei auf die stichprobenweise Überprüfung der von den Anfragenden – etwa von Kreditinstituten vor der Gewährung eines Kredits oder von Telekommunikationsunternehmen vor dem Abschluss eines Handyvertrags – geltend gemachten Interessen beschränken. Ein schutzwürdiges Interesse der Betroffenen liegt allerdings nicht bereits dann vor, wenn sie nur mit „Kleinstbeträgen“ im Zahlungsverzug sind. Dieser Umstand vermag nämlich durchaus etwas über ihr Zahlungsverhalten und damit über ihre Kreditwürdigkeit auszusagen. Eine wichtige Verpflichtung trifft die Auskunftei vor jeder Übermittlung: Sie muss sich davon überzeugen, ob sich die Informationen, die weitergegeben werden sollen, tatsächlich auf die Personen beziehen, zu der die Anfrage erfolgt ist. Verwechslungen können zu fatalen Nachteilen für den Betroffenen, aber auch für die anfragende Stelle führen (vgl. hierzu unten 7. Teil, 3. Abschnitt, Nr. 4).

– Nach § 35 Absatz 2 Satz 2 Nr. 4 BDSG muss die Auskunftei die bei ihr gespeicherten Daten grundsätzlich nach einer Speicherdauer von vier

Jahren, beginnend mit dem Jahr, das nach der Speicherung folgt, daraufhin überprüfen, ob die weitere Speicherung noch erforderlich ist. Wurde die Forderung erst im folgenden Jahr nach ihrer Fälligkeit eingemeldet, verkürzt sich diese Prüffrist. Vergleichbares gilt für den Fall, dass sich der der Speicherung zugrunde liegende Sachverhalt erledigt hat und der Betroffene nicht widerspricht. Dann beträgt die Prüffrist nur drei Jahre. Eine Erledigung in diesem Sinne tritt allerdings nicht dadurch ein, dass der sich in Verzug befindliche Schuldner die Forderung begleicht, mit ihm eine Zahlungsvereinbarung getroffen wird oder der offene Betrag beigetrieben werden konnte. Will die Auskunftei die jeweiligen Daten auch weiterhin speichern, muss es dafür einen besonderen Grund geben, weshalb potenzielle Vertragspartner unbedingt vor dem Betroffenen gewarnt werden müssen. Das bloße Nichtbegleichen einer Forderung reicht dafür nicht aus. Vielmehr müssen sonstige erhebliche Umstände hinzukommen. Gibt es bei einer Auskunftei keine Speicherungen mehr, die etwas über die Kreditwürdigkeit des Betroffenen aussagen, müssen auch dessen Grundpersonalien gelöscht werden.

– Die Auskunftei hat den Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten, deren Herkunft und zumindest die Kategorie von Empfängern zu erteilen, an die die Daten gegebenenfalls übermittelt werden sollen. Nur ausnahmsweise darf die speichernde Stelle Angaben zur Herkunft der Daten verweigern, wenn die einmeldende Stelle in besonderem Maße schutzwürdig ist, was die Auskunftei allerdings bei einer datenschutzrechtlichen Kontrolle belegen können muss. Hat die Auskunftei Zweifel an der Identität des Anfragenden beziehungsweise daran, welcher Datensatz ihm zuzuordnen ist, darf sie Erhebungen zur näheren Identifizierung des um Selbstauskunft Ersuchenden vornehmen. Unter Umständen kann sie sich dann, aber nur dann, sogar die Kopie des Personalausweises vorlegen lassen. Für eine einmal im Jahr verlangte Selbstauskunft darf keine Gebühr erhoben werden. Weitere Selbstauskünfte innerhalb eines Jahres sind nur gebührenpflichtig, wenn die Auskunftei darlegt, dass der Anfragende sie zu wirtschaftlichen Zwecken nutzt.

Die damals zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hatte im Berichtszeitraum in einem mehrjährigen Verfahren eine in Baden-Württemberg ansässige Auskunftei geprüft und dabei eine Reihe von Unzulänglichkeiten festgestellt, die mit dem geltenden Datenschutzrecht nicht in Einklang standen. So sahen die „Einmelderichtlinien“ dieser Auskunftei nicht vor, dass nur Forderungen eingemeldet werden dürfen, die auch berechtigterweise gespeichert werden können. Es wurden unter Umständen also auch bestrittene Forderungen gespeichert. Hinzu kam, dass Einmeldungen über nicht bezahlte Rechnungen ungeachtet der im Gesetz vorgesehenen Prüfverpflichtungen bis zu zehn Jahren gespeichert blieben, ohne dass es dafür einen triftigen Grund gab. Eine Datenlöschkonzeption, in der die Gründe aufgelistet sind, die eine längere Speicherung rechtfertigen können, existierte nicht. Personalgrunddaten, die gar nichts über die Bonität eines Betroffenen aussagen, blieben bei dieser Auskunftei ewig gespeichert. Bestritt der Betroffene eine Forderung gegenüber der Auskunftei oder verlangte er deren Berichtigung, setzte sich die Auskunftei mit der einmeldenden Stelle in Verbindung. Behauptete diese gegenüber der Auskunftei deren Richtigkeit, verwies die Auskunftei den Betroffenen an die einmeldende Stelle, statt das angegriffene Datum umgehend zu löschen beziehungsweise zu berichtigen, wie es das Gesetz vorschreibt. Die Auskunftei verkannte zudem, dass sie für die Speicherung verantwortliche Stelle war. Blieb bei einer Anfrage zweifelhaft, ob die Person, zu der das Auskunftsersuchen erfolgte, und die, zu der bei der Auskunftei Speicherungen vorhanden waren, identisch sind, nahm die Auskunftei eine Beauskunftung „unter Vorbehalt“ vor, wobei sie in Kauf nahm, dass unzutreffende Daten übermittelt wurden. Nachträgliche Änderungsmeldungen erfolgten gegenüber einer Stelle, die Auskünfte empfangen hatte, auch in den Fällen, in denen sich die Speicherung zugunsten des Betroffenen später geändert hatte, nur, wenn dies zwischen der Auskunftei und der Stelle, der die Auskunft zugegangen war, ausdrücklich vereinbart worden war. Unzulässigerweise erteilte die Auskunftei nur Selbstauskünfte, wenn der Betroffene eine Kopie seines Personalausweises vorlegte.

Die betreffende Auskunftei hat ihre Betriebsabläufe an das geltende Datenschutzrecht anzupassen. Gespräche über die inhaltliche und zeitliche Umsetzung wurden aufgenommen. Die Aufsichtsbehörde hat die Ergebnisse ihrer mehrjährigen Prüfungen der Auskunftei noch kurz vor dem Zuständigkeitswechsel in einem umfassenden Bericht zusammengefasst, der nun Punkt für Punkt abzuarbeiten ist. Unabhängig davon werden meine Mitarbeiter und ich Beschwerden in jedem Einzelfall nachgehen, um die Rechte der Betroffenen zu wahren.

2. Scoring

Nicht unbedenklich – und dies keineswegs nur in datenschutzrechtlicher Hinsicht – ist die Tatsache, dass Auskunfteien für ihre Vertragspartner einen sog. Scorewert über Privatpersonen ermitteln und damit deren Wertigkeit im Wirtschaftsleben mit einer Punktzahl taxieren dürfen.

Bei dem Scorewert handelt es sich um eine Zahlenangabe, die auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei einer Auskunftei gespeicherten Angaben zum Zahlungsverhalten einer Person errechnet wird. Dieser Wert soll eine Aussage über die künftige Zahlungsbereitschaft des Betroffenen treffen und damit einen Beitrag zur Einschätzung seiner Kreditwürdigkeit durch den Empfänger des Scorewertes leisten. Empfänger sind die Vertragspartner der Auskunftei, die zu entscheiden haben, ob sie einer bestimmten Person einen Kredit gewähren oder mit dieser einen sonstigen Vertrag abschließen, und wenn ja, zu welchen Konditionen. Je schlechter aber der Scorewert ist, desto schlechter sind auch die Bedingungen, unter denen der Kredit gewährt oder etwa ein Kaufvertrag geschlossen wird. Im ungünstigsten Fall wird der Abschluss eines Vertrages abgelehnt oder er kommt nur bei Vorauszahlung durch den angeblich risikobehafteten Kunden zustande. Die Empfänger legen den Scorewert erfahrungsgemäß ungeprüft ihren Entscheidungen zugrunde.

Nach § 28 b BDSG ist es zulässig, dass Auskunfteien zum Zwecke der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses einen Wahrscheinlichkeitswert zum künftigen Verhalten des Betroffenen ermitteln und weitergeben, wenn dafür ein wissenschaftlich anerkanntes mathematisch-statistisches Verfahren eingesetzt wird, die in die Berechnung eingehenden Daten dafür „erheblich“ sind und von der Auskunftei nach § 28 a BDSG gespeichert werden dürfen sowie wenn für die Berechnung des Wahrscheinlichkeitswertes nicht nur „Anschriftendaten“ genutzt werden. Man wird daher datenschutzrechtlich nichts dagegen einwenden können, dass eine Auskunftei aufgrund ihrer Erkenntnisse zum Zahlungsverhalten einer Person etwas dazu sagt, wie diese mutmaßlich künftig finanzielle Verpflichtungen erfüllen wird. Das Bundesdatenschutzgesetz lässt zu, dass bei der Berechnung des Scorewertes die Anschrift und damit das Wohnumfeld des Betroffenen sowie die zu dessen Zahlungsverhalten zu Recht gespeicherten Daten verwendet werden, vorausgesetzt, diese Erkenntnisse sind aktuell, also nicht älter als drei Jahre. Nicht zulässig ist es dagegen – um Beispiele aus der Aufsichtspraxis anzuführen –, dass die Auskunftei aus dem Vornamen des Betroffenen auf dessen Alter schließt, dass die Wohndauer an einem bestimmten Wohnort mit einfließt und dass das Baujahr des Wohngebäudes, in dem der Betroffene wohnt, Berücksichtigung findet. Zwar akzeptiert der Gesetzgeber, dass Rückschlüsse auf die Kreditwürdigkeit aus dem Wohnumfeld des Betroffenen gezogen werden dürfen, wenn noch andere Erkenntnisse in die Berechnung mit einfließen. Doch auch dies ist aus meiner Sicht bedenklich, da es keine Lebenserfahrung gibt, dass jemand bereits deswegen ein säumiger Zahler sein wird, weil in seiner Wohnumgebung solche wohnen. Da ist es auch nur ein schwacher Trost, dass der Betroffene vor Berechnung des Score-Wertes über die beabsichtigte Nutzung der Anschrift zu unterrichten ist (§ 28 b Nr. 4 BDSG).

Eigentlich würde es ausreichen, wenn die Auskunfteien künftigen Gläubigern eines Betroffenen nur bonitätsrelevante Tatsachen zu dessen Zahlungsverhalten in der Vergangenheit offenbaren, weil diese ohnehin selbst entscheiden müssen, inwieweit sie eine Person für kreditwürdig erachten.

Dass man Menschen „berechnet“ und den zu ihnen ermittelten Wert einem Dritten, der eigentlich eine eigenverantwortliche Entscheidung zu treffen hat, zugänglich macht, ist mehr als fragwürdig und wird auch künftig den Datenschutz beschäftigen.

3. Datenschutz bei Durchleiteauskunfteien

Die Auskunftserteilung von Bonitätsdaten hat sich zu einem bedeutenden Wirtschaftszweig entwickelt. Auf diesem Markt betätigen sich auch sogenannte Durchleiteauskunfteien, die selbst keine Bonitätsdaten speichern. Dennoch unterliegen sie im vollen Umfang den für Auskunfteien geltenden datenschutzrechtlichen Vorschriften.

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hat bereits in ihrem Vierten Tätigkeitsbericht 2007 (C 3.5, S. 86 ff.) das Geschäftsmodell sogenannter Durchleiteauskunfteien und die dafür geltenden datenschutzrechtlichen Anforderungen dargestellt. Bei einer Durchleiteauskunftei handelt es sich um einen Dienstleister, der Bonitätsauskünfte erteilt, dabei aber nicht auf eigene Daten, sondern ausschließlich auf die Datenbestände einer oder mehrerer klassischer Auskunfteien zugreift.

Im Zusammenhang mit der Überprüfung einer in Baden-Württemberg ansässigen Durchleiteauskunftei bestand Anlass zur Klarstellung, dass auch diese Dienstleister verantwortliche Stelle im Sinne des Datenschutzrechts sind. Dies gilt unbeschadet des Umstands, dass die Durchleiteauskunftei selbst keine Bonitätsdaten speichert. Insbesondere stellt ihre Tätigkeit keine Verarbeitung personenbezogener Daten im Auftrag der klassischen Auskunftei dar, deren Daten sie sich für die Auskunftserteilung bedient. Die von der Aufsichtsbehörde überprüfte Durchleiteauskunftei, die auch Ärzte zu ihren Kunden zählt, hatte diesen eine Mustererklärung für die Einwilligung der Patienten in die Einholung von Bonitätsauskünften und die hierfür notwendige Schweigepflichtentbindung zur Verfügung gestellt. Darin hatte sie angegeben, personenbezogene Daten im Auftrag einer namentlich genannten klassischen Auskunftei zu verarbeiten. Die Aufsichtsbehörde hat daraufhin eine Änderung der Mustererklärung bewirkt.

Da die Durchleiteauskunftei verantwortliche Stelle für die Übermittlung der beauskunfteten Bonitätsdaten ist, hat sie auch die für Auskunfteien geltenden Vorgaben des Datenschutzrechts vollumfänglich zu wahren. Sie ist daher unter anderem verpflichtet, nachträglich stichprobenweise zu überprüfen, ob bei den abfragenden Stellen zum Zeitpunkt der Abfrage ein berechtigtes Interesse an der Erteilung einer Bonitätsauskunft vorgelegen hat. Dabei darf die Durchleiteauskunftei nicht auf Stichproben der klassischen Auskunftei zurückgreifen, sondern muss eigene Stichproben durchführen. Zwischen den Auskunfteien und den Datenschutzaufsichtsbehörden wurde verabredet, dass die Auskunfteien mindestens 1 % aller Bonitätsabfragen einer Stichprobe unterziehen, wobei sie eine Mindestzahl von jährlich zwölf Stichproben erreichen sollen. Die abfragenden Stellen müssen die Art des berechtigten Interesses bereits bei der Abfrage dokumentieren.

Als verantwortliche Stelle ist die Durchleiteauskunftei auch selbst zur Auskunftserteilung an den Betroffenen verpflichtet. Die pflichtgemäße Auskunft umfasst zum einen etwaige Daten, die bei der Durchleiteauskunftei selbst gespeichert sind, wie zum Beispiel Protokolldaten und Daten über den Selbstauskunftsantrag des Betroffenen. Darüber hinaus ist nach der zum 1. April 2010 in Kraft getretenen Vorschrift des § 34 Absatz 3 Satz 2 Nr. 2 BDSG auch über diejenigen Daten Auskunft zu erteilen, die die verantwortliche Stelle nicht selbst speichert, aber zum Zweck der Auskunftserteilung nutzt. Mithin sind Gegenstand der Selbstauskunft auch die aktuell bei der klassischen Auskunftei gespeicherten Daten, soweit die Durchleiteauskunftei diese auf eine Bonitätsabfrage hin übermitteln würde. Hingegen genügt die Durchleiteauskunftei ihrer Pflicht zur Selbstauskunft nicht, wenn sie den Betroffenen insoweit an die klassische Auskunftei verweist.

Hinsichtlich der von einer klassischen Auskunftei bezogenen Daten hat die Durchleiteauskunftei in der Selbstauskunft den Namen und die Anschrift der klassischen Auskunftei anzugeben. Als Empfänger der Daten sind die

Stellen anzugeben, denen eine Bonitätsauskunft erteilt wurde. Dabei sind in der Selbstauskunft auch das Datum und der Inhalt der Auskunft zu vermerken.

Darüber hinaus ist die Durchleiteauskunftei ebenso wie eine klassische Auskunftei verpflichtet, den Betroffenen zu benachrichtigen, wenn sie erstmals dessen personenbezogene Daten im Rahmen einer Bonitätsauskunft an einen Dritten übermittelt. Zwar gilt die Benachrichtigungspflicht gemäß § 33 Absatz 1 Satz 2 BDSG dem Wortlaut nach nur für Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen speichern. Eine Durchleiteauskunftei speichert die Bonitätsdaten im Gegensatz zur klassischen Auskunftei nicht selbst. Da sie aber nach außen wie eine eigenständige Auskunftei auftritt, muss sie sich in datenschutzrechtlicher Hinsicht auch wie eine solche behandeln lassen. Auch Durchleiteauskunfteien müssen den Betroffenen daher über eine erstmalige Übermittlung seiner personenbezogenen Daten unterrichten.

Durchleiteauskunfteien sind ebenso wie klassische Auskunfteien, die selbst personenbezogene Daten speichern, verantwortliche Stellen im Sinne des Datenschutzrechts. Sie haben daher in gleichem Maße die Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten.

4. Personenverwechslung beim Inkasso

Von Zeit zu Zeit kommt es vor, dass Inkassobüros mit ihren Maßnahmen zur Forderungseinziehung versehentlich nicht den Schuldner, sondern einen gleichnamigen Dritten treffen. Schuld daran ist mangelnde Sorgfalt der mit der Adressermittlung befassten Stelle.

Gelegentlich beschweren sich Bürger bei mir darüber, dass Inkassounternehmen versuchen, bei ihnen Forderungen einzuziehen, obwohl sie selbst nicht deren Schuldner sind und auch sonst zu keinem Zeitpunkt in einer Geschäftsbeziehung mit dem Auftraggeber des Inkassobüros gestanden haben. Dies liegt zuweilen daran, dass der Betroffene mit einem Schuldner gleichen Namens verwechselt worden ist. Versehen dieser Art können für den Betroffenen zu schwerwiegenden Beeinträchtigungen führen, wenn die Forderung bei einer Auskunftei eingemeldet und in der Folge zu Unrecht als negatives Bonitätsmerkmal des Betroffenen beauskunftet wird.

In einem konkreten Fall hatte ein Inkassounternehmen zunächst eine in Baden-Württemberg ansässige Auskunftei eingeschaltet, um die Anschrift des Schuldners zu aktualisieren. Die Auskunftei unterhielt Geschäftsbeziehungen zu mehreren Dienstleistern, deren Aufgabe es war, die vom Inkassobüro gemeldete Schuldneranschrift durch Einholung von Melderegisterauskünften zu überprüfen. Die auf diese Weise ermittelten Adressdaten wurden sodann über die Auskunftei an das anfragende Inkassounternehmen weitergeleitet.

Einer der Dienstleister, der von der Auskunftei mit der Adressermittlung beauftragt worden war, fragte bei der in einem anderen Land gelegenen Meldebehörde des ehemaligen Schuldnerwohnsitzes nach der aktuellen Anschrift, wobei er in der Anfrage den Namen, die Voranschrift und das Geburtsdatum des Schuldners angab. Da unter der gleichen Anschrift vormals auch ein Namensvetter des Schuldners gewohnt hatte, teilte die Meldebehörde dem anfragenden Dienstleister dessen neue Adresse mit, vermerkte in der Auskunft jedoch, dass das von ihm angegebene Geburtsdatum nicht mit dem im Melderegister gespeicherten übereinstimmte. Dennoch gab der Dienstleister nur die neue Anschrift, nicht aber die vollständige Melderegisterauskunft an die Auskunftei weiter. Die Auskunftei erfuhr daher nicht, dass das in der Anfrage des Dienstleisters genannte Geburtsdatum nicht mit dem beim Melderegister gespeicherten übereinstimmte. Die Auskunftei übermittelte sodann die neue Anschrift des Beschwerdeführers an das Inkassounternehmen.

Bei der dargestellten Verfahrensweise haben mehrere Beteiligte gegen das Datenschutzrecht verstoßen. Da das Geburtsdatum in der Anfrage des Dienstleisters von dem im Melderegister gespeicherten abwich, hätte die Meldebehörde die Auskunft über die neue Anschrift des Betroffenen bereits nicht erteilen dürfen. Ebenso hätte der Dienstleister die ermittelte Adresse

nicht an die Auskunftei weiterleiten dürfen, ohne sie auf die mangelnde Übereinstimmung der Geburtsdaten hinzuweisen.

Der mit der Adressermittlung beauftragte Dienstleister versah diese Aufgabe im Wege der Auftragsdatenverarbeitung für die Auskunftei. Diese war somit für die Datenschutzkonformität der Adressdatenerhebung verantwortlich. Die Auskunftei wäre daher verpflichtet gewesen, mit dem Dienstleister vertragliche Festlegungen darüber zu treffen, wie bei Melderegisteranfragen und bestimmten Melderegisterauskünften zu verfahren sei. Zur effektiven Vermeidung von Personenverwechslungen wäre außerdem zu vereinbaren gewesen, wie lange Melderegisterauskünfte aus früheren Verfahren vom Dienstleister im Auftrag der Auskunftei verwendet werden dürfen. Die Verpflichtung zur schriftlichen Fixierung solcher Abreden folgt für den Fall der Auftragsdatenverarbeitung aus § 11 Absatz 2 Satz 2 BDSG. Die Vorschrift enthält eine nicht abschließende Aufzählung der Vertragsbestandteile, die im Einzelnen schriftlich zu regeln sind. Besteht die Auftragsdatenverarbeitung in der Einholung von Melderegisterauskünften, so ist auch das dabei einzuhaltende Verfahren zwischen der verantwortlichen Stelle und dem Auftragnehmer schriftlich zu vereinbaren.

Um zu vermeiden, dass Inkassounternehmen gegen den falschen Betroffenen vorgehen, sind Adressermittlungen durch alle beteiligten Stellen nur mit größter Sorgfalt durchzuführen.

5. Rechtsanwälte und der Datenschutz

Rechtsanwälte berufen sich immer wieder darauf, wegen des Mandantengeheimnisses nicht verpflichtet zu sein, sich an das Bundesdatenschutzgesetz halten zu müssen. Insbesondere verweigern sie Auskünfte gegenüber der unabhängigen Aufsichtsbehörde sowie die Beantwortung von Auskunftsersuchen von Bürgern.

Für Rechtsanwälte gelten besonders strenge datenschutzrechtliche Bestimmungen. Zum einen machen sie sich nach § 203 des Strafgesetzbuches strafbar, wenn sie eine Information, die ihnen von ihrer Mandantschaft anvertraut worden ist, ohne deren Einwilligung offenbaren. Diese Vorschrift wird ergänzt durch § 43 a Absatz 2 der Bundesrechtsanwaltsordnung, wonach der Anwalt zur Verschwiegenheit über alles verpflichtet ist, was ihm bei seiner Berufsausübung bekannt wurde. Darüber hinaus gilt das Bundesdatenschutzgesetz auch für Rechtsanwälte.

Das hat in der Tat zur Folge, dass ein Anwalt nur meinen Auskunftsersuchen nach § 38 Absatz 3 BDSG entsprechen darf, soweit ihn seine Mandantschaft von der Schweigepflicht befreit hat. Denn diese Vorschrift regelt ausdrücklich, dass besagte Auskunftspflicht dann nicht besteht, wenn der Betroffene sich durch deren Erfüllung strafbar machen würde. Vergleichbares gilt nach § 34 Absatz 7 in Verbindung mit § 33 Absatz 2 Nr. 3 BDSG für die Beantwortung sog. Selbstauskunftsverlangen. Wer also wissen will, was ein von einer Firma beauftragter Anwalt über ihn gespeichert hat, sollte sich an diese wenden. Sie kann am ehesten sagen, welche Informationen sie an ihren Anwalt weitergegeben hat, kann sich aber selbst unter Umständen auf das Auskunftsverweigerungsrecht des § 34 Absatz 7 in Verbindung mit § 33 Absatz 2 Nr. 7 b BDSG berufen, wenn die Beantwortung des Selbstauskunftsersuchens ihre eigenen Geschäftszwecke, etwa die Führung eines Prozesses, gefährden würde.

Ungeachtet dessen unterliegen auch die Anwälte meiner Kontrolle, soweit die bei ihnen gespeicherten Daten automatisiert verarbeitet werden, im Hinblick darauf, ob sie den oben zitierten Bestimmungen Rechnung tragen, nicht zuletzt im Interesse ihrer Mandaten. Denn diese haben so gut wie keine Möglichkeit, sich selbst davon zu überzeugen, ob der von ihnen beauftragte Anwalt auch die nötige Sorgfalt im Umgang mit den ihm anvertrauten Informationen walten lässt. Eine derartige Kontrollkompetenz sehen die § 38 Absatz 4 in Verbindung mit § 26 Absätze 2 und 6 BDSG ausdrücklich für den Datenschutzbeauftragten auch hinsichtlich solcher Daten vor, die einem besonderen Berufsgeheimnis, hier dem Mandantengeheimnis, unterliegen. Auch die Bundesregierung hatte diese Rechtsauffassung anläss-

lich ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Jahr 2007 ausdrücklich bestätigt. Allerdings darf die Kontrollbehörde bei ihrer Überprüfung zwar Einsicht in sämtliche Unterlagen des Anwalts in dessen Kanzleiräumen nehmen. Einem Beschwerdeführer, der sich an mich wendet, der Anwalt würde seine personenbezogenen Daten rechtswidrig verarbeiten, darf ich aber nach Abschluss meiner Kontrolle nur mitteilen, ob dies zutrifft oder nicht und dass ich gegebenenfalls Anordnungen zur Beseitigung des Missstandes gegenüber dem Anwalt getroffen habe. Die Unterrichtungsbefugnis gegenüber einem Petenten geht nämlich nicht weiter als die Auskunftsverpflichtung des Anwaltes nach § 34 Absatz 7 BDSG selbst.

Der Anwalt eines Telekommunikationsunternehmens hatte sich in der Vergangenheit stets geweigert, Auskunftsersuchen der Datenschutzaufsicht zu beantworten. Jetzt hat sich das Unternehmen selbst bereit erklärt, in bestimmten Fällen auf die Geheimhaltungspflicht durch seinen Anwalt zu verzichten. In den Fällen, in denen sich Bürger über die Datenverarbeitung durch einen Anwalt beschweren, ohne diesen von seiner Schweigepflicht befreien zu können, habe ich durchaus die Möglichkeit, der Beschwerde nachzugehen. Konkretisieren sich die Vorwürfe gegen den Anwalt, gebe ich dem Anwalt Gelegenheit, sich zu „entlasten“. Es liegt nun an diesem, sich von seinem Mandanten von der Schweigepflicht entbinden zu lassen. Tut er dies nicht, obwohl es ihm beziehungsweise seinem Mandanten zumutbar ist, kann die Datenschutzbehörde aus der Mitwirkungsverweigerung für den Anwalt und seine Art, wie er mit ihm anvertrauten personenbezogenen Daten umgeht, nachhaltige Schlüsse ziehen.

Gerade das Rechtsstaatsprinzip erfordert, dass auch Anwälte sich an das Datenschutzrecht halten und entsprechend beaufsichtigt werden. Wir werden uns in Zukunft verstärkt dieses Personenkreises annehmen.

4. Abschnitt: Versicherungen

1. Das neue Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft

Zu den Grundproblemen der Versicherungswirtschaft gehört der Zielkonflikt zwischen dem berechtigtem Interesse, Versicherungsmissbrauch und -betrug zu verhindern und der gleichzeitigen Wahrung der informationellen Selbstbestimmung der Versicherungsnehmer und Antragsteller. Seit der Inbetriebnahme des neuen HIS besteht hierfür ein datenschutzkonformes Instrument.

Am 1. April 2011 ist das neue Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft in Betrieb genommen worden, das der Verhinderung von Versicherungsmissbrauch und -betrug dient. Betreiber des Systems ist die informa Insurance Risk and Fraud Prevention GmbH (IIRFP) mit Sitz in Baden-Baden. Das Unternehmen gehört der arvato-infoscore-Gruppe an, zu der auch die zweitgrößte deutsche Auskunftei, die infoscore Consumer Data GmbH (ICD), gehört. Die Versicherungsunternehmen melden Informationen in das HIS ein, die für die Risikobeurteilung von Belang sind oder die auf einen Betrugsverdacht hindeuten könnten. Die eingemeldeten Daten werden im HIS in zwei voneinander getrennten Datensammlungen gespeichert. Ein sog. A-Pool enthält Daten über die Antragstellung für den Abschluss von Versicherungsverträgen. In einem L-Pool werden Daten über Leistungsfälle geführt. Unter den einschlägigen Voraussetzungen des Bundesdatenschutzgesetzes können die Versicherungen aus beiden Datenbanken personenbezogene Daten zur Risikoprüfung im Antragsbereich oder zur Schadensfallprüfung im Leistungsbereich abrufen.

Das neue HIS ersetzt das bereits seit 1993 vom Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) verwendete alte HIS, das früher auch Uniwagnis genannt wurde. Dieses System genügte in vielerlei Hinsicht nicht den Anforderungen des Datenschutzrechts (vgl. Vierter Tätigkeitsbericht des Innenministeriums 2007, Abschnitt C 4.1.3; Fünfter Tätigkeitsbericht des Innenministeriums 2009, Abschnitt B 4.1.3). Insbesondere konnte der einzelne Versicherungsnehmer aufgrund der von den Versiche-

rungsunternehmen vorformulierten Einwilligungserklärung nicht überblicken, welche Datenübermittlungen bei welcher Gelegenheit stattfinden konnten und welche Folgen dies für ihn hatte. Da die Einwilligungserklärung zudem anlässlich der Antragstellung unterzeichnet wurde, war auch ihre Freiwilligkeit zweifelhaft.

Angesichts dieser Mängel hatten die Datenschutzaufsichtsbehörden das alte HIS bereits 2007 als datenschutzrechtlich unzulässig beanstandet und seine befristete Weiternutzung nur unter Auflagen geduldet. Hierzu gehörten eine bessere Information der Versicherungsnehmer über die im Rahmen des HIS stattfindenden Datenverarbeitungsvorgänge, Einschränkungen hinsichtlich der Einmeldung von Daten in das HIS sowie die Gewährleistung des Selbstauskunftsanspruchs der Betroffenen durch den GDV. Die Duldung der befristeten Weiternutzung des alten HIS stand zudem unter der Bedingung, dass dieses zeitnah durch ein neues, datenschutzkonformes System ersetzt werde. Der GDV hat das neue HIS in enger Abstimmung mit einer Arbeitsgruppe der Datenschutzaufsichtsbehörden der Länder konzipiert.

Da die IIRFP als Betreiberin des neuen HIS in Baden-Baden ansässig ist, hat sich die somit zuständige baden-württembergische Aufsichtsbehörde in mehreren Tests davon überzeugt, dass das System den Vorgaben des Datenschutzrechts genügt. Für die nunmehr erreichte Datenschutzkonformität sind insbesondere die folgenden Faktoren von Bedeutung:

- Das neue HIS wird als reine Auskunftei ausschließlich auf der Grundlage der hierfür bestehenden gesetzlichen Vorschriften des Bundesdatenschutzgesetzes betrieben. Daher bedarf es für die zulässige Einmeldung personenbezogener Daten ins HIS, für die Speicherung dort und für den Datenabruf durch die Versicherungsunternehmen nicht mehr der Einwilligung des Versicherungsnehmers. Verantwortliche Stelle ist die IIRFP, deren einziger Geschäftszweck der Betrieb des HIS ist. Das System ist streng von der Datenbank der ICD getrennt.
- Eine strenge Datentrennung besteht auch zwischen dem Antragsbereich (A-Pool) und dem Leistungsbereich (L-Pool) sowie zwischen den verschiedenen Versicherungssparten. Auf diese Weise ist gewährleistet, dass dem jeweils zuständigen Sachbearbeiter nur diejenigen Daten offenbart werden, die er für die Bearbeitung seines Aufgabenbereichs benötigt.
- Die IIRFP erteilt Auskünfte aus dem HIS nur an Versicherungen. Voraussetzung hierfür ist, dass diese im Einzelfall ein berechtigtes Interesse am Datenabruf haben. Alle Abfragen werden protokolliert. Die abfragenden Versicherungsunternehmen müssen die Gründe für das Vorliegen ihres berechtigten Interesses dokumentieren, damit die IIRFP stichprobenweise überprüfen kann, ob die Abfragen zulässig waren. Eine Übermittlung sämtlicher zu einem Betroffenen vorliegenden Daten in regelmäßigen Abständen findet nicht statt.
- Die Versicherung, die eine Einmeldung an das HIS vornimmt, hat den Betroffenen unverzüglich hiervon zu benachrichtigen. Auf diese Weise kann er bei der IIRFP frühzeitig eine Selbstauskunft über die dort gespeicherten Daten beantragen. Wie jede Auskunftei hat auch die IIRFP die Selbstauskunft einmal jährlich kostenlos zu erteilen.
- Die Selbstauskunft weist ein hohes Maß an Transparenz auf. Der Betroffene muss aus ihr ersehen können, wann welche Daten über ihn innerhalb der letzten zwölf Monate übermittelt wurden. Sollten personenbezogene Daten unrichtig oder zu Unrecht gespeichert sein, kann er von der IIRFP die Berichtigung oder Löschung seiner Daten verlangen. Die IIRFP wird allerdings in der Regel nicht beurteilen können, ob das Anliegen des Betroffenen begründet ist und wird sich zur Klärung dieser Frage an die einmeldende Versicherung wenden müssen. Der Betroffene kann seinen Anspruch auf Berichtigung oder Löschung aber auch selbst beim Versicherungsunternehmen geltend machen und verlangen, dass es die Erfüllung des Anspruchs bei der IIRFP veranlasst.

Seit der Inbetriebnahme des neuen HIS sind bereits mehrere Beschwerden gegen die IIRFP und einmeldende Versicherungsbehörden bei meiner Be-

hörde eingegangen. Das ist nicht verwunderlich, denn trotz der datenschutzkonformen Ausgestaltung des Systems ist nicht ausgeschlossen, dass im Einzelfall unrichtige oder unberechtigte Einmeldungen erfolgen. Bislang konnten jedoch noch keine Datenschutzverstöße festgestellt werden. Einige Betroffene haben auch bei zutreffenden Meldungen die Besorgnis geäußert, hierdurch als potenzielle Betrüger stigmatisiert zu werden. Angesichts der Zielsetzung des Systems, den Versicherungsmissbrauch und -betrug zu verhindern, habe ich Verständnis für diese Sorge. Dennoch erscheint auch die Einmeldung von – für sich allein betrachtet – unverdächtigen Vorfällen für das Funktionieren des Systems notwendig. So stieß es beispielsweise bei Beschwerdeführern auf Ablehnung, dass im Fall einer Diebstahlsversicherung bereits der erstmalige Diebstahl eines Kraftfahrzeugs beim Versicherungsnehmer an das HIS gemeldet wurde. Zu berücksichtigen bleibt jedoch, dass eine Häufung von Versicherungsfällen, die einen Betrugsverdacht begründet, nur festgestellt werden kann, wenn auch zunächst unverdächtige Einzelfälle eingemeldet werden.

Meine Mitarbeiter und ich werden auch weiterhin den Einsatz des neuen HIS kritisch begleiten.

2. Neue Einwilligung und Schweigepflichtentbindungen

In ihrem Fünften Tätigkeitsbericht 2009 (Abschnitt C 4.1.1) berichtete die Aufsichtsbehörde über den Entwurf einer Einwilligungs- und Schweigepflichtentbindungserklärung für das Versicherungswesen, der vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) erarbeitet worden war. Inzwischen wurden in Abstimmung mit den Datenschutzaufsichtsbehörden erhebliche Verbesserungen erreicht.

Für das Versicherungswesen sind Einwilligungs- und Schweigepflichtentbindungserklärungen gerade in Bezug auf Gesundheitsdaten notwendig, denn obwohl die Versicherungen ein berechtigtes Interesse daran haben, den Gesundheitszustand des Versicherten zu kennen, sind sie gesetzlich nicht befugt, diese Daten ohne Einwilligung des Betroffenen beispielsweise bei dessen Arzt zu erheben oder zu verwenden. Hinzukommt, dass Angehörige von Heilberufen einer Verschwiegenheitspflicht unterliegen, sodass sie sich mit der Weitergabe von Patientendaten ohne dessen Schweigepflichtentbindung strafbar machen würden.

Der GDV hat die erforderlichen Texte nach einem „Baukastensystem“ gestaltet. Es sieht zunächst einen maximalen Rahmen für die Einwilligungs- und Schweigepflichtentbindungserklärungen vor. Wegen des Prinzips der Datensparsamkeit sind aber je nach Versicherungssparte nur die Textabschnitte zu verwenden, die eine tatsächlich erforderliche Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorsehen. Beispielsweise ist die Textpassage über den Umgang mit Gesundheitsdaten nicht in den Formularen der Reisegepäck- oder Kraftfahrzeugversicherungen zu verwenden. Hingegen ist sie bei Kranken-, Unfall- oder Lebensversicherungen notwendig.

Die Klausel geht nunmehr vom Grundsatz der Direkterhebung beim Betroffenen aus. Eine Erhebung personenbezogener Daten durch Versicherungsunternehmen bei Dritten, wie etwa bei Ärzten oder Angehörigen anderer Heilberufe, soll nur stattfinden, soweit dies zur Risikobeurteilung oder zur Prüfung der Leistungspflicht erforderlich ist. Der Versicherungsnehmer soll die Wahl zwischen einer Pauschal- und einer Einzeleinwilligung haben. Anstatt also generell in die Erhebung seiner Daten bei Dritten zu den in der Klausel festgelegten Zwecken einzuwilligen, kann er auch erklären, dass er in jedem Einzelfall informiert werden und dann einzelfallbezogen entscheiden will, ob er in die Erhebung bei Dritten einwilligt oder die erforderlichen Unterlagen selbst beibringt.

Die Verwendungszwecke der personenbezogenen Daten des Versicherungsnehmers sind in der Klausel differenziert und abschließend genannt. Der Betroffene wird daher hinreichend über den vorgesehenen Umgang mit seinen personenbezogenen Daten informiert, um eine wirksame Einwilligungserklärung abgeben zu können.

Die Klausel sieht keinen Umgang mit personenbezogenen Daten für Zwecke der Werbung vor. Auf diese Weise wird dem Umstand Rechnung getragen, dass das Bundesdatenschutzgesetz bereits eine Rechtsgrundlage für die Verwendung anderer als Gesundheitsdaten zu Werbezwecken enthält. Indem die Klausel das Thema der Werbung vollständig ausklammert wird der unzutreffende Eindruck vermieden, der Betroffene habe es selbst in der Hand, durch die Nichterteilung einer Einwilligung darüber zu entscheiden, ob seine Daten für die Werbung verwendet werden dürfen. Insoweit ist die gesetzliche Grundlage in § 28 Absatz 3 BDSG zu beachten.

Vertreter der Versicherungswirtschaft haben inzwischen beklagt, dass ein flächendeckender Einsatz der neuen Einwilligungs- und Schweigepflichtentbindungsklausel nicht vor Ende 2012 zu erwarten sei, da zu ihrer Umsetzung auch eine Anpassung organisatorischer und IT-gestützter Prozesse sowie des Informationsmaterials der Versicherungsunternehmen erfolgen müsse. Im Interesse der Versicherten lässt sich das meines Erachtens nicht vermeiden.

Die Versicherungsunternehmen sollten die neue Einwilligungs- und Schweigepflichtentbindungsklausel baldmöglichst und ohne unnötige Verzögerungen einführen.

3. Der Beitrag hängt vom Fahrstil ab

Viele tragische Verkehrsunfälle werden durch zu schnelles Fahren verursacht. Manche Versicherungen versuchen daher, Anreize für ein regelkonformes Fahrverhalten zu schaffen, indem sie die Beitragshöhe davon abhängig machen, wie oft der Fahrzeughalter die zulässige Höchstgeschwindigkeit überschreitet. Solche Modelle setzen aber eine Überwachung des Fahrverhaltens voraus und stellen daher ein Risiko für die informationelle Selbstbestimmung dar.

Eine in Baden-Württemberg ansässige Versicherung plant einen Tarif für die Kraftfahrzeug-Haftpflichtversicherung, bei dem der Versicherungsnehmer einen Beitragsnachlass von bis zu 30 % auf den regulären Versicherungstarif erhält, wenn er die vorgeschriebene Höchstgeschwindigkeit einhält. Dies wird mit Hilfe einer sog. On-Board-Unit (OBU) kontrolliert, die in das entsprechend versicherte Fahrzeug eingebaut wird. In der OBU ist digitales Kartenmaterial mit Informationen zu den auf den verschiedenen Straßen jeweils zulässigen Höchstgeschwindigkeiten gespeichert. Die OBU bestimmt die Position des Fahrzeugs mittels GPS-Daten und vergleicht die zulässige mit der tatsächlich gefahrenen Geschwindigkeit. Wird die zulässige Höchstgeschwindigkeit um ein bestimmtes Maß überschritten, so warnt sie den Fahrer durch ein akustisches Signal. Dauert die Geschwindigkeitsüberschreitung länger als fünf Sekunden an, so speichert die OBU einen Verkehrsverstoß.

Das Unfallrisiko hängt aber nicht allein von der Geschwindigkeit, sondern auch von Zeit und Ort der Fahrt ab. Beispielsweise ist die Fahrt auf einer Landstraße samstagnachts zur typischen Diskotheken-Besuchszeit gefährlicher als eine Tour durch die Innenstadt am Sonntagvormittag. Die OBU soll daher auch die Straßenkategorien (zum Beispiel innerorts, außerorts oder Autobahn), die Kilometerleistung sowie Wochentag und Uhrzeit der Fahrten erheben und speichern. Gleiches gilt für Daten zum Beschleunigungs- und Bremsverhalten, um zu analysieren, ob der Fahrer eine aggressive Fahrweise pflegt. Auf Grundlage der erhobenen Daten werden in der OBU Indexwerte ermittelt, die wiederum für die Beitragshöhe entscheidend sind. Die Indexwerte sollen in regelmäßigen Abständen an ein Rechenzentrum übertragen werden, das von einem technischen Dienstleister betrieben wird, und dort zur Beitragsberechnung genutzt werden.

Ein solches System ermöglicht die Erstellung detaillierter Verhaltensprofile des Fahrzeughalters, der in der Regel mit dem Versicherungsnehmer identisch ist. Das Verfahren unterliegt daher in datenschutzrechtlicher Hinsicht strengen Anforderungen. Der Versicherungsnehmer ist deshalb vor Vertragsschluss detailliert über den beabsichtigten Umgang mit seinen personenbezogenen Daten zu unterrichten.

In Ermangelung einer gesetzlichen Rechtsgrundlage kann die Erhebung und Verwendung der Daten nur mit Einwilligung des betroffenen Versicherungsnehmers zulässig sein. Daher ist sicherzustellen, dass die Einwilligung freiwillig erfolgt und insbesondere nicht auf einem wirtschaftlichen Zwang beruht. Bei der Tarifgestaltung ist ferner darauf zu achten, dass dem Versicherungsnehmer die Option eines Tarifs mit fahrstilunabhängigen Beiträgen ohne Einbau und Verwendung einer OBU finanziell zumutbar bleiben muss.

Hat sich der Versicherungsnehmer für den Tarif mit fahrstilabhängiger Beitragshöhe entschieden, so hat das Versicherungsunternehmen als für den Datenumgang verantwortliche Stelle zu gewährleisten, dass die Daten vor Missbrauch und unbefugter Kenntnisnahme geschützt sind. Die Übertragung der in der OBU gespeicherten Daten an das Rechenzentrum hat daher unter Einsatz aktueller Verschlüsselungstechnik zu erfolgen.

Da die Einzeldaten, auf denen die Indexwerte beruhen, ausführliche Erkenntnisse über das Fahrverhalten und somit auch über die individuelle Lebensgestaltung des Versicherungsnehmers gestatten, sind diese Daten von den für die Beitragsberechnung relevanten Indexwerten zu trennen. Gegen eine sofortige automatisierte Löschung der Einzeldaten spricht das mögliche Bedürfnis des Versicherungsnehmers, kontrollieren zu können, ob die Indexwerte korrekt berechnet worden sind. Auch für diesen Fall ist aber sicherzustellen, dass der Versicherungsnehmer die Herrschaft über diese Daten behält. Dies kann entweder dadurch geschehen, dass der Versicherungsnehmer die Übertragung der Einzeldaten an das Rechenzentrum selbst initiieren muss. Stattdessen ist auch möglich, dass die Daten asymmetrisch verschlüsselt beim Rechenzentrum abgelegt werden und dort nur verwendet werden können, wenn der Versicherungsnehmer sie über das Internet unter Verwendung seines privaten Schlüssels freigegeben hat. Ebenso muss der Versicherungsnehmer die Einzeldaten lesen können, nachdem er sich beim Internet-Portal des Versicherers oder des von diesem beauftragten Dienstleisters angemeldet hat. Verzichtet er auf die Möglichkeit, die Indexwerte zu überprüfen, so muss er auch in der Lage sein, die den Indexwerten zugrunde liegenden Einzeldaten zu löschen.

Das Versicherungsunternehmen bedient sich bei dem beschriebenen System zum einen eines technischen Dienstleisters, der die OBU zur Verfügung stellt und das Rechenzentrum betreibt, sowie der Kraftfahrzeug-Werkstätten, die die OBU in die Fahrzeuge der Versicherungsnehmer einbauen. Soweit diese Stellen personenbezogene Daten des Versicherungsnehmers verarbeiten, geschieht dies im Wege der Auftragsdatenverarbeitung für die Versicherung. Diese hat daher ihren Auftragnehmer durch schriftliche Vereinbarungen zur Einhaltung der datenschutzrechtlichen Vorschriften zu verpflichten und dies regelmäßig überwachen.

Meine Behörde wird die Einführung verhaltensabhängiger Versicherungstarife weiterhin kritisch begleiten.

4. Abgabe der Akten der Gebäudebrandversicherung an Archive

Das Landesarchivgesetz schreibt vor, dass alle Behörden, Gerichte und sonstige Stellen des Landes alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, dem Landesarchiv anzubieten haben. Diese Regelung soll gewährleisten, dass die Akten der öffentlichen Verwaltung und der Gerichte auch nach Abschluss eines Vorgangs der Nachwelt erhalten bleiben, damit Wissenschaftler und sonstige Interessierte später noch feststellen können, wie in einer bestimmten Epoche öffentliche Aufgaben erledigt worden sind. Natürlich muss das Archiv von dem ihm überlassenen Material nur solches aufbewahren, dem ein bleibender Wert, also eine bestimmte Aussagekraft zu den heutigen Lebensverhältnissen zukommt. Auch muss sichergestellt sein, dass das Archivgut nicht in unbefugte Hände gelangt und dem Daten- und Persönlichkeitsschutz der davon betroffenen Personen Rechnung getragen wird. Für Letzteres sorgen gesetzlich vorgeschriebene Sperrfristen, innerhalb derer Archivgut mit personenbezogenem Inhalt nicht genutzt werden darf.

Die Sparkassenversicherung AG ist an die Stelle der beiden Gebäudebrandversicherungsanstalten in Baden und Württemberg getreten und hat deren

Akten- und Datenmaterial übernommen. Von diesem will sich die Sparkassenversicherung AG nunmehr zumindest teilweise trennen. Diesen Dokumenten kommt sicher eine nicht unerhebliche Bedeutung für die Landes- und Kommunalgeschichte zu. Da in der Vergangenheit jedes Gebäude in Baden-Württemberg bei einer der beiden Rechtsvorgängerinnen der Sparkassenversicherung AG gegen Feuer und andere Elementarschäden pflichtversichert sein musste, gibt es dort in den Einschätzungsunterlagen Aufzeichnungen über alle Liegenschaften, zu deren Lage, zur Ausstattung und zu ihrem Versicherungswert. Eine wahre Fundgrube für künftige Landeshistoriker!

Datenschutzrechtlich sind damit jedoch zwei Fragen verbunden: Trifft diese Abgabepflicht an ein Archiv auch die Sparkassenversicherung AG, wo sie doch im Gegensatz zu ihren Rechtsvorgängerinnen gar keine öffentlich-rechtliche Institution mehr ist, und kann diese Abgabe nur an das Landesarchiv oder auch an Archive der Gemeinden und der Landkreise erfolgen?

Dass die Sparkassenversicherung AG berechtigt, ja sogar verpflichtet ist, ihre nicht mehr benötigten Unterlagen einem öffentlichen Archiv anzubieten, folgt aus zweierlei Gründen: Zum einen hat sie als Rechtsnachfolgerin besagter Versicherungsanstalten alle rechtlichen Verpflichtungen übernommen, die jene als öffentliche Stellen zu erfüllen hatten. Zum anderen schreibt § 2 Absatz 3 des Landesarchivgesetzes vor, dass das Landesarchiv Schriftgut auch von privaten Stellen übernehmen kann. Allerdings würde die Abgabe dieser Unterlagen an ein kommunales Archiv nicht im Einklang mit dem Datenschutz- und Archivrecht stehen. Die öffentlichen Stellen des Landes und deren private Rechtsnachfolger dürfen nämlich die bei ihnen nicht mehr benötigten Akten, die – wie hier die Einschätzungsunterlagen der versicherten Gebäude – oftmals recht sensible Angaben über die davon betroffenen Personen enthalten, nur ausnahmsweise einem anderen Archiv als dem Landesarchiv anvertrauen. Ein solcher Ausnahmefall ließ sich hier jedoch nicht erkennen.

Auch das Ministerium für Wissenschaft und Kunst vertritt die Auffassung, dass die Sparkassenversicherung die Rechtsverpflichtung der beiden Staatlichen Gebäudeversicherungen übernommen und ihr Archivgut dem Landesarchiv anzubieten hat.

5. Abschnitt: Devisen nur gegen Identitätsnachweis?

Um nicht versehentlich die Finanztransaktionen von Terroristen zu unterstützen, erheben Kreditinstitute beim Sortentausch unter Vorlage des Personalausweises Kundendaten, gleichen sie mit Listen terrorverdächtiger Personen ab und speichern sie. Der informationellen Selbstbestimmung der Kunden wird hierdurch nicht hinreichend Rechnung getragen.

Ein Arzt aus Südbaden staunte nicht schlecht, als er vor einem Kurzurlaub in der Schweiz noch schnell bei seiner örtlichen Sparkasse knapp 500 € in Schweizer Franken umtauschen wollte. Denn der Sparkassenangestellte hinter dem Schalter verlangte zunächst seinen Personalausweis und gab die Daten sodann in einen Computer ein. Als der Kunde später die Sparkasse um Auskunft bat, bekam er zu hören, die Identitätsfeststellung sei erforderlich, damit die Sparkasse nicht gegen außenwirtschaftliche Vorschriften verstoße; deshalb sei ein Abgleich mit den sog. Antiterrorlisten notwendig. Unsere Überprüfung hat Folgendes ergeben:

Die datenschutzrechtliche Problematik des Abgleichs von Mitarbeiterdaten mit Antiterrorlisten auf Grundlage der Verordnungen (EG) Nummer 881/2002 und Nummer 2580/2001 ist in diesem Tätigkeitsbericht bereits dargestellt worden (6. Teil, 2. Abschnitt, Nr. 5). In gleicher Weise überprüft in Baden-Württemberg auch eine Vielzahl von Kreditinstituten beim Sortentausch, ob Kunden, die Geld wechseln wollen, auf den Antiterrorlisten zu finden sind. Schon beim Wechsel von Geldsummen unter 1.000 € wird der Kunde aufgefordert, seinen Personalausweis vorzulegen. Der Mitarbeiter des Kreditinstituts gibt sodann den Namen, das Geburtsdatum und den Geburtsort des Kunden in das Rechnersystem ein, um den Datenabgleich durchzuführen. Unabhängig vom Ergebnis der Überprüfung bleiben die genannten Daten im elektronischen Kassen-

journal gespeichert. Für die Durchführung dieses Verfahrens ist es ohne Bedeutung, ob der Kunde bei dem Kreditinstitut ein Konto oder Wertpapierdepot hat oder ob er lediglich Devisen eintauschen wollte.

Ebenso wie bei Mitarbeiterdaten entbehrt auch der systematische und anlasslose Abgleich von Kundendaten mit den Antiterrorlisten einer tragfähigen rechtlichen Grundlage und ist daher nicht mit den Vorgaben des Datenschutzrechts vereinbar. Der im Datenabgleich liegende Rechtsverstoß wird jedoch durch die Speicherung der Kundendaten im Kassenjournal noch verstärkt. Dies gilt umso mehr, als der Kunde unter Umständen keine weiteren Geschäftskontakte zum protokollierenden Kreditinstitut gepflegt hat und seine Daten daher ohne den rechtswidrigen Datenabgleich bei diesem zu keinem Zeitpunkt Eingang in die dortigen Datenbestände gefunden hätten. Die Speicherung wird von den Kreditinstituten damit begründet, dass die Korrektheit ihres Handelns nachträglich überprüfbar sein müsse. Dieses Argument überzeugt jedoch nicht, denn selbst wenn eine Pflicht zum Datenabgleich bestünde, würde es für spätere Überprüfungen ausreichen, im Zusammenhang mit der jeweiligen Transaktion zu dokumentieren, dass der Abgleich stattgefunden hat.

Die Überprüfung des konkreten Falles ist leider noch nicht abgeschlossen, weil die betreffende Sparkasse den Sparkassenverband und dieser wiederum die Bundesbank und das Bundeswirtschaftsministerium eingeschaltet hat. Die Bundesbank hat zwischenzeitlich erklärt, dass sie sich einer Auslegung der Rechtsakte der EU zu dem Finanzembargo gegen terrorverdächtige Personen enthalte, zumal die entsprechenden Vorschriften unmittelbar gelten würden. Die Antwort des Bundeswirtschaftsministeriums steht noch aus.

6. Abschnitt: Sonstiges

1. Datenschutz an der Ladenkasse

EC-Karten haben inzwischen als Mittel zum bargeldlosen Bezahlen weite Verbreitung gefunden. Dabei sind sich die Nutzer selten der mit der Kartennutzung einhergehenden Datenflüsse bewusst. Vor der Entscheidung, ob eine Kartenzahlung mit PIN oder Unterschrift erfolgen soll, werden oft Zahlungsdaten von zurückliegenden Transaktionen bei einer Vielzahl von Händlern ausgewertet.

Die Idee des bargeldlosen Zahlungsverkehrs ist nicht zuletzt durch die Nutzung von EC-Karten in weiten Bereichen des Alltags Wirklichkeit geworden. Dabei stehen den Beteiligten, abgesehen vom GeldKarten-System, bei dem lediglich ein zuvor aufgeladener Betrag mittels einer „elektronischen Geldbörse“ ausgegeben werden kann, im Wesentlichen das Electronic Cash-Verfahren und das elektronische Lastschriftverfahren zur Verfügung. Beiden ist gemein, dass die Transaktionen mithilfe von speziellen technischen Diensteanbietern, sogenannten Netzbetreibern, abgewickelt werden. Zu diesem Zweck wird die EC-Karte des Kunden in das vom Netzbetreiber zur Verfügung gestellte Kassenterminal eingeführt. Dort werden die zur Karte gehörende Kontonummer, die Bankleitzahl, das Kartenverfallsdatum und die Kartenfolgenummer zusammen mit Angaben zur Höhe des zu zahlenden Betrags sowie zu Zeit und Ort der Transaktion an den Netzbetreiber übermittelt. Der Netzbetreiber schickt dem Händler daraufhin aufgrund ihm vorliegender Informationen zur Karte eine Empfehlung, ob die Abwicklung im Wege des Electronic Cash-Verfahrens oder mittels des elektronischen Lastschriftverfahrens durchgeführt werden sollte.

– Funktionsweise der Kartenverfahren

  Beim Electronic Cash-Verfahren veranlasst der Kunde durch Eingabe seiner PIN eine Online-Überprüfung des zur Karte gehörenden Kontos durch den Netzbetreiber. Ist das Konto ausreichend gedeckt und die Karte gültig, so garantiert die Bank dem Händler bei erfolgreicher Autorisierung den Zahlungsbetrag bis zu einer zuvor festgelegten Höchstsumme. Aufgrund dieser Garantie ist das Verfahren für den Händler mit relativ hohen Gebühren verbunden, die die Bank vom Zahlungsbetrag abzieht.

Die Händler bevorzugen daher vielfach das kostengünstigere elektronische Lastschriftverfahren. Dabei erteilt der Kunde dem Händler durch seine Unterschrift auf dem Kassenbeleg die Ermächtigung, den Forderungsbetrag bei seiner Bank einzuziehen. Mit derselben Unterschrift ermächtigt der Kunde die Bank, dem Händler seine ladungsfähige Anschrift mitzuteilen, wenn die Einziehung der Forderung mangels Kontodeckung scheitert. Der Kunde befreit seine Bank insoweit vom Bankgeheimnis. Beim elektronischen Lastschriftverfahren liegt das Risiko eines Zahlungsausfalls somit beim Händler.

Der Netzbetreiber trifft die Entscheidung über die an den Händler zu übermittelnde Zahlungswegempfehlung aufgrund verschiedener bei ihm gespeicherter Daten. Zum einen führt der Netzbetreiber oft Sperrdateien, in denen zu den einzelnen EC-Karten unter anderem Daten zu sogenannten Rücklastschriften gespeichert werden. Dies sind Lastschriften, die von der Bank des Kunden nicht eingelöst oder die vom Kunden widerrufen worden sind. Der Netzbetreiber erlangt diese Daten durch eine entsprechende Meldung des bei ihm angeschlossenen Händlers, der seine Forderung nicht einziehen konnte. In den Sperrdateien der Netzbetreiber werden Rücklastschriftdaten zumeist nicht nach Händlern getrennt, sondern händlerübergreifend gesammelt. Für die Zahlungswegempfehlung gegenüber einem bestimmten Händler werden die Daten ebenfalls händlerübergreifend genutzt, das heißt, es werden dafür auch solche Rücklastschriften berücksichtigt, die aus einem Kundenkontakt des anfragenden Händlers stammen.

Darüber hinaus werden für die Zahlungswegempfehlung auch sogenannte Positivdaten über erfolgreich abgewickelte Transaktionen verwendet. Dies dient dazu, auffällige Muster zu erkennen, die auf einen Kartenmissbrauch, wie etwa nach einem Diebstahl der EC-Karte, hindeuten. Dies kann beispielsweise der Fall sein, wenn innerhalb eines kurzen Zeitraums ungewöhnlich hohe Zahlungen erfolgen. Weiterhin werden die Positivdaten verwendet, um sicherzustellen, dass innerhalb bestimmter Zeiträume bestimmte Höchstbeträge (Limits) bei der Zahlung im elektronischen Lastschriftverfahren nicht überschritten werden. Beides dient nicht nur dem Schutz des Karteninhabers, sondern auch dem des Händlers, denn bei Missbrauch der Karte ist mit einem Widerruf der Lastschrift und bei der Überschreitung von Zahlungslimits damit zu rechnen, dass die Forderung mangels Kontodeckung nicht eingelöst wird.

– Datenschutzrechtliche Zulässigkeit

Die Netzbetreiber haben versucht, den oben beschriebenen Umgang mit den personenbezogenen Daten der Kunden durch entsprechende Einwilligungsklauseln auf den Kassenbelegen zu legitimieren. Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben gegenüber den Netzbetreibern die Ansicht vertreten, dass angesichts der Komplexität der Verfahren eine informierte und somit wirksame Einwilligung des Kunden jedoch nicht möglich ist. Wer selbst schon einmal an einer Ladenkasse einen langen Papierstreifen mit einer kleingedruckten, umfangreichen Erläuterung – womöglich mit ungeduldigen weiteren Kunden hinter sich – zu unterschreiben hatte, weiß, wovon ich rede. Der Umgang mit personenbezogenen Daten durch die Netzbetreiber im Rahmen des elektronischen Lastschriftverfahrens kann daher allein auf gesetzlicher Grundlage zulässig sein.

Rücklastschrift- und Positivdaten aus eigenen Kundenkontakten eines Händlers dürfen von diesem aufgrund einer Abwägung mit den schutzwürdigen Interessen des Kunden gespeichert und genutzt werden, um missbräuchliche Kartennutzungen zu verhindern und Zahlungsausfälle zu vermeiden. Dabei kann sich der Händler eines Netzbetreibers bedienen, der je nach Ausgestaltung des Vertragsverhältnisses entweder im Wege der Auftragsdatenverarbeitung tätig wird oder selbst als verantwortliche Stelle auftritt. In letzterem Fall darf der Netzbetreiber die vom Händler übermittelten Daten nur zu den vorgenannten Zwecken nutzen, zu denen sie ihm übermittelt worden sind.

Die händlerübergreifende Nutzung von Rücklastschriftdaten ist datenschutzrechtlich zulässig, soweit sie der Verhinderung von Zahlungsaus-

fällen dient. Hiergegen könnte zwar sprechen, dass das Handeln des Netzbetreibers bei der händlerübergreifenden Datennutzung Ähnlichkeit mit der Tätigkeit einer Auskunftei hat, denen Daten über unbezahlte Forderungen nur unter den engen Voraussetzungen des § 28 a BDSG, etwa bei Vorliegen eines Vollstreckungstitels oder nach ausdrücklichem Anerkenntnis des Schuldners, übermittelt werden dürfen. Die für Auskunfteien geltenden Vorschriften sind jedoch nach der mehrheitlichen Ansicht der Datenschutzaufsichtbehörden auf die Netzbetreiber nicht anzuwenden. Dies liegt darin begründet, dass die von ihnen verwendeten Daten nur im Verkehr mit den angeschlossenen Händlern, nicht aber gegenüber sonstigen Stellen wie etwa Vermietern oder Kreditinstituten verwendet werden, und daher eine deutlich geringere Streubreite aufweisen.

Bei der Verwendung von Daten über Rücklastschriften ist zu beachten, dass dem Karteninhaber kein Nachteil daraus entstehen darf, wenn er mit dem Widerruf einer Lastschrift lediglich Rechte aus dem der Zahlung zugrundeliegenden Grundgeschäft geltend macht, wenn er also beispielsweise vom Kaufvertrag wegen Mangelhaftigkeit der Ware zurücktritt oder einen wegen arglistiger Täuschung angefochtenen Vertrag rückabwickeln will. Der Netzbetreiber hat daher sicherzustellen, dass solche Rücklastschriften nicht in die Entscheidung über die Zahlungswegempfehlung einfließen. Zu diesem Zweck muss er den Händler vertraglich und in sanktionsbewehrter Weise verpflichten, ihm die Geltendmachung entsprechender Rechte durch den Karteninhaber anzuzeigen. Wünschenswert wäre zudem, dass der Netzbetreiber überprüfen kann, ob der Händler seiner Anzeigepflicht genügt. Dies ist jedenfalls dann der Fall, wenn sich der Netzbetreiber die Forderungen vom Händler abtreten lässt. Unter diesen Umständen erfährt er spätestens bei der Einziehung der Forderung, ob der Karteninhaber mit dem Widerruf der Lastschrift Rechte aus dem Grundgeschäft geltend machen wollte.

Im Vergleich zu Rücklastschriftdaten unterliegt der händlerübergreifende Umgang mit Positivdaten strengeren Regeln. Solche Daten dürfen ausschließlich zur Bekämpfung von Kartenmissbrauch verwendet werden und sind vom Netzbetreiber schon nach wenigen Tagen, keinesfalls aber mehr als zwei Wochen, zu löschen.

Netzbetreiber dürfen EC-Kartendaten aus händlerübergreifenden Datenpools nur unter strenger Wahrung der Betroffenenrechte verwenden.

2. Datenentsorgung in der Mülltonne

Immer wieder werden Unterlagen, die ihr bisheriger Inhaber entsorgen wollte, mit teils höchst sensiblen personenbezogenen Daten in Mülltonnen gefunden.

Gleich drei durchaus gravierende Fälle wurden der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Berichtszeitraum bekannt: Am Bodensee sollte eine Zahnarzthelferin in der Praxis ihres Chefs nicht mehr benötigte Unterlagen, aus denen sich all die Informationen ergaben, die ein Zahnarzt für die Behandlung seiner Patienten und die Abrechnung benötigt, entsorgen. Sie warf das sensible Datenmaterial kurzerhand in einen Papierkorb am Bahnhof, wo es von einer Reinigungskraft entdeckt wurde. Im Unterland wollte sich ein Arzt anlässlich des Umzugs seiner Praxis ebenfalls von Patientenakten mit entsprechenden Aufzeichnungen trennen. In der Hektik der Räumung der bisherigen Praxis warf die Ehefrau, die zugleich Mitarbeiterin des Arztes war, die Karteikarten in den Müllcontainer einer Versandfirma, wo sie einer Angestellten dieses Betriebes in die Hände fielen. Und auf einer Autobahnraststätte der Rheintalautobahn fand ein sog. Flaschensammler umfangreiche Unterlagen eines Waffenhändlers, unter anderem mit Kopien von Waffenscheinen und Personalausweisen, die dieser dort entsorgt hatte.

Obwohl sich die Betroffenen von den Unterlagen trennen wollten und sogar deren Vernichtung anstrebten, handelt es sich hier nicht um eine Datenlöschung, denn zum Zeitpunkt des Auffindens durch Dritte waren die Datenträger ja noch vorhanden. Die darauf aufgezeichneten Informationen

konnten von anderen Personen – wenn dies auch nicht von den bisherigen Inhabern der Unterlagen beabsichtigt war – unbefugterweise zur Kenntnis genommen werden. Datenschutzrechtlich muss man hier von einer Datenübermittlung an einen unbestimmten Personenkreis ausgehen, denn es war reiner Zufall, wer in die Mülltonnen oder Papierkörbe hineinsah. Natürlich hatten diejenigen, die sich des Datenmaterials entledigen wollten, kein berechtigtes Interesse an einer derartigen Datenübermittlung. Dagegen waren die Personen, deren Daten betroffen waren, schutzwürdig. Sie hätten erwarten können, dass bei der Entsorgung der ärztlichen und waffenrechtlichen Unterlagen die technisch-organisatorischen Maßnahmen getroffen werden, die erforderlich sind, damit diese Daten nicht unbefugt gelesen werden können. Öffentlich zugängliche Mülltonnen und Papierkörbe sind für eine ordnungsgemäße Datenlöschung sicher nicht geeignet. Angesichts der Tatsache, dass es sich um medizinische Daten und Daten aus dem Waffenbereich gehandelt hatte, sah sich die Aufsichtsbehörde gezwungen, empfindliche Geldbußen gegenüber den jeweiligen Betroffenen zu verhängen.

Wie aber hätten sich diese verhalten müssen, damit die Entsorgung ihrer Unterlagen datenschutzgerecht erfolgt wäre? Dazu gibt es zum einen die Möglichkeit, das Datenmaterial vor dem Deponieren in einem Müllcontainer oder bevor es einem Müllentsorger überlassen wird, zu schreddern oder anderweitig so zu vernichten, dass es Dritten nicht mehr möglich ist, die Unterlagen zu lesen oder wieder herzustellen. Auch spricht nichts dagegen, ein auf die Entsorgung solcher Unterlagen spezialisiertes Unternehmen mit dem Abholen und Vernichten zu beauftragen. Rechtlich gesehen handelt es sich beim Tätigwerden des Unternehmers um eine Auftragsdatenverarbeitung. § 11 Absatz 2 BDSG schreibt dazu vor, dass der Unternehmer im Hinblick auf seine Zuverlässigkeit und Vertrauenswürdigkeit sorgfältig ausgesucht werden muss. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere festgelegt werden muss, welche Daten zu vernichten sind, welche technisch-organisatorischen Maßnahmen, die verhindern, dass dabei Dritte unbefugterweise Kenntnis erhalten, zu ergreifen sind, dass der Auftraggeber sich zumindest stichprobenweise von der ordnungsgemäßen Vernichtung überzeugen kann, ob der Auftragnehmer Unteraufträge an andere Firmen – und wenn ja, an welche – erteilen darf und wie zu verfahren ist, wenn dem Auftragnehmer eine alsbaldige Vernichtung nicht möglich ist, also eine Zwischenlagerung erforderlich wird.

Es genügt also nicht, dass die für die Verarbeitung von personenbezogenen Daten verantwortlichen Stellen ihre Pflicht, diese zu löschen, sobald sie nicht mehr benötigt werden, „irgendwie“ erfüllen. Vielmehr muss man dabei auch sorgfältig dafür sorgen, dass das Datenmaterial „bis zum Schluss“ optimal gegen die Kenntnisnahme Dritter gesichert ist.

3. Das Leih-Notebook als Datenfundgrube

Hätte ein Elektronikfachmarkt, der seinen Kunden Notebooks verleiht, dafür Sorge tragen müssen, dass personenbezogene Daten des Entleihers nach Rückgabe des Geräts rückstandslos gelöscht werden?

Ein aufmerksamer Kunde, der sein Notebook in einer Filiale eines großen Elektronikfachmarktes zur Reparatur gegeben hatte, staunte nicht schlecht, als er auf dem Leihgerät, das ihm der Markt für die Dauer der Reparatur ersatzweise zur Verfügung gestellt hatte, zahlreiche Dateien diverser Vorbesitzer vorfand. Er hatte lediglich ein im Internet kostenlos verfügbares Programm zur Wiederherstellung „einfach“ gelöschter Daten auf das Gerät aufspielen müssen – und schon gewährte ihm das Leih-Notebook unerwartete Einblicke in die Lebensverhältnisse seiner Vorbesitzer. Das Spektrum der abrufbaren Dateien reichte nach seinen Angaben von privaten Fotografien über Rechnungen und Kontoauszüge eines Autohändlers bis hin zu Bewerbungsschreiben mit beigefügtem Lebenslauf. Offenbar waren all diese teils sehr persönlichen Daten mithilfe der unter Windows standardmäßig verfügbaren Löschfunktion eben nur logisch, nicht aber physikalisch gelöscht worden (eine physikalische Löschung erfolgt in der Regel dadurch, dass die zu löschenden Daten mehrfach mit einer zufällig gewählten Bitfolge überschrieben werden).

Dabei habe er – so beschwerte sich der Kunde bei der Aufsichtsbehörde – bei Abschluss des Leihvertrags eigens mündlich nachgefragt, ob denn nach Rückgabe des Leihgeräts die von ihm aufgespielten Daten fachgerecht gelöscht würden – was ihm von einem Service-Mitarbeiter des Elektronikfachmarktes zugesagt worden sei. Nunmehr behaupte die Service-Abteilung des Fachmarktes hingegen, sie sei ihren Verpflichtungen mit einem einfachen „Recovery" des Leihgeräts nachgekommen und könne eine „rückstandslose" Löschung der vom Entleiher aufgespielten Daten nur gegen Entgelt anbieten.

Die Aufsichtsbehörde wollte dies natürlich genauer wissen und forderte den Fachmarkt auf, Stellung zu nehmen. Dieser bestritt – letztlich unwiderlegbar –, dem Kunden eine vollständige Löschung seiner Daten zugesichert zu haben. Vielmehr weise man die Kunden, denen man Leihgeräte aushändige, darauf hin, dass sie selbst für ihre Daten verantwortlich seien. Als verantwortliche Stelle im Sinne des § 3 Absatz 7 BDSG sei nämlich diejenige Person anzusehen, die die Daten für sich selbst erhebe, verarbeite oder nutze bzw. dieses durch Dritte tun lasse. Dies sei zunächst der Besitzer des Leihgerätes, der auf dieses Daten aufspiele. Von Seiten des Fachmarktes erfolge hingegen keinerlei „voluntative" Befassung mit den von Entleihern gespeicherten Daten, sodass diese ihm letztlich aufgedrängt würden. Da dieser „aufgedrängten" Datenherrschaft jedes finale Element fehle, könne weder die Rede davon sein, dass der Fachmarkt die in Rede stehenden Daten erhoben, noch davon, dass er sie (an die nachfolgenden Kunden) übermittelt hätte.

Diese Rechtsauffassung ließ sich in der Tat vertreten. Die Aufsichtsbehörde wollte den Fachmarkt dennoch nicht von jeder datenschutzrechtlichen Mitverantwortung freisprechen. Insbesondere bemängelte sie, dass es der Markt bis dato versäumt habe, seine Kunden bei der Aushändigung des Leihgeräts mit der gebotenen Deutlichkeit darauf hinzuweisen, dass sie zunächst selbst dafür verantwortlich seien, ihre personenbezogenen Daten zu löschen, ehe sie das Leihgerät wieder zurückgeben. Diese Kritik nahm der Fachmarkt an und erklärte sich bereit, sein Leihvertrags-Muster um einen mit der Aufsichtsbehörde abgestimmten entsprechenden Passus zu ergänzen. Zudem werde er den Kunden künftig mit einem Hinweis in dem Leihschein anraten, eigene Daten nur auf externen Datenträgern zu speichern.

Nicht nur für entliehene Rechner gilt: Wer Daten datenschutzgerecht löschen möchte, muss sie mehrmals mit unterschiedlichen Mustern überschreiben. Geeignete, teils kostenlose Software kann man zum Beispiel bei https://www.bsi-fuer-buerger.de – Stichworte: Richtig löschen – finden.

4. Steckbriefe im Modecenter

Gegen den Aushang von Aufnahmen mutmaßlicher Kaufhausdiebe in den Filialen einer Modehaus-Kette bestanden datenschutzrechtliche Bedenken.

Ein Modehaus mit Unternehmenssitz in Baden-Württemberg, das erheblich unter den Diebeszügen einer offenbar besonders dreisten Diebesbande zu leiden hatte, griff zu einer unorthodoxen Maßnahme der Selbsthilfe: Wohl auch auf Anraten einer bayerischen Polizeidienststelle wies sie ihre Filialen in Baden-Württemberg und Bayern an, fahndungsplakatähnliche Aushänge mit Fotografien der mutmaßlichen Bandenmitglieder auszuhängen, deren fettgedruckte Aufschrift „Hausverbot" jeden Betrachter des Aushangs darüber aufklärte, dass die abgebildeten Personen unerwünscht seien. Dabei setzte man vor allem auf den zu erwartenden Abschreckungseffekt, hoffte nach eigenem Bekunden aber auch, die Übeltäter mithilfe der aufmerksamen Öffentlichkeit und der eigenen Mitarbeiter überführen zu können.

Niemand lässt sich gerne bestehlen, weswegen man sicherlich ein gewisses Verständnis dafür aufbringen kann, dass sich die Geschäftsleitung des Modehauses zur Wehr setzen wollte. Ihr Einfall, die mutmaßlichen Diebe per „Steckbrief" vom Betreten der eigenen Filialen abzuhalten, begegnete indes erheblichen datenschutzrechtlichen Bedenken. Gerade das Recht natürlicher Personen am eigenen Bild ist – als Ausfluss des allgemeinen Persönlichkeitsrechts – durch das Kunsturheberrechtsgesetz (KunstUrhG) nämlich be-

sonders geschützt. Gemäß § 22 KunstUrhG, der grundlegenden Norm dieses Gesetzes, dürfen „Bildnisse“ nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Von diesem Grundsatz lässt das Kunsturhebergesetz einige Ausnahmen zu, die in den §§ 23 und 24 KunstUrhG normiert sind. So dürfen Behörden für Zwecke der Rechtspflege und der öffentlichen Sicherheit nach Maßgabe des § 24 KunstUrhG Bildnisse ohne Einwilligung des abgebildeten vervielfältigen, verbreiten und öffentlich zur Schau stellen – eine Ausnahmevorschrift – welche das „klassische“ Fahndungsfoto als Instrument der Strafverfolgung und der Gefahrenabwehr legitimiert. Strafverfolgung und öffentliche Sicherheit sind aber nun einmal Sache des Staates – das Modehaus war hierfür sicherlich nicht zuständig!

Glücklicherweise zeigte sich das Unternehmen alsbald einsichtig und beendete seine fragwürdige Aktion sofort, nachdem erste kritische Stimmen laut geworden waren – so hatte unter anderem die durch Presseberichte auf den Vorgang aufmerksam gewordene bayerische Datenschutzaufsichtsbehörde rechtliche Bedenken geäußert. Die „Steckbriefe“ wurden also unverzüglich wieder abgehängt. Da überdies von Seiten des Modehauses ersichtlich kein böser Wille am Werke gewesen war, konnte von aufsichtsrechtlichen Maßnahmen letztlich abgesehen werden.

Das Recht am eigenen Bild genießt nach Maßgabe des § 22 KunstUrhG besonderen Schutz; Bildnisse dürfen grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Ausnahmen lassen die §§ 23 und 24 KunstUrhG nur in engen Grenzen zu.

8. Teil: Datenschutz im Verein

1. Der wahlkämpfende Vereinskassierer

Mitglieder eines baden-württembergischen Sportvereins erhielten per Post oder E-Mail ein Schreiben ihres Kassierers, der sich ihnen als Gemeinderatskandidat vorstellte – hatte er personenbezogene Daten von Vereinsmitgliedern zweckentfremdet?

Ziemlich ungewöhnliche Brief- oder elektronische Post von ihrem bestallten Hauptkassierer erhielten Mitglieder eines baden-württembergischen Sportvereins: Nicht etwa von den Vereinsfinanzen oder Mitgliedsbeiträgen war in dem Anschreiben die Rede, vielmehr präsentierte sich dessen Verfasser als Bewerber für die anstehende Gemeinderatswahl und bat um Stimme und Unterstützung.

Das Schreiben schlug hohe Wellen, beschäftigte die örtliche Presse und zeitweilig sogar die Staatsanwaltschaft, denn längst nicht alle Adressaten des Wahlwerbeschreibens waren damit einverstanden, dass ihre persönlichen Daten, die dem Verein infolge ihrer eigenen Mitgliedschaft oder dem Vereinsbeitritt eines Angehörigen bekannt geworden waren, mutmaßlich für ersichtlich vereinsfremde Zwecke verwendet wurden. Auch die Aufsichtsbehörde, damals noch beim Innenministerium, schaltete sich ein.

In seiner Stellungnahme machte der Hauptkassierer geltend, er habe keineswegs auf Adressbestände des Vereins zurückgegriffen, sondern persönliche Freunde und Bekannte sowie einige ihm zumindest dem Namen nach bekannte Mitglieder des Sportvereins beziehungsweise, wenn diese noch minderjährig waren, deren Eltern angeschrieben. Die Post- und E-Mail-Anschriften dieses Adressatenkreises habe er selbst zusammengestellt. Deshalb habe er seine Vereins-Vorstandskollegen über seine Aktion auch nicht informiert. Die Aufsichtsbehörde vermochte diese Sachverhaltsdarstellung des Hauptkassierers nicht zu widerlegen, sah aber dennoch hinreichenden Anlass, die Werbeaktion zu beanstanden.

Soweit der Kassierer seine Werbeschreiben per elektronischer Post versandt hatte, musste er sich nämlich unabhängig von der Herkunft der E-Mail-Anschriften seiner Adressaten vorwerfen lassen, dass die Nutzung dieser personenbezogenen Daten weder durch eine vorherige (schriftliche) Einwilligung der Betroffenen noch durch einen gesetzlichen Erlaubnistatbestand gedeckt war. Insbesondere konnte sich der Kassierer nicht auf § 28 Absatz 1 Satz 1 Nummer 2 BDSG berufen, denn die Rechtsprechung erkennt im unverlangten Zusenden von Wahlwerbung per E-Mail einen Eingriff in das allgemeine Persönlichkeitsrecht, gegen den ein Unterlassungsanspruch besteht. Datenschutzrechtlich hat dies zur Folge, dass das schutzwürdige Interesse der Adressaten, die diesen Unterlassungsanspruch geltend machen können, an dem Ausschluss der Verarbeitung oder Nutzung ihrer Daten zu Zwecken der Wahlwerbung grundsätzlich höher zu bewerten ist als das Interesse des Kandidaten daran, potenzielle Wähler zu gewinnen.

Soweit der Kassierer hingegen per Briefpost um die Stimmen seiner Adressaten geworben hatte, kreidete ihm die Aufsichtsbehörde an, dass er es entgegen § 28 Absatz 4 Satz 2 BDSG versäumt hatte, die Empfänger auf ihr Recht hinzuweisen, der Nutzung ihrer Daten zu Zwecken der Wahlwerbung zu widersprechen.

Kritik musste sich im Übrigen auch der Vorstand des Sportvereins gefallen lassen, weil er keinerlei vereinsinterne Regelungen über den Umgang mit personenbezogenen Daten getroffen hatte. Die Aufsichtsbehörde forderte ihn deshalb auf, das Versäumte umgehend nachzuholen. Der Verein hat sich schließlich einsichtig gezeigt und einen Datenschutzbeauftragten bestellt, der derzeit im Dialog mit der Aufsichtsbehörde Vorschläge für eine entsprechende Ergänzung der Vereinssatzung entwickelt.

Unabhängig von der Herkunft der elektronischen Adressen stellt Wahlwerbung per E-Mail einen Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar, der regelmäßig nur mit deren vorheriger schriftlicher Einwilligung zulässig ist. Bei jeder werblichen Ansprache sind die Betroffenen

außerdem nach Maßgabe des § 28 Absatz 4 Satz 2 BDSG über ihr Recht zu unterrichten, der Verarbeitung und Nutzung ihrer personenbezogenen Daten zu Werbezwecken zu widersprechen.

2. Erhebung personenbezogener Daten beim Erwerb von Eintrittskarten

Im Berichtszeitraum erreichten die Aufsichtsbehörde im nicht-öffentlichen Bereich verschiedene Beschwerden, welche die Datenerhebungspraxis eines Fußballbundesligavereins bei der Bestellung von Eintrittskarten zum Gegenstand hatten.

Die Beschwerden richteten sich gegen die Datenerhebung beim Verkauf von Auswärtsdauerkarten zum einen und beim Verkauf von Karten für Auswärtsspiele zum anderen. Ein Fußballfan beschwerte sich, dass im Rahmen der Bestellung einer Auswärtsdauerkarte die Einreichung einer Kopie des Personalausweises verlangt wurde. Eine Überprüfung ergab, dass auf dem Bestellformular zusätzlich Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum sowie Bankverbindung erfragt wurden. Eine datenschutzrechtliche Belehrung beziehungsweise einen Hinweis darauf, welche Angaben nur freiwillig zu machen sind, gab es nicht. Ähnlich verhielt es sich mit der Bestellung von Auswärtskarten. Hier wurde zwar keine Kopie des Personalausweises, jedoch die Angabe der Personalausweisnummer verlangt.

Der Fußballverein gab an, die Personalausweiskopie beziehungsweise die Personalausweisnummer sei erforderlich, um vor dem Verkauf der Eintrittskarten abzuklären, ob es sich bei dem Bewerber um eine gewaltbereite Person handelt, gegenüber der ein Stadionverbot ausgesprochen worden ist. Dieses Interesse hat die Aufsichtsbehörde dem Fußballbundesligisten nicht abgesprochen, jedoch angemerkt, dass die Vorgehensweise nicht geeignet ist, um gewaltbereite Fans von dem Erwerb von Eintrittskarten abzuhalten. Da die Karte nicht persönlich abgeholt werden muss und beim Betreten des Stadions keine Ausweiskontrolle erfolgt, kann eine Bestellung unter fremdem Namen unter Vorlage einer Kopie eines fremden Ausweises beziehungsweise unter Nennung einer fremden Personalausweisnummer erfolgen und so der Abgleich mit der Stadionsverbotsliste ins Leere laufen. Die Erhebung der Ausweisdaten ist deshalb ungeeignet und folglich datenschutzrechtlich nicht zulässig. Zu der Erhebung der Telefonnummer und der E-Mail-Adresse ist zu sagen, dass diese Daten zwar für den Verein für etwaige Rückfragen sinnvoll sein mögen, jedoch sollte dem Besteller freigestellt sein, ob er eine derartige Kontaktaufnahme gestatten möchte. Schließlich ist die Erhebung des Geburtsdatums zur Überprüfung der Geschäftsfähigkeit ebenfalls unzulässig, da eine Nachprüfung der Angaben nicht erfolgt. Ausreichend erscheint, die Bestätigung der Volljährigkeit zu verlangen.

Dem Fußballverein wurde aufgegeben, seine Bestellformulare zu ändern und darauf hinzuweisen, dass es sich bei Telefonnummer und E-Mail-Adresse um freiwillige Angaben handelt, eine Nennung aber zur erleichterten Kontaktaufnahme sinnvoll sein kann. Wer personenbezogene Daten erhebt, muss außerdem den Betroffenen darauf hinweisen, zu welchem Zweck er die Daten erhebt, welche Daten zur Bearbeitung eines Antrags erforderlich sind, welche freiwillig erfolgen und welche Nachteile dem Betroffenen drohen, wenn er die einzelnen Angaben nicht macht. Das Verlangen einer Kopie des Personalausweises oder der Personalausweisnummer ist ebenso unzulässig wie die Erhebung des Geburtsdatums. Der Verein ist den genannten Anforderungen zwischenzeitlich nachgekommen.

Bei der Gestaltung von Bestellformularen ist große Sorgfalt geboten. Nicht jede Angabe, die für den Verkäufer sinnvoll erscheint, darf ohne Weiteres als Pflichtangabe verlangt werden.

3. Schiri, wir wissen, wann du Geburtstag hast!

Ein Fußballschiedsrichter hatte sich bei der Aufsichtsbehörde darüber beschwert, dass seine Schiedsrichtergruppe alle der Gruppe angehörigen Schiedsrichter mit Foto, Name und Vorname, Heimatverein, Geburtstag

und dem Datum der Beginn der Schiedsrichtertätigkeit für jeden im Internet zugänglich veröffentlicht hat. Er sei vorher nicht um Zustimmung gebeten worden und habe seine Einwilligung hierzu auch nicht erteilt.

Im Interesse der Werbung für die wichtige Tätigkeit der Fußballschiedsrichter war ich bereit, die Schiedsrichter als Funktionsträger ihrer Vereine zu akzeptieren, hatte also keine durchgreifenden datenschutzrechtlichen Bedenken gegen die Veröffentlichung des Namens des Betroffenen, des Heimatvereins und des Datums des Eintritts in die Schiedsrichtergruppe. Als datenschutzrechtlich unzulässig zu werten war dagegen die Veröffentlichung eines Fotos und des vollständigen Geburtsdatums ohne eine schriftliche Einwilligung des betroffenen Schiedsrichters. Vertiefend verweise ich auf Punkt 5.6 des Merkblatts „Datenschutz im Verein“, welches auf meiner Internet-Seite abgerufen werden kann.

Bei einer stichprobenweisen Überprüfung der Internet-Auftritte anderer Schiedsrichtergruppen konnte ich feststellen, dass dort die Veröffentlichung personenbezogener Daten ähnlich praktiziert wurde. Um eine verbandsweite Lösung zu finden, habe ich daraufhin den zuständigen Fußballverband gebeten, auf eine datenschutzgerechte Gestaltung des Internet-Auftritts der Schiedsrichtergruppen hinzuwirken. Der Verband hat umgehend reagiert und die Thematik an den Verbandsschiedsrichterausschuss herangetragen. Inzwischen wurde zugesagt, dass künftig nur erforderliche Daten von Funktionsträgern veröffentlicht und gegebenenfalls schriftliche Einwilligungen der Betroffenen eingeholt werden sollen.

Die Veröffentlichung personenbezogener Daten durch einen Verein im Internet ist grundsätzlich unzulässig, wenn sich der Betroffene nicht ausdrücklich damit einverstanden erklärt hat. Ausnahmen gelten für die Funktionsträger eines Vereins. Persönliche Informationen von Funktionsträgern, die mit ihrer Funktion im Verein zusammenhängen, zum Beispiel Daten zur „dienstlichen“ Erreichbarkeit, dürfen auch ohne Einwilligung veröffentlicht werden.

9. Teil: Technik und Medien

1. Videoüberwachung

1.1 Achtung, wachsamer Nachbar!

Meine Dienststelle erreichen zahlreiche Eingaben von Bürgern, die sich über Videoüberwachungsanlagen in der Nachbarschaft beschweren. Es ist deshalb angebracht, hierzu einige allgemeine datenschutzrechtliche Hinweise zu geben.

Bei der Beurteilung der Zulässigkeit von Videokameras, die an Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kamera zu unterscheiden. Das Bundesdatenschutzgesetz regelt in § 6 b den Einsatz von Videoüberwachungstechnik zur Beobachtung öffentlich zugänglicher Räume, also von Bereichen, die von einer unbestimmten Zahl von Personen betreten und genutzt werden kann. Hiernach kann eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke ausnahmsweise zulässig sein. Voraussetzung ist allerdings, dass keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dem Persönlichkeitsrecht des Betroffenen, zum Beispiel eines Passanten, der von der Kamera erfasst wird, ist in diesem Zusammenhang ein hoher Stellenwert einzuräumen. Die Beobachtungsbefugnis des Hausrechtsinhabers endet zudem grundsätzlich an den Grenzen seines Grundstücks. Wer neben seinem Grundstück auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen in der Regel hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mitüberwacht werden. Das Beobachten fremder Grundstücke mit einer Videoanlage kann strafrechtliche Konsequenzen haben, wenn damit der höchstpersönliche Lebensbereich der beobachteten Person verletzt wird (vgl. § 201 a des Strafgesetzbuchs).

Nicht in jedem Einzelfall ist es mir möglich, die Zulässigkeit einer Videoüberwachungsanlage zu überprüfen. Wird der Einsatz der Überwachungstechnik auf Räumlichkeiten beschränkt, die nicht öffentlich zugänglich sind, wie dies beispielsweise bei verschlossenen Tiefgaragen, Hausfluren von reinen Wohnanlagen oder dem Garten des Nachbarn der Fall ist, findet das Bundesdatenschutzgesetz in der Regel keine Anwendung. Die Anlage unterliegt dann nicht meiner Kontrolle. Videoüberwachten Nachbarn oder Mietern stehen jedoch in diesem Fall unter Umständen zivilrechtliche Mittel zur Verfügung. Die zielgerichtete ständige Beobachtung von Dritten mittels Videokamera ohne eine Einwilligung ist eine Persönlichkeitsrechtsverletzung und kann für die Betroffenen Unterlassungs-, Beseitigungs-, aber auch Schadensersatzansprüche begründen, die im Streitfall auf dem Zivilrechtsweg geltend zu machen sind.

Videoüberwachung im Nachbarschaftsverhältnis ist ein brisantes Thema, da nicht selten ein schwelender Nachbarschaftsstreit zugrunde liegt. Die Überwachung öffentlich zugänglicher Flächen wie Straßen und Wege dürfte in den allermeisten Fällen unzulässig sein. Wer sich gegen eine Kamera wehren will, von der er vermutet, dass sie auf sein Grundstück gerichtet ist, sollte sich zur Geltendmachung möglicher zivilrechtlicher Abwehransprüche an einen Rechtsanwalt wenden.

1.2 Videoüberwachung in Gaststätten

In ihrem Fünften Tätigkeitsbericht 2009 musste sich die damalige Aufsichtsbehörde mit der Frage befassen, inwieweit es zulässig ist, dass der Gastraum in einem Lokal mit Kameras überwacht wird (B 11.2). Im vergangenen Berichtszeitraum ging es nun darum, ob beziehungsweise unter welchen Voraussetzungen der Gastwirt Videoaufnahmen von seinen Mitarbeitern bei der Arbeit machen darf.

Der Betreiber eines Imbissbetriebes hatte zwei Kameras so installiert, dass er die Mitarbeiter bei der Arbeit beobachten konnte. Angeblich waren sämtliche Beschäftigten damit einverstanden. Die Kameras waren 23 Stunden am Tag in Betrieb. Die Bilder wurden auf einer Festplatte aufgezeichnet, wo sie fünf bis acht Tage gespeichert blieben. In dieser Zeit konnte der Wirt die Aufnahmen nach Bedarf ansehen. Die Notwendigkeit begründete er damit, dass auf diesem Wege Auseinandersetzungen zwischen den Mitarbeitern verhindert werden sollten. Auch könne er so feststellen, wie lange gegrillte Ware zum Verkauf vorrätig ist. Ferner würden die Kameras nachts dem Einbruchsschutz dienen.

In der derzeit geltenden Fassung des Bundesdatenschutzgesetzes gibt es nur eine Regelung für die Kameraüberwachung in öffentlich zugänglichen Räumen. Da es sich bei dem Bereich, in dem sich in einer Gaststätte nur das Personal aufhalten darf, nicht um einen solchen handelt, kann für die datenschutzrechtliche Beurteilung des in Rede stehenden Falles nicht unmittelbar auf eine gesetzliche Regelung zurückgegriffen werden, wohl aber auf die ständige Rechtsprechung des Bundesarbeitsgerichts, der sich die Aufsichtsbehörde angeschlossen hat. Danach ist die Überwachung von Arbeitnehmern mittels Kameras durch den Arbeitgeber selbst dann nur ausnahmsweise zulässig, wenn sie offen erfolgt, die Arbeitnehmer also wissen, dass ihr Arbeitsplatz videoüberwacht ist. Maßgeblich ist insbesondere, ob der Arbeitgeber ein berechtigtes Interesse an den Kameraaufnahmen hat, etwa um Diebstählen oder dem Vandalismus durch sein Personal vorzubeugen. Hat er ein solches, berechtigt ihn dies jedoch nicht ohne weiteres zur Überwachung. Vielmehr muss sein Interesse mit den schutzwürdigen Interessen des Arbeitnehmers, nicht in seinem Persönlichkeitsrecht verletzt zu werden, abgewogen werden. Das Persönlichkeitsrecht schützt den Beschäftigten vor einer lückenlosen Überwachung am Arbeitsplatz durch Videoaufnahmen, die ihn einem ständigen Überwachungsdruck aussetzen, dem er sich nicht entziehen kann. Deswegen überwiegt das Arbeitnehmerinteresse, von einer derartigen Dauerüberwachung verschont zu bleiben, grundsätzlich, wenn der Arbeitgeber mit der Überwachung nur befürchteten Verfehlungen seiner Arbeitnehmer begegnen will, ohne dass hierfür konkrete Anhaltspunkte bestehen. Aber selbst wenn es einen entsprechenden Verdacht gibt, dass es zu einem Fehlverhalten der Mitarbeiter gekommen ist oder kommen wird, darf die Videoüberwachung nur während einer angemessenen Zeit stattfinden, längstenfalls bis zur Ermittlung der für den fraglichen Vorfall verantwortlichen Person. Auch muss die Verfehlung von einem nicht unerheblichen Gewicht sein, damit eine derartige Dauerüberwachung nicht als unverhältnismäßig zu qualifizieren ist.

Bezogen auf den konkreten Fall kam die Aufsichtsbehörde zum Ergebnis, dass der Betreiber der Imbissgaststätte seine Mitarbeiter nicht ständig per Kamera überwachen durfte. Zum einen ließ sich nicht feststellen, dass es zwischen dem Personal in der Vergangenheit zu Streitigkeiten gekommen war noch gab es dafür konkrete Anhaltspunkte. Zum anderen ist es unzulässig, Mitarbeiter ständig zu beobachten, nur um festzustellen, wie viel verkaufsfähige Ware – noch – vorhanden ist. Im Übrigen konnte sich der Betreiber nicht darauf berufen, dass seinen Mitarbeitern die Kameraüberwachung bekannt war und sie damit einverstanden waren. Ein Arbeitnehmer kann nämlich in die ständige Videoüberwachung durch den Arbeitgeber schon deswegen nicht rechtswirksam einwilligen, weil es ihm bei seiner Entscheidung an der dafür erforderlichen Freiwilligkeit nach § 4 a BDSG gegenüber seinem Chef fehlt.

In einem künftigen Arbeitnehmerdatenschutzgesetz soll geregelt werden, dass die Beobachtung von Betriebsstätten mit optisch-elektronischen Einrichtungen, die auch zur Erhebung von Beschäftigtendaten geeignet sind, nur zur Zutrittskontrolle, zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums, zur Sicherheit der Beschäftigten, zur Sicherung von Anlagen, zur Abwehr von Gefahr für die Sicherheit des Betriebes und zur Qualitätskontrolle zulässig ist, soweit sie zur Wahrung diesbezüglicher Interessen erforderlich ist und wenn nach Art und Ausmaß der Videoüberwachung die schutzwürdigen Interessen der Arbeitnehmer am Unterbleiben der Datenerhebung nicht überwiegen. Dabei bezieht sich der Begriff „Qualitätskontrolle“ in erster Linie auf die Beschaffenheit eines Produktes und nicht etwa auf die Tätigkeit der Mitarbeiter.

Das Vorgehen des Wirts war sowohl nach der bisherigen Rechtslage nicht zulässig und wird auch nach der zu erwartenden gesetzlichen Regelung des Beschäftigtendatenschutzes künftig nicht zulässig sein, soweit es die Überwachung seiner Mitarbeiter betrifft. Der Einsatz der Kameras zur Verhinderung von Einbrüchen außerhalb der Geschäftszeiten begegnete hingegen keinen datenschutzrechtlichen Bedenken.

1.3 Waschen, Schneiden, Föhnen, Videobeobachten

Die Technik der Videoüberwachung ist auch in kleinen Unternehmen weit verbreitet. Die frühere Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hatte die datenschutzrechtliche Zulässigkeit von Videokameras in mehreren Filialen eines Friseursalons zu prüfen.

Mal wieder war es zunächst die Presse, die auf die Videoüberwachungsanlagen hinwies und die Aufsichtsbehörde veranlasste, eine Stellungnahme der Betreiberin des Salons einzuholen. Danach seien die Kameras immer auf die Eingangstür sowie den davor stehenden Kassenbereich gerichtet. Die Bilder könnten von der Zentrale zu beliebigen Zeiten eingesehen werden. Als Gründe der Videoüberwachung wurden Einbruch in eine Filiale mit Diebstahl von einem Tresor mit mehreren Tageseinnahmen, Einbruch in eine Filiale mit Beschädigung der Innenausstattung, Diebstahl von Verkaufsprodukten, Zubehör und Trinkgeldkassen im Tagesbetrieb sowie eingeschlagene Schaufensterscheiben angegeben.

Die datenschutzrechtliche Überprüfung ergab, dass die Voraussetzungen des § 6 b BDSG, der die Videoüberwachung regelt, nicht vorlagen. Zwar kann eine Videoüberwachung nach entsprechenden Vorkommnissen zur Abschreckung und Verfolgung von Einbrüchen, Sachbeschädigungen und Diebstählen in Betracht kommen, allerdings nur, sofern die schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen nicht überwiegen. Für jede einzelne Kamera müssen die Zwecke, die mit der Überwachung verfolgt werden, festgelegt und jeweils eine Interessenabwägung vorgenommen werden. Die Tatsache, dass während des Geschäftsbetriebs hin und wieder Verkaufsprodukte, Zubehör und Trinkgeldkassen abhanden gekommen waren, berechtigte die Inhaberin der Friseursalonkette jedoch nicht, aus präventiven Gründen in allen Filialen die Kundschaft während des Geschäftsbetriebs ständig zu überwachen. Vielmehr konnte durch andere geeignete Maßnahmen, wie zum Beispiel entsprechende Gestaltung der Verkaufsräume und Schulung des Personals, Diebstählen während des Geschäftsbetriebs vorgebeugt werden. Die angeführten Schadensereignisse außerhalb der Geschäftszeiten konnten allenfalls eine Videoüberwachung außerhalb der Öffnungszeiten bei den betroffenen Salons rechtfertigen.

Zu berücksichtigen war ferner, dass von der Überwachung nicht nur die Kunden, sondern auch die Mitarbeiter der Friseurfilialen betroffen waren, die ihre Tätigkeit in einem öffentlich zugänglichen Raum ausübten. Die Videoüberwachung zur Mitarbeiterkontrolle ist nach der arbeitsgerichtlichen Rechtsprechung nur zulässig, wenn ein hinreichend konkreter Verdacht einer Straftat oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht und die Überwachung zur Aufklärung von Straftaten geeignet, erforderlich und unter Berücksichtigung der damit verbundenen Eingriffe in das Persönlichkeitsrecht der

Mitarbeiter angemessen ist. Anhaltspunkte, die eine Überwachung der Mitarbeiter rechtfertigen konnten, lagen jedoch nicht vor.

Der Datenschutzverstoß wurde beanstandet, die Videoüberwachungsmaßnahme musste eingestellt werden. Ich appelliere an alle Geschäftsinhaber, vor der Installation einer Videoüberwachungsanlage die Rechtmäßigkeitsvoraussetzungen sorgfältig zu prüfen. Unter Umständen ist zudem eine Vorabkontrolle nach § 4 d Absatz 5 BDSG und die Bestellung eines betrieblichen Datenschutzbeauftragten erforderlich.

2. Datenschutzprobleme im Internet

2.1 Das Datenleck beim Dienstleister I

Unbekannten war es gelungen, auf den Server des externen Dienstleiters eines baden-württembergischen Drogerieriesen ein Schadprogramm aufzuspielen. War dem Unternehmen deshalb ein datenschutzrechtlicher Vorwurf zu machen?

Manchem Online-Kunden eines baden-württembergischen Drogerieriesen mag es im August 2010 bei der Lektüre dieser Nachricht die Sprache verschlagen haben: Bei dem Unternehmen habe sich, so vermeldeten die Gazetten, ein klaffendes Sicherheitsleck aufgetan. Mehr als sieben Millionen E-Mail-Adressen von Newsletter-Kunden des Marktes sowie 150 000 komplette Kundendatensätze seien zeitweise frei im Internet zugänglich gewesen. Bahnte sich da erneut ein spektakulärer Datenschutzskandal im Lande an?

Ganz so dramatisch, wie die ersten Medienberichte glauben machten, stellte sich der Vorfall glücklicherweise doch nicht dar: Zwar musste man tatsächlich von einer großen Anzahl potenziell Betroffener ausgehen, dass deren Daten indes für jedermann zugänglich gewesen seien, traf so nicht zu. Es bedurfte vielmehr schon eines gewissen technischen Sachverstandes, um unter Ausnutzung des fraglichen „Lecks“ an die Kundendaten der Betroffenen zu gelangen. Im Übrigen hatte sich diese Sicherheitslücke gar nicht bei dem Drogerieriesen selbst aufgetan, sondern bei einem externen, nicht in Baden-Württemberg ansässigen Dienstleister, der im Rahmen einer Auftragsdatenverarbeitung die Adressdaten von Online-Kunden des Unternehmens betreut hatte. Unbekannten war es gelungen, auf einen Server dieses Dienstleisters ein Schadprogramm aufzuspielen, das es einem fachkundigen Nutzer, der um dieses Einfallstor wusste, in der Tat vorübergehend ermöglichte, über das Internet auf die von dem Auftragnehmer verwalteten Datenbestände zuzugreifen. Das Einfallstor war aber bereits wieder geschlossen worden, als sich die Aufsichtsbehörde einschaltete.

War dem Drogerieriesen bei dieser Sachlage überhaupt ein datenschutzrechtlicher Vorwurf zu machen? Das Datenschutzrecht jedenfalls nimmt den Auftraggeber einer Auftragsdatenverarbeitung durchaus in die Pflicht: Gemäß § 11 Absatz 1 BDSG bleibt er im Rahmen einer Auftragsdatenverarbeitung für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Um dieser Verantwortung gerecht zu werden, hat er gemäß § 11 Absatz 2 BDSG verschiedene Verpflichtungen zu erfüllen: Er muss den Auftragnehmer zunächst unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen und ihm einen schriftlichen Auftrag erteilen, in dem Festlegungen unter anderem zu Gegenstand und Dauer des Auftrags, über den Umfang, die Art und den Zweck der Datenverwendung, aber auch bezüglich der zum Schutz der Daten erforderlichen technischen und organisatorischen Maßnahmen zu treffen sind. Vor Beginn der Datenverarbeitung und sodann „regelmäßig“ hat er sich von der Einhaltung der beim Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen zu überzeugen und das Ergebnis zu dokumentieren.

Die Prüfung der Aufsichtsbehörde ergab, dass die Drogeriekette ihren Pflichten nicht vollumfänglich gerecht geworden war. Zwar hatte sich

das Unternehmen einen zweifellos renommierten Auftragnehmer ausgesucht, der auf prominente Referenzkunden verweisen konnte; gerade deshalb hatte das Unternehmen jedoch unzulässigerweise auf die vorgeschriebene Erstkontrolle der vom Dienstleister umzusetzenden technischen und organisatorischen Datenschutzmaßnahmen verzichtet. Überdies musste die Aufsichtsbehörde bemängeln, dass im schriftlichen Auftrag, den der Drogerieriese seinem Dienstleister erteilt hatte, verbindliche Absprachen über eine angemessene Protokollierung der Nutzung des Systems fehlten. Offenbar waren die Vertragspartner der Auffassung gewesen, auf eine vertraglich fixierte „Protokollierungs-Policy" verzichten zu können, weil sie sich auf die einschlägige Konfiguration der speziellen Software des Dienstleisters verließen. Naturgemäß nutzt jedoch auch eine akribische Protokollierung wenig, wenn sie nicht auch in angemessenem Umfang ausgewertet wird. Wie es der Auftragnehmer damit gehalten hatte, konnte von der Aufsichtsbehörde, deren örtliche Zuständigkeit sich ja auf Baden-Württemberg beschränkte, nicht geprüft werden. Ergänzend ist noch zu berichten, dass die Staatsanwaltschaft am Sitz des Dienstleisters inzwischen auf Antrag des Auftraggebers ein strafrechtliches Ermittlungsverfahren eingeleitet hat, von dessen Ausgang wir uns weitere Erkenntnisse über die Ursachen des Datenlecks erhoffen.

Auf die Einleitung eines Bußgeldverfahrens gegen die Drogeriemarktkette verzichtete die Aufsichtsbehörde seinerzeit, nicht zuletzt, weil schon der eingetretene Imageschaden beträchtlich war und zweifelhaft blieb, ob die mit erheblicher krimineller Energie durchgeführte Cyber-Attacke auf den Dienstleister selbst bei einer besseren Ausgestaltung und Kontrolle der Auftragsdatenverarbeitung zu verhindern gewesen wäre.

Wer personenbezogene Daten im Auftrag verarbeiten lässt, sollte die Pflichten des Auftraggebers nach § 11 BDSG schon im eigenen Interesse gewissenhaft erfüllen.

2.2 Das Datenleck beim Dienstleister II – Personenbezogene Kundendaten im Internet

Die frühere Aufsichtsbehörde im nicht-öffentlichen Bereich wurde auf eine Sicherheitslücke eines Dienstleisters aufmerksam, der Busreisen zu auswärtigen Spielen eines baden-württembergischen Fußballbundesligavereins organisiert.

Die Organisation hatte unbemerkt personenbezogene Angaben zu Kunden einschließlich Kontendaten sowie persönliche Bemerkungen zu diesen Personen so gespeichert, dass diese Informationen von Dritten im Internet abgerufen werden konnten. Versäumt worden war, die notwendigen technischen und organisatorischen Maßnahmen zur Absicherung der Daten zu ergreifen.

Die Aufsichtsbehörde wertete dies aufgrund der Art der personenbezogenen Daten, die über das Internet für jedermann frei zugänglich waren, als einen schwerwiegenden Datenschutzverstoß. Die Organisation konnte sich nicht darauf berufen, dass sie einen „erfahrenen Programmierer" mit der Entwicklung und Betreuung des Internet-Auftritts nach sämtlichen Sicherheitsstandards beauftragt hatte. Als verantwortliche Stelle war die Organisation selbst für die Einhaltung insbesondere der in der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen verpflichtet und für die festgestellten Datenschutzverstöße verantwortlich.

Nachdem sich die Aufsichtsbehörde mit der Angelegenheit befasst hatte, hat die Organisation die Sicherheitslücke geschlossen und alles unternommen, um künftig derartige unbefugte Zugriffe auszuschließen. Gegen den Geschäftsführer der Organisation wurde ein Bußgeld verhängt.

Wer Kundenbestellungen über das Internet abwickelt, hat dafür Sorge zu tragen, dass die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden und keine Sicherheitslücken bestehen. Die Einschaltung eines Dritten als Programmierer entbindet nicht von der datenschutzrechtlichen Verantwortlichkeit.

3. Abschied von der GEZ? Der 15. Rundfunkänderungsstaatsvertrag

Die gerätebezogene Rundfunkgebühr soll ab 2013 auf einen wohnungsbezogenen Rundfunkbeitrag umgestellt werden. Datenschutzrechtliche Probleme bleiben.

Die Tätigkeit der Gebühreneinzugszentrale (GEZ), die im Auftrag der öffentlich-rechtlichen Rundfunkanstalten unter anderem „Schwarzhörer“ und „Schwarzseher“ aufspüren soll, ist für viele Menschen seit jeher ein Stein des Anstoßes gewesen, die ein Ausforschen privater Lebensumstände durch diese Einrichtung befürchten. Auch wenn nicht ich, sondern der Datenschutzbeauftragte des Südwestrundfunks sich zuständigkeitshalber mit den zahlreichen Eingaben wegen der vermeintlichen „Schnüffelpraxis“ der GEZ befassen muss, war es doch auch ein langjähriger Wunsch der Datenschutzbeauftragten des Bundes und der Länder gewesen, endlich zu einer grundlegenden Neuorientierung der Rundfunkfinanzierung zu kommen und dabei datenschutzfreundlichen Modellen den Vorzug zu geben (vgl. insoweit bereits die Entschließung der Datenschutzkonferenz vom 30. April 2003, abgedruckt als Anhang 10 zum 24. Tätigkeitsbericht 2003). Nach langer Vorbereitung auf Seiten der Rundfunkanstalten und der Landesmedienreferenten wurde schließlich im Frühjahr 2010 mit dem Entwurf des 15. Rundfunkänderungsstaatsvertrages (15. RÄStV; Rundfunkbeitragsstaatsvertrag, RBStV) ein grundlegender Systemwechsel bei der Erhebung der finanziellen Mittel für die Tätigkeit des öffentlich-rechtlichen Rundfunks in Deutschland eingeleitet. Die bisherige, an den Besitz eines Empfangsgerätes gekoppelte Rundfunkgebühr soll danach ab 2013 durch die Erhebung eines an das Innehaben einer Wohnung oder Betriebsstätte anknüpfenden Beitrages ersetzt werden. Erklärtes Ziel des neuen Beitragsmodells war außer einer höheren Beitragsgerechtigkeit auch eine deutlich datenschutzgerechtere Beitragserhebung. Zwar war diese Zielsetzung auch aus meiner Sicht zu begrüßen; der Systemwechsel war aber eher dem Umstand geschuldet, dass es durch die zunehmende Medienkonvergenz immer schwieriger geworden war, die Gebührenpflicht an herkömmliche Rundfunkgeräte oder an medienfähige Computer zu binden. Immerhin räume ich ein, dass die Umstellung auf eine wohnungsbezogene Abgabe wahrscheinlich zu einer geringeren Zahl zu speichernder Beitragszahler führen wird. Andererseits bestand aufgrund des Entwurfs die Sorge, dass im Gegenzug die Datenverarbeitungsbefugnisse der für den Einzug der Finanzmittel zuständigen öffentlich-rechtlichen Rundfunkanstalten nach dem Grundsatz der Erforderlichkeit nicht entsprechend beschränkt werden würden. So sollten die Landesrundfunkanstalten zum Beispiel in § 11 Absatz 4 RBStV ermächtigt werden, die für die Beitragserhebung notwendigen Daten ohne Kenntnis des Betroffenen – bei öffentlichen und nicht-öffentlichen Quellen (also auch beim Adresshandel) – zu erheben. Diese Ermächtigung würde mit dem fundamentalen Prinzip brechen, dass Daten grundsätzlich beim Betroffenen zu erheben sind, was nur bei zwingender Notwendigkeit akzeptabel wäre. Ein anderer Kritikpunkt betraf die Vorlage und die Speicherung von Nachweisen zur Befreiung oder Ermäßigung der Beitragspflicht (in der Regel handelt es sich hierbei um Unterlagen, mit denen der Betroffene eine ungünstige finanzielle oder gesundheitliche Situation nachweisen kann). Vorgesehen ist, dass derartige Nachweise im Original oder in beglaubigter Kopie eingereicht werden müssen und dann eingescannt und gespeichert werden. Aus Sicht des Datenschutzes hätte es eher dem Grundsatz der Datensparsamkeit entsprochen, wenn die Nachweispflicht auf die Vorlage von Leistungsbescheinigungen beschränkt worden wäre, die lediglich den Leistungsgrund und den Leistungszeitraum erkennen lassen. Als unverhältnismäßig wurde von den Datenschutzbeauftragten auch der mögliche Zugriff der GEZ (beziehungsweise der geplanten Nachfolgeeinrichtung) auf alle Daten aller Beitragsschuldner und nicht etwa nur auf die einer bestimmten Rundfunkanstalt kritisiert.

Die Datenschutzbeauftragten des Bundes und der Länder wurden durch die federführende Staatskanzlei Rheinland-Pfalz relativ frühzeitig beteiligt, konnten aber – um das Ergebnis vorwegzunehmen – an dem partei- und länderübergreifend zu diesem Zeitpunkt bereits weitgehend festgezurrten Entwurf nur noch marginale Änderungen erreichen. So wurde meine branden-

burgische Kollegin zwar als Vorsitzende des Arbeitskreises Medien und stellvertretend für die Datenschutzkonferenz in Gesprächsrunden mit Rundfunkanstalten und Medienreferenten eingeladen, in der Substanz konnte aber auch sie keinen Einfluss mehr nehmen. Vielmehr konterten die Rundfunkanstalten grundlegende datenschutzrechtliche Zweifel an dem neuen Modell durch ein „Gegengutachten" des früheren Bundesdatenschutzbeauftragten, Prof. Dr. Hans-Peter Bull, der an dem Staatsvertragsentwurf nichts auszusetzen hatte. Kein Wunder, dass auch der Appell der Datenschutzbeauftragten in ihrer Entschließung und in der Stellungnahme vom 11. Oktober 2010 (vgl. Anhänge 7 und 8) zunächst weitgehend ungehört verhallte.

Immerhin hatten inzwischen die Landesparlamente registriert, dass es gegen das neue Rundfunkbeitragsmodell nicht nur Widerstand von Hauseigentümerverbänden und Mittelstandsvereinigungen, sondern auch von Datenschutzseite gab. Wie andere Landtage forderte auch der Landtag von Baden-Württemberg in einer Entschließung vom 25. November 2010 die Landesregierung auf, diese Bedenken eingehend zu bewerten und gegebenenfalls auf entsprechende Änderungen hinzuwirken (vgl. LT-Drucksache 14/7229, Ziffer IV). In seinem Bericht vom 24. Januar 2011 verwies das Staatsministerium für die Landesregierung darauf, dass es die datenschutzrechtlichen Fragestellungen nachdrücklich in das Abstimmungsverfahren der Länder eingebracht habe und einige Änderungen erreicht worden seien (vgl. LT-Drucksache 14/7529, S. 3). In der Zwischenzeit hatten die Ministerpräsidenten der Länder aber bereits den Staatsvertrag unterschrieben und das Ratifizierungsverfahren eingeleitet. Als mir das Staatsministerium im Juni 2011 schließlich die Gelegenheit zu einer Stellungnahme zum Entwurf des Zustimmungsgesetzes (vgl. LT-Drucksache 15/197) gab, war mir natürlich bewusst, dass es für inhaltliche Änderungen zu spät war, denn die Landtage konnten den Staatsvertrag ja nur noch in Gänze ablehnen oder ihm zustimmen. So wiederholte ich noch einmal meine früheren Bedenken und wies darauf hin, dass die Rundfunkanstalten ja nicht alle durch den Staatsvertrag eröffneten Möglichkeiten der Datenverarbeitung ausschöpfen, sondern sich im Zuge der Umsetzung freiwillig selbst beschränken könnten. In diesem Sinne wandte ich mich im Verlauf des Gesetzgebungsverfahrens auch an den Ständigen Ausschuss des Landtags, der den Entwurf am 29. September 2011 beriet (vgl. LT-Drucksache 15/563); dabei gab ich der Hoffnung Ausdruck, dass der Landtag einen Appell zur Selbstbeschränkung an die Adresse der Rundfunkanstalten richten möge. Erfreulicherweise wurde diese Anregung aufgegriffen: Bei der Verabschiedung des Gesetzes (LT-Drucksache 15/693) am 12. Oktober 2011 verabschiedete der Landtag einstimmig einen Entschließungsantrag aller vier Fraktionen (LT-Drucksache 15/671), in dem die Rundfunkanstalten unter Bezugnahme auf meine Kritikpunkte aufgefordert wurden, bei der Erhebung und Verwendung von Daten zur Entrichtung des Rundfunkbeitrags den Grundsatz der Verhältnismäßigkeit zu wahren und – was aus meiner Sicht noch wichtiger als die Erinnerung an die eigentlich selbstverständliche Beachtung rechtsstaatlicher Prinzipien ist – in die ohnehin vorgesehene Evaluierung des neuen Finanzierungsmodells explizit Aspekte der Datenschutzkonformität einzubeziehen. In die Vorbereitung und Durchführung dieser Evaluierung sollen zudem die Landesdatenschutzbeauftragten einbezogen werden; außerdem soll der Evaluierungsbericht veröffentlicht werden und als Muster für spätere Änderungen des Rundfunkstaatsvertrages mit dem Ziel der Stärkung von Datenschutzaspekten dienen. Dieses politische Signal, das meines Wissens auch in anderen Landesparlamenten Beachtung und Nachahmer gefunden hat, ist unter den gegebenen Umständen rundum erfreulich und als Zeichen der Hoffnung zu werten, dass dem Datenschutz bei der Erhebung der Rundfunkbeiträge künftig noch mehr Beachtung geschenkt wird.

Wie geht es nun weiter? Die Hoffnung mancher Zeitgenossen, dass die GEZ aufgelöst wird, wird sich nicht erfüllen, denn natürlich werden die öffentlich-rechtlichen Rundfunkanstalten zur Eintreibung der neuen Beiträge weiterhin eine entsprechende Einrichtung brauchen, auch wenn diese dann nicht mehr GEZ heißen mag. Und auch die Hoffnung mancher Medienpolitiker, die das stetige Wachstum des Finanzbedarfs der Sender – und damit des von den Bürgerinnen und Bürgern zu entrichtenden Rundfunkbeitrags – mit Sorge sehen und der GEZ gerne eine Schrumpfkur verordnen würden,

wird enttäuscht werden, denn die Nachfolgeeinrichtung der GEZ wird vorübergehend sogar mehr Personal benötigen, weil das neue Beitragsmodell nach § 14 Absatz 9 RBStV mit einem aufwändigen einmaligen Abgleich der vorhandenen Datenbestände der GEZ mit den bundesweit vorhandenen Meldedaten beginnen wird. Aus Datenschutzsicht erfreulich ist immerhin, dass der nach dem Staatsvertrag grundsätzlich mögliche Ankauf privater Adressen durch die Landesrundfunkanstalten bis Ende 2014 ausgesetzt wird (§ 14 Absatz 10 RBStV). Um die Möglichkeiten einer datenschutzfreundlichen Umsetzung des Staatsvertrags auszuloten, habe ich an einem Gespräch zwischen Vertretern der Rundfunkanstalten, einigen Medienreferenten der Staatskanzleien und Datenschutzbeauftragten teilgenommen, das Anfang Oktober 2011 in Mainz stattfand. Dabei wurde insbesondere erörtert, wie – ungeachtet divergierender Standpunkte – im praktischen Vollzug der Beitragserhebung datenschutzgerechtere Lösungen entwickelt werden könnten, etwa durch die weitere Konkretisierung unbestimmter Rechtsbegriffe, die Präzisierung von Zweckbestimmungen, die Modalitäten der Unterrichtung der Betroffenen über die Datenquelle, das Verfahren beim Zugriff auf die für die Beitragsbefreiung erforderlichen Unterlagen oder schlicht durch die Gestaltung bestimmter Formulare. Einzelne Punkte bieten sich gegebenenfalls für eine Aufnahme in die nach § 9 Absatz 2 RBStV von der zuständigen Rundfunkanstalt zu erlassende Satzung an. Die Überlegungen sind noch nicht abgeschlossen und bedürfen noch der weiteren Präzisierung und Abstimmung, sowohl unter den Datenschutzbeauftragten als auch unter den Rundfunkanstalten. Im Interesse der Betroffenen sind aber manchmal auch viele kleine Schritte sinnvoll, um zu einem vertretbaren Ziel zu gelangen.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010/2011

Anhang 1	Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung
Anhang 2	Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich
Anhang 3	Körperscanner – viele offene Fragen
Anhang 4	Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!
Anhang 5	Keine Vorratsdatenspeicherung!
Anhang 6	Beschäftigtendatenschutz stärken statt abbauen
Anhang 7	Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!
Anhang 8	Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. September 2010 zum Entwurf des 15. Rundfunkänderungsstaatsvertrages
Anhang 9	Erweiterung der Steuerdatenbank enthält große Risiken
Anhang 10	Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs
Anhang 11	Keine Volltextsuche in Dateien der Sicherheitsbehörden
Anhang 12	Förderung des Datenschutzes durch Bundesstiftung
Anhang 13	Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene
Anhang 14	Beschäftigtendatenschutz stärken statt abbauen
Anhang 15	Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze
Anhang 16	Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten
Anhang 17	Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!
Anhang 18	Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen
Anhang 19	Funkzellenabfrage muss eingeschränkt werden!
Anhang 20	Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick
Anhang 21	Datenschutz als Bildungsaufgabe
Anhang 22	Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing
Anhang 23	Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!
Anhang 24	Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anhang 25 Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Anhang 26 Anonymes elektronisches Bezahlen muss möglich bleiben!

Beschlüsse des Düsseldorfer Kreises seit 1. Juli 2009

Anhang 27 Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!

Anhang 28 Gesetzesänderung bei der Datenverwendung für Werbezwecke

Anhang 29 Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Anhang 30 Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Anhang 31 Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Anhang 32 Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Anhang 33 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Anhang 34 Minderjährige in sozialen Netzwerken wirksamer schützen

Anhang 35 Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4 f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Anhang 36 Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Anhang 37 Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Anhang 38 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Anhang 39 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Anhang 40 Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Anhang 41 Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Anhang 42 Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Anhang 43 Datenschutz in sozialen Netzwerken

Anhang 44 Stellungnahme „Fertigung von Luftbildaufnahmen zur Ermittlung von kommunalen Abwassergebühren“

Anhang 1

**Entschließung der 79. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010**

**Klare gesetzliche Regelungen zur Abrechnung
durch private Stellen in der gesetzlichen Krankenversicherung**

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1 b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechnungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

Anhang 2

**Entschließung der 79. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010**

Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden:

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z. B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),
- die Leistung, Wirkung sowie der Erfolg und die Effizienz,
- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

Anhang 3

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Körperscanner – viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.
2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.
3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.
4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Anhang 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010

Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Anhang 5

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt". Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

Anhang 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zugunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.
- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln – etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen –, weiterhin zu unterbleiben haben.
- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken sys-

tematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv – und nicht erst auf Nachfrage – darüber aufzuklären, woher die verwendeten Daten stammen.

– Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

– Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Anhang 7

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 11. Oktober 2010

Rundfunkfinanzierung:
Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,
- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und
- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

Anhang 8

Stellungnahme der
Konferenz der Datenschutzbeauftragten des Bundes und der Länder

zum

Entwurf des 15. Rundfunkänderungsstaatsvertrages

(Stand 15. September 2010)

Vorbemerkung

Mit dem vorgelegten Entwurf des 15. Rundfunkänderungsstaatsvertrages (RBStV-E) soll ein grundlegender Systemwechsel bei der Erhebung der finanziellen Mittel für die Tätigkeit des öffentlich-rechtlichen Rundfunks in Deutschland vollzogen werden. Die bisherige an den Besitz eines Empfangsgerätes gekoppelte Rundfunkgebühr soll durch die Erhebung eines an das Innehaben einer Wohnung oder Betriebsstätte anknüpfenden Beitrages ersetzt werden. Ziel des neuen Beitragsmodells ist außer einer höheren Beitragsgerechtigkeit auch eine deutlich datenschutzgerechtere Beitragserhebung. Das letztgenannte Ziel droht der vorliegende Entwurf zu verfehlen. Die Umstellung auf eine wohnungsbezogene Abgabe wird zwar wahrscheinlich zu einer geringeren Zahl zu speichernder Beitragszahler führen, dies aber ohne entsprechend die Datenverarbeitungsbefugnisse der für den Einzug der Finanzmittel zuständigen öffentlich-rechtlichen Rundfunkanstalten nach dem Grundsatz der Erforderlichkeit zu beschränken.

Aus datenschutzrechtlicher Sicht widersprechen die Datenverarbeitungsbefugnisse des Staatsvertragsentwurfs durch zu umfangreiche Ermächtigungen der Rundfunkanstalten und ihrer Hilfsorgane den Grundsätzen der Verhältnismäßigkeit und Datensparsamkeit sowie den Grundsätzen der Normklarheit und Transparenz. Es entsteht der Eindruck, dass die Verfasser des Entwurfs befürchtet haben, dass auch in Zukunft umfangreiche Datenerhebungsbefugnisse für den Gebühreneinzug gebraucht werden, um für jede Wohnung trotz Anmeldepflicht oftmals mehrerer beitragspflichtiger volljähriger Gesamtschuldner einen zahlungswilligen Beitragsschuldner zu finden.

Datenschutzrechtliche Bewertung im Einzelnen:

I. Regelung der Datenverarbeitungsbefugnisse

In *§ 11 Absatz 4 RBStV-E* werden die Landesrundfunkanstalten ermächtigt, die für die Beitragserhebung notwendigen Daten ohne Kenntnis des Betroffenen zu erheben. Die Befugnis erstreckt sich auf öffentliche und nicht-öffentliche Quellen. Diese Ermächtigung bricht mit dem fundamentalen Prinzip, dass Daten grundsätzlich beim Betroffenen zu erheben sind. Eine Abweichung von diesem Grundprinzip wäre nur bei zwingender Notwendigkeit akzeptabel. Dies ist hier jedoch nicht der Fall. Die Länder bzw. Landesrundfunkanstalten haben bisher nicht darlegen können, welchen zusätzlichen Erkenntnisgewinn die Nutzung nicht öffentlicher Datenquellen gegenüber einer ausschließlichen Nutzung der öffentlichen Quellen tatsächlich erbringen soll.

Zunächst einmal unterliegt jeder Beitragspflichtige nach § 8 Abs. 1 RBStV-E einer Meldepflicht, nach der er selbst die erforderlichen und im Staatsvertrag genannten Daten an die Rundfunkanstalten zu übermitteln hat. Sollte für eine Wohnung kein Wohnungsinhaber namentlich bekannt sein, weil der Meldepflicht nicht nachgekommen wurde, besteht über die Meldebehörde oder die Datenerhebung beim Grundbuchamt als einer öffentlichen Stelle die Möglichkeit, den Eigentümer einer Liegenschaft und über dessen Auskunftspflicht die Nutzer der jeweiligen Wohnung oder Betriebsstelle zu ermitteln.

Es ist mithin kein Grund ersichtlich, warum darüber hinaus auch bei nicht öffentlichen Stellen Daten erhoben werden sollen. Die Art der zu nutzenden nicht-öffentlichen Quellen ist in keiner Weise konkretisiert. Es kommen also alle denk-

baren Möglichkeiten, wie zum Beispiel Arbeitgeber, Versicherungen, Versandhäuser, Inkassounternehmen und Auskunfteien in Betracht. Über diese Ermächtigung soll auch zukünftig die Möglichkeit bestehen, Adressdaten aus privaten Quellen anzukaufen, was sich mit dieser Deutlichkeit beim Lesen des Regelungstextes für den Beitragsschuldner nicht unmittelbar ergibt. Gerade der Ankauf von Adressdaten bei privaten Stellen, das heißt Adresshändlern, ist aber nach einer Umstellung von der Geräteabgabe auf eine Wohnungsabgabe nicht mehr erforderlich. Hinzu kommt, dass hier keine Möglichkeit für die Rundfunkanstalt besteht, die Qualität der nicht öffentlichen Datenquelle zu überprüfen, und somit ein erhebliches Risiko besteht, hier mit falschen Daten zu arbeiten, was sich in der Vergangenheit immer wieder gezeigt hat. Außerdem stellt der Ankauf von großen Mengen von Adressdaten bei Dritten auch keine zielgerichtete Form der Datenerhebung dar. Es werden sozusagen auf Verdacht Daten erhoben, die „ins Blaue hinein“ überprüft werden auf mögliche, noch unbekannte Wohnungsinhaber.

Auch hinsichtlich der Möglichkeit der Datenerhebung bei öffentlichen Stellen ist eine Begrenzung zu fordern. Das Fehlen jeglicher sachlicher Grenzen widerspricht dem Gebot der Normenbestimmtheit. Die Einhaltung dieses Gebots ist umso wichtiger, als der Betroffene keine Kenntnis von der Datenerhebung hat und somit seine Interessen nicht selbst verfolgen kann.

Unter diesen Gesichtspunkten stellt sich die Befugnis der Rundfunkanstalten, die Datenerhebung beim Betroffenen oder öffentlichen Stellen zusätzlich auch auf private Quellen auszuweiten, als unzulässig dar.

Der Staatsvertragsentwurf sieht zudem eine Löschungsfrist von 12 Monaten für so erlangte nicht benötigte Daten vor. Die Erforderlichkeit einer derart langen Speicherdauer ist nicht ersichtlich.

Der Entwurf bedarf dringend der systematischen nach der Eingriffstiefe abgestuften Klarstellung, dass die Daten ausschließlich beim Betroffenen zu erheben sind und nur in begründeten Ausnahmefällen ein Rückgriff auf weitere öffentliche Quellen zulässig ist. Diese Bestimmung des Gesetzesinhalts darf insbesondere nicht im Rahmen der Satzungsermächtigung gemäß § 9 Abs. 2 erfolgen.

Sichergestellt werden muss außerdem, dass spezialgesetzliche Erhebungs- und Verarbeitungsbefugnisse durch die Rechtfertigungstatbestände des Rundfunkbeitragsstaatsvertrages nicht umgangen werden. Mit § 11 Abs. 4 RBStV-E wird ein Paralleltatbestand zur Erhebung von Daten aus öffentlichen Registern geschaffen. Die dafür erlassenen bereichsspezifischen Übermittlungstatbestände können so ausgehebelt werden. Die Landesrundfunkanstalten haben z. B. die Wahl, entweder über die melderechtlichen Vorschriften auf das Melderegister zuzugreifen oder § 11 Abs. 4 RBStV-E als Rechtsgrundlage heranzuziehen. Den bereichsspezifischen Vorschriften ist hier inhaltlich bestimmt und normenklar der Vorrang einzuräumen.

II. Datenerhebungsbefugnisse bei Befreiungstatbeständen

Der Staatsvertragsentwurf sieht vor, dass sich Bürger beim Vorliegen von besonderen Voraussetzungen gemäß *§ 4 RBStV-E* von der Beitragspflicht befreien lassen können oder zumindest einen Anspruch auf Ermäßigung des Rundfunksbeitrages haben. Die Befreiungstatbestände sind überwiegend im sozialen Bereich begründet. Die Befreiung/Ermäßigung wird auf Antrag bei Nachweis der Voraussetzungen gewährt.

Nach den vorgesehenen Vorschriften wären die Rundfunkanstalten berechtigt, zum Nachweis der Berechtigung sich eine Bescheinigung oder die Originalbescheide bzw. beglaubigte Kopien dieser Bescheide vorlegen zu lassen und diese zu speichern. Der Entwurf orientiert sich dabei ausschließlich an praktischen Belangen der Rundfunkanstalten, wonach die gesamte Eingangspost bei der Gebühreneinzugszentrale (GEZ) eingescannt wird. Nur deshalb erfolgt eine vollständige Erfassung der Bescheide. Nach eigenen Aussagen der GEZ ist bei dieser Verfahrensweise eine partielle Löschung nicht benötigter Daten nicht möglich. Allein deshalb werden auch sensitive Gesundheits- und/oder Sozialdaten gespeichert, die von niemandem bestritten für die Entscheidung über eine Beitragsbefreiung nicht erforderlich sind.

Die Verarbeitung nicht erforderlicher Daten widerspricht jedoch den Grundsätzen unserer Datenschutzordnung, insbesondere dem Grundsatz der Datensparsamkeit,

der über Art. 6 Absatz 1 Ziffer c der Europäischen Datenschutzrichtlinie Eingang in unsere Rechtsordnung gefunden hat. Auch das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung die Geltung des, sich durch das Datenschutzrecht weithin durchziehenden Grundsatzes der Datensparsamkeit zum Ausdruck gebracht (BverfG 1 BvR 256/08, in Juris, Rn. 270). Dieser Grundsatz durchzieht nicht nur das BDSG, sondern auch zahlreiche weitere Landes- und spezielle Gesetze über den Datenschutz.

Datenschutzgerecht wäre es hier, die Nachweispflicht auf die Vorlage von Leistungsbescheinigungen zu beschränken, die lediglich den Leistungsgrund und den Leistungszeitraum erkennen lassen. Vielfach stellt die Leistungsverwaltung deshalb speziell sog. Drittbescheinigungen aus. Deshalb sollte eine geänderte Regelung vorsehen, dass grundsätzlich Drittbescheinigungen vorzulegen sind (die dann gescannt werden könnten) und nur dann, wenn die Beschaffung einer Drittbescheinigung nicht möglich ist, die Vorlage des Leistungsbescheids im Original oder in beglaubigter Kopie verlangt werden kann (der dann von den Rundfunkanstalten bzw. deren Auftragsdatenverarbeiter nicht gescannt werden darf, sondern aus dem die entscheidungserheblichen Daten händisch gespeichert werden und der Bescheid anschließend zurückgesendet wird).

Da mit einer hohen Zahl von Befreiungsanträgen aufgrund der gesamtschuldnerischen Haftung aller volljährigen Wohnungsinhaber zu rechnen ist, könnte der nicht erforderliche Datenbestand durch den Modellwechsel noch anwachsen, wenn keine Änderung des Verfahrens geregelt wird.

Ein weiterer Befreiungstatbestand (§ 4 Absatz 6 RBStV-E) soll nach dem Staatsvertragsentwurf in sog. Härtefällen vorliegen. Welche konkreten Nachweispflichten hier bestehen, ist dem Entwurf nicht zu entnehmen. Es ist jedoch anzunehmen, dass hier neben der Übermittlung von Gesundheits- und/oder Sozialdaten auch die Offenlegung von Finanz- und Steuerdaten erforderlich ist. In jedem Falle ist hier eine gesetzliche Konkretisierung des Datenerhebungsumfangs notwendig, um bei den Beitragsschuldnern die erforderliche Rechtsklarheit zu schaffen. Diesbezügliche Erläuterungen in der Regelungsbegründung sind nicht ausreichend.

III. Funktionsübertragungsmöglichkeiten auf private Dritte

Gemäß *§ 10 Absatz 7 Satz 1 RBStV-E* bedienen sich die Rundfunkanstalten bei der Beitreibung des Rundfunkbeitrages einer „im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene(n) Stelle“, mit dieser Beschreibung ist die heutige GEZ gemeint. Diese Stelle verarbeitet die erforderlichen Daten für die Beitragserhebung. Datenschutzrechtlich ist das Verhältnis zwischen den Rundfunkanstalten und der genannten Stelle als Datenverarbeitung im Auftrag zu betrachten. Einzige Aufgabe dieser Stelle ist es, die Rundfunkbeiträge von den Bürgern einzuziehen und den Rundfunkanstalten bereitzustellen. Vor diesem Hintergrund ist es nicht nachvollziehbar, dass in § 10 Absatz 7 Satz 1 RBStV-E die Landesrundfunkanstalten außerdem ermächtigt werden sollen, diese Aufgabe zusätzlich „ganz oder teilweise“ auf Dritte zu übertragen. Dies führt zu einer weiteren Datenverarbeitung durch Dritte und ist nicht notwendig, es sei denn, die von den Rundfunkanstalten betriebene gemeinsame Stelle ist nicht in der Lage, die Aufgabe zu erfüllen, die ihre Existenzberechtigung ausmacht. Hinzu kommt, dass eine vollständige („ganz“) Übertragung von Aufgaben auf Dritte eine unzulässige Funktionsübertragung darstellen würde.

IV. Zugriff auf Daten Beitragspflichtiger anderer Rundfunkanstalten

Zur Erfüllung Ihrer Aufgaben hält die im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle die kompletten Datensätze aller beitragspflichtigen Bürger der gesamten Bundesrepublik vorrätig. Eine logische Trennung dieses *Registers* nach Zugehörigkeit zu einer bestimmten Landesrundfunkanstalt erfolgt nicht. Umgekehrt haben die einzelnen Landesrundfunkanstalten Zugriff auf den kompletten Datensatz aller Beitragsschuldner der Bundesrepublik. Bereits in anderen Rechtsbereichen wurde die Existenz solcher bundesweiten zentralen Register als unzulässig kritisiert. Unabhängig von der grundsätzlichen datenschutzrechtlichen Kritik an solchen zentralen Datensammlungen ist hier mit dem neuen Modell der Rundfunkfinanzierung auch kein Bedarf für einen bundesweiten Zugriff auf alle Rundfunkbeitragsschuldnerdaten er-

kennbar. Wurde beim jetzigen Finanzierungsmodell noch an eine Person angeknüpft, die ein Empfangsgerät bereithält, ist zukünftig eine Wohnung oder Betriebsstätte Anknüpfungspunkt für die Zahlungspflicht. Da diese in der Regel ortsfest sein werden, ist nur noch der Zugriff einer Rundfunkanstalt auf die Daten erforderlich, die sich auf Wohnungen und/oder Betriebsstätten im eigenen Sendegebiet beziehen. Jede weitere Möglichkeit der Datenverarbeitung wäre unverhältnismäßig und damit unzulässig.

V. Einmaliger Meldedatenabgleich über einen Zeitraum von zwei Jahren

Der Entwurf des Staatsvertrages sieht in *§ 14 Absatz 9 RBStV-E* vor, dass die Rundfunkanstalten innerhalb einer Frist von 2 Jahren ab Inkrafttreten des Staatsvertrages von allen Meldebehörden einen festgelegten Datensatz aller volljährigen Personen übermittelt bekommen, um eine Bestands- und Ersterfassung der Beitragsschuldner zu ermöglichen. Dieses gewählte Verfahren erscheint mit dem Grundsatz der Datensparsamkeit nicht vereinbar, da ein Grund für eine pauschale Datenübermittlung durch die Meldebehörden aufgrund der Vermutungsregelung nach § 14 Abs. 3 RBStV-E nicht besteht. Nur in Zweifelsfällen ist eine Datenübermittlung bei konkreter Anforderung erforderlich; auf diese sollte daher die Datenübermittlungsbefugnis beschränkt werden. Auch sollte zumindest die Anzeigepflicht nach § 14 Abs. 1 RBStV-E gestrichen werden, da eine voraussetzungslose und umfassende Anzeigepflicht Privater Bedenken im Hinblick auf den Verhältnismäßigkeitsgrundsatz begegnet; Beitragsausfälle dürften aufgrund der Vermutungsregelung kaum eintreten und Streitfälle ließen sich durch konkrete Datenanforderungen bei den Meldebehörden lösen, auch existiert bereits jetzt eine Meldedatenübermittlungsermächtigung in den Landesmeldegesetzen.

VI. Weitere datenschutzrechtliche Problempunkte

1. Begriff der Wohnung

Obwohl seit April 2010 von den Datenschutzbeauftragten immer wieder angesprochen, ist noch immer keine Klarheit im Staatsvertragsentwurf geschaffen worden in der Frage, was eigentlich eine *Wohnung i. S. des RBStV-E* ist und wie die Inhaberschaft letztlich nachgewiesen werden soll. Der Staatsvertragsentwurf wählt hier in § 3 Absatz 1 Ziffer 1 subjektive Deutungsbegriffe wie „zum Wohnen und Schlafen geeignet“, um eine Wohnung zu beschreiben. Es sind durchaus Orte denkbar, die wohl die o. g. Geeignetheit aufweisen, aber im Allgemeinen nicht als Wohnung bezeichnet werden. Wie soll diese Geeignetheit festgestellt werden? Denkbar sind hier Hausbesuche oder Besichtigungen von Beitragsbeauftragten, die aber rechtlich unzulässig wären.

Die Inhaberschaft einer Wohnung wird vermutet, wenn der Betreffende melderechtlich erfasst ist oder im Mietvertrag genannt wird, so § 2 Absatz 2 RBStV-E. Dass Mietverträge auch in nicht schriftlicher Form existieren oder von Personen abgeschlossen werden, die nur die Mietzahlung übernehmen, bleibt unberücksichtigt. Es stellt sich die Frage, wie in diesem Fall und vor allem durch Offenbarung welcher Daten hier der positive oder auch negative Nachweis der Inhaberschaft einer Wohnung durch den Betroffenen erbracht werden kann. Es sollte daher auf die einschlägigen melderechtlichen Vorschriften Bezug genommen werden; zumindest sollten diese gesetzlichen Begriffsbestimmungen unverändert übernommen werden.

2. Gesamtschuldnerische Haftung von Beitragsschuldnern

Ein Strukturmangel des Entwurfs des 15. Rundfunkänderungsstaatsvertrags in datenschutzrechtlicher Hinsicht ist die Ausweitung der künftigen Rundfunkbeitragsschuld auf alle volljährigen Personen, die in Deutschland mit einem Wohnsitz gemeldet sind bzw. ein Mietverhältnis begründet haben. Anknüpfungspunkt für die Beitragsschuld ist eine gesetzlich angeordnete Fiktion, wonach jede Person als Wohnungsinhaber gilt, die nach dem Melderecht gemeldet oder im Mietvertrag für eine Wohnung als Mieter genannt ist. Der Personenkreis, der nach dem Rundfunkstaatsvertrag künftig als Wohnungsinhaber gilt, haftet den Rundfunkanstalten bzw. den Beitragsgläubigen gemäß § 3 Abs. 2 Satz 1 RBStV-E als Gesamtschuldner.

Aus der Sicht der Beitragsgläubiger stellt die Fiktion der Wohnungsinhaberschaft eine Erleichterung bei der Durchsetzung des Rundfunkbeitrags dar. Denn der Gesamtschuldner schuldet grundsätzlich die gesamte Leistung, d. h. den gesamten Rundfunkbeitrag für die Wohnung, in der er wohnt, und zwar unabhängig davon, ob er selbst Inhaber der Wohnung oder bloßer Mitbewohner ist. Dies bedeutet unter Datenschutzgesichtspunkten eine Ausdehnung des Kreises von möglichen Beitragsschuldnern auf Personen, die, ohne einen eigenen Haushalt zu führen, künftig legitimes Subjekt des Datenerhebungsinteresses der Beitragsgläubiger werden können. Statt eine Lösung zu wählen, die die Rechtspflichten an die tatsächliche Wohnungsinhaberschaft nur eines Haushaltsvorstands knüpft, arbeitet das Regelungskonzept mit einer großen Streubreite, bei der eine kollektive Haftbarmachung der Bevölkerung die Verantwortlichkeit auf die Betroffenen selbst verlagert. Insofern wäre ein grundlegendes Umsteuern des Entwurfs in dem Sinne, dass nur eine Person pro Haushalt Beitragsschuldner ist, mehr als nur wünschenswert. Sonst müsste, besonders bei den Löschungsvorschriften, klarer zwischen Beitragsschuldnern und Beitragszahlern unterschieden werden, damit deutlich wird, dass die Daten aller übrigen in einer Wohnung gemeldeten und im Mietvertrag genannten Personen gelöscht werden, wenn ein Beitragszahler ermittelt wurde.

3. Nachweispflichten

An unterschiedlichen Stellen werden im dem Staatsvertragsentwurf den Beitragsschuldnern für verschiedene Sachverhalte pauschal *Nachweispflichten* auferlegt. So hat ein Beitragsschuldner, der einen Antrag auf Befreiung von der Beitragspflicht stellt, gemäß *§ 4 Absatz 7 RBStV-E* in diesem Antrag nicht nur die weiteren volljährigen Bewohner seiner Wohnung zu benennen, sondern hat dies, gemeint ist wohl deren Existenz und die Tatsache, dass diese auch Bewohner der Wohnung sind, nachzuweisen. Diese Pflicht betrifft jeden Antragsteller, unabhängig davon, ob er die Wohnungsabgabe bezahlen will oder aber nur im Innenverhältnis als Gesamtschuldner einen Nachweis benötigt, dass er nicht zahlen muss. Im Gesetzestext ist zudem nicht erkennbar, in welchem Umfang diese Nachweispflicht besteht. Es stellt sich die Frage, wie weit der Betroffene hier gezwungen ist, im Einzelfall Daten Dritter zu erheben und an die Rundfunkanstalt zu übermitteln, um seiner Nachweispflicht zu genügen? Die Regelung verletzt den Grundsatz der Datenerhebung beim Betroffenen. Sie birgt die konkrete Gefahr in sich, dass persönliche, darunter ggf. auch sensitive Daten Dritter, gegen deren Willen den Rundfunkanstalten offenbart werden.

4. Glaubhaftmachung bei Betriebsstilllegung

In *§ 5 Absatz 5 RBStV-E* wird einem Betriebsstätteninhaber eine Befreiung vom Rundfunkbeitrag gewährt, wenn er glaubhaft macht und auf Verlangen nachweist, dass seine Betriebsstätte für mehr als 3 Monate stillgelegt wird. Auch hier ist nicht erkennbar, welchen Umfang die Nachweispflicht hat. Aufgrund der Unklarheit ist anzunehmen, dass hier im Einzelfall auch gesundheitliche, familiäre oder sonstige private Tatsachen belegt werden müssen. Eine solche erzwungene Offenlegung stellt regelmäßig einen erheblichen Grundrechtseingriff dar. Zwar wird für die Konkretisierung auf die Satzungsermächtigung in § 9 Absatz 2 RBStV-E hingewiesen, dies kann jedoch zur Schaffung von Rechtsklarheit nicht ausreichen. Erhebliche grundrechtsrelevante Eingriffe müssen im Gesetz selbst, also durch die Legislative, geregelt werden. Hier diese Befugnis auf die Exekutive zu delegieren, entspricht nicht den grundgesetzlichen Anforderungen an den Grundsatz des Vorbehalts des Gesetzes.

5. Mitteilung eines Lebenssachverhaltes bei Abmeldung

In *§ 8 Absatz 5 Ziffer 3 RBStV-E* wird von einem Beitragsschuldner, der pflichtgemäß das Ende des Innehabens einer Wohnung oder Betriebsstätte anzeigt (Abmeldung) gefordert, dass er den „die Abmeldung begründenden Sachverhalt“ mitteilt. Für den Abmeldevorgang allein würde die Mitteilung, dass eine Wohnung oder Betriebsstätte verlassen oder aufgegeben wird, ausreichen. Warum sollten die Rundfunkanstalten daran interessiert sein, zu erfahren, aus welchen in seiner Person liegenden Gründen ein Beitragsschuldner die Abmeldung vornimmt? Der Betroffene könnte nach der Formulierung im Staatsvertrag gezwungen werden,

Gesundheits-, Sozial-, Finanz- und/oder Steuerdaten zu offenbaren und ggf. familiäre Verhältnisse offen zu legen. Auch die in § 8 Abs. 5 Nr. 3 a. E. RBStV-E vorgesehene Datenerhebung über Dritte beim (bisherigen) Beitragsschuldner begegnet Bedenken. Personenbezogene Daten sind nach dem Grundsatz der Direkterhebung grundsätzlich beim Betroffenen selbst zu erheben. Ausnahmen hiervon können zwar durch Gesetz angeordnet werden, setzen aber die strikte Beachtung des Verhältnismäßigkeitsgrundsatzes voraus. Inwieweit hier die Datenerhebung bei einem Dritten erforderlich ist, erschließt sich nicht, da nach § 8 Abs. 1 RBStV-E der neue Beitragsschuldner selbst zur Meldung verpflichtet ist und von ihm auch nach § 9 Absatz 1 RBStV-E Auskunft begehrt werden kann.

6. Auskunftsrecht bei Eigentümern und Verwaltern

Nach *§ 9 Abs.1 Satz 4 RBStV-E* soll die zuständige Landesrundfunkanstalt im Einzelfall weitere Daten, die über die Daten nach § 8 Abs. 4 und 5 hinausgehen, bei Eigentümern und Verwaltern erheben dürfen, soweit dies nach Satz 1 erforderlich ist. *Der Begriff „weitere Daten“* ist ein unbestimmter Rechtsbegriff, der im Staatsvertrag schon deswegen zu konkretisieren ist, da nach § 9 Abs. 1 Satz 6 RBStV-E auch insoweit Zwangsbefugnisse eröffnet werden sollen. Für den Auskunftspflichtigen muss klar erkennbar sein, wie weit seine Auskunftspflicht tatsächlich geht. Erforderlich ist in den Fällen, in denen der Beitragsschuldner unbekannt ist, allein die Benennung des Wohnungs- oder Betriebsstätteninhabers und damit eines möglichen Beitragsschuldners. Alle weiteren Angaben haben die Landesrundfunkanstalten dann bei den Betroffenen selbst zu erheben.

7. Löschungsfristen

Der Staatvertragsentwurf geht davon aus, dass nicht benötigte Daten zu löschen sind, dies ist grundsätzlich richtig. Der Entwurf legt hierfür jedoch regelmäßig eine Frist von 12 Monaten fest, so in §§ 11 Absatz 4 Satz 3, Absatz 5 Satz 2 oder § 14 Abs. 9 Satz 5 RBStV-E. Das Erheben, Speichern oder das anderweitige Verarbeiten von personenbezogenen Daten, die für die Aufgabenerfüllung nicht benötigt werden, ist durch öffentliche Stellen grundsätzlich unzulässig. Nicht erforderliche Daten sind daher unverzüglich oder innerhalb einer kurz zu bemessenden Frist zu löschen. Dies bedarf der Klarstellung.

Einige der hier angesprochen Probleme sollen nach Äußerungen der Rundfunkreferenten der Länder im Rahmen einer Begründung zum Staatsvertragsentwurf ausgeräumt werden. Diese Begründung liegt derzeit nicht vor, sodass Ausführungen hierzu nicht gemacht werden können. Es ist aber bereits jetzt anzumerken, dass strukturelle Unklarheiten einer Rechtsnorm nicht durch eine noch so kreative Begründungsformulierung beseitigt werden können. Auch ist eine Gesetzesbegründung nicht in der Lage, die fehlende Bestimmtheit von Ermächtigungen und Pflichten im Gesetzeswortlaut auszugleichen. Zudem erscheint es untunlich, zuerst den Staatsvertrag durch die Landesregierungen unterzeichnen zu lassen und einigen Regelungen erst danach eine inhaltliche Bedeutung zu geben.

Auch der schon geäußerte Gedanke, die Rechtsprechung könne unklare Begrifflichkeiten mit weiteren Konturen versehen, geht fehl. Zwar ist die Rechtsprechung grundsätzlich berufen, unbestimmte Rechtsbegriffe auszufüllen. Es kann jedoch nicht ihre Aufgabe sein, unklare und missverständliche Begriffe erstmals in etwaigen Prozessen überhaupt verständlich zu machen.

Anhang 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Erweiterung der zentralen Steuerdatenbank um elektronische Lohnsteuerabzugsmerkmale (ELStAM) vom 24. Juni 2010

Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

– Vorherige Information der Arbeitnehmer

  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

– Keine Speicherung auf Vorrat

  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

– Verhindern des unzulässigen Datenabrufs

  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

– Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept

  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

Anhang 10

Entschließung
der 80. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. November 2010

Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den

technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

Anhang 11

Entschließung
der 80. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. November 2010

Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

Anhang 12

Entschließung
der 80. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 3./4. November 2010

Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Anhang 13

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[14] – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und -Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

[14] Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

Anhang 14

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis
  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.

- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere
  - zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.

  - für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.

– Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.

– In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

  - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,
  - zur privaten Nutzung von Telekommunikationsdiensten,
  - zum Thema Whistleblowing,
  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

Anhang 15

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe *http://www.kbv.de/rechtsquellen/24631.html).*

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.
3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.
6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.
7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) – eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

– mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie

– die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Anhang 16

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

Anhang 17

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

Anhang 18

Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2009 auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck hat eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die genannten Arbeitskreise haben die Orientierungshilfe verabschiedet.

Sie konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Für die Datenschutzbehörden wird das vorliegende Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise sind aufgefordert, diesen Revisionsprozess zu koordinieren und das Ergebnis spätestens im Frühjahr 2012 der Konferenz vorzulegen.

Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.

Anhang 19

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011

Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100 g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100 a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

Anhang 20

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

Anhang 21

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und
5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

Anhang 22

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,
- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[15] der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

[15] http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Anhang 23

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zurzeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzende sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.
- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.
- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.
- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.
- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.
- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).

- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.
- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.
- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, sodass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

Anhang 24

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir"-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen.

Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

Anhang 25

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

Anhang 26

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedsstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

Anhang 27

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 13. Juli 2009

Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sog. eBorders-Projekts die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedsstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedsstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge erfolgt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4 a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt.

Die Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt. Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

Anhang 28

**Beschluss der obersten Aufsichtsbehörden
für den Datenschutz im nicht-öffentlichen Bereich
am 26./27. November 2009 in Stralsund**

Gesetzesänderung bei der Datenverwendung für Werbezwecke

Vom 1. September 2009 an gelten nach § 28 Abs. 3 BDSG neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

Anhang 29

Beschluss
der obersten Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
am 26./27. November 2009 in Stralsund

Datenschutzkonforme Ausgestaltung von Analyseverfahren
zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.
- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

Anhang 30

**Beschluss der obersten Aufsichtsbehörden
für den Datenschutz im nicht-öffentlichen Bereich
am 26./27. November 2009 in Stralsund**

Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofils genutzt werden kann.

Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“, publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

Anhang 31

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. Oktober 2009

Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.

2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:
   - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;
   - sonstige Daten über negatives Zahlungsverhalten, bei denen
     - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder – sofern sie sich zwischenzeitlich erledigt hat – die Erledigung nicht länger als ein Jahr zurückliegt und
     - eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2. erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

Hintergrund:

Nach § 29 Absatz 2 Nr. 1a Bundesdatenschutzgesetz ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder -unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressen-

ten erteilen dürfen. Vorzuziehen – so der damalige Beschluss – seien branchenspezifische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber sogenannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28 a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer 2 genannten Katalog hinausgehen.

Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

Anhang 32

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23. August 2010)

Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor)[16]. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsministerium veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Habor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[17] gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

[16] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25. August 2000, S. 7.

[17] Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

Anhang 33

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 24./25. November 2010

Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

Anhang 34

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 24./25. November 2010

Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.
- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.
- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von lnternetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.
- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzern sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

Anhang 35

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 24./25. November 2010

Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4 f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4 f Abs. 2 Satz 1 BDSG

§ 4 f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle
   - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und
   - umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,
   - Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten
   - Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
   - Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
   - betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
   - Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und
   - Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement,

Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse *bereits zum Zeitpunkt des Bestellung* zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4 f Abs. 3 BDSG

Gemäß § 4 f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4 f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne lnteressenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.
2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4 f Abs. 3 Satz 3 ff. BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4 f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 – 2 Jahren empfohlen.
3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4 f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4 g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.
2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4 g Abs. 2 BDSG) und haben hierfür die erforderlichen Unterlagen zu erhalten.
3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.
4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet

sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.

5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4 f Abs. 5 BDSG).

Anhang 36

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 24./25. November 2010

Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.

Anhang 37

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. April 2011

Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotenzial für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.
- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.
- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

Anhang 38

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 4./5. Mai 2011

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe *http://www.kbv.de/rechtsquellen/24631.html).*

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten. An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.
3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.
6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.
7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b) – eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,

– mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie

– die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

Anhang 39

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 4./5. Mai 2011

Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die Aufsichtsbehörden im nicht-öffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nicht-öffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

Anhang 40

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 4./5. Mai 2011

Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche" Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps"), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche".

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

– Transparenz bezüglich der Preisgabe personenbezogener Daten:

  In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

– Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:

  Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z. B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

– Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:

  Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

– Anonyme und pseudonyme Nutzungsmöglichkeiten:

  Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitä-

ten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design v. 29. Oktober 2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones;
http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risksopportunities-and-recommendations-for-users/at_download/fullReport).

Anhang 41

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22.23. November 2011

Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener „White Cards“ erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. „Micropayment“) zu erhalten.[18]

[18] vgl. Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: „Anonymes elektronisches Bezahlen muss möglich bleiben!“

Anhang 42

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22./23. November 2011

Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24. April 2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten“ (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt.

Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 3. Dezember 2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25 c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.
- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.
- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

Anhang 43

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. Dezember 2011

Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38 a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.
- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.
- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.
- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.
- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.

- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.
- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.
- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

Anhang 44

**Stellungnahme
des Landesbeauftragten für den Datenschutz
„Fertigung von Luftbildaufnahmen zur Ermittlung von
kommunalen Abwassergebühren“**

Im Zusammenhang mit der Einführung der gesplitteten Abwassergebühr erwerben zahlreiche Gemeinden beim Landesamt für Geoinformation und Landentwicklung (LGL) Luftaufnahmen bzw. hieraus hergestellte Orthophotos (Bodenauflösung 10 cm) zur Ermittlung von versiegelten Grundstücksflächen. Andere Gemeinden haben private Unternehmen beauftragt, entsprechende Aufnahmen herzustellen. Nach unserer Kenntnis variiert die Bodenauflösung bei den verschiedenen privaten Anbietern; neben einer Bodenauflösung von 10 cm scheint es auch Aufnahmen mit einer Bodenauflösung von z. B. 5 cm zu geben.

Die nachfolgenden Ausführungen beziehen sich auf die Datenerhebung durch die Gemeinden beim LGL (also bei Dritten) bzw. die Datenerhebung durch von den Gemeinden beauftragte Firmen (Datenverarbeitung im Auftrag, § 7 LDSG).

1. Verarbeitung personenbezogener Daten

   Nach § 3 Absatz 1 LDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Luftbildaufnahmen bzw. die hieraus hergestellten Orthophotos mit einer Auflösung von 5, 10, 20 oder 25 Zentimetern stellen Angaben über die sachlichen Verhältnisse der Bewohner oder Eigentümer der abgebildeten Grundstücke/Gebäude dar. Es handelt sich damit um personenbezogene oder zumindest personenbeziehbare Daten. Gemäß § 4 Absatz 1 LDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.

Einschlägige Regelungen

1.1 Sinngemäße Anwendung der Abgabenordnung (AO) nach § 3 des Kommunalabgabengesetzes (KAG)

   Das Beschaffen der Luftbildaufnahmen/Orthophotos dient zunächst der Ermittlung der Grundlagen für die Gebührenkalkulation einer zu erlassenden Abwassersatzung und erst im Nachgang der eigentlichen Gebührenerhebung beim Gebührenschuldner.

   Es stellt sich daher die Frage, ob sich der Verweis in § 3 Absatz 1 KAG auf die dort genannten Bestimmungen der Abgabenordnung auch auf die zur Ermittlung der Grundlagen der Gebührenkalkulation durchgeführten Datenerhebungen bezieht. Dies ist zu bejahen.

   Da § 3 Absatz 1 KAG die Vorschriften der Abgabenordnung für sinngemäß auf Kommunalabgaben anwendbar erklärt und nicht nur die Gebührenberechnung bzw. Erhebung beim Gebührenschuldner nennt, ist nach dem Wortlaut der Vorschrift die Anwendung des § 3 Absatz 1 KAG auf die Ermittlung der Grundlagen für die Gebührenkalkulation möglich.

   Auch der Gemeindetag scheint § 3 Absatz 1 KAG in diesem Sinne aufzufassen. So wird in einem Beitrag – Zeitschrift des Gemeindetags Baden-Württemberg (BWGZ 21/2001, Seite 832) – auch bezüglich der zur Kalkulation des Gebührensatzes benötigten Daten auf die Abgabenordnung verwiesen.

   Schließlich hebt auch das Verwaltungsgericht Freiburg in einem Urteil vom 10. Dezember 2003, Az. 7 K 427/02, für die Ermittlung der Bemessungsgrundlagen zur Kalkulation des Gebührensatzes einer zu erlassenden Abwassersatzung auf § 3 KAG in Verbindung mit § 90 AO ab (in diesem Fall ging es unter anderem um die Mitwirkungspflicht eines Bürgers nach § 90 AO bei einer Fragebogenaktion der Gemeinde zur Erhebung der versiegelten Flächen als Kalkulationsgrundlage für die Satzung).

1.2 Beweismittelregelungen der Abgabenordnung als lex specialis, § 92 AO in Verbindung mit den §§ 93 ff. AO

Für den Erwerb der Luftbilder bzw. Orthophotos durch die Gemeinden beim LGL und die Herstellung von Luftbildaufnahmen bzw. Orthophotos durch Firmen im Auftrag der Gemeinden zum Zwecke der Kalkulation des Gebührensatzes, also zur Vorbereitung der Abwassersatzung, finden daher über § 3 Absatz 1 Nr. 3 a KAG die §§ 92 ff. AO Anwendung. In § 92 AO in Verbindung mit den §§ 93 ff. AO finden sich die Rechtsgrundlagen für die Anforderung von Beweismitteln zur Ermittlung des Sachverhalts. Es handelt sich damit um Vorschriften zur Datenerhebung. § 92 AO in Verbindung mit den §§ 93 ff. AO stellen Spezialregelungen zu den in § 13 LDSG enthaltenen Regelungen über die Erhebung personenbezogener Daten dar, die nach § 2 Absatz 5 Satz 1 LDSG den Regelungen des Landesdatenschutzgesetzes zur Datenerhebung vorgehen; diese finden daher auf die vorliegenden Fallkonstellationen keine Anwendung.

2. Zulässigkeit der Datenerhebung

2.1 Datenerhebung durch Auskunftseinholung beim Betroffenen (§ 93 Absatz 1 AO) als Grundsatz der Abgabenordnung

Das in § 92 AO genannte Auswahlermessen bei der Wahl der Erhebungsmethoden wird durch die §§ 93 ff. AO hinsichtlich Reihenfolge und Form erheblich eingeschränkt. In der Kommentierung von Tipke/Kruse zur Abgabenordnung ist folgende Beweismittel-Reihenfolge genannt: § 93 Absatz 1 Satz 3 AO, § 95 Absatz 1 Satz 2 AO, § 97 Absatz 2 AO (Tipke/Kruse, AO, Stand: Mai 2000, § 92 Rdnr. 12). Nur soweit Ermittlungsmaßnahmen nicht in Rechte der Beteiligten oder anderer Personen eingreifen (die von den Gemeinden vorgenommenen Erhebungen stellen Eingriffe in das informationelle Selbstbestimmungsrecht dar), bedarf es über die §§ 85, 88 AO hinaus keiner besonderen Rechtsgrundlage (Tipke/Kruse § 88 Rdnr. 9).

Aus § 3 Absatz 1 Nr. 3 KAG in Verbindung mit den genannten Vorschriften der Abgabenordnung ergibt sich somit, dass es nicht im Ermessen der Gemeinden steht, welche Erhebungsmethoden sie zur Ermittlung der versiegelten Grundstücksflächen wählen. Vielmehr ist gemäß § 3 Absatz 1 Nr. 3 a KAG in Verbindung mit § 93 Absatz 1 Sätze 1 und 3 AO zunächst vom Grundsatz der Auskunftseinholung (Datenerhebung) beim Betroffenen auszugehen.

2.2 Zulässigkeit der Datenerhebungen nach § 3 Absatz 1 Nr. 3a KAG in Verbindung mit § 93 Absatz 1 AO

Gemäß § 3 Absatz 1 Nr. 3a KAG in Verbindung mit § 93 Absatz 1 Sätze 1 und 3 AO sind Daten, die zur Feststellung eines für die Besteuerung (bzw. im vorliegenden Fall für die Heranziehung von Abgaben) erheblichen Sachverhalts erforderlich sind, grundsätzlich durch Auskunft des Beteiligten zu erheben. Andere Personen, hierunter fallen auch Behörden (§ 93 Absatz 1 Satz 2 AO), sollen dagegen erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht.

Die Ermittlung der versiegelten Grundstücksflächen ist zweifellos erforderlich, um eine den Anforderungen des § 2 Absatz 1 KAG entsprechende Satzung für eine Niederschlagsabwassergebühr erlassen zu können. Angesichts

- der Ausführungen des Verwaltungsgerichtshofs Baden-Württemberg in seinem Urteil vom 4. März 2010, Az. 2 S 2938/08, zum Abwassersplitting, in dem dargelegt ist, dass für die Gemeinden die Möglichkeit der Selbstveranlagung der Gebührenschuldner und eine stichprobenweise Überprüfung durch die Gemeinde besteht,
- der Ausführungen des Verwaltungsgerichts Freiburg in seinem Urteil vom 10. Dezember 2003, Az. 7 K 420/02, dass die für die Gebührenkalkulation erforderliche Ermittlung der versiegelten Grundstücksflächen mittels Erhebung dieser Flächen bei den Betroffenen über eine Fragebogenaktion möglich ist,
- der Antwort des Innenministeriums vom 13. April 2010 auf den Antrag der Abgeordneten Dr. Gisela Splett u. a. GRÜNE zur Einführung der gesplitte-

ten Abwassergebühr (LT-Drucksache 14/6077) zu 7., dass die Selbstveranlagung der Grundstückseigentümer auf der Grundlage von Fragebögen eine Möglichkeit zur Erfassung der versiegelten Flächen sei und

– der Tatsache, dass viele Gemeinden und Städte (darunter auch große Städte wie Düsseldorf und – nach Auskunft des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein – sämtliche Gemeinden in Schleswig-Holstein) ausschließlich die Selbstveranlagung der Gebührenschuldner durchgeführt haben bzw. in ihren Satzungen vorsehen,

ist diese Vorgehensweise, die versiegelten Grundstücksflächen durch Auskunft der Beteiligten zu erheben, unseres Erachtens auch geeignet, verhältnismäßig und zumutbar.

Bereits aus den vorstehenden Ausführungen ergibt sich, dass die in § 93 Absatz 1 Satz 3 Variante 1 AO genannte Ausnahme vom Grundsatz der Auskunftseinholung beim Betroffenen (die Sachaufklärung beim Beteiligten verspricht keinen Erfolg) bei den hier zu beurteilenden Fallkonstellationen nicht angenommen werden kann. Auch die Ausnahme, dass die Sachaufklärung beim Beteiligten nicht zum Ziel geführt hat, ist nicht einschlägig, da diese eine vorausgegangene Befragung der Beteiligten voraussetzt.

§ 93 Absatz 1 Satz 3 AO ist zwar keine Muss-Vorschrift, aber auch keine bloße Kann-Vorschrift. Das „sollen“ bedeutet, dass die Finanzbehörde bzw. die Gemeinde in der Regel nach § 93 Absatz 1 Satz 3 AO verfahren muss – also Befragungen der Beteiligten durchzuführen hat – und nur in atypischen Fällen hiervon abweichen darf (Tipke/Kruse § 93 Rdnr. 18).

Ob ein atypischer Sonderfall vorliegt, ist am Zweck der Vorschrift zu messen.

Das in § 93 Absatz 1 Satz 3 AO enthaltene Subsidiaritätsprinzip ist unter anderem Ausfluss des informationellen Selbstbestimmungsrechts, das vom Grundsatz der Direkterhebung beim Betroffenen ausgeht, um ihm so die Mitwirkung bei der Datenbeschaffung zu ermöglichen.

Die vom Innenministerium genannte Eilbedürftigkeit stellt angesichts des Zwecks des Subsidiaritätsprinzips keinen atypischen Sonderfall dar. Auch Tipke/Kruse (§ 93 Rdnr. 19) führen aus, dass allein zur Beschleunigung der Sachaufklärung vom Grundsatz der Direkterhebung beim Betroffenen nicht abgegangen werden kann.

Für den Fall, dass die Befragung des Betroffenen keine vollständigen Informationen ergibt, sehen die §§ 93 ff. AO weitere Ermittlungsmaßnahmen vor. Dies zeigt, dass der Gesetzgeber die Konstellation, dass sich eine Befragung als nicht ausreichend erweist, bereits berücksichtigt hat, diese Konstellation also keinen Sonderfall darstellt. Die Ausführungen des Innenministeriums, ohne die beigefügten Luftbilder seien nicht alle Betroffenen in der Lage, vollständige Angaben zu machen, sind daher nicht geeignet, einen atypischen Sonderfall i. S. d. § 93 Absatz 1 Satz 3 AO zu begründen.

Da das Subsidiaritätsprinzip auch Ausdruck des Verhältnismäßigkeitsgrundsatzes ist, kann die Tatsache, dass die Befliegungen und die dadurch gewonnenen Luftbildaufnahmen und Orthophotos nicht geeignet sind, die rechtlich vorrangige Befragung der Gebührenschuldner zu ersetzen, sondern diese lediglich vorbereitet, ebenfalls nicht zur Begründung eines atypischen Sonderfalls herangezogen werden.

Vor Befragung der Betroffenen Datenerhebungen durch den Erwerb von Luftbildaufnahmen bzw. Orthophotos beim LGL vorzunehmen bzw. solche Aufnahmen durch beauftragte private Unternehmen herstellen zu lassen, um zu verhindern, dass einige Bürger bewusst oder unbewusst falsche Angaben machen, erscheint außerdem unverhältnismäßig.

Zusammenfassend ist festzustellen, dass die Datenerhebung durch Erwerb der Luftbildaufnahmen bzw. Orthophotos beim LGL (also bei Dritten) mangels Vorliegen eines atypischen Sonderfalls nicht auf § 3 Absatz 1 Nr. 3 a KAG in Verbindung mit den §§ 92, 93 Absatz 1 Sätze 1 und 3 AO gestützt werden kann.

Auch für die Datenerhebung der Gemeinden durch Beauftragung privater Unternehmen zur Herstellung von Luftbildaufnahmen bzw. Orthophotos (Auftragsda-

tenverarbeitung im Sinne des § 7 LDSG) ist keine Rechtsgrundlage ersichtlich, die eine Abweichung von dem in § 93 Absatz 1 Sätze 1 und 3 AO enthaltenen Grundsatz der Befragung der Beteiligten zulassen würde.

Mangels Rechtsgrundlage ist im Rahmen der Einführung der gesplitteten Abwassergebühr damit sowohl der Erwerb von Luftbildern bzw. Orthophotos beim LGL durch die Gemeinden als auch die Beauftragung privater Unternehmen durch die Gemeinden, entsprechende Aufnahmen herzustellen, aus datenschutzrechtlicher Sicht derzeit nicht zulässig.

3. Anwendbarkeit des § 13 LDSG

Das Innenministerium hat die Anwendbarkeit des § 93 AO auf die vorliegende Fragestellung in Zweifel gezogen, weshalb nachfolgend hilfsweise die Anwendbarkeit des § 13 LDSG geprüft wird.

Die vorstehenden Ausführungen zum Vorrang der Datenerhebung beim Betroffenen durch Befragung in § 93 Absatz 1 Sätze 1 und 3 AO entsprechen dem in § 13 Absatz 2 LDSG enthaltenen Grundsatz der Datenerhebung beim Betroffenen mit seiner Kenntnis.

Werden personenbezogene Daten ohne Beteiligung des Betroffenen erhoben, liegt eine Erhebung nach § 13 Absatz 2 LDSG auch dann nicht vor, wenn der Betroffene von der Datenerhebung Kenntnis hat (Bergmann/Möhrle/Herb, Datenschutzrecht, Bd. 2, § 13 Anm. 5.4).

Für die Fallkonstellation der Beauftragung einer privaten Firma durch die Gemeinde (Datenverarbeitung im Auftrag gemäß § 7 LDSG; bei dieser Konstellation bleibt die Gemeinde verantwortliche Stelle) wäre – bei Anwendbarkeit des Landesdatenschutzgesetzes – daher § 13 Absatz 3 LDSG zu prüfen:

Nach § 13 Absatz 3 LDSG dürfen personenbezogene Daten beim Betroffenen ohne seine Kenntnis nur erhoben werden, wenn entweder eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt (Nr. 1) oder die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen (Nr. 2).

Dass keine der in § 13 Absatz 3 Nr. 1 LDSG genannten Varianten vorliegt, ergibt sich aus den vorstehenden Ausführungen zur Abgabenordnung. (Auch dass die Erhebung darauf gerichtet ist, eine Satzung zu erlassen, entspricht nicht den Anforderungen der Vorschrift).

Auch die Voraussetzungen des § 13 Absatz 3 Nr. 2 LDSG wären – bei Anwendbarkeit des Landesdatenschutzgesetzes – nicht erfüllt. Die Nr. 2 betrifft Fälle, bei denen die Erhebung mit Kenntnis des Betroffenen entweder überhaupt nicht oder nur unter Gefährdung der Aufgabenerfüllung möglich ist.

Für die Fallkonstellation, dass die Gemeinde beim LGL Luftbildaufnahmen bzw. Orthophotos erwirbt (nach Auskunft des bisherigen Ministeriums für Ländlichen Raum, Ernährung und Verbraucherschutz liegt hier keine Auftragsdatenverarbeitung im Sinne des § 7 LDSG vor), also eine Datenerhebung durch die Gemeinde bei Dritten erfolgt, wäre – bei Anwendbarkeit des Landesdatenschutzgesetzes – § 13 Absatz 4 LDSG zu prüfen:

Nach dieser Vorschrift dürfen personenbezogene Daten bei Dritten nur erhoben werden, wenn einer der in § 15 Absatz 2 Nr. 1 bis 6 LDSG genannten Fälle vorliegt (Nr. 1) oder die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen (Nr. 2).

Keine dieser Varianten wäre bei der genannten Konstellation einschlägig. Bezüglich § 15 Absatz 2 Nr. 1 LDSG kann auf die Ausführungen zu § 13 Absatz 3 Nr. 1 LDSG verwiesen werden. Die Nummern 2 bis 5 in § 15 Absatz 2 LDSG passen offensichtlich nicht auf die zu prüfenden Sachverhalte. Bezüglich § 15 Absatz 2 Nr. 6 LDSG (wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde …) wird auf die vorstehenden Ausführungen der unter 3.2 genannten Urteile des Verwaltungsgerichtshofs Baden-Württemberg und des Verwaltungsgerichts Freiburg verwiesen, in denen die Befragung der Betroffenen als geeignetes Mittel zur Erhebung der

versiegelten Grundstücksflächen genannt ist. Darüber hinaus „erspart“ die Erhebung von Luftaufnahmen die Befragung der Betroffenen nicht. Bezüglich § 13 Absatz 4 Nr. 2 LDSG kann auf die Ausführungen zu § 13 Absatz 3 Nr. 2 LDSG verwiesen werden.

Auch die wegen § 2 Absatz 5 Satz 1 LDSG ausgeschlossene Anwendung des § 13 LDSG auf die vorliegenden Konstellationen würde somit nicht zu einem anderen Ergebnis führen als die Anwendung des § 3 Absatz 1 KAG in Verbindung mit den §§ 92 ff. AO.

4. Sonstiges

Im Übrigen ist darauf hinzuweisen, dass eine Datenverarbeitung im Auftrag nach § 7 LDSG im Zusammenhang mit Kommunalabgaben nur in dem in § 2 Absatz 3 KAG genannten engen Umfang zulässig ist.

Schließlich weisen wir auf die Vorschrift des § 30 AO (Steuergeheimnis) und die in dieser Vorschrift genannten Offenbarungsbefugnisse (Absatz 4) hin, die nach Maßgabe des § 3 Absatz 1 Nr. 1 c KAG auf Kommunalabgaben sinngemäß Anwendung finden und gegebenenfalls die Nutzung von Daten zulassen, die im Rahmen der Erhebung anderer Kommunalabgaben bei der Gemeinde bereits angefallen sind.