Landtag von Baden-Württemberg **Drucksache 15 / 4600**

15. Wahlperiode **17. 01. 2014**

Mitteilung

des Landesbeauftragten für den Datenschutz

31. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2012/2013

Schreiben des Landesbeauftragten für den Datenschutz Baden-Württemberg vom 17. Januar 2014:

Anbei übersende ich Ihnen unseren 31. Tätigkeitsbericht, der mit Zustimmung des Ständigen Ausschusses vom 25. April 2013 abweichend von § 31 Absatz 2 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg erst jetzt vorgelegt wird, um die Entwicklung des Datenschutzes im gesamten Berichtszeitraum darstellen zu können.

Klingbeil

Eingegangen: 17. 01. 2014 / Ausgegeben: 05. 02. 2014

31. Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz
Baden-Württemberg
2012/2013

Inhaltsverzeichnis

Vorwort **7**

1. Zur Situation **9**

1.1 O Tempora, o mores - ist die Privatsphäre angesichts des Spähskandals der Geheimdienste noch zu retten? 9

1.2 Big Data - eine Daten-Goldgrube für Wirtschaft und Sicherheitsbehörden 15

1.3 Europäischer und internationaler Datenschutz 18

1.3.1 Die EU-Datenschutz-Grundverordnung - eine schwere Geburt 18

1.3.2 Die Europäische Datenschutzrichtlinie für Polizei und Justiz 21

1.3.3 Elektronische Identifizierung mit datenschutzrechtlichen Defiziten 22

1.3.4 Flugpassagierdaten für die USA - jetzt auch für andere Staaten? 23

1.3.5 Was hat die Bekämpfung von Produkt- und Markenpiraterie mit dem Datenschutz zu tun? Das ACTA-Abkommen 24

1.3.6 FATCA - Die Neugier des großen Bruders ist unerschöpflich 25

1.3.7 Internationaler Datentransfer: Safe Harbor in stürmischen Zeiten 26

1.4 Datenschutz auf Bundesebene 28

1.4.1 Die Weiterentwicklung des Bundesdatenschutzgesetzes (BDSG): Still ruht der See - auch im Bereich des Beschäftigtendatenschutzes 28

1.4.2 Das E-Government-Gesetz des Bundes 30

1.4.3 Die Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestags 32

1.4.4 Die Bundesstiftung Datenschutz nimmt ihre Arbeit auf - ohne die Datenschützer 33

1.4.5 Die freiwillige Selbstregulierung bei sozialen Netzwerken - eine Blamage für die Bundespolitik 34

1.4.6 Aussichten für den Datenschutz in der 18. Legislaturperiode des Deutschen Bundestags - Erwartungen an die Politik 35

1.5 Aus der Dienststelle 37

2. Innere Sicherheit **40**

2.1 Notwendige, freiwillige und unterlassene Änderungen des Polizeirechts 40

2.1.1. Gesetz zur Änderung des Polizeigesetzes und des Gesetzes zur Ausführung des Personenstandsgesetzes vom 20. November 2012 (LT-Drs. 15/2675) 40

2.1.2 Änderungen durch das Gesetz zur Umsetzung der Polizeistrukturreform vom 23. Juli 2013 (LT-Drs. 15/2675) 42
2.1.3 Geplante Änderungen im Polizeigesetz und im Landesverfassungsschutzgesetz 42
2.1.4 Der Sinneswandel im Polizeirecht 44
2.2 Datenverarbeitung durch Sicherheits- und Ordnungsbehörden 46
2.2.1 Der Polizeivollzugsdienst und seine Dateien 46
2.2.2 Was der Tatort nicht zeigt - die Mitarbeiterdatenbank der Polizei 48
2.2.3 Drohen Drohnen? Überlegungen zur polizeilichen Videoüberwachung aus der Luft 50
2.2.4 Zuverlässigkeitsprüfungen in allen Varianten 51
2.2.5 Das Nationale Waffenregister 57
2.3 Die Polizeistrukturreform - auch eine Herausforderung für den Datenschutz 57
2.3.1 Das Interessenbekundungsverfahren (IBV) - der Datenschutz zwischen Organisations- und Personalinteressen 58
2.3.2 Profitiert der Datenschutz von der Strukturreform? 60
2.4 Der Verfassungsschutz in schwerer See 61
2.4.1 Verfassungswidrige Zustände im Verfassungsschutzrecht noch immer nicht behoben 61
2.4.2 Terrorismusabwehr im Spannungsfeld von kollektivem Sicherheitsdenken und individuellen Freiheitsrechten 62
2.4.3 Die Neustrukturierung des nachrichtendienstlichen Informationssystems NADIS 65
2.4.4 Auskunft nach dem Landesverfassungsschutzgesetz 66

3. Justiz 68

3.1 Europäische Ermittlungsanordnung 68
3.2 Schuldnerverzeichnis im Internet 68
3.3 Quellen-Telekommunikationsüberwachung im Ermittlungsverfahren - Kontrollbesuch bei einer Staatsanwaltschaft 69
3.4 Teilprivatisierung im Justizvollzug 71
3.5 Adressangaben von Zeugen in der Anklageschrift 72

4. Steuern und Statistik 74

4.1 Die Elektronischen LohnSteuerAbzugsMerkmale (ELStAM) 74
4.2 Zensus und Haushaltsstatistiken 74
4.3 Zentrale Informations- und Annahmestellen bei Finanzämtern 75

5. Kommunales **77**

5.1 Kontrolle und Beratung - beides ist wichtig 77

5.2 Gespräche mit den Kommunalen Landesverbänden und kommunalen Praktikern über Veröffentlichungen durch Kommunen 78

5.3 Die Bettensteuer und der Datenschutz 79

5.4 Die Neuregelung des Bundesmeldegesetzes - kaum verabschiedet, schon wieder repariert 81

6. Verkehr **84**

6.1 Das intelligente Auto und der Datenschutz 84

6.2 Kontrollbesuch bei der Zentralen Bußgeldstelle des Regierungspräsidiums Karlsruhe - das Verfahren OWi 21 86

6.3 Datenschutz auf der Autobahn - die temporäre Seitenstreifenfreigabe auf der A 8 88

6.4 Die intelligente Straße wird noch intelligenter - das Projekt BLIDS auf der B 27 90

7. Gesundheit und Soziales **92**

7.1 Das Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten 92

7.2 Das Krebsfrüherkennungs- und registergesetz des Bundes - was wird aus dem Krebsregister Baden-Württemberg? 94

7.2.1 Das Krebsfrüherkennungs- und -registergesetz (KFRG) 94

7.2.2 Das Landeskrebsregister heute 95

7.2.3 Was passiert mit dem bestehenden Krebsregister? 95

7.3 Die Pseudonymisierung von Krebsregisterdaten 96

7.4 Orientierungshilfe Krankenhausinformationssysteme (OH KIS) 97

7.4.1 Fortschreibung der OH KIS 97

7.4.2 Handreichung der Deutschen Krankenhausgesellschaft (DKG) 98

7.4.3 Umsetzung der Orientierungshilfe auf Landesebene 98

7.4.4 Umsetzung an einem Referenzkrankenhaus 99

7.5 Datenschutz im Krankenhaus 100

7.5.1 Der Verlust von Patientendaten 100

7.5.2 Die Entsorgung von Patientenakten durch einen externen Dienstleister 101

7.6 Babygalerien 104

7.7 Datenschutz in Pflegestützpunkten und Pflegeeinrichtungen 104

7.7.1 Kontrollbesuch bei einem Pflegestützpunkt 104

7.7.2 Kontrollbesuche bei Pflegeeinrichtungen 106

7.8 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft 107

7.9 Verrechnungsstellen und Forderungen für ärztliche Privatpatienten-Leistungen 108
7.10 Wann müssen Arztpraxen einen betrieblichen Datenschutzbeauftragten bestellen? 108
7.11 Clearingstelle für Apotheken 109
7.12 ELENAs Nachkommen 110
7.13 Datenschutz im Jobcenter 111
7.14 Benötigt das Sozialamt MDK-Gutachten? 113

8. Datenschutz in Kindertageseinrichtungen und Schulen 115

8.1 Datenschutz in Kindertageseinrichtungen 115
8.1.1 Broschüre zum Datenschutz in Kindertageseinrichtungen 115
8.1.2 Der Rechtsanspruch auf einen Platz in einer Kindertageseinrichtung und der Datenschutz 115
8.2 Datenschutz an Schulen 116
8.2.1 Datenschutzrechtliche Zusammenarbeit mit ausgewählten Schulen 117
8.2.2 Verfahrensverzeichnis 117
8.2.3 Schulverwaltungsprogramm 117
8.2.4 Datenverarbeitung im Auftrag 118
8.2.5 Umgang mit Fehlzeiten 118
8.2.6 Datenweitergabe bei Umzug 119
8.2.7 Soziale Netzwerke im Schulbetrieb 119
8.2.8 Einführung einer landeseinheitlichen Bildungsnummer 121
8.2.9 Lehreraus- und -fortbildung 122
8.3 Datenschutz als Unterrichtsthema 123
8.3.1 Datenschutz macht Schule 123
8.3.2 Medienkompetenz macht Bildung 124
8.3.3 Die Bildungsplanreform 2015 und der Datenschutz 125

9. Datenschutz in der Arbeitswelt 126

9.1 Die Feststellung der Alkoholisierung von Beschäftigten am Arbeitsplatz 126
9.2 Die Einholung von Auskünften über Arbeitnehmer und Bewerber durch Arbeitgeber bei anderen Arbeitgebern (sog. Arbeitgeberauskunft) 126
9.3 Datenschutzrechtliche Fragen bei Personalakten 127

10. Datenschutz in der Wirtschaft 129

10.1 Kündigung des betrieblichen Datenschutzbeauftragten im Insolvenzverfahren? 129

10.2 Datenschutzkonformes „Double-Opt-in“ bei Werbung per E-Mail 131

10.3 Rechtliche Anforderungen an eine gesetzeskonforme Datenschutzerklärung für Internetseiten 132

10.3.1 Verpflichtende Bestandteile 135

10.3.2 Freiwillige, aber ratsame Bestandteile 137

10.4 Nicht alles ist Spam: Datenschutzkonforme elektronische Werbung aufgrund des Privilegs nach § 7 Absatz 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) 138

10.5 Datenschutz und digitales Wasserzeichen bei erworbenen und heruntergeladenen Musikdateien 140

10.5.1 Verfolgung über die IP-Adresse am Ende der Kette 141

10.5.2 Verfolgung über das digitale Wasserzeichen am Anfang der Kette 141

10.6 Geldwäscheprävention und Beschäftigtendatenschutz 143

10.7 Der übereifrige Hausverwalter 143

10.8 Die verweigerte Selbstauskunft 145

10.9 Datenübermittlungen an Auskunfteien bei Anfragen nach Kreditkonditionen 145

10.10 Bei Anruf Bonitätsbeichte 146

10.11 Auskunft unter Vorbehalt 147

10.12 Das Register nach §§ 38 Absatz 2, 4d, 4e BDSG - wer muss was an die Aufsichtsbehörde melden? 148

11. Technik und Medien 150

11.1 Videoüberwachung 150

11.1.1 Einleitung 150

11.1.2 Videoüberwachung in und an Taxis 150

11.1.3 Videoüberwachung in Arztpraxen 151

11.1.4 Zulässigkeit von Wildkameras 152

11.1.5 Videoüberwachung an Schulen nach § 20a LDSG 153

11.2 Soziale Netzwerke 154

11.2.1 Facebook und der Datenschutz 154

11.2.2 Mitwirkung an Vorgaben für die Landesverwaltung 158

11.2.3 Die Verwendung des Facebook-Like-Buttons durch öffentliche Stellen in Baden-Württemberg 159

11.3 Neue Vorgaben zur Datenträgervernichtung - die neue DIN 66399 160

11.3.1 Grundlagen und Begriffe (DIN 66399-1) 160

11.3.2 Anforderungen an Maschinen zur Vernichtung von Datenträgern (DIN 66399-2) 161

11.3.3 Prozess der Datenträgervernichtung (DIN SPEC 66399-3) 161
11.3.4 Löschen personenbezogener Daten auf Datenträgern 161
11.4 Cloud-Lösungen für Verwaltung und Wirtschaft 162
11.4.1 Cloud Computing - zum Stand der Diskussion 162
11.4.2 Kann Dropbox unbedenklich genutzt werden? 166

Inhaltsverzeichnis des Anhangs 169

Stichwortverzeichnis 203

Vorwort

Was nutzt ein umfangreicher Bericht, wenn er nicht gelesen wird? Schon seit einigen Jahren hatte ich den Eindruck, dass der sehr textlastige Bericht meiner Dienststelle, wenn schon nicht wesentlich inhaltlich, so doch wenigstens optisch verändert und lesefreundlicher gestaltet werden könnte. Während sich die 30 Vorgängerberichte aus Kostengründen bislang am Layout einer Landtagsdrucksache orientierten, ist dieser Bericht zweispaltig gestaltet und weist farbige Textteile auf. Dank einer Absprache mit dem Landtag konnte diese Gestaltung auch für die Landtagsdrucksache selbst übernommen werden, so dass sich bei Verweisen auf die Drucksache keine Unterschiede zur Broschüre ergeben; hierfür danke ich der Landtagsverwaltung, die mich auch bei anderen Gelegenheiten nach Kräften unterstützt, sehr. Das neue Layout ist - ebenso wie der seit Ende April 2013 neu gestaltete und wesentlich ausgeweitete Internetauftritt meiner Dienststelle - Ausdruck des Bemühens, Informationen zum Thema Datenschutz noch benutzerfreundlicher anzubieten. Neu ist auch der in Absprache mit dem Ständigen Ausschuss des Landtags verschobene Termin der Veröffentlichung: Der Bericht erscheint nun erst zu Beginn des auf den Berichtszeitraum folgenden Jahres, um Entwicklungen periodengerecht darstellen zu können. Auch für dieses Zugeständnis bedanke ich mich. Wie jeder Bericht in der Vergangenheit, so ist aber auch dieser das Ergebnis einer Teamarbeit, für die mein Dank meinen Mitarbeiterinnen und Mitarbeitern gilt.

Inhaltlich bleibt es vorerst bei den bekannten Schwerpunkten, die seit dem 30. Tätigkeitsbericht auch den Datenschutz im nicht-öffentlichen Bereich, also etwa bei Unternehmen oder Vereinen mit Sitz in Baden-Württemberg, umfassen. Der Zusammenschluss der beiden Aufsichtsbehörden zum 1. April 2011 hat sich insgesamt bewährt, wenngleich die in der Koalitionsvereinbarung in Aussicht gestellte Zuständigkeit für die Verfolgung und Ahndung von datenschutzrechtlichen Ordnungswidrigkeiten nach wie vor eine sinnvolle Abrundung darstellen würde. Aber was nicht ist, kann ja noch bis zum Ende der Legislaturperiode werden. Bis dahin wird sich auch zeigen, ob der Landesgesetzgeber mir die zusätzliche Aufgabe eines Beauftragten für die Informationsfreiheit überträgt. Der entsprechende Gesetzentwurf soll in den nächsten Monaten das Licht der Welt erblicken.

Im letzten Tätigkeitsbericht hatte ich noch die Neuordnung des Rechtsrahmens auf europäischer Ebene als spannende Herausforderung der kommenden Monate bezeichnet. Die Spannung über den Verlauf des Reformprozesses hat bis heute nicht nachgelassen, da die Verhandlungen über den von der EU-Kommission im Januar 2012 vorgestellten Entwurf einer Datenschutz-Grundverordnung noch längst nicht abgeschlossen sind. Der Wunsch des EU-Parlaments, den Trilog mit Kommission und Ministerrat bis zu den Europawahlen am 25. Mai 2014 abzuschließen, wird sich voraussichtlich nicht erfüllen. Dies ist mehr als bedauerlich, da der Entwurf trotz mancher Schwächen doch von dem Bemühen geprägt ist, wesentliche Elemente unseres deutschen Datenschutzrechts auch auf der europäischen Ebene zu verankern. Leider hat die Bundesregierung in den Beratungen des Ministerrats oft eher zögerlich gewirkt. Wenn die EU-Verordnung in wenigen Jahren in Kraft treten sollte, dann wird sie das nationale Datenschutzrecht verdrängen und für gravierende Veränderungen, auch hinsichtlich der Befugnisse der Aufsichtsbehörden und ihres Zusammenwirkens untereinander sorgen. Eine stärkere internationale Ausrichtung der Dienststelle wird dann schon angesichts der zentralen Zuständigkeit für international agierende Unternehmen aus unserem Land vermutlich unausweichlich sein; es würde mich daher nicht wundern, wenn Englisch mittelfristig zur zweiten Amtssprache wird. Die Positionsbestimmung in zahlreichen datenschutzrechtlichen Fragen verlagert sich ohnehin zunehmend auf die europäische Ebene, für die die maßgeblichen Dokumente (zumindest zunächst) nur in englischer Sprache zur Verfügung stehen. Auf diese Entwicklung sind wir bislang weder personell noch finanziell hinreichend vorbereitet. Da die Internationalisierung

auch veränderte berufliche Qualifikationen erfordern wird, ist eine stärkere personelle Verzahnung mit der Landesverwaltung wünschenswert, die ja ebenfalls immer mehr von Europa beeinflusst wird. Die bei der Novellierung des Landesdatenschutzgesetzes 2011 seitens der Landesregierung versprochene Einbeziehung meiner Mitarbeiterinnen und Mitarbeiter in den allgemeinen Personalaustausch der Landesverwaltung muss jedenfalls noch mit Leben erfüllt werden. So sehr die Unabhängigkeit der Datenschutzaufsicht auch europarechtlich geboten sein mag, so sehr kann sie in der Praxis doch in Sachen Personalpolitik in die Isolation führen.

Internationale Herausforderungen für den Datenschutz haben sich im Berichtszeitraum auch von gänzlich unerwarteter Seite durch die Spähaffäre angloamerikanischer Geheimdienste ergeben, auf die ich - obwohl meine Dienststelle davon nicht unmittelbar betroffen war - gleich zu Beginn dieses Berichts eingehe. Der NSA-Skandal hat die Ohnmacht Deutschlands auf politischer, rechtlicher und technischer Ebene überaus deutlich gemacht und wie ein Weckruf für alle Verantwortlichen gewirkt. Wenn ich vorher skeptisch gewesen sein mag, so bin ich mir jetzt recht sicher, dass die Europäische Datenschutzreform kommen wird und europäische Datenschutzstandards im Dialog mit den transatlantischen Partnern erfolgreich durchgesetzt werden können, wenngleich für Geheimdienste weiterhin Sonderrechte gelten mögen. Voraussetzung hierfür wird allerdings sein, dass die Affäre - anders als bei dem ähnlichen Echelon-Skandal 2001 - nicht vorzeitig wieder in Vergessenheit gerät. Es bleibt jedenfalls zu hoffen, dass nun zügig für Aufklärung gesorgt wird und - soweit möglich - wirksame Gegenmaßnahmen ergriffen werden. Wenn man sich vor Augen führt, um welche Alltagsprobleme der Bürger sich meine Dienststelle tagtäglich zu kümmern hat - um die unerwünschte Werbe-E-Mail ebenso wie um die Videoüberwachungsanlage des streitsüchtigen Nachbarn, um die Registrierung vermeintlicher „Jugendsünden“ im Polizeicomputer ebenso wie um die unzureichende Größe mancher Behördenbriefkästen - und wenn man den hiermit bei uns verbundenen Aufwand ins Kalkül zieht, so wird doch eine gewisse Diskrepanz zu den bisher so nicht bekannten Realitäten, den schier unbegrenzten technischen Möglichkeiten der Geheimdienste und der offenkundigen Bereitschaft, hiervon ungeniert Gebrauch zu machen, augenfällig. Ich gestehe, dass mich die Spähaffäre auch deshalb vorübergehend sprachlos gemacht hat.

Dessen ungeachtet habe ich mich im Berichtszeitraum bemüht, meinen Beitrag zu einer strukturellen Verbesserung der Datenschutzniveaus im Land beizutragen. Dazu zählt die Veröffentlichung von zahlreichen Merkblättern und Handreichungen ebenso wie die verstärkte praktische Zusammenarbeit mit den Kommunalen Landesverbänden, mit Polizei und Staatsanwaltschaften oder mit Schulen, die in diesem Bericht dargestellt wird. Hierzu hat nicht zuletzt auch die Abordnung entsprechender Mitarbeiter an meine Dienststelle beigetragen, für die ich sehr dankbar bin.

Vor kurzem hat sich das wegweisende Volkszählungsurteil des Bundesverfassungsgerichts zum 30. Mal gejährt. Ich halte es gerade vor dem Hintergrund der Spähaffäre und angesichts der rasanten technischen Entwicklung - als Stichworte mögen hier Begriffe wie Big Data und Industrie 4.0 genügen - für aktueller denn je. Das Grundrecht auf informationelle Selbstbestimmung muss weiterhin der Maßstab für den Datenschutz der Zukunft sein, nicht nur wegen der Freiheitsrechte des Einzelnen, sondern wegen des Zusammenhalts unserer Gesellschaft überhaupt. Die damalige Feststellung des Gerichts, unter den Bedingungen der modernen Datenverarbeitung gebe es kein belangloses Datum mehr, gilt heute erst recht. Wir brauchen nun aber in Anbetracht veränderter technischer Rahmenbedingungen wie der weltweiten Vernetzung via Internet gemeinsame europäische Antworten.

Jörg Klingbeil

1. Zur Situation

1.1 O Tempora, o mores - ist die Privatsphäre angesichts des Spähskandals der Geheimdienste noch zu retten?

O tempora, o mores - was für Zeiten, was für Sitten! Man ist geneigt, angesichts der ständig neuen Enthüllungen über die weltweiten Spähaktivitäten angloamerikanischer Geheimdienste in diesen Ausruf Ciceros einzustimmen, mit dem er den Verfall der Sitten beklagte, auch wenn Cicero nicht das britische Spähprogramm TEMPORA meinte. Denn was ist es anderes als ein Sittenverfall, wenn sich die umfassende Ausspähung auch gegen befreundete Nationen und Regierungen richtet und selbst vor dem Mobiltelefon der Bundeskanzlerin nicht Halt macht? In Anbetracht der Gefährdung der nicht minder schützenswerten Privatsphäre der Bürgerinnen und Bürger möchte man mit Cicero an die Adresse der Geheimdienste hinzufügen: „Wie lange noch werdet Ihr unsere Geduld missbrauchen?“[1]

Seit Anfang Juni 2013 berichten die internationalen Medien nahezu ununterbrochen über umfangreiche und weltweite **Spionageaktivitäten westlicher Nachrichtendienste**, insbesondere der US-amerikanischen National Security Agency (**NSA**) und des britischen Government Communications Headquarters (**GCHQ**). Diese Meldungen gehen zurück auf Informationen des US-amerikanischen Whistleblowers und ehemaligen NSA-Analysten **Edward Snowden**, der sich zur Zeit in Moskau aufhält. Ein Ende der Enthüllungen ist noch nicht in Sicht, zumal Snowden über 30.000 Dokumente verfügen soll. Von einem Ende der Spähaffäre, wie der Chef des Bundeskanzleramtes noch im August 2013 verlauten ließ, kann keine Rede sein. Die Aktivitäten der Nachrichtendienste zielen mit mehreren Spähprogrammen unterschiedlicher Funktionalität (PRISM, TEMPORA, XKEYSCORE, BULLRUN, MUSCULAR etc.) auf die weltweite Kommunikation via Internet und Telefon. Dabei werden offenbar nicht nur massenhaft Standort- und Verbindungsdaten abgesaugt und Kommunikationsinhalte nach Stichworten durchforstet, sondern sogar internationale Glasfaserleitungen physikalisch angezapft und Verschlüsselungsverfahren überwunden. Die Spähangriffe sollen offiziell nur der Terrorabwehr dienen, erfassen faktisch aber auch normale Bürgerinnen und Bürger, ja selbst Behörden und Politiker hierzulande. Besonderen Wirbel und erhebliche politische Verstimmungen löste Ende Oktober 2013 die Nachricht aus, dass ein Mobiltelefon der Bundeskanzlerin abgehört worden sei. Dass dies der Terrorabwehr dienen sollte, erscheint unglaubwürdig.

Methodik, Umfang und Tiefe der Spionageaktivitäten sind nur partiell geklärt; letztlich unklar ist auch die Einbindung der jeweiligen Regierungen oder von international agierenden Unternehmen der Internet- und Telekommunikationsbranche. Der Ruf nach Aufklärung und Transparenz verstummt nicht, zumal ständig neue Spähprogramme und Einzelheiten bekannt werden. So wurde Anfang Dezember 2013 durch Unterlagen von Edward Snowden publik, dass die NSA schon 2012 täglich weltweit fünf Milliarden Standortdaten von Mobiltelefonen mit Hilfe des Programms CO-TRAVELER erfasst habe[2], die in einer gigantischen Datenbank namens FASCIA gesammelt würden. Ziel sei es hierbei, unbekannte Kontakte, etwa mit Zielpersonen, anhand sich überschneidender Bewegungenzu erkennen, was wiederum nur funktioniere, wenn Standortdaten auf der ganzen Welt methodisch gesammelt würden. Die NSA sammele somit - ohne konkreten Anlass - Daten von Hunderten von Millionen Mobilfunknutzern auf der ganzen Welt, um rückwirkend Bewegungsprofile anlegen zu können. Beobachter mutmaßen, dass sich die NSA mit dem Wissen von z. T. ausländischen Mobilfunkbetreibern oder Dienstleistungsfirmen Zugang zu Roaming-Datenbanken verschafft hat, in denen Telefongesellschaften Informationen über ihre Kunden austau-

[1] Ciceros Ausspruch in der ersten Rede gegen Catilina im Jahre 63 v.Chr. lautete im lateinischen Originaltext: „*Quousque tandem abutere, Catilina, patientia nostra?*“.

[2] vgl. Meldung der Washington Post vom 4. Dezember 2013: *http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html*

schen, und dass sie außerdem in großem Stil Glasfaserkabel angezapft hat, mit denen Mobilfunknetze verbunden sind. Die Datensammlung beschränke sich damit nicht auf Daten, die für laufende Ermittlungsverfahren als relevant gelten. Der Zeitpunkt der Löschung wurde nicht genannt, allerdings habe die Rechnerkapazität ausgebaut werden müssen, da das Spähprogramm zur Handyortung fast zur Überlastung der Ressourcen geführt habe. Wie bei vorangegangenen Enthüllungen erklärte die NSA auch diese Totalüberwachung für legal, solange sie nicht absichtlich US-Bürger betreffe. Damit wurde erneut bestätigt, dass Nicht-Amerikaner vor dieser Ausspähung ihrer Privatsphäre nicht geschützt sind. Deutlich wurde auch, dass die Geheimdienste von der IT-Branche gezwungenermaßen oder freiwillig unterstützt werden.

Das **Bundesverfassungsgericht** hat zwar in seiner Entscheidung zur Vorratsdatenspeicherung vom 2. März 2010 (vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 55) deutlich gemacht, wie viel Standort- und Verbindungsdaten über einen Menschen verraten können und welche hohen Hürden für staatliche Eingriffe in die Grundrechte der Bürger zu gelten haben; an diese wegweisende Entscheidung sind ausländische Geheimdienste jedoch nicht gebunden. Das Diktum des Gerichts, das Verbot einer Totalüberwachung der Bevölkerung gehöre zur verfassungsrechtlichen Identität Deutschlands, die auch auf internationaler Ebene zu wahren sei, kann aber weiterhin als Auftrag an den Staat bzw. konkret an die Bundesregierung verstanden werden, sich stärker für die Grundrechte der Bürger auch gegenüber verbündeten Regierungen einzusetzen. Zwar hat der amerikanische Präsident mittlerweile ein **Expertengremium** eingesetzt und schärfere Regeln zur „Selbstbeschränkung“ für die Überwachungspraxis des Geheimdienstes NSA in Aussicht gestellt. Über die 46 Reformvorschläge der Experten[3] will er in den nächsten Wochen entscheiden. U. a. schlugen die Experten vor, die zentrale Speicherung der Verbindungsdaten durch eine dezentrale bei den Telekomunternehmen zu ersetzen, den Zugriff durch Geheimdienste einer stärkeren richterlichen Kontrolle zu unterwerfen, organisatorische Änderungen vorzunehmen und insgesamt mehr Transparenz zu schaffen. Andererseits wurde betont, dass die USA zum Schutz der nationalen Sicherheit weiterhin weltweit Kommunikationsdaten sammeln müssten. Darin kommt meines Erachtens auch zum Ausdruck, dass Geheimdienstaktivitäten in allen Staaten traditionell als Teil der nationalen Souveränität verstanden werden. Insofern bin ich skeptisch, ob sich die Vereinigten Staaten von Amerika auf wirksame Beschränkungen der Befugnisse ihrer Geheimdienste einlassen werden, wenn sie ihre nationalen Sicherheitsinteressen tangiert sehen.

Die aktuellen Ereignisse erinnern an die **ECHELON-Affäre**, die die Überwachung des satellitengestützten Telekommunikationsverkehrs durch US-Geheimdienste, auch von Deutschland aus, betraf. Der Bericht des vom Europaparlament eingesetzten Sonderausschusses vom 11. Juli 2001[4] geriet schon zwei Monate später wegen der Anschläge vom 11. September 2001 aus dem Blickfeld. Dem Bericht zufolge sollen die aufgedeckten Aktivitäten auch der Wirtschaftsspionage gedient haben.

Die Bundesregierung, aber auch andere Staaten und die Europäische Union bemühen sich seit Monaten auf politischer und fachlicher Ebene um Aufklärung. Das **Europäische Parlament** hat am 4. Juli 2013 den **LIBE-Ausschuss** mit der Untersuchung der Affäre beauftragt und bei dieser Gelegenheit die Einrichtung einer parlamentarischen Kontrollkommission auf europäischer Ebene gefordert. Interessante Einzelheiten und Hintergründe zu den Überwachungsprogrammen gehen u. a. aus einem Kurzgutachten (in englischer Sprache) des Experten Caspar Bowden (früher Datenschutzbeauftragter der Firma Microsoft) an den

[3] Der ca. 300 Seiten starke Bericht wurde am 18. Dezember 2013 auf der Internetseite des Weißen Hauses veröffentlicht: *http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf*

[4] *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE*

LIBE-Ausschuss vom September 2013 hervor[5]. Darin wird u. a. hervorgehoben, dass die von Edward Snowden an die Medien herausgegebenen Dokumente vermutlich authentisch sind und bisher im Kern nicht bestritten wurden. Einen regelmäßig aktualisierten Überblick über die Spähaffäre bieten verschiedene Medien auf ihren Internetseiten[6]. Der Deutsche Bundestag erwägt ebenfalls die Einsetzung eines Untersuchungsausschusses.

Die **Landesregierung** verfügt - wie sich aus LT-Drs. 15/3662 und LT-Drs. 15/3727 ergibt - über keine wesentlichen eigenen Erkenntnisse. Auch meine Dienststelle bezieht ihre Informationen überwiegend aus den Medien, daneben aus Kontakten mit den anderen Datenschutzbeauftragten und mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI). Die Anfragen besorgter Bürger halten sich in Grenzen.

Die Bundeskanzlerin hat in einer Pressekonferenz am 19. Juli 2013 ein **„Acht-Punkte-Programm für einen besseren Schutz der Privatsphäre“** vorgestellt, in dem u. a. ein Zusatzprotokoll zu Artikel 17 zum Internationalen Pakt über Bürgerliche und Politische Rechte der Vereinten Nationen für einen besseren Schutz der Privatsphäre unter Einbeziehung der Tätigkeit der Nachrichtendienste angestrebt wird[7]. Als weiteres Ziel werden die zügige Verabschiedung der EU-Datenschutz-Grundverordnung und darin eine Auskunftspflicht für Firmen gegenüber den Betroffenen bei Datenweitergabe an Drittstaaten formuliert (was inzwischen vorgesehen ist). In einem „**Fortschrittsbericht**“ vom 14. August 2013 wurde über die seither eingeleiteten Schritte berichtet[8]. Darin wurde auch der Wunsch nach einer unverzüglichen **Evaluierung des Safe-Harbor-Abkommens** (durch die Europäische Kommission) bekräftigt (siehe hierzu Kapitel 1.3.7). Weitere Vorschläge zur Bewältigung der Spähaffäre bzw. für „Gegenmaßnahmen“ reichen von einem Abkommen zur Unterlassung gegenseitiger Spionageaktivitäten („no-spy“-Abkommen) bis hin zur Aufkündigung oder zumindest Aussetzung internationaler Abkommen mit den USA, zum Beispiel zur Übermittlung von Finanztransaktionsdaten (**SWIFT**). Das Europäische Parlament hat sich am 23. Oktober 2013 in einer Resolution zwar dafür ausgesprochen, das SWIFT-Abkommen auszusetzen[9]. Die Entschließung hatte allerdings eher symbolische Bedeutung; für die weitere Umsetzung ist noch die Zustimmung von zwei Dritteln der Mitgliedsstaaten erforderlich. Die Europäische Kommission erteilte mittlerweile der Kündigung der bilateralen Abkommen eine Absage, erklärte am 27. November 2013 aber auch[10], dass vertrauensbildende Maßnahmen im transatlantischen Verhältnis dringend erforderlich seien. Hierzu zählte sie eine rasche Verabschiedung der Europäischen Datenschutzreform (siehe Kapitel 1.3.1) sowie eine Beseitigung der Defizite des Safe-Harbor-Verfahrens (siehe Kapitel 1.3.7).

Die Spähaffäre belastet auch die im Jahr 2013 aufgenommenen Verhandlungen zwischen der EU und den USA über ein **transatlantisches Freihandelsabkommen** (Transatlantic Trade and Investment Partnership; TTIP). Offiziell waren die Spionageaktivitäten der NSA dabei bisher kein Thema; in den Medien wurde allerdings über Forderungen, u. a. des Präsidenten des EU-Parla-

[5] *http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf*

[6] vgl. z. B. Heise-Online, Meldung vom 8. November 2013: *http://www.heise.de/newsticker/meldung/NSA-Skandal-Von-Merkels-Handy-Muscular-NSA-GCHQ-BND-PRISM-Tempora-und-dem-Supergrundrecht-was-bisher-geschah-2039019.html*.

[7] Am 18. Dezember 2013 wurde auf Initiative Deutschlands und Brasiliens immerhin eine – durch Einfluss der USA gegenüber der ursprünglichen Fassung allerdings verwässerte – Resolution zum Schutz der Privatsphäre im Internet von der UN-Generalversammlung verabschiedet.

[8] *http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/massnahmen-fuer-einen-besseren-schutz-der-privatsphaere,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf*

[9] *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//DE&language=DE*.

[10] *http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm*

ments, berichtet, die Verhandlungen bis zur Aufklärung der Spähaffäre auf Eis zu legen, was der EU-Ministerrat bei seiner Sitzung in Brüssel am 24./25. Oktober 2013 aber nicht aufgriff. Auch die EU-Kommission erklärte am 27. November 2013, dass Datenschutzstandards kein Verhandlungsgegenstand des TTIP seien. Vereinzelt wurde auch eine Aussetzung des Abkommens zur Übermittlung von Flugpassagierdaten an das Heimatschutzministerium der USA (**PNR-Abkommen**) thematisiert. Die **Datenschutzbeauftragten des Bundes und der Länder** wiesen in einer Entschließung vom 13./14. März 2013 (vgl. Anhang 14) auf die Notwendigkeit hin, bei den Verhandlungen über die transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren und sich für das in der Europäischen Grundrechtecharta verbriefte Recht auf Datenschutz einzusetzen. Die Verhandlungen dürften sich auch nicht negativ auf den Reformprozess des EU-Datenschutzrechts auswirken. Die Konferenz erinnerte zudem daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstelle.

Mittlerweile setzen sich auch Wirtschaftskreise in Europa und in den USA für mehr Transparenz in der Spähaffäre und für einen besseren internationalen Schutz vor Ausspähung ein. So hat der Branchenverband **BITKOM** am 7. November 2013 darauf hingewiesen, dass das Vertrauen von Internet-Nutzern und Unternehmen in den Schutz und die Sicherheit ihrer Daten beschädigt sei und dass sich dies nachteilig auf die Nutzung neuer Technologien auswirken könne[11]. Bereits im Juli 2013 hatten Umfragen ergeben, dass das Vertrauen der deutschen Internet-Nutzer in Staat und Behörden in Bezug auf den Umgang mit ihren persönlichen Daten im Internet massiv zurückgegangen war. Das Vertrauen in die Datenverarbeitung durch die Wirtschaft hatte ebenfalls nachgelassen. Davon sind insbesondere neue Entwicklungen in der IT-Branche wie **Cloud Computing** betroffen, bei dem Rechenleistungen und Speicherkapazität flexibel und bedarfsgerecht über das Internet zur Verfügung gestellt werden können (siehe Kapitel 11.4.1). Soweit in diesem Zusammenhang US-amerikanische Anbieter in Anspruch genommen werden, ist vor dem Hintergrund der Spähaffäre zunächst besondere Vorsicht geboten. Auch eine Verschlüsselung hilft nur bedingt, falls Meldungen zutreffen sollten, dass sich die Geheimdienste die Schlüsselzertifikate verschafft haben.

Die bisher geltenden **Regelungen zum internationalen Datentransfer** werden angesichts der Spähaffäre derzeit von verschiedener Seite in Frage gestellt. So sprach sich der Vorstandsvorsitzende der Deutschen Telekom auf dem „Cyber Security Summit“ am 11. November 2013 in Bonn für eine Neuverhandlung des „Safe-Harbor-Abkommens“ aus, dessen Geschäftsgrundlage durch die Spionageaktivitäten entzogen worden sei. Stattdessen regte er einen „sicheren Datenraum in der EU“ an und schlug hierfür die Schaffung einer „Schengen-Cloud“ (also ohne Großbritannien) und eines „Schengen-Routing“ (d. h. die Durchleitung von E-Mails innerhalb des Schengen-Raums) vor. Die EU-Kommissarin Neelie Kroes warnte bei derselben Veranstaltung indessen davor, die Daten im europäischen Binnenmarkt wieder „in nationale Grenzen zu sperren“. Bei einer Anhörung im Untersuchungsausschuss des EU-Parlaments am 8. Oktober 2013 hatten sich Experten gegen einen raschen Abschied vom umstrittenen Safe-Harbor-Abkommen, jedoch für dessen gründliche Überarbeitung ausgesprochen, denn wirklich funktioniert habe der „Kompromiss zwischen zwei sehr unterschiedlichen Systemen zum Datenschutz“ bisher nicht.

Die Europäische Kommission hatte seit dem Jahr 2000 in mehreren Entscheidungen Grundsätze zum sicheren Datentransfer in die USA (Safe Harbor) und in andere Drittstaaten (Standardverträge) aufgestellt, um zu gewährleisten, dass personenbezogene Daten dort einem angemessenen Datenschutzniveau unterliegen. Daten verarbeitende Unternehmen aus diesen Drittstaaten können nach einer - bisher offenbar kaum kontrollierten - Selbstzertifizierung dem **Safe-Harbor-Abkommen** beitreten (d. h. sich beim US De-

[11] *http://www.bitkom.org/de/presse/8477_77860.aspx*

partment of Commerce registrieren lassen), was praktisch alle großen US-amerikanischen Internetkonzerne getan haben. Auf die Befugnisse US-amerikanischer Sicherheits- und Justizbehörden, unter Berufung auf den **US Patriot Act** auf Daten zuzugreifen, die auf Servern dieser US-Firmen lagern (auch außerhalb der USA!), und dabei dem Betreiber eine Auskunft gegenüber dem Betroffenen mit Hilfe eines sog. Security Letters zu verbieten, hatte ich im Zusammenhang mit dem Thema Cloud Computing bereits im 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 46) hingewiesen. Vergleichbare Befugnisse verschafft übrigens der **Foreign Intelligence Surveillance Act (FISA)**, der auch die Rechtsgrundlage für das NSA-Spähprogramm PRISM gebildet haben soll. Die Safe-Harbor-Vereinbarung erlaubt zwar Zugriffe durch Sicherheitsbehörden, wenn Belange der nationalen Sicherheit dies erfordern, die Anwendung war nach bisherigem Verständnis aber auf Einzelfälle im Rahmen des tatsächlich Erforderlichen beschränkt gewesen. Die offenbar praktizierte systematische und anlasslose Ausspähung von personenbezogenen Daten durch die angloamerikanischen Nachrichtendienste kann mit Belangen der nationalen Sicherheit in einer demokratischen Gesellschaft nicht gerechtfertigt werden. Die **Datenschutzbeauftragten des Bundes und der Länder** haben deshalb in einer Pressemitteilung vom 24. Juli 2013[12] angekündigt, bis zu einer effektiven Begrenzung der unbeschränkten Zugriffe ausländischer Nachrichtendienste auf die personenbezogenen Daten der Menschen in Deutschland u. a. zu prüfen, ob konkrete Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens auszusetzen sind. Ferner wurde die Europäische Kommission aufgefordert, ihre Entscheidungen zu Safe Harbor und zu den sog. Standardvertragsklauseln bis auf Weiteres zu suspendieren. Die EU-Kommission hat am 27. November 2013 bekanntgegeben, dass sie die Überprüfung des Abkommens erst im Sommer 2014 abschließen werde, und der US-Seite dreizehn Empfehlungen zu Safe Harbor an die Hand gegeben (siehe Kapitel 1.3.7).
Am 5. September 2013 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder außerdem eine **Entschließung zur Spähaffäre** gefasst (vgl. Anhang 17). Darin wird eine umfassende Aufklärung angemahnt und daran erinnert, dass ein Verbot der totalen Erfassung und Registrierung der Freiheitswahrnehmung der Bürger nach der Rechtsprechung des Bundesverfassungsgerichts „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland“ gehöre, für die sich der Staat in europäischen und internationalen Zusammenhängen einsetzen müsse. Zugleich haben die Datenschutzbeauftragten eine intensivere parlamentarische Kontrolle auch der deutschen Nachrichtendienste für erforderlich gehalten.

Die **Industrie- und Handelskammer Region Stuttgart** hat mir berichtet, dass es im Hinblick auf die finanziellen und technischen Möglichkeiten der beteiligten Nachrichtendienste nach Meinung hiesiger Unternehmen schwierig sei, geeignete Schutzmaßnahmen zu implementieren; in erster Linie sei die Politik gefordert. Bezüglich des Safe-Harbor-Abkommens herrsche bei den Unternehmen Verunsicherung. Nicht nur wegen der aktuellen Spähaffäre, sondern auch aufgrund sonstiger Cyberattacken aller Art würden aber die Sicherheitsmaßnahmen derzeit verstärkt. Insgesamt sei zu berücksichtigen, dass der Daten- und teilweise auch der Telekommunikationsverkehr weitgehend über ein privates globales Netz stattfinde, so dass fraglich sei, wie sicher eine Verschlüsselung wirklich ist. Diese Einschätzung deckt sich mit Informationen von Edward Snowden, wonach die Nachrichtendienste bei den (zumeist amerikanischen) Herstellerfirmen auf den Einbau von „Hintertüren“ in Software und Hardware gedrängt hätten. In den Medien wurde außerdem berichtet, dass die Nachrichtendienste NSA und GCHQ im Rahmen der Programme BULLRUN (USA) bzw. EDGEHILL (UK) systematisch **Verschlüsselungsprogramme** umgehen und teilweise „knacken“. So hätten sich die Nachrichtendienste z. B. die für eine Transportverschlüsselung erforderlichen Zertifikate bei den Zertifizierungsinstanzen (Certification Authorities) im Wege der techni-

[12] *http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/07/Presseerklärung-Safe-Harbor.pdf#* (Anmerkung: Die Pressemitteilung trägt irrtümlich das Datum 24. Juni 2013*)*

schen Infiltration verschafft. Aus diesem Grund werden von Sicherheitsexperten für die Verschlüsselung zunehmend Open-Source-Produkte empfohlen, deren Quellcode für die fachlich Interessierten offen zutage liegt und bei denen eine eingebaute „Hintertür“ leichter auffällt. Die bisher bekannt gewordenen Veröffentlichungen hätten aber keine Hinweise darauf geliefert, dass es NSA oder GCHQ bisher gelungen wäre, aktuell als stark eingestufte Verschlüsselungsverfahren wie AES mit ausreichend langen Schlüsseln zu kompromittieren. Auch Edward Snowden habe bestätigt, dass starke Verschlüsselungsverfahren noch Schutz böten.

Die **rechtliche Einordnung** der Spähaffäre erweist sich bisher als schwierig. So ist weder klar, ob die ausländischen Nachrichtendienste systematisch gegen Gesetze ihrer Heimatländer verstoßen haben (bislang wurde das bestritten) noch ob der deutsche Auslandsnachrichtendienst **BND** unzulässigerweise Daten erhoben und/oder an ausländische Nachrichtendienste weitergeleitet hat. Immerhin gehört die strategische Auslandsaufklärung, darunter auch die Fernmeldeaufklärung, zum Aufgabenspektrum des BND (vgl. §§ 1, 2 des Gesetzes über den Bundesnachrichtendienst [BND-Gesetz], §§ 1, 5 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheinmisses, [G 10]). Die in diesem Zusammenhang besonders interessierende Frage, ob der Grundrechtsschutz der Bürger durch die Zusammenarbeit der Nachrichtendienste verschiedener Staaten mit unterschiedlichen Erhebungsvoraussetzungen umgangen werde, beantwortete das Bundesinnenministerium am 24. Juni 2013 im Bundestags-Unterausschuss Neue Medien mit dem Hinweis, dass es davon ausgehe, dass „die Partnerdienste jeweils im Rahmen der ihrer Tätigkeit zugrundeliegenden nationalen Rechtsgrundlagen arbeiten“. Zu der weiteren Frage, in welchem Umfang der BND seinerseits Daten an ausländische Partnerdienste übermittelt, erklärte die Bundesregierung, dass nur im Einzelfall personenbezogene Daten aus der strategischen Aufklärung des Fernmeldeverkehrs weitergeleitet worden seien (vgl. Vorbemerkung und Antwort auf Frage 11 in BT-Drs. 17/14456, zugleich Anlage zu LT-Drs. 15/3727). Tatsache ist, dass die Schutzvorschriften des G 10 nicht für Telekommunikationsanschlüsse im Ausland gelten, sofern nur ausgeschlossen werden kann, dass deutsche Nutzer hierdurch nicht gezielt erfasst werden (§ 5 Absatz 2 Satz 3 G 10). Die Argumentation der NSA klingt im Grunde ähnlich. Im Rahmen der aktuellen Untersuchungen des EU-Parlaments sollen übrigens auch die Überwachungsaktivitäten der eigenen Nachrichtendienste der Mitgliedsstaaten unter die Lupe genommen werden. Die **Bundesanwaltschaft** hat am 5. November 2013 erklärt, dass derzeit kein Anfangsverdacht für Spionage durch einen ausländischen Nachrichtendienst vorläge; dies gelte sowohl für die angebliche Ausspähung des Mobiltelefons der Bundeskanzlerin als auch für die etwaige Überwachung der Internetkommunikation durch die NSA. Aus den bislang übermittelten Informationen ergäben sich „keine zureichenden tatsächlichen Anhaltspunkte für eine in die Zuständigkeit der Bundesanwaltschaft fallende Straftat“. Kritik hat in den letzten Monaten die **innerstaatliche Kontrolle der Nachrichtendienste** im Rahmen des Parlamentarischen Kontrollgremiums des Deutschen Bundestags erfahren. Selbst in dessen nichtöffentlichen Sitzungen habe die Regierung massiv geschwärzte Dokumente an Abgeordnete verteilt, die zudem teilweise bereits Wochen zuvor in dieser Form im Internet standen.

Die Spähaffäre wird Politik, Wirtschaft und Gesellschaft noch lange beschäftigen. Das Vertrauen in die Vertraulichkeit und Integrität informationstechnischer Systeme, das nach der Rechtsprechung des Bundesverfassungsgerichts Verfassungsrang hat, ist massiv beschädigt worden. Der nationale Rechtsrahmen hat sich unter den technischen Rahmenbedingungen des globalen Netzes als weitgehend wirkungslos erwiesen und kann die Privatsphäre offenbar kaum noch schützen. Umso dringlicher sind nun die Harmonisierung des europäischen Datenschutzrechts auf hohem Niveau und der Abschluss wirksamer völkerrechtlicher Vereinbarungen zur Eindämmung der Aktivitäten ausländischer Geheimdienste.

1.2 Big Data - eine Daten-Goldgrube für Wirtschaft und Sicherheitsbehörden

Die von der Menschheit hervorgebrachten Datenmengen vermehren sich sprunghaft. Die Daten liegen überwiegend jedoch unstrukturiert vor und stammen aus vielfältigen Quellen. Hier setzt die moderne schnelle Datenauswertung unter dem Begriff Big Data[13] mit Hilfe verschiedener Methoden und Technologien an, um aus dem strategischen Rohstoff der Daten wirtschaftlichen Nutzen für die Unternehmen zu erzeugen. Geheimdienste wie NSA verfahren in ähnlicher Weise.

Bereits von 2000 bis 2002 sind von der Menschheit nach Schätzungen mehr Daten hervorgebracht worden als in den 40 000 Jahren davor. Von 2003 bis 2005 vervierfachte sich die **Datenmenge** und stieg weiter exponentiell an, so dass 2012 mit rd. 2,5 Zettabytes (1 Zettabyte = 10^{21} Byte) bereits die zehnfache Menge des Jahres 2006 erreicht wurde. Allein im Internet werden tagtäglich so viele Daten transportiert, dass rd. 250 Mio. DVDs gebraucht würden, um sie alle abzuspeichern. Forscher gehen mittlerweile von einer Verdoppelung der Datenmenge alle zwei Jahre aus, die von Suchmaschinen, sozialen Netzwerken, Industrieanlagen, Sensoren, RFID-Chips, Videokameras, Fahrzeugen, Alltagsgeräten usw. erzeugt werden; in Anbetracht der zunehmenden Durchdringung nahezu aller Lebensbereiche durch die Informationstechnik und der weltweiten Internetvernetzung erscheint das plausibel. Der Großteil des Datenvolumens soll auf Bilder und Videos zurückgehen. Große Datenvolumina fallen bekanntermaßen auch in der Finanzindustrie (Finanztransaktionen, Börsendaten), im Energiesektor (Verbrauchsdaten), im Gesundheitsbereich (z. B. Verschreibungen) oder in der Forschung (z. B. Klimaforschung, Genetik) an. Neben der schieren Menge an Daten stellen die gewünschte Verarbeitungsgeschwindigkeit - bis hin zur Echtzeit - und die Vielfältigkeit und Komplexität der Datenquellen (z. B. soziale Netzwerke, Videos, Fotos, Suchmaschinen, Tweets, E-Mails und Videotelefonie) enorme Herausforderungen für die unter dem Kunstwort Big Data zum Einsatz kommenden Methoden und Techniken dar. Unternehmen versprechen sich von der verbesserten Analyse großer Datenmengen das frühzeitige Erkennen von Trends, genauere Prognosen und somit insgesamt Wettbewerbsvorteile, Einsparpotenziale und die Erschließung neuer Geschäftsfelder. Dabei stehen unternehmensinterne Anwendungen (z. B. Prozess- und Produktionsoptimierung, Personaleinsatz, Finanz- und Risikocontrolling) gleichermaßen im Fokus wie kundenorientierte Anwendungen, etwa in Marketing und Vertrieb. Welche Verheißungen mit Big Data-Analysen in der IT-Branche insoweit verbunden werden, machen Szenarien auf der Internetseite der Messe CeBIT deutlich, die im Jahr 2014 dem „Top-Thema“ Big Data unter dem Schlagwort „Datability“ gewidmet ist:

> „Im Einzelhandel können über die Überwachungskameras zum Beispiel die Kundenbewegungen im Shop ausgewertet werden, woraus sich wiederum Produktplatzierungen perfektionieren lassen. Theoretisch können Kameras auch erfassen, ob der Kunde allein im Geschäft ist oder zu welcher Tageszeit vielleicht eher die Mutter mit Kind einkauft. Zielgruppengenau kann nun Werbung über Displays oder Lautsprecher … eingespielt werden. … Auch ist über die Auswertung von Kundendaten eine viel gezieltere Personalplanung möglich. Banken können über die CRM-Systeme[14] ganz genau feststellen, welcher Kundentyp an welchen Tagen und zu welcher Uhrzeit bevorzugt die Geschäftsräume aufsucht und welche Abschlüsse tätigt. Dementsprechend kann das ohnehin in Gleitzeit arbeitende Fachpersonal besser auf die Filialen und Arbeitszeiten aufgeteilt werden. … Auch die Auswertung von Social-Media-Kanälen kann weitaus mehr Relevanz als reine Marketingaspekte haben. Über die Überwachung von Keywords lässt sich recht schnell ein Fehler in der Produktion eines Produkts feststellen, wenn sich Käufer zum Beispiel via Twitter über eine mangelnde Qualität beschweren. … Die jüngsten Automobilgenerationen werden für den in den USA obligatorischen Notruf mit SIM-Karten ausgerüstet. Hierüber können die Automobilunternehmen zusätzlich die Telemetriedaten der

[13] Zum Begriff siehe auch die Ausarbeitung des Wissenschaftlichen Dienstes des Deutschen Bundestags vom 6. November 2013: *http://www.bundestag.de/dokumente/analysen/2013/Big_Data.pdf*

[14] CRM = Customer Relationship Management (Management von Kundenbeziehungen, z. B. mit Hilfe von Kundendatenbanken)

Fahrzeuge abrufen und … über die gesammelten Daten aller Fahrzeuge Unregelmäßigkeiten vorab erkennen und Fahrzeuge in die Werkstatt rufen, bevor ein Schaden eintritt…
Diese kleinen Beispiele zeigen die vielfältige Einsetzbarkeit von Big Data Analysen. Durch den Einsatz von Technologien wie RFID, GPS, Kameras oder Internet-Suchmaschinen lassen sich beliebig viele Informationen abfragen und verwerten. Die Möglichkeiten sprengen alle klassischen Datenerhebungen aus Marktanalysen oder ‚repräsentativen' Umfragen, denn oftmals ergeben sich nun die wirklich spannenden Fragen erst bei der Sichtung und Auswertung der bereits vorhandenen, aber bislang ungenutzten Daten."

Die Energiewirtschaft sieht Anwendungsbereiche von Big Data etwa im Zusammenhang mit der Optimierung einer intelligenten Energieverbrauchssteuerung (Smart Metering). Die Logistikbranche erwartet bessere Stauprognosen und Fahrzeugauslastungen; zum Beispiel will der Hamburger Hafen - wie das Nachrichtenmagazin „Der Spiegel" in seiner dem Thema Big Data gewidmeten Ausgabe vom 13. Mai 2013 berichtete - trotz flächenmäßiger Begrenzung seinen Containerumschlag mit Hilfe einer totalen Vernetzung („smart port") bis 2025 verdreifachen. Das öffentliche Gesundheitswesen und die Pharmaindustrie erhoffen sich frühzeitige Erkenntnisse über die Ausbreitung von Epidemien, wenn in sozialen Netzwerken entsprechende Meldungen verbreitet werden. Die Charité in Berlin will umfangreiche Datenanalysen in Echtzeit einsetzen, um dem Arzt bei Krebspatienten praktisch am Krankenbett die Wahl der richtigen Therapie zu erleichtern. Der öffentliche Verkehrssektor erwartet von der Echtzeitanalyse der Verkehrsströme eine bessere Vernetzung der Verkehrsträger, eine effizientere Auslastung der Straßen und frühzeitige Hinweise auf Störungen, Schäden und Reparaturbedarf. Als Beispiel wird in diesem Zusammenhang das intelligente Verkehrssystem der Stadt Stockholm genannt, das durch Integration von Verkehrs- und Wetterdaten mit Hilfe von GPS, Sensoren, Unfall- und Staumeldungen, Videotechnik usw. zu 20 % weniger Verkehr, 50 % kürzeren Fahrzeiten und einem Rückgang der Emissionen von 20 % geführt habe. Angesichts dieser und ähnlicher Einsatzszenarien verwundert es nicht, dass Unternehmen nach Umfragen das Thema Big Data als wichtig ansehen und verstärkt in entsprechende Technik investieren. So soll nach Schätzungen des Branchenverbandes BITKOM der deutsche Big-Data-Markt im Jahr 2013 auf rd. 650 Mio. € und damit um 85 % gegenüber dem Vorjahr angewachsen sein; bis 2016 soll er auf rd. 1,7 Mrd. € weiter wachsen. Die Bevölkerung weiß hingegen mit dem Begriff Big Data noch nicht viel anzufangen; nach BITKOM-Umfragen vom Frühjahr 2013 wussten nur 15 % der Befragten, was der Begriff bedeutet, und jeder Vierte gab an, dass ihm die Analyse großer Datenmengen wohl keinen persönlichen Vorteil bringen werde. Selbst in der Politik haben Big-Data-Anwendungen Einzug gehalten: So soll der amerikanische Präsident 2012 in seinem Wahlkampf 50 Datenanalytiker eingesetzt haben, um mit Hilfe detaillierter Datenanalysen die besonders umkämpften Wählergruppen erheblich zielgenauer ansprechen zu können.

Die Einsatzszenarien beleuchten zugleich die datenschutzrechtlichen Risiken, die mit der Analyse großer Datenbestände einhergehen können, sobald personenbezogene Daten einbezogen werden. Je mehr Daten und je mehr Auswertungsmöglichkeiten, desto größer die Gefahr des Missbrauchs und des Kontrollverlusts. Nicht von ungefähr stand eine gemeinsame Veranstaltung des Bundesverbraucherschutzministeriums und von BITKOM anlässlich des „Safer Internet Day" am 5. Februar 2013 in Berlin unter dem Motto „Big Data - Goldmine oder Dynamit?". Dabei wurde zutreffend darauf hingewiesen, dass die Akzeptanz der Bürger für umfangreiche Datenanalysen sich nur gewinnen lasse, wenn der Datenschutz auf hohem Niveau sichergestellt und gleich beim Design der Big-Data-Anwendungen berücksichtigt werde. Eine massenhafte Auswertung dürfe es nur bei effektiv anonymisierten Daten geben. Die Auswertung personenbezogener Daten durch Big-Data-Anwendungen kann in der Tat mit zentralen datenschutzrechtlichen Prinzipien, wie dem Grundrecht auf informationelle Selbstbestimmung, dem Schutz personenbezogener Daten, dem Grundsatz der Verhältnismäßigkeit, der Pflicht zur Transparenz und insbesondere der Zweckbindung von erhobenen Daten kollidieren. Wenn es zutrifft, dass sich bei Big Data Ziel und Zweck der Analy-

se erst nach der Erhebung im Rahmen der Sichtung und Auswertung der Daten herauskristallisieren, dann steht das in einem Spannungsverhältnis zu dem datenschutzrechtlichen Postulat, dass bereits die Datenerhebung zu einem bestimmten, ausdrücklich benannten und überdies rechtmäßigen Zweck erfolgen muss und die Daten anschließend nicht für beliebige andere Zwecke ausgewertet werden dürfen (vgl. auch Artikel 6 Absatz 1 b der EU-Datenschutzrichtlinie 95/46/EG). Diese Klippe kann in der Regel rechtskonform auch nicht mit Hilfe von Einwilligungen überwunden werden, weil diese bei unbestimmten Nutzungszwecken zwangsläufig rechtlich zu unbestimmt ausfallen, wie die gerichtlichen Auseinandersetzungen großer (häufig US-amerikanischer) Internetkonzerne mit den deutschen Verbraucherzentralen um die Rechtsgültigkeit von Allgemeinen Geschäftsbedingungen oder Datenschutzbestimmungen immer wieder deutlich machen.

Nüchtern betrachtet zielen die von der Industrie propagierten Datenanalysen häufig nicht auf personenbezogene Daten, so dass zunächst der Grundsatz der Datensparsamkeit, also auch des Verzichts auf personenbezogene Daten, beim Design einer Big-Data-Anwendung beachtet werden sollte. Die Auswertung der digitalen Nutzerspuren kann - wie europäische Internetanbieter gezeigt haben - durchaus so aggregiert werden, dass im Internet z. B. gezielte Werbung datenschutzkonform geschaltet werden kann. Wichtig ist bei allen Formen der Anonymisierung oder Pseudonymisierung im Rahmen von Big Data, dass eine Re-Identifizierung im Nachhinein nicht mehr möglich ist. Dies ist - je mächtiger die Analysewerkzeuge und je ökonomisch wertvoller Personenprofile in Zukunft werden - eine erhebliche Herausforderung. Manche Forscher halten anonymisierte Personenprofile allerdings für eine Illusion. So seien zum Beispiel unsere Mobilitätsmuster so verschieden, dass sie recht einfach und mit einer Trefferquote von 95 % Individuen zuzuordnen sind. Und 33 Bits an Information reichten uns, um eine Person eindeutig zu identifizieren.

Die **Artikel-29-Gruppe**, der Zusammenschluss der europäischen Datenschutzaufsichtsbehörden, hat am 2. April 2013 eine Stellungnahme (opinion) in Form eines Arbeitspapiers (working paper) zum Thema Zweckbindung (purpose limitation) veröffentlicht[15], die auch für das Thema Big Data von zentraler Bedeutung ist. Darin werden mehrere Beispiele gegeben, welche Anforderungen an die Angabe von „festgelegten, eindeutigen und rechtmäßigen Zwecken“ i. S. der Europäischen Datenschutzrichtlinie zu stellen sind; danach sind heute verbreitete vage Zweckbeschreibungen wie „Verbesserung der Nutzungserfahrung“ oder „für Werbezwecke“ nicht ausreichend. Eine etwaige Zweckänderung bedarf nach Auffassung der Artikel-29-Gruppe einer sorgfältigen Analyse im Einzelfall, um festzustellen, ob eine Verarbeitung für einen anderen Zweck mit dem ursprünglichen Zweck vereinbar ist; dabei seien vier zentrale Punkte zu berücksichtigen:

- Die Beziehung zwischen dem ursprünglichen Zweck der Datenerhebung und dem Zweck der weiteren Verarbeitung,
- der Kontext, in dem die Daten erhoben wurden, und die angemessenen Erwartungen der betroffenen Person bezüglich der weiteren Nutzung der Daten,
- die Art der Daten und die Auswirkungen einer weiteren Verarbeitung auf die betroffenen Personen, sowie
- die Sicherheitsmaßnahmen, die die verantwortliche Stelle vorgenommen hat, um eine faire Datenverarbeitung zu gewährleisten und einer unangemessenen Beeinträchtigung der Betroffenen vorzubeugen.

Soweit es bei der Datenanalyse (nur) um die Sichtbarmachung von Informationstendenzen und -beziehungen gehe, seien die technischen und organisatorischen Sicherheitsmaßnahmen der verantwortlichen Stellen von zentraler Bedeutung; hierbei sei eine komplette, funktionale Trennung der Verarbeitung von personenbezogenen Daten für Big-Data-Zwecke sicherzustellen sowie deren Vertraulichkeit und Sicherheit zu garantieren. Soweit die Verarbeitung von Big Data hingegen ein-

[15] *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf*

zelne Personen betreffe, werde fast immer eine spezifische Einwilligung („opt-in“) erforderlich sein, zum Beispiel für die Profilbildung mittels verhaltensbasierter Werbung und die digitale Marktforschung durch Individualverfolgung. Unternehmen sollten dabei betroffenen Personen und Kunden leichten Zugang zu solchen Profilen gewähren und die zugrunde liegenden Entscheidungskriterien offenlegen. Die Artikel-29-Gruppe hat als Ergebnis ihrer Beratungen konkrete **Änderungen am Entwurf der EU-Datenschutz-Grundverordnung** vorgeschlagen, um die o. g. Vereinbarkeitsanalyse in dem Regelungswerk zu verankern. Insgesamt hat auch diese Ausarbeitung deutlich gemacht, dass für die datenschutzkonforme Ausgestaltung von Big-Data-Anwendungen noch erhebliche konzeptionelle und technisch-organisatorische Arbeiten zu leisten sind.

Big Data steht aber heute nicht mehr nur für die Verheißungen der Wirtschaft, sondern auch für die Rasterung der Internetdaten durch die **Geheimdienste** (dazu siehe Kapitel 1.1). Denn im Grunde kommt hier die gleiche Technik zur Anwendung. Diese zielt explizit allerdings nicht auf die statistische Auswertung anonymisierter Daten zu Marktforschungszwecken ab, sondern direkt auf personenbezogene Daten in allen denkbaren Zusammenhängen. Die NSA setzt für Zwecke des Data Mining beispielsweise ein durch Edward Snowden bekanntgewordenes Computersystem namens BOUNDLESS INFORMANT ein, das aus einer Fülle nachrichtendienstlicher Daten (etwa E-Mails und Telefonmetadaten), die mit Hilfe des Programms PRISM aus dem weltweiten Datenstrom herausgeholt wurden, signifikante Zusammenhänge herausfiltern soll. Das Programm und die dahinterstehende Hardware sollen so mächtig sein, dass die Auswertung der Daten fast in Echtzeit möglich sei. Allein im März 2013 soll die NSA 97 Mrd. Datensätze weltweit gesammelt haben.

Aber nicht nur die Tätigkeit der Geheimdienste, auch die anderer Sicherheitsbehörden soll durch Big-Data-Anwendungen erleichtert werden. Was in dem Film „Minority Report“ von Steven Spielberg aus dem Jahr 2002 noch wie Science Fiction klang, versucht die **Polizei** in einigen Städten der USA seit 2010 bereits in die Tat umzusetzen: Mit Hilfe moderner Datenanalyse will sie vorhersagen, wo und wann Verbrechen geschehen, um vorher da zu sein und den Täter verhaften zu können. „Predictive Policing“ nennt sich das Verfahren, bei dem Computer täglich mit Statistiken über Verbrechen und Verbrecher, aber auch mit zahllosen anderen Daten, etwa über das Wetter oder die Nähe zu Buslinien, gefüttert werden und anschließend nach wiederkehrenden Mustern suchen sollen. Das mache die Vorhersage über Zeitpunkt und Tatort künftiger krimineller Akte viel zuverlässiger als früher. In Deutschland soll nach Medienberichten „predictive policing“ noch kein Thema sein und sich die Polizei nicht als Hellseher betätigen wollen. Ich hoffe, dass dies so bleibt und das vom Bundesverfassungsgericht verhängte Verbot einer Totalüberwachung weiterhin Maßstab staatlichen Handelns sein wird.

Big Data ist mit oder ohne Big Brother eine erhebliche Herausforderung für den Datenschutz der Zukunft. Auch hier sind klare Rechtsgrundlagen auf europäischer Ebene dringend erforderlich.

1.3 Europäischer und internationaler Datenschutz

1.3.1 Die EU-Datenschutz-Grundverordnung - eine schwere Geburt

Mit Spannung blickt die Welt des Datenschutzes spätestens seit dem 25. Januar 2012 auf Brüssel und Straßburg. Denn dort soll derzeit im Ringen zwischen Europäischer Kommission, Europäischem Parlament und den Mitgliedsstaaten ein einheitliches und zeitgemäßes Datenschutzrecht für ganz Europa entstehen. Schon aufgrund des Umfangs und der Komplexität der Materie und der Vielzahl berührter (sich häufig widersprechender) Interessen und beteiligter Akteure überrascht es kaum, dass der Weg zu einer Einigung im europäischen Gesetzgebungsverfahren steinig ist. Die Konferenz der deutschen Datenschutzbeauftragten hat sich wieder aktiv in die rechtspolitische Diskussion um das neue europäische *Datenschutzrecht eingebracht.*

Am 25. Januar 2012 hat die EU-Kommission den Entwurf für eine **Datenschutz-Grundverordnung** (DS-GVO, KOM [2012] 11) veröffentlicht, die die Maßstäbe für den Schutz personenbezogener Daten in der EU künftig vereinheitlichen soll (vgl. auch BR-Drs. 52/12 und LT-Drs. 15/1302). Das europäische Gesetzgebungsverfahren hierzu befindet sich inzwischen in der entscheidenden Phase.

Im **Europäischen Parlament** ist der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) federführend für die Datenschutz-Grundverordnung zuständig. Der LIBE-Ausschuss hat am 9. und 10. Oktober 2012 eine interparlamentarische Expertenanhörung durchgeführt. Am 17. Dezember 2012 hat der Berichterstatter des LIBE-Ausschusses, Jan-Philipp Albrecht, einen Berichtsentwurf für den LIBE-Ausschuss vorgelegt. Die Datenschutz-Grundverordnung wurde außer im LIBE-Ausschuss auch in den Ausschüssen für Industrie, Forschung und Energie (ITRE), im Rechtsausschuss (JURI), im Ausschuss für Beschäftigung und Soziales (EMPL), im Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO) sowie im Ausschuss für Wirtschaft und Finanzen (ECON) behandelt. Die Mitglieder der genannten Ausschüsse haben insgesamt über 4.000 Änderungsvorschläge zur Datenschutz-Grundverordnung in Form von Berichtsentwürfen (draft opinions und amendments) und abschließender Berichte (opinions) vorgelegt. Am 21. Oktober 2013 haben sich alle größeren Fraktionen des Europäischen Parlaments im federführenden LIBE-Ausschuss auf eine Kompromissfassung der DS-GVO geeinigt und zugleich dem Berichterstatter des LIBE-Ausschusses ein Mandat erteilt, ohne erste Lesung im Plenum des Europäischen Parlaments direkte Verhandlungen mit dem Rat und der Kommission aufzunehmen (sog. Trilog). Sobald zwischen LIBE-Ausschuss, Rat und Kommission eine Einigung erzielt wird, wird der LIBE-Ausschuss dem Plenum des Europäischen Parlaments die Angelegenheit zur Diskussion und Entscheidung vorlegen. Das Europäische Parlament hofft, die Gesetzesinitiative noch vor den Neuwahlen im Mai 2014 unter Dach und Fach bringen zu können.

Aus der am 21. Oktober 2013 beschlossenen Kompromissfassung des Europäischen Parlaments zur DS-GVO sind vor allem folgende Punkte hervorzuheben:

- Das Erfordernis einer **expliziten Einwilligung** von Betroffenen. Internetanbieter sollen nur dann berechtigt sein, Nutzungsprofile zu erstellen, wenn die Betroffenen, z. B. durch die Privatsphäre-Einstellung ihres Internetbrowsers, ihr Einverständnis hiermit zum Ausdruck bringen;
- **die Bestellung eines betrieblichen Datenschutzbeauftragten** und festen Vertreters in der EU (letzteres nur für außereuropäische Unternehmen) sowie die Durchführung von Risikoanalysen und Folgeabschätzungen ist für alle Unternehmen verpflichtend, die jährlich Daten von **mehr als 5.000 Betroffenen** verarbeiten;
- die Weitergabe personenbezogener Daten an Behörden in Drittstaaten darf nur noch auf der Basis von Rechtshilfeabkommen oder internationalen Vereinbarungen und bei voller Transparenz gegenüber Aufsichtsbehörden und Betroffenen im Einzelfall erfolgen (sog. „**Anti-FISA-Artikel**“);
- der **Zugang zu Dienstleistungen und die Durchführung von Verträgen** darf nicht von der Einwilligung des Betroffenen in eine Datenverarbeitung zu ganz anderen Zwecken abhängig gemacht werden;
- **Anhebung des Sanktionsrahmens** für Geldbußen auf 100 Mio. € oder 5 % des weltweiten Jahresumsatzes eines Unternehmens;
- Aufnahme eines **Mindeststandards** für die von den Mitgliedsstaaten zu treffenden Regelungen **zum Beschäftigtendatenschutz** (u. a. Verpflichtung des Arbeitgebers zur Regelung der privaten Nutzung dienstlicher Telekommunikationseinrichtungen und Verbot sog. „schwarzer Listen“);
- **Stärkung des Europäischen Datenschutzausschusses**: Im Interesse eines einheitlichen Verwaltungsvollzugs in Europa soll dieser mit einer Zwei-Drittel-Mehrheit für die Aufsichtsbehörden verbindliche Entscheidungen treffen können.

Der **Rat** hat in der zweiten Jahreshälfte 2012 unter zypriotischer Ratspräsidentschaft eine erste Lesung der Datenschutz-Grundverordnung abschließen können und im Zuge dessen eine kommentierte Gesamtfassung des Textes erstellt. Im Jahr 2013 tagte die zuständige Ratsarbeitsgruppe (DAPIX) zunächst unter irischem Vorsitz. Beginnend mit der DAPIX-Sitzung am 13. und 14. März 2013, bei der die Artikel 1 bis 10 DS-GVO verhandelt wurden, hat die irische Ratspräsidentschaft eine zweite Lesung eingeleitet, die auch unter litauischer Präsidentschaft in der zweiten Jahreshälfte 2013 noch nicht zum Abschluss gekommen ist, sodass ein endgültiges Verhandlungsmandat des Rates bis zum Jahresende noch nicht zustande kam. Ein Schwerpunktthema, das im Rat zuletzt besonders intensiv und kontrovers diskutiert wurde, ist die vorgesehene zentrale Anlaufstelle (sog. one-stop-shop) und sind die damit verbundenen Fragen der Zuständigkeit, der Befugnisse der Aufsichtsbehörden sowie der Abstimmung und Zusammenarbeit zwischen ihnen. Sobald eine Einigung im Rat erzielt wird, können die Erörterungen mit dem Parlament und der Kommission beginnen. Entgegen früheren Erwartungen wird dies aber wohl nicht mehr in der laufenden Legislaturperiode des Europaparlaments der Fall sein, denn nach der Sitzung des EU-Ministerrats am 24./25. Oktober 2013 erklärten der französische Präsident und die deutsche Bundeskanzlerin gegenüber der Presse, die „Zielmarke“ für die EU-Datenschutzreform sei mit Rücksicht auf die Europawahlen auf „Ende 2014 oder Anfang 2015“ verschoben worden. Der Berichterstatter des LIBE-Ausschusses und andere Beobachter warfen der Bundesregierung daraufhin eine „Blockade-Haltung“ und eine Verschleppungstaktik vor; so habe die deutsche Delegation in der Ratsarbeitsgruppe so viele Prüfvorbehalte angebracht wie kaum eine andere Nation. Das Bundesinnenministerium wies die Vorwürfe zurück und erklärte, dass noch viel handwerkliche Arbeit notwendig sei, um den Entwurf der EU-Datenschutz-Grundverordnung praxistauglich zu machen.

Die **Europäische Kommission** betonte im Berichtszeitraum weiterhin die Vorteile der vorgesehenen Datenschutzreform für die Wirtschaft (geschätzte Einsparungen von ca. 2,3 Mrd. € jährlich) und wies im übrigen darauf hin, dass der Abschluss des europäischen Gesetzgebungsverfahrens noch in dieser Legislaturperiode des Europäischen Parlaments unabdingbar sei. In Bezug auf die vielfach erhobene Forderung, die Zahl der delegierten Rechtsakte und Durchführungsrechtsakte drastisch zu beschränken, hat die Kommission inzwischen Kompromissbereitschaft erkennen lassen. Der vom Parlament vorgeschlagene „Anti-FISA-Artikel“ wird von der Kommission ausdrücklich begrüßt.

Die deutschen **Datenschutzaufsichtsbehörden des Bundes und der Länder** haben sich im Berichtszeitraum mit Entschließungen (Entschließungen vom 21./22. März 2012, 7./8. November 2012 sowie 13./14. März 2013, vgl. Anhänge 3, 11 und 16) und einer umfangreichen Stellungnahme vom 11. Juni 2012 (abrufbar auf meiner Internetseite unter http://www.baden-wuerttemberg.datenschutz.de/eu-datenschutzreform) in die laufende rechtspolitische Debatte eingebracht. Nachdem die Berichtsentwürfe der mitberatenden Ausschüsse im Europäischen Parlament teilweise Änderungsvorschläge enthielten, die eine Absenkung des derzeitigen Datenschutzniveau der europäischen Datenschutzrichtlinie von 1995 bedeutet hätten - so wurde etwa vorgeschlagen, bestimmte Bußgeldtatbestände zu streichen oder die Höhe der maximal möglichen Bußgelder abzusenken -, haben die Datenschutzbeauftragten des Bundes und der Länder alle Beteiligten des europäischen Gesetzgebungsverfahrens insbesondere daran erinnert, dass das Ziel der Datenschutzreform nicht die Absenkung, sondern die Weiterentwicklung, Erweiterung und Stärkung des derzeit gültigen Datenschutzrechts sein müsse.

Die Entschließungen zeigen die wesentlichen Erörterungspunkte, die im laufenden europäischen Gesetzgebungsverfahren von Bedeutung sind, auf. Dabei handelt es sich um

- die Definition von personenbezogenen Daten und insbesondere den notwendigen Einbezug

pseudonymer Daten und von Identifizierungsmerkmalen wie IP-Adressen,
- die Rechtsgrundlagen für die Datenverarbeitung (insbesondere das berechtigte Interesse und die Einwilligung),
- die Zweckbindung personenbezogener Daten,
- die Beschränkung der Profilbildung und gesetzliche Regelung der Tätigkeit von Auskunfteien und des Scoring,
- die Aufnahme der elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technische und organisatorische Maßnahmen,
- die obligatorische Einführung betrieblicher Datenschutzbeauftragter in ganz Europa,
- die Frage der federführenden Behörde bzw. der Kontrollzuständigkeit,
- einfache, unbürokratische und praktikable Formen der Zusammenarbeit und Abstimmung der Aufsichtsbehörden untereinander sowie des europaweiten Vollzugs verwaltungsbehördlicher Entscheidungen
- Öffnungsklauseln für die nationalen Gesetzgeber, durch die diese zumindest für ihre jeweiligen öffentlichen Verwaltungen ein höheres Datenschutzniveau durch nationales Recht vorsehen können, wenn es im Hinblick auf die Sensitivität der Daten oder sonstige Umstände erforderlich ist,
- die Festlegung europaweit einheitlicher qualifizierter Mindestanforderungen für den Beschäftigtendatenschutz,
- wirksame, flexible und spürbare Bußgeldregelungen,
- eine Reduzierung der in der EU-Datenschutz-Grundverordnung enthaltenen Ermächtigungen der Kommission zum Erlass tertiärer Rechtsakte auf das unbedingt erforderliche Maß,
- die völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission, wodurch ein Letztentscheidungsrecht der Kommission ausgeschlossen ist.

Die Chance, ein einheitliches hohes Datenschutzniveau für ganz Europa zu schaffen, sollte jetzt ergriffen werden. Die Beteiligten am europäischen Gesetzgebungsverfahren stehen in der Pflicht, sich auf Lösungen zu einigen, die die bewährten hohen deutschen Datenschutzstandards soweit wie möglich erhalten, den Herausforderungen des Internets und der Globalisierung wirksam begegnen, praxistauglich sind, Rechtsklarheit schaffen und das Persönlichkeitsrecht der Bürgerinnen und Bürger, zu dessen Gewährleistung die europäische Verfassung verpflichtet, stärken.

1.3.2 Die Europäische Datenschutzrichtlinie für Polizei und Justiz

Am 25. Januar 2012 hat die Europäische Kommission ihre Überlegungen für eine Datenschutzreform in der Europäischen Union vorgestellt. Für den Bereich der polizeilichen und justiziellen Zusammenarbeit schlug sie eine Richtlinie (sog. JI-Richtlinie, vgl. BR-Drs. 51/12) vor, mit der einerseits der Schutz der personenbezogenen Daten, andererseits aber auch der Datenaustausch zwischen den zuständigen Behörden der Mitgliedstaaten gewährleistet werden soll. Die Richtlinie erlaubt zudem, die Besonderheiten des jeweiligen Gefahrenabwehr- und Strafprozessrechts in einem Mitgliedstaat zu berücksichtigen.

Bereits in ihrer Entschließung vom 21./22. März 2012 (vgl. Anhang 2) hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert, dass der Richtlinienentwurf hinter dem Entwurf der Datenschutz-Grundverordnung und dem deutschen Datenschutzniveau zurückbleibt. In einer eingehenden Stellungnahme schlug die Konferenz im Juni 2012 zudem folgende Kernpunkte zur Verbesserung der datenschutzrechtlichen Elemente des Entwurfs vor:

- Festschreibung eines Mindeststandards für ein möglichst hohes Datenschutzniveau mit der Möglichkeit, in den Mitgliedstaaten datenschutzfreundlichere Regelungen zu treffen;
- Ergänzung und Präzisierung der Grundsätze der Datenverarbeitung, insbesondere bezüglich der Erforderlichkeit sowie der Einhaltung der technischen und organisatorischen Maßnahmen;

- offenere Regelung der schutzbedürftigen Datenkategorien;
- Reduzierung der Möglichkeiten, Betroffenenrechte einzuschränken;
- Verpflichtung der Verantwortlichen zur Folgenabschätzung einer Datenverarbeitung;
- Begrenzung der Ausnahmeregelungen für Übermittlungen in Drittstaaten oder an internationale Organisationen.

Aufgrund der weiteren Diskussion hat die Konferenz in einer Entschließung vom 7./8. November 2012 nochmals an die Bundesregierung appelliert, sich im Rat für ein harmonisiertes Datenschutzrecht auf hohem Niveau einzusetzen (vgl. Anhang 9).

Während die Diskussion über den Entwurf der Datenschutz-Grundverordnung mit einer Vielzahl von Änderungsvorschlägen im Europäischen Parlament öffentlichkeitswirksam fortgesetzt wurde, blieb das Schicksal des Richtlinienentwurfs lange unklar. Immerhin war aus dem Europäischen Parlament zu hören, dass an einer „Paketlösung", d. h. dem Ziel einer gleichzeitigen Verabschiedung von Grundverordnung und JI-Richtlinie, festgehalten wird.

Mitte Oktober 2013 veröffentlichte der federführende LIBE-Ausschuss des Europäischen Parlaments ein Kompromisspapier zum Richtlinienentwurf, das erfreulicherweise einige der Kernforderungen der Datenschutzkonferenz aufgriff. Entscheidend wird allerdings sein, inwieweit die Forderungen des Europäischen Parlaments in den anschließenden Verhandlungen (sog. Trilog) mit Kommission und Rat Bestand haben werden.

Bis zur Verabschiedung der Richtlinie ist noch eine längere Wegstrecke zurückzulegen. Da sie zudem erst zwei Jahre danach in Kraft treten soll, ist zu hoffen, dass bis dahin Einigkeit über ein höheres Datenschutzniveau erreicht werden kann

1.3.3 Elektronische Identifizierung mit datenschutzrechtlichen Defiziten

Der Verordnungsentwurf der EU-Kommission **„Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" (eIAS),** COM 2012 (238), hat mit dem Industrieausschuss des EU-Parlaments am 15. Oktober 2013 eine weitere Hürde genommen. Die eIAS soll die Nutzung elektronischer Signaturen und vergleichbarer Identifikationssysteme vereinfachen und harmonisieren, um Unternehmen, Behörden und Bürgern die europaweite elektronische Unterzeichnung und Zertifizierung von Dokumenten zu ermöglichen. Dazu sollen alle EU-Mitgliedsstaaten verpflichtet werden, die Systeme zur elektronischen Identifikation anderer EU-Mitgliedsstaaten, und damit auch die De-Mail und die eID-Funktion des neuen Personalausweises, gegenseitig anzuerkennen. In dem Verordnungsentwurf sind Regelungen zu elektronischen Signaturen und Zeitstempeln, elektronischen Siegeln und elektronischen Dokumenten normiert.

Durch die eIAS soll die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signaturrichtlinie) reformiert und ein umfassender EU-weiter Anwendungsbereich für sichere, vertrauenswürdige und einfach zu nutzende elektronische Transaktionen, für die elektronische Identifizierung und Authentifizierung sowie für elektronische Signaturen eröffnet werden.

So begrüßenswert dieses Ziel des Verordnungsentwurfs ist, so nachbesserungsbedürftig ist er aus datenschutzrechtlicher Sicht. In den Regelungen des Verordnungsentwurfs zur elektronischen Identifikation werden weder eine konkrete Definition von Identifikationsdaten noch handlungsbegrenzende Maßstäbe aus dem Bereich der Datenvermeidung und Datensparsamkeit geliefert. Der Verordnungsentwurf sollte daher um Regelungen nach dem Beispiel des § 18 Absatz 4 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) erweitert werden, wonach ein

Diensteanbieter zwar auch personenbeziehbare Daten wie Tag der Geburt, Anschrift, Angabe, ob ein bestimmtes Alter über- oder unterschritten wird, oder die Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht, abfragen kann, der Diensteanbieter dafür aber ein berechtigtes Interesse begründen muss. Sind bestimmte personenbezogene Daten für den Diensteanbieter erforderlich, erhält er vom Bundesverwaltungsamt ein Zertifikat, das ihn aber nur zur Abfrage der erforderlichen Daten berechtigt.

Der Verordnungsentwurf weist zudem an einer weiteren entscheidenden Stelle erhebliche Schwächen auf. Die sog. Root Certificate Authority und der „qualifizierte“ Vertrauensdiensteanbieter können zwar zukünftig „qualifizierte“ Zertifikatssignaturen ausgeben. Diese genügen aber nicht mehr den Anforderungen des § 2 Nr. 3 i. V. m. § 7 des Gesetzes über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) und entsprechen damit nicht mehr der im deutschen Rechtsraum bekannten Qualität, sondern sind eher mit den Anforderungen vergleichbar, die nach § 2 Nr. 2 SigG derzeit an die fortgeschrittene Signatur gestellt werden. Qualifizierte Signaturen unterscheiden sich von fortgeschrittenen Signaturen unter anderem dadurch, dass qualifizierte Signaturen nach § 2 Nr. 3a SigG mit einem Zeitstempel versehen sind. Dieser Zeitstempel ist bei der fortgeschrittenen elektronischen Signatur nicht erforderlich. Damit können „qualifizierte“ Zertifikatssignaturen i. S. des Verordnungsentwurfs, die keinen Zeitstempel aufweisen müssen, nicht mehr auf ihre Richtigkeit zum Zeitpunkt des Signaturvorgangs kontrolliert werden. Das Vertrauen in qualifizierte elektronische Signaturen wird entscheidend geschwächt. Auch die beiden deutschen Konzepte ArchiSig und ArchiSafe zur elektronischen Beweissicherung elektronischer Signaturen und zur Archivierung signierter oder zeitgestempelter Dokumente könnten dann nicht mehr eingesetzt werden.

Im Allgemeinen sind für die Verwendung von Signaturen, Siegeln und Zeitstempeln im Rahmen des eGovernments hohe Sicherheitsstandards zu fordern. Diese können nur mit der qualifizierten Signatur, dem qualifizierten Siegel und dem qualifizierten Zeitstempel verwirklicht werden. Diese zusammen sind der „manuellen“ Unterschrift gleichgestellt. Die zukünftige Verordnung sollte daher nicht unter diesem Niveau bleiben. „Fortgeschrittene“ Signaturen, Siegel oder Zeitstempel sind eben nicht „qualifiziert“ und daher nicht ausreichend. Die durch die Verordnung beabsichtigte Rechtssicherheit ist auf diese Weise nicht zu gewährleisten.

Zur Sicherstellung eines angemessenen datenschutzrechtlichen Niveaus sollte der Verordnungsentwurf um Regelungen ergänzt werden, die § 18 PAuswG entsprechen.

1.3.4 Flugpassagierdaten für die USA - jetzt auch für andere Staaten?

Ende des Jahres 2011 hatte das Europäische Parlament endgültig der Übermittlung der Flugpassagierdaten (Passenger Name Record - PNR) an die Vereinigten Staaten von Amerika zugestimmt, eine aus datenschutzrechtlicher Sicht unbefriedigende Regelung. Dadurch erhalten die Vereinigten Staaten nicht nur die aus jedem Pass auslesbaren Daten zu einem Flugpassagier, sondern auch eine Vielzahl weiterer Informationen über die Person, die eigentlich nur die Fluggesellschaft interessieren sollten. Hierdurch sind offenbar auch bei anderen Staaten Begehrlichkeiten geweckt worden. Darauf hatte ich bereits in meinem 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 32 f.) hingewiesen.

Durch die Umfrage eines andern Landesbeauftragten wurde bekannt, dass die Deutsche Lufthansa aufgrund einer Verordnung der Russischen Föderation die **PNR-Daten** aller Flugpassagiere mitzuteilen habe. Ansonsten ginge sie ihrer Lande- und Überflugsrechte verlustig. Dabei gehe es nicht nur um die Daten der Flugpassagiere, deren Ziel in der Russischen Föderation liegt, sondern auch um die, deren Flug über das Hoheitsgebiet Russlands führt, ohne dort einen Flughafen anzusteuern. Die Verordnung sei bis Ende 2013 ausgesetzt; die Europäische Kommission sei in den Vorgang bereits involviert. Derzeit gehe ich wie mein Kollege davon aus, dass eine Übermittlung

der PNR-Daten mangels einer Vereinbarung zwischen der Europäischen Union und der Russischen Föderation nicht zulässig ist. Die weitere Entwicklung bleibt abzuwarten.

Bereits im Jahr 2009 hatte das Vereinigte Königreich von Großbritannien und Nordirland den Wunsch auf Übermittlung der PNR-Daten geäußert, realisiert wurde dieses bisher nicht, da der europäische Rechtsrahmen dafür keine Handhabe bietet.

Von den PNR-Daten zu unterscheiden sind die Daten, die im Vorab-Passagier-Informationssystem (Advance Passenger Information System, APIS) von einer Fluggesellschaft dem Staat, in dem der Zielflughafen des Flugpassagiers liegt, zu übermitteln sind. Diese **API-Daten** haben nunmehr die Fluggesellschaften bei innereuropäischen Flügen den britischen Behörden mitzuteilen. Auch wenn es bisher dafür keine europäische Regelung gibt, erlaubt es das deutsche Passgesetz (§ 18 Absatz 4), dass diese Daten an einen anderen Staat durch eine nicht-öffentliche Stelle wie eine Fluggesellschaft übermittelt werden:

> Beförderungsunternehmen dürfen personenbezogene Daten aus der maschinenlesbaren Zone des Passes elektronisch nur auslesen und verarbeiten, soweit sie auf Grund internationaler Abkommen oder Einreisebestimmungen zur Mitwirkung an Kontrolltätigkeiten im internationalen Reiseverkehr und zur Übermittlung personenbezogener Daten verpflichtet sind. Biometrische Daten dürfen nicht ausgelesen werden. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung dieser Pflichten nicht mehr erforderlich sind.

Soweit also gesetzliche Bestimmungen in Großbritannien die Mitwirkung der Fluggesellschaften vorschreiben, ist das Auslesen der Daten aus einem deutschen Pass und die Übermittlung an die britischen Einreisebehörden zulässig.

Das wachsende Interesse von Staaten, möglichst viele Daten über Flugpassagiere zu erhalten, führt nicht zuletzt aufgrund der Erfahrungen mit der Dauer der Speicherung der PNR-Daten in den USA zu Vorratsdatenspeicherungen in nicht abschätzbarem Umfang. Die Europäische Union beabsichtigt zudem, durch europäische Verordnungen ein Registrierungsprogramm für Reisende (RTP) und ein Einreise-/Ausreisesystem (EES) zur Erfassung der Einreise- und Ausreisedaten einzuführen. Der Schutz der personenbezogenen Daten scheint nur noch eine bescheidene Rolle im Vergleich zu anderen Zielen der Mitgliedstaaten zu spielen. Der viel beschworene Raum der Freiheit, der Sicherheit und des Rechts in der Europäischen Union, der seit dem Haager Programm von 2004 entwickelt wird, bekommt dadurch eine ganz besondere Note.

1.3.5 Was hat die Bekämpfung von Produkt- und Markenpiraterie mit dem Datenschutz zu tun? Das ACTA-Abkommen

ACTA ad acta! So lauteten die Schlagzeilen im Sommer 2012, als das geplante Übereinkommen zur Bekämpfung der Produkt- und Markenpiraterie nach Massenprotesten vom Europäischen Parlament gekippt wurde. Daran war der Datenschutz nicht ganz schuldlos.

Das **„Anti-Counterfeiting Trade Agreement“ (ACTA)**, das Handelsübereinkommen zur Bekämpfung von Produkt- und Markenpiraterie, bewegte im Berichtszeitraum die Gemüter und führte zu Massenprotesten in mehreren europäischen Staaten sowie in der Netzgemeinde. Weil dabei auch der Datenschutz ins Feld geführt wurde, sei hier kurz darauf eingegangen, obwohl meine Dienststelle mit dem Thema nicht unmittelbar befasst war.

Das internationale Handelsübereinkommen ACTA sollte dem stärkeren Schutz des geistigen Eigentums dienen und andere Abkommen der Welthandelsorganisation ergänzen. Die Verhandlungsinhalte waren erst 2010 auf Druck von Bürgerrechtlern offengelegt worden. Die Anbieter von Telekommunikationsdienstleistungen sollten verpflichtet werden, ihre Kunden im Hinblick auf etwaige Verstöße, z. B. gegen das Urheberrecht, strenger zu überwachen, was vermutlich nicht ohne die Registrierung von IP-Adressen und Verkehrsdaten gegangen wäre. Zwar wurde diese

Verpflichtung später wieder abgeschwächt, der Vertragstext blieb jedoch an vielen Stellen so unbestimmt, dass in der Netzgemeinde die Sorge vor Internetzensur und Netzsperren sowie generell vor einer Überwachung des Internets zunahm und schließlich in reale Straßendemonstrationen umschlug. Im Februar 2012 gingen in ganz Europa Zehntausende auf die Straße, in Stuttgart und Mannheim nach Angaben der Veranstalter jeweils rd. 1.500 Menschen. Die Befürworter des Abkommens, insbesondere Medienunternehmen, hielten die Kritik für überzogen und warnten vor Panikmache. Angesichts der massiven Proteste erklärte das Bundesjustizministerium, dass Deutschland das Abkommen zunächst nicht ratifizieren werde. Auch weitere europäische Staaten stoppten den Ratifizierungsprozess. Die Europäische Kommission teilte schließlich mit, dass sie den Entwurf des Abkommens zunächst durch den Europäischen Gerichtshof im Hinblick auf die Vereinbarkeit mit den europäischen Grundrechten überprüfen lassen wolle. Dazu kam es dann aber nicht mehr, weil das Europäische Parlament am 4. Juli 2012 mit großer Mehrheit das Abkommen ablehnte.

Auch mit dem Ende von ACTA ist das Problem, wie das geistige Eigentum in der digitalen Welt künftig gesichert werden kann, nicht gelöst. Dem Schutz der personenbezogenen Daten sollte in künftigen internationalen Vereinbarungen aber besser Rechnung getragen werden. Zur Vertiefung in die schwierige Thematik sei die Lektüre des Dritten Zwischenberichts der Enquete-Kommission des Deutschen Bundestags „Internet und digitale Gesellschaft", BT-Drs. 17/7899, empfohlen.

1.3.6 FATCA - Die Neugier des großen Bruders ist unerschöpflich

Die heimliche Überwachung deutscher Bürger und Politiker durch die US-amerikanische National Security Agency erscheint umso befremdlicher, als auch ohne derartige Maßnahmen Möglichkeiten zum offiziellen behördlichen Datenaustausch zwischen Deutschland und den USA bestehen oder eingerichtet werden. Dies gilt nicht zuletzt im Bereich der Steuerdaten, insbesondere bei der Umsetzung des amerikanischen Foreign Account Tax Compliance Act (FATCA).

FATCA ist ein 2010 in Kraft getretenes US-Gesetz und verfolgt den Zweck, im Ausland belegene Vermögenswerte von Personen zu erfassen, die in den USA steuerpflichtig sind. Ausländische Finanzinstitute, wie etwa deutsche Banken, Investmentfonds und Versicherungen, sollten sich nach FATCA gegenüber der US-Bundessteuerbehörde (Internal Revenue Service - IRS) durch Einzelvereinbarungen verpflichten, dem IRS steuerlich relevante Kundendaten von „US-Steuerbürgern" zu melden. Zu diesen Daten gehören Name, Adresse, Steueridentifikationsnummer, Konto- und Depotnummern, Kontosalden, Depotbestände und Buchungsdaten. Verweigert ein Finanzinstitut den Abschluss der genannten Vereinbarung mit dem IRS oder kommt es seiner Meldepflicht nicht nach, so soll nach FATCA in den USA eine 30 %ige Quellensteuer auf die Auszahlungen der gesamten US-Kapitalanlagen dieses Instituts erhoben werden. Nach deutschem Recht besteht aber bislang keine Rechtsgrundlage für eine derartige Datenübermittlung durch hiesige Finanzinstitute in die USA.

Zur Umsetzung des FATCA bei gleichzeitiger Vermeidung der Quellensteuer hat das US-Finanzministerium mit dem Bundesministerium der Finanzen (BMF) sowie Frankreich, Großbritannien, Italien und Spanien ein im Juli 2012 veröffentlichtes Musterabkommen erarbeitet. Es sieht auf der Seite der beteiligten europäischen Staaten den Erlass von Durchführungsvorschriften vor, auf deren Grundlage die inländischen Finanzinstitute die nach FATCA geforderten Daten an nationale Steuerbehörden (in Deutschland an das Bundeszentralamt für Steuern - BZSt) zu übermitteln haben. Ein gegenseitiger Datenaustausch zwischen den USA und den nationalen Steuerbehörden soll sodann auf der Grundlage bereits bestehender bilateraler Doppelbesteuerungsabkommen erfolgen. Die USA haben sich im Gegenzug dazu verpflichtet, darauf zu verzichten, dass jedes hiesige Finanzinstitut eine Einzelvereinbarung mit dem IRS abschließt.

Das entsprechende bilaterale Abkommen zwischen Deutschland und den USA wurde im Mai 2013 unterzeichnet. Der Bundesrat hat dem Ratifikationsgesetz im Juli 2013 zugestimmt. Als Durchführungsvorschrift und Befugnisnorm für die Übermittlung der Steuerdaten durch inländische Finanzinstitute an das BZSt wurde in die Abgabenordnung (AO) ein neuer § 117c eingefügt (vgl. BR-Drs. 740/13 S. 41f.). Aufgrund eines Verweises der Vorschrift auf § 150 Absatz 6 AO findet für die Übermittlung an das BZSt ein sicheres Verfahren Anwendung, das das übermittelnde Finanzinstitut authentifiziert und die Vertraulichkeit und Integrität des elektronisch übermittelten Datensatzes gewährleistet. § 117c AO ermächtigt auch das BMF, das Nähere hierzu durch eine Rechtsverordnung zu regeln, die der Zustimmung des Bundesrats bedarf.

Die vorgenannte Änderung der AO erfolgte im Rahmen des Gesetzes vom 18. Dezember 2013 zur Umsetzung der Richtlinie 2011/61/EU über die Verwalter alternativer Investmentfonds (AIFM [Alternative Investment Fund Manager]-Richtlinie), das am 23. Dezember 2013 im Bundesgesetzblatt erschien (vgl. Artikel 13 AIFM-Steuer-Anpassungsgesetz, BGBl. I 2013 S. 4318) und pünktlich am Heiligabend in Kraft trat. Bei der Erarbeitung der Rechtsverordnung des BMF wird darauf zu achten sein, dass die Belange des Datenschutzes hinreichend beachtet werden.

Der amerikanischen Bundessteuerbehörde sind personenbezogene Daten nur auf der Grundlage von Rechtsvorschriften zu übermitteln, die dem Recht auf informationelle Selbstbestimmung hinreichend Rechnung tragen.

1.3.7 Internationaler Datentransfer: Safe Harbor in stürmischen Zeiten

Die Enthüllungen der letzten Monate über einen massenhaften Zugriff angloamerikanischer Geheimdienste auf Daten vorwiegend amerikanischer Internetunternehmen und die elektronische Kommunikation weltweit haben in der Öffentlichkeit und bei deutschen Unternehmen für erhebliche Verunsicherung gesorgt. Die Frage, ob und unter welchen Voraussetzungen ein Transfer personenbezogener Daten in die USA und sonstige Drittstaaten weiterhin datenschutzrechtlich zulässig ist, stellt sich daher aktuell mit besonderer Schärfe, ohne dass sich zufriedenstellende Lösungen abzeichnen. Bereits mit Beschluss vom 28./29. April 2010[16] haben die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis") festgelegt, dass - solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist - auch die exportierenden Unternehmen in Deutschland gewisse Mindestkriterien zu prüfen haben, bevor sie personenbezogene Daten an ein auf der sog. Safe-Harbor-Liste geführtes Unternehmen in einem Drittstaat übermitteln. Aus gegebenem Anlass muss hieran erinnert werden.

Ein Transfer personenbezogener Daten in Drittstaaten wie die USA ist in datenschutzrechtlicher Hinsicht grundsätzlich nur zulässig, wenn neben den allgemeinen Voraussetzungen, die an jede Übermittlung personenbezogener Daten zu stellen sind (z. B. eine Einwilligung des Betroffenen, ein gesetzlicher Erlaubnistatbestand oder ein Vertrag), ein angemessenes Datenschutzniveau beim Datenimporteur, d. h. in dem Drittstaat, besteht und der Datenexporteur ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts der Betroffenen und der Ausübung der damit verbundenen Rechte vorweisen kann. An das allgemeine Erfordernis einer solchen zweistufigen Prüfung bei Datenübermittlungen in Drittstaaten hat der Düsseldorfer Kreis mit Beschluss vom 11./12. September 2013 erinnert (vgl. Anhang 25).

Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts der Betroffenen und der Ausübung der damit verbundenen Rechte können sich aus **(Standard-)Vertragsklauseln**[17] oder verbindli-

[16] vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, Anhang 32
[17] Entscheidung der Kommission Nr. 2001/497/EG v. 15.6.2001 - K(2001) 1539; Entscheidung der Kommission Nr. 2004/915/EG v. 27.12.2004 - K(2004) 5271; Beschluss der Kommission Nr. 2010/87/EU v. 5.2.2012 - K(2010) 593.

chen Unternehmensregelungen (sog. **Binding Corporate Rules, BCR**) ergeben. Für die USA hat die Europäische Kommission im Jahr 2000 durch einen gesetzesgleichen Durchführungsrechtsakt zudem die Möglichkeit eröffnet, die notwendigen Garantien für ein angemessenes Datenschutzniveau durch eine Selbstzertifizierung des Datenimporteurs zu schaffen.[18] Danach können sich Unternehmen in den USA zur Einhaltung datenschutzrechtlicher Prinzipien, durch die in etwa ein den gültigen europäischen Datenschutzvorgaben entsprechendes Datenschutzniveau geschaffen wird, verpflichten und in eine Liste zertifizierter Unternehmen beim US-Handelsministerium eintragen lassen (**Safe Harbor**).

Die **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** hat am 24. Juli 2013 angekündigt, im Hinblick auf die Enthüllungen über Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency, bis zu einer endgültigen Klärung der Vorwürfe keine neuen Genehmigungen für Datenübermittlung in Drittstaaten mehr zu erteilen und zudem zu prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind.

Die **Europäische Kommission** hat vor dem Hintergrund der PRISM-Affäre eine Überprüfung des Safe-Harbor-Abkommens in Angriff genommen und am 27. November 2013 bekannt gegeben, dass sie beabsichtige, eine Entscheidung über eine vorübergehende Aussetzung, inhaltliche Abänderung oder Aufhebung des Rechtsakts zu Safe Harbor erst im Sommer 2014 zu treffen.[19]

Bis dahin wurden der US-Seite dreizehn Empfehlungen an die Hand gegeben, mittels derer der auf Safe Harbor gestützte Datentransfer optimiert werden könne. Diese betreffen:

- eine **verstärkte Information der Betroffenen** auf der Internet-Präsenz der betroffenen Unternehmen, z. B. über den aktuellen Stand der Zertifizierung, den Wortlaut der „privacy policy“ des Unternehmens, Unterauftragsverhältnisse, Beschwerdemöglichkeiten und allgemeine Informationen über im US-Recht vorgesehene Zugriffsmöglichkeiten für US-Geheimdienste;
- eine **Intensivierung der Kontrollen** und verhängten Sanktionen durch die US-Aufsichtsbehörden (U.S. Department of Commerce und U.S. Federal Trade Commission), z. B. die Veröffentlichung festgestellter Datenschutzverstöße, stichprobenartige, anlassunabhängige Vorortkontrollen sowie regelmäßige Nachkontrollen bei festgestellten Verstößen;
- einen Appell an die Behörden der USA, die für die Erfordernisse der **nationalen Sicherheit** vorgesehenen Ausnahmeregelungen künftig nur noch **im unbedingt erforderlichen Umfang** und unter **strikter Beachtung des Gebots der Verhältnismäßigkeit** in Anspruch zu nehmen.

Solange ein Transfer personenbezogener Daten in die USA auf der Grundlage des Safe-Harbor-Rechtsakts der Kommission weiter zulässig ist, stellt sich für alle betroffenen Unternehmen die Frage, wie sie als datenexportierende Stellen ihren **Prüfpflichten** in Bezug auf den Importeur in den USA nachkommen können und was hierfür konkret zu veranlassen ist. Hierzu lässt sich Folgendes sagen:

Für die Prüfung muss zunächst der Status der Eintragung auf der Safe-Harbor-Liste überprüft werden. Das Unternehmen muss als "current" geführt sein. Zudem sollte das US-Unternehmen der Zusammenarbeit mit europäischen Datenschutzbehörden zugestimmt haben. Dies gilt je-

[18] sog. Safe-Harbor-Abkommen, Entscheidung der Kommission Nr. 2000/520/EG v. 26.7.2000 - K(2000) 2441.

[19] European Commission calls on the U.S. to restore trust in EU-U.S. data flows, European Commission - IP/13/1166 27/11/2013; Restoring Trust in EU-US data flows - Frequently Asked Questions, European Commission - MEMO/13/1059 27/11/2013; COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Rebuilding Trust in EU-US Data Flows, COM(2013) 846; COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847.

denfalls dann, wenn Beschäftigtendaten übermittelt werden (vgl. Anhang II, FAQ 9, Frage 4 der Entscheidung der Kommission vom 26. Juli 2000 gemäß der RL 95/46/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/520/EG).

Als weitere **Prüfungsmaßnahmen** kommen zudem in Betracht:

- Prüfung der "privacy policy" des Importeurs: Soweit hier Unklarheiten bestehen, z. B. in Bezug auf Konflikte mit den Safe-Harbor-Grundsätzen oder in Bezug auf die in der policy genannten Verarbeitungszwecke, müssen diese aufgeklärt werden;
- Prüfung, ob die Informationen für die Betroffenen hinreichend sind (vgl. näher dazu Fußnote 2 des Beschlusses der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 28./29. April 2010 in der überarbeiteten Fassung vom 23. August 2010, siehe 30. Tätigkeitsbericht, LT-Drs. 15/955, Anhang 32);
- Prüfung und Test des in der policy beschriebenen Systems zur Durchsetzung von Betroffenenrechten auf Plausibilität und Funktionsfähigkeit;
- Kontaktaufnahme mit Personen, die als Ansprechpartner genannt werden und Befragung zu den entsprechenden Aufgaben;
- im Falle der Auftragsdatenverarbeitung: Sicherstellung, dass Informationen für die Beantwortung z. B. von Auskunftsersuchen an den Auftraggeber in annehmbarer Zeit weitergeleitet werden;
- Prüfung, wie im Falle von Weiterübermittlungen der Daten ("onward transfers") durch den Importeur verfahren wird, d. h. insbesondere die Frage nach existierenden Vertragsmustern für die Weitergabe in Form der Auftragsdatenverarbeitung, Einräumung eines Widerspruchsrechts/Einholung der Einwilligung der Betroffenen.

Die Tätigkeiten, die im Zusammenhang mit dieser Prüfung erfolgen, sollten dokumentiert werden, um die Prüfung auf Anfrage der Aufsichtsbehörde nachweisen zu können.

1.4 Datenschutz auf Bundesebene

1.4.1 Die Weiterentwicklung des Bundesdatenschutzgesetzes (BDSG): Still ruht der See - auch im Bereich des Beschäftigtendatenschutzes

Obwohl die Datenschutzbeauftragten des Bundes und der Länder im Jahre 2010 Vorschläge für eine grundlegende Modernisierung des deutschen Datenschutzrechts unterbreitet haben[20], hat sich seither nichts getan. Alles wartet auf Europa, auch im Bereich des Beschäftigtendatenschutzes.

Trotz des Reformstaus im deutschen Datenschutzrecht hat sich im Verlauf der 17. Legislaturperiode des Deutschen Bundestags nichts wesentlich Neues ergeben. Weder ist der Themenkomplex des Beschäftigtendatenschutzes weiter geregelt worden, noch wurden die vom Bundesrat bereits 2011 angestoßenen **Änderungen im Telemedienrecht** umgesetzt (vgl. BR-Drs. 156/11), um dem informationellen Selbstbestimmungsrecht und dem Verbraucherschutz im Internet und insbesondere in sozialen Netzwerken zur Geltung zu verhelfen. Auch die vom Bundesinnenminister im November 2011 angeregte freiwillige Selbstverpflichtung sozialer Netzwerke blieb ohne Ergebnis, nachdem die marktbeherrschenden US-amerikanischen Unternehmen sich aus den Gesprächen zurückzogen (vgl. dazu Kapitel 1.4.5). Damit wird nicht verkannt, dass es außerhalb des allgemeinen Datenschutzrechts im Berichtszeitraum eine ganze Reihe von datenschutzrelevanten Änderungen im Bundesrecht gab. Hierzu wird auf die regelmäßig aktualisierte Übersicht auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) verwiesen[21].

[20] vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 21 f.
[21] http://www.bfdi.bund.de/SharedDocs/Publikationen/GesetzeVerordnun-

Besonders bedauerlich ist der legislatorische Stillstand auf Bundesebene hinsichtlich der überfälligen **Neuregelung des Beschäftigtendatenschutzes**, was ich bereits im 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 24 ff.) kritisiert hatte. Nur kurzzeitig schien im Januar 2013 Bewegung in die Sache zu kommen, als am 10. Januar 2013 überraschend ein Änderungsantrag der Regierungsfraktionen im Deutschen Bundestag eingebracht wurde, der schon wenige Tage später im Innenausschuss beraten werden sollte (vgl. Ausschussdrucksache 17(4)636). Darin waren zwar einige Verbesserungen, aber überwiegend Verschlechterungen gegenüber dem vielfach kritisierten Entwurf der Bundesregierung (vgl. BR-Drs. 535/10, BT-Drs. 17/4230 mit Änderungsvorschlägen des Bundesrats in Anlage 3) vorgesehen. Auch die von den Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom März 2011 unterbreiteten konkreten Änderungsvorschläge (vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, Anhang 14) waren nicht aufgegriffen worden. Zwar wäre es beim Verbot der heimlichen Videoüberwachung der Beschäftigten geblieben; allerdings wäre in Anbetracht der unpräzise formulierten Überwachungszwecke eine Ausweitung der offenen Videoüberwachung von Betriebsstätten nicht ausgeschlossen gewesen. Auch die Möglichkeiten zur Überwachung der telefonischen Kommunikation der Beschäftigten in Call-Centern wären gegenüber dem Regierungsentwurf noch einmal einseitig zu Lasten der Arbeitnehmer verschärft worden. So sollte der Arbeitgeber die Möglichkeit erhalten, Gespräche mitzuhören, aufzuzeichnen sowie zu nutzen und damit die Arbeitsleistung seiner Beschäftigten auch ohne deren konkretes Wissen im Einzelfall stichprobenweise oder anlassbezogen zu kontrollieren. Die Beschäftigten hätten noch nicht einmal über Zeitpunkt und Zeitraum, zu dem die Kontrollen durchgeführt werden, informiert werden müssen. Schließlich wollten die Initiatoren auch die im Regierungsentwurf vorgesehene Eingrenzung der Datenerhebung im Bewerbungsverfahren lockern. So hätten öffentlich zugängliche Daten über Bewerber generell genutzt werden dürfen, auch wenn sie aus sozialen Netzwerken stammten. Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, sollte demgegenüber entfallen. Weiterhin wurden in dem Änderungsantrag bedeutsame Regelungen nicht aufgenommen, etwa zur automatisierten Personalaktenführung, zur privaten Nutzung von Telekommunikationsdiensten und zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung. Schließlich enthielt der Änderungsantrag auch weitergehende Änderungen zur Auftragsdatenverarbeitung in Drittstaaten, die über den Arbeitnehmerdatenschutz weit hinausgingen und eine gründlichere Beratung erfordert hätten. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb in einer Entschließung vom 25. Januar 2013 (vgl. Anhang 12) noch einmal an den Bundesgesetzgeber appelliert, den Beschäftigtendatenschutz nicht abzubauen, sondern zu stärken. In einer Pressemitteilung hatte ich am 14. Januar 2013 bereits die Sorge geäußert, dass der monatelang im Bundestag liegengebliebene Regierungsentwurf nun offenkundig in einer Hauruck-Aktion zu Lasten der Arbeitnehmer übers Knie gebrochen werden solle. Die von vielen Seiten vorgetragene Kritik zeigte schließlich Wirkung; die Beratungen im Innenausschuss des Deutschen Bundestags zu dem Änderungsantrag und zu dem Regierungsentwurf wurden abgesetzt. Seither ist es um das Thema wieder still geworden.

Nach der **Koalitionsvereinbarung** für die 18. Legislaturperiode des Deutschen Bundestags soll eine nationale Regelung zum Beschäftigtendatenschutz erst dann geschaffen werden, wenn mit einem Abschluss der Verhandlungen zur Europäischen Datenschutz-Grundverordnung „nicht in angemessener Zeit“ gerechnet werden kann. Dabei hatte schon Artikel 82 des Kommissionsentwurfs vom 25. Januar 2012 durchaus weitergehende gesetzliche Regelungen der Mitgliedsstaaten zum Beschäftigtendatenschutz zugelassen. Allerdings hat das **Europäische Parlament** am 21. Oktober 2013 (vgl. hierzu Kapitel 1.3.1) wichtige Mindeststandards und Präzisierungen für Artikel 82 vorgeschlagen, etwa zur Freiwilligkeit der Einwilligung des Arbeitnehmers in die Daten-

gen/AktuelleBundesgesetzgebung.pdf?__blob=publicationFile (letzte Aktualisierung vom 20. September 2013)

verarbeitung, zur offenen oder heimlichen Videoüberwachung am Arbeitsplatz und in Sozialräumen, zur Datenverarbeitung im Zusammenhang mit Gesundheits- oder Eignungsuntersuchungen, zum Verbot des Führens „schwarzer Listen“ (z. B. über die Mitgliedschaft des Arbeitnehmers in Gewerkschaften oder dessen politische Orientierung) oder zur privaten Nutzung von E-Mail und Internet am Arbeitsplatz. Insofern liegt es in der Tat nahe, das Ergebnis des Trilogs zur Europäischen Datenschutzreform zunächst abzuwarten. Dabei hat es die Bundesregierung selbst in der Hand, für eine rasche Beratung und Verabschiedung der EU-Datenschutz-Grundverordnung zu sorgen und damit auch einen Beitrag für einen verbesserten Datenschutz am Arbeitsplatz zu leisten.

Es bleibt abzuwarten, ob der Beschäftigtendatenschutz in der 18. Legislaturperiode des Deutschen Bundestags zeitnah wieder auf die Agenda gesetzt wird.

1.4.2 Das E-Government-Gesetz des Bundes

Am 1. August 2013 ist das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz – EGovG) in Kraft getreten (vgl. BGBl. I 2013, S. 2749). Ziel des Gesetzes ist es, die elektronische Kommunikation mit der Verwaltung zu erleichtern und Bund, Ländern und Kommunen zu ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten. Aus datenschutzrechtlicher Sicht ist das Gesetz nicht durchweg erfreulich.

So enthält das **E-Government-Gesetz** in § 6 z. B. eine Vorschrift zur elektronischen Aktenführung. Die Schaffung einer gesetzlichen Grundlage hierfür ist grundsätzlich zu begrüßen. Allerdings bringt eine elektronische Aktenführung besondere Risiken für das informationelle Selbstbestimmungsrecht des Einzelnen mit sich. Im Unterschied zu einer herkömmlichen Papierakte besteht bei elektronischen Akten in völlig anderem Maße die Möglichkeit von Volltextrecherchen, Verknüpfungen, Auswertungen und Profilbildungen ohne Rücksicht auf den fachlichen Kontext und die jeweiligen Sachgebiete, für die die Daten z. B. erhoben wurden. Die Einhaltung der datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Zweckbindung, der informationellen Gewaltenteilung und der Datensparsamkeit erlangen in diesem Zusammenhang ebenso wie die notwendigen technischen und organisatorischen Maßnahmen besondere Bedeutung. Wünschenswert wäre gewesen, wenn diese Risiken in der Gesetzesbegründung dargestellt worden wären und in der Vorschrift sämtliche Schutzziele der Datensicherheit - namentlich Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität, Nichtverkettbarkeit, Revisionsfähigkeit und Transparenz - aufgeführt worden wären. Die Schutzziele sowie die Grundprinzipien der ordnungsgemäßen Aktenführung wurden leider nur unzureichend normiert.

Zu kritisieren ist außerdem die in § 14 EGovG vorgesehene **Georeferenzierung**. Diese Regelung verpflichtet die Behörden, in elektronische Register, die Angaben mit Bezug zu Grundstücken enthalten, eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) zu dem jeweiligen Flurstück oder dem Gebäude aufzunehmen. Dies ist datenschutzrechtlich hoch problematisch. Zwar handelt es sich bei einer Geokoordinate zunächst um ein neutrales Datum, jedoch führt die inhaltliche Verknüpfung mit den sonstigen Registerdaten dazu, dass das betreffende Grundstück und damit der Eigentümer eindeutig bestimmbar werden. Deshalb dürfte in vielen Fällen die Geokoordinate als personenbezogenes Datum zu qualifizieren sein. Ausweislich der Gesetzesbegründung (BT-Drs. 17/11473, S. 42) soll durch die Speicherung der Koordinaten eine direkte räumliche und technisch einfache Zuordnung und Verknüpfung verschiedener Informationen möglich sowie eine Auswertung deutlich vereinfacht werden. Hierin liegt jedoch ein großes Risiko für das informationelle Selbstbestimmungsrecht. Es besteht die Gefahr, dass die Zweckbindung der Registerdaten nicht eingehalten wird und Daten unzulässig zusammengeführt werden. Des Weiteren sind detaillierte Profilbildungen denkbar. Angesichts der hohen datenschutzrechtlichen Gefährdungslage ist die Erforderlichkeit der Vorschrift insbesondere für die Register im Personenstands-, Melde-, Pass- und

Personalausweiswesen in Frage zu stellen. Diese ist auch vom Bundesrat in seiner Stellungnahme vom November 2012 bezweifelt worden (vgl. BR-Drs. 557/12 (B), Nr. 13).

Die nötige Sensibilität hinsichtlich des Persönlichkeitsrechts der Bürger lässt außerdem § 15 E-GovG vermissen. Dieser sieht vor, dass die Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden kann. Insbesondere Veröffentlichungen von Gemeinden in ihren Mitteilungs- und Verkündungsblättern enthalten häufig personenbezogene Daten, die durch eine Veröffentlichung im Internet dauerhaft und weltweit verfügbar gemacht werden. Hieraus ergibt sich eine spezifische Gefährdung des informationellen Selbstbestimmungsrechts des Betroffenen. Die Gefährdungslage ist als gravierend einzustufen, weil durch eine Internetveröffentlichung nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche es jedem Internet-Nutzer jederzeit erlauben würde, durch die Eingabe des Namens der Betroffenen in eine Suchmaschine sämtliche zu diesen Personen vorhandenen Angaben zu sammeln und - losgelöst vom ursprünglichen Informationszweck - zur Erstellung eines Persönlichkeitsprofils zu nutzen. Nicht ersichtlich ist, weshalb eine weltweite dauerhafte Veröffentlichung erforderlich ist. Die generelle Einführung der Veröffentlichung via Internet bei personenbezogenen Daten ist daher abzulehnen, jedenfalls ist aber vor einer Internetveröffentlichung eine Interessenabwägung zu fordern. Dem Vorschlag des Bundesrates, die Dauer der Veröffentlichung in der elektronischen Ausgabe zu begrenzen, wenn dies zum Schutz des Persönlichkeitsrechts Betroffener erforderlich ist (vgl. BR-Drs. 557/12 (B), Nr. 14), ist der Bundestag leider nicht gefolgt.

Schließlich ist zu befürchten, dass das E-Government-Gesetz zu einer **Senkung des Sicherheitsniveaus** bei der elektronischen Kommunikation führen wird. Nach bisheriger Rechtslage war als elektronisches Äquivalent der Schriftform allein die qualifizierte elektronische Signatur nach dem Signaturgesetz zugelassen. Mit dem E-Government-Gesetz werden in § 3a Absatz 2 des Verwaltungsverfahrensgesetzes (VwVfG), in § 36a Absatz 2 des Ersten Buches des Sozialgesetzbuchs (SGB I) sowie in § 87a Absatz 3 der Abgabenordnung (AO) nun **weitere Alternativen zur elektronischen Ersetzung der Schriftform** eingeführt: Zum einen die Verwendung von elektronischen Formularen der Verwaltung, die in Verbindung mit einer sicheren elektronische Identifizierung, insbesondere durch die Online-Ausweisfunktion (eID-Funktion) des neuen Personalausweises, übermittelt werden; zum anderen der Versand einer De-Mail unter Verwendung der Versandoption nach § 5 Absatz 5 des De-Mail-Gesetzes, welche eine „sichere Anmeldung“ (§ 4 Absatz 1 Satz 2 des De-Mail-Gesetzes) des Erklärenden voraussetzt. Diese Technologien stellen jedoch kein Äquivalent zur Schriftform dar, das mit der qualifizierten elektronischen Signatur vergleichbar und hinreichend sicher ist. Die eID-Funktion ermöglicht lediglich eine sichere Authentifizierung des Absenders. Durch das Übermitteln der persönlichen Personalausweisdaten kann weder gewährleistet werden, dass eine zusätzlich übersendete Erklärung inhaltlich von demjenigen herrührt, der sich als Aussteller ausgibt, noch ist überprüfbar, ob die Mitteilung nach dem Absendevorgang verändert wurde. Ob die Nachricht auf dem Versandweg verändert wurde, kann auch der Empfänger einer De-Mail nicht erkennen. Da der Nachweis des Absenders nur durch die Anmeldung am De-Mail-Konto erfolgt, kann im Übrigen der Absender einer De-Mail nicht sicher bestimmt werden.

Aus Datenschutzsicht ist die Einführung einer De-Mail-Nachricht als Möglichkeit der rechtsverbindlichen und sicheren Behördenkommunikation außerdem aufgrund der fehlenden Ende-zu-Ende-Verschlüsselung bedenklich. Eine durchgängige Verschlüsselung zwischen Sender und Empfänger ist standardmäßig nicht vorgesehen. Dies ist bereits im Zusammenhang mit der Entstehung des De-Mail-Gesetzes von den Datenschutzbeauftragten des Bundes und der Länder kritisiert worden (vgl. Entschließung vom 16. April 2009, 29. Tätigkeitsbericht, LT-Drs. 14/5500, Anhang 30). Eine De-Mail liegt auf dem Versandweg im Verantwortungsbereich des Diensteanbieters kurz

unverschlüsselt vor, um die Nachricht auf Schadsoftware zu überprüfen. Dieses bereits im De-Mail-Gesetz angelegte Defizit ist nun bedauerlicherweise auf den Bereich der elektronischen Verwaltung erstreckt worden.

Der Einsatz von De-Mail für die Kommunikation mit der Verwaltung ohne Ende-zu-Ende-Verschlüsselung ist insbesondere beim Versand besonders geschützter Daten, z. B. Sozial- oder Steuerdaten, problematisch. Diese Daten bedürfen eines angemessenen Schutzniveaus, da nur so das Sozial- und das Steuergeheimnis gewahrt werden können. Im Zusammenhang mit dem E-Government-Gesetz wurde in § 67 Absatz 6 Satz 2 Nr. 3 des Zehnten Buches des Sozialgesetzbuchs (SGB X) sowie in § 30 Absatz 7 der Abgabenordnung (AO) festgelegt, dass das Senden von Sozial- bzw. Steuerdaten durch eine De-Mail-Nachricht an die jeweiligen akkreditierten Diensteanbieter - zur kurzfristigen automatisierten Entschlüsselung zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht - kein Übermitteln bzw. unbefugtes Offenbaren ist. Dadurch wird eine De-Mail rechtlich einer E-Mail mit Ende-zu-Ende-Verschlüsselung gleichgestellt, obwohl sie im Hinblick auf die Datensicherheit faktisch nicht vergleichbar ist. Das hat zur bedenklichen Folge, dass der hohe technische Maßstab, den das Zehnte Buch des Sozialgesetzbuchs sowie die Abgabenordnung in Bezug auf Datensicherheit wegen der besonderen Sensibilität der zu übermittelnden Daten insbesondere aufgrund des Verschlüsselungsgebots in Anlage zu § 78a SGB X und in § 87a Absatz 1 Satz 2 AO setzt, im Bereich der De-Mail umgangen wird. Wünschenswert wäre daher gewesen, ein Ende-zu-Ende-Verschlüsselungsverfahren standardmäßig vorzusehen.

Nichtsdestotrotz bedeuten die Änderungen durch das E-Government-Gesetz keinen Freibrief für die öffentliche Verwaltung, elektronisch ohne Ende-zu-Ende-Verschlüsselung zu kommunizieren. Bei der elektronischen Übertragung personenbezogener Daten müssen die Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt sein. Je schützenswerter ein Datum ist, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Um ein angemessenes Schutzniveau bei der Versendung besonders schutzbedürftiger personenbezogener Daten (z. B. Sozialdaten oder Daten, die Rückschlüsse auf den Gesundheitszustand einzelner Betroffener zulassen) mittels De-Mail zu gewährleisten, ist aus datenschutzrechtlicher Sicht eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach im Rahmen des Gesetzgebungsverfahrens auf die datenschutzrechtlichen Defizite hingewiesen. Bedauerlicherweise blieben selbst die Vorschläge des Bundesrates zum Schutz des Persönlichkeitsrechts der Bürgerinnen und Bürger unberücksichtigt.

Ich unterstütze das Ziel des Gesetzes, die rechtlichen Rahmenbedingungen für E-Government zu verbessern, rechtliche Unsicherheiten zu beseitigen und die elektronische Kommunikation mit der Verwaltung zu erleichtern. Dieses Ziel darf jedoch nicht auf Kosten des bestehenden Datenschutzniveaus verwirklicht werden. Ich appelliere an den Landesgesetzgeber, sich bei einem E-Government-Gesetz für das Land Baden-Württemberg nicht an den Schwächen des Bundesgesetzes zu orientieren.

1.4.3 Die Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestags

Im Berichtszeitraum hat die Enquete-Kommission des Deutschen Bundestags „Internet und digitale Gesellschaft“ ihre Beratungen abgeschlossen. Neues für den Datenschutz ist dabei nicht herausgekommen.

Bereits im 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 30 f.) hatte ich über die schleppende, weil dissonante Behandlung des Themas Datenschutz in der Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestags berichtet. Die Differenzen betrafen indes auch andere Themenbereiche, in denen die politischen, wirt-

schaftlichen und gesellschaftlichen Präferenzen der Kommissionsmitglieder offen zutage traten. Am 18. April 2013 legte die Enquete-Kommission schließlich ihre Arbeitsergebnisse vor, nicht in einem einzigen konsistenten **Abschlussbericht**, sondern in insgesamt 14 Teilberichten mit umfangreichen Bestandsaufnahmen und Handlungsempfehlungen. Dazu gehörte auch ein ausdrücklich als „**Zwischenbericht**“ bezeichnetes Werk **der Projektgruppe „Datenschutz, Persönlichkeitsrechte“ vom 15. März 2012** (BT-Drs. 17/8999[22]), was darauf schließen lässt, dass es seit dieser Zwischenbilanz bis zum Ende der Enquete-Kommission keinen weiteren Beratungsfortschritt zum Thema Datenschutz gab. Dennoch und ungeachtet der zahlreichen Sondervoten wird in dem Bericht (S. 53) festgehalten, dass es einen breiten Konsens über die Grundprinzipien, Ziele und Werte des Datenschutzes gegeben habe. Alle Mitglieder der Kommission hätten hervorgehoben, dass Datenschutz und eine Gewährleistung des Grundrechts auf informationelle Selbstbestimmung Akzeptanz und Vertrauen schaffen würden, was wiederum unabdingbar sei für den technologischen Fortschritt in einer digitalen Gesellschaft sei. Neben diesem eher allgemein gehaltenen Konsens sind in dem Zwischenbericht allerdings auch deutlich abweichende Auffassungen zu durchaus wichtigen datenschutzrechtlichen Fragen zu finden, z. B. zu der Idee des sog. Datenbriefs, mit dem ein Betroffener ggf. von Behörden und Unternehmen erfahren soll, wer welche Daten über ihn weshalb speichert. Die Mehrheit lehnte diesen Vorschlag als zu bürokratisch und als mit dem Prinzip der Datensparsamkeit nicht zu vereinbaren ab. Insgesamt stellen der Zwischenbericht der Enquete-Kommission zum Themenkomplex Datenschutz, aber auch die auf der Internetseite des Deutschen Bundestags dokumentierten Ausschussprotokolle und Materialien[23], eine wertvolle Übersicht über den politischen und fachlichen Diskussionsstand zu einem bestimmten Zeitpunkt dar, nicht mehr, aber auch nicht weniger.

[22] vgl. http://dipbt.bundestag.de/dip21/btd/17/089/1708999.pdf

[23] http://www.bundestag.de/internetenquete/dokumentation/Datenschutz/index.jsp

1.4.4 Die Bundesstiftung Datenschutz nimmt ihre Arbeit auf - ohne die Datenschützer

Im Berichtszeitraum hat die Bundesstiftung Datenschutz ihre Arbeit aufgenommen; allerdings haben sich die Datenschutzbeauftragten, aber auch die Verbraucherschützer daran vorerst nicht beteiligt.

Auf die von der Bundesregierung geplante **„Stiftung Datenschutz“** war ich bereits in meinem 30. Tätigkeitsbericht (vgl. LT-Drs. 15/955, S. 28) mit einigen kritischen Anmerkungen eingegangen. Das Konzept wurde dem Bundestag im Zusammenhang mit einem Antrag der FDP-Bundestagsfraktion (BT-Drs. 17/10092) vorgelegt und am 28. Juni 2012 mit den Stimmen der Regierungsfraktionen gebilligt (vgl. Plenarprotokoll 17/187, S. 22437 ff.). Im Herbst 2012 wurde der Entwurf einer Satzung für die Stiftung vorgelegt. Als Hauptzwecke werden darin die Förderung der Belange des Datenschutzes durch die Entwicklung von Auditierungsverfahren einschließlich der Vergabe von Zertifikaten, Bildungsaktivitäten, die Stärkung des Selbstdatenschutzes durch Aufklärung und die Prüfung von Produkten und Dienstleistungen im Hinblick auf ihre Datenschutzfreundlichkeit genannt. Das Stiftungskapital, das als einmaliger Zuschuss bereits im Bundeshaushalt 2011 bereitgestellt worden war, beträgt 10 Mio.€. Organe der Stiftung sind der Vorstand („Präsident“), der (von den Bundesministerien zu beschickende) Verwaltungsrat sowie der **Beirat**. Die Satzung sieht für diesen Beirat außer den vom Bundestag zu benennenden (bis zu neun) Personen weitere 25 Mitglieder vor, darunter 14 Mitglieder aus den Bereichen der datenverwendenden Wirtschaft (z. B. auf Vorschlag von Verbänden wie BITKOM, GDV, DDV, BDI usw.), ein Mitglied auf Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, ein Mitglied auf Vorschlag der Datenschutzbeauftragten der Länder, ein Mitglied auf Vorschlag der Datenschutzaufsichtsbehörden der Länder („Düsseldorfer Kreis“), ein Mitglied auf Vorschlag der Verbraucherzentrale Bundesverband e.V. sowie ein Mitglied auf Vorschlag der Stiftung Warentest.

Das **Bundesinnenministerium** lud im Herbst 2012 die o. g. Gremien und Verbände zur Entsendung von Vertretern in den Beirat ein. Die Datenschutzbeauftragten bzw. die Aufsichtsbehörden des Bundes und der Länder sahen jedoch aufgrund der Dominanz von Wirtschaftsvertretern im Beirat und wegen Zweifeln an einer hinreichenden Unabhängigkeit der - finanziell vermutlich auf Zustiftungen aus der Wirtschaft angewiesenen - Stiftung vorerst davon ab, Vertreter in den Beirat zu entsenden. Die Stiftung Warentest, der Verbraucherzentrale Bundesverband und die damaligen Oppositionsparteien im Deutschen Bundestag sind diesem Schritt gefolgt. Die Stiftung, die ihren Sitz in Leipzig genommen hat, wurde schließlich im Januar 2013 nach sächsischem Stiftungsrecht als rechtsfähig anerkannt und hat im Verlauf des Jahres 2013 schon einige Aktivitäten bei Tagungen sowie durch Forschungsaufträge zur Bedeutung der Privatsphäre entfaltet. Ob ihr ein langes Leben beschieden sein wird, erscheint mittlerweile zweifelhaft: In der **Koalitionsvereinbarung** für die 18. Legislaturperiode ist im Kapitel „Verbraucherschutz“ zu lesen, dass die noch junge Stiftung in die **Stiftung Warentest** integriert werden solle.

Grundsätzlich ist jeder Akteur zu begrüßen, der die Anliegen des Datenschutzes in unserer Gesellschaft unterstützt und befördert. Die Begleitumstände der Gründung der Bundesstiftung Datenschutz zeigen allerdings, wie eine an sich gute Idee schlecht umgesetzt werden kann.

1.4.5 Die freiwillige Selbstregulierung bei sozialen Netzwerken - eine Blamage für die Bundespolitik

Freiwilligkeit ist grundsätzlich sicher besser als Zwang. Aber nicht alles darf man dem freien Spiel der Kräfte überlassen, vor allem wenn diese ungleich verteilt sind.

Nicht nur die Datenschutzbeauftragten wurden hellhörig, als der damalige **Bundesinnenminister** am 2. November 2011 im Anschluss an eine Gesprächsrunde mit „allen verantwortlichen Akteuren“ vor die Presse trat und vollmundig den Startschuss für die Entwicklung eines **Kodex für soziale Netzwerke** bekanntgab, mit dem ein besserer Schutz der Nutzer erreicht werden solle. Zugleich wurde als ordnungspolitische Marschroute ausgegeben, dass das Bundesinnenministerium im Bereich seiner Netzpolitik verstärkt auf die **Selbstregulierung** der betroffenen Branchen setze. Dies könne ein effizienter Weg sein, schnell und flexibel Vereinbarungen zu treffen, bei denen für die Nutzer am Ende deutlich mehr Klarheit und Verlässlichkeit entstehe. Diese Regelungen gälten dann unabhängig davon, wo das betreffende Unternehmen seinen Sitz habe. So ganz schien der Bundesinnenminister den Beteiligten aber doch nicht zu trauen, denn er schloss zugleich flankierende gesetzliche Schritte für den Fall nicht aus, dass bei den anstehenden Verhandlungen keine angemessenen Regelungen gefunden würden. Solche gesetzlichen Leitplanken hatte der **Bundesrat** zuvor - bis dato vergeblich - gefordert (vgl. BR-Drs. 156/11, s. o. Kapitel 1.4.1).

Im 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 49 f.) hatte ich die damals angelaufenen Gespräche, die unter **Federführung des Vereins der Freiwilligen Selbstkontrolle der Multimediaanbieter (FSM)** stattfanden, zwar als Schritt in die richtige Richtung bezeichnet, zugleich aber auch betont, dass es auf die Ergebnisse ankommen werde, die nach der damaligen Zeitplanung bei der CeBIT 2012 präsentiert werden sollten. Meine an der eingangs genannten Gesprächsrunde beteiligten Kollegen aus Berlin und Düsseldorf hatten zudem darauf hingewiesen, dass Verhaltensregeln für soziale Netzwerke nur in Zusammenarbeit mit den Aufsichtsbehörden Verbindlichkeit erlangen könnten (vgl. auch § 38 a BDSG), dass das geltende Datenschutzrecht aber hierdurch nicht ersetzt werden könne; zudem reiche es nicht aus, nur das datenschutzrechtliche Minimum zu beschreiben. Vielmehr müssten Verhaltensregeln auch wirksame Sanktionsmöglichkeiten enthalten und weitere Anforderungen - etwa an Transparenz, datenschutzfreundliche Voreinstellungen und Minderjährigenschutz - erfüllen.

In den folgenden Monaten drangen nur Gerüchte über schleppende Verhandlungen nach außen. Insbesondere die an den Gesprächen beteiligten

Vertreter der großen US-amerikanischen Netzwerke sähen Probleme, sich auf die von den europäischen Anbietern eingehaltenen Standards einzulassen. 2009 hatten sich bereits drei deutsche Anbieter auf einen gemeinsamen Kodex verständigt. Zur CeBIT 2012 wurde jedenfalls noch kein Ergebnis präsentiert und auch nicht zur CeBIT 2013. Die Vermutung von Branchenkennern, dass es keinen Konsens geben werde, bestätigte sich schließlich Anfang Mai 2013, als FSM das vorläufige **Scheitern der Verhandlungen** bekanntgab, weil mit Facebook, Google und den Karriere-Netzwerken LinkedIn und Xing zentrale Unternehmen der Branche den geplanten Kodex nicht unterzeichnen wollten. Selbst der Initiator der Gespräche, der Bundesinnenminister, sprach daraufhin von einer „Verweigerungstaktik" der großen Online-Netzwerke; die Unternehmen hätten eine Chance vertan. Und ein Sprecher des Bundesverbraucherschutzministeriums kritisierte, die Beteuerungen dieser Anbieter zum Datenschutz und zum Jugendschutz seien offenbar nur „Lippenbekenntnisse" gewesen. Das Ministerium sei von vornherein der Ansicht gewesen, dass es klare gesetzliche Vorgaben auf europäischer Ebene geben müsse und dass man selbst die Spielregeln vorgeben müsse, unter denen die Anbieter in Europa Geschäfte machen können. Die internationale Dimension scheinen die US-Anbieter übrigens ähnlich zu sehen: Das Scheitern der Verhandlungen wurde von ihnen nämlich vor allem damit erklärt, dass man sich nicht an regionalen (!) Absprachen beteiligen könne, während der Trend zu einer international einheitlichen Regulierung gehe. Selten ist so deutlich geworden, dass sich die Kampfzone um die Zukunft auch des nationalen Datenschutzes von Berlin nach Brüssel verlagert hat.

Aus meiner Sicht haben die großen internationalen Anbieter die deutsche Politik durch eine Verschleppungstaktik schonungslos vorgeführt. Sie haben auf Zeit gespielt und sich nicht einbinden lassen. Inzwischen sind deutsche Anbieter weitgehend vom Markt verschwunden; so hat SchülerVZ zum 30. April 2013 den Betrieb eingestellt. Nun ist der Gesetzgeber gefordert. Die europäische Datenschutzreform ist dringlicher denn je. Die Bundesregierung sollte dabei eine einheitliche ordnungspolitische Haltung vertreten und deutlich machen, dass sie den Grundrechtsschutz der Bürger nicht zur Disposition der Marktakteure stellt.

1.4.6 Aussichten für den Datenschutz in der 18. Legislaturperiode des Deutschen Bundestags - Erwartungen an die Politik

Die Datenschutzbeauftragten des Bundes und der Länder haben im Oktober 2013 den aktuellen datenschutzpolitischen Handlungsbedarf auf verschiedenen Politikfeldern artikuliert. Sie verbanden dies mit der Erwartung an die neue Bundesregierung, entschlossener als bisher für die Grundrechte der Bürgerinnen und Bürger einzutreten. Die rasante technische Entwicklung macht das vom Bundesverfassungsgericht vor 30 Jahren entwickelte Grundrecht auf informationelle Selbstbestimmung andernfalls zur Illusion.

Der deutschen Datenschutzpolitik stehen schwierige Zeiten bevor. Die seit mehr als zehn Jahren überfällige umfassende Modernisierung des nationalen Datenschutzrechts wird allenfalls in anderer Form kommen, weil mittlerweile eine Datenschutzreform auf europäischer Ebene eingeleitet wurde, die voraussichtlich das nationale Recht verdrängen wird. Zugleich droht die rasante technische und wirtschaftliche Entwicklung mit einer allgegenwärtigen, über das Internet vernetzten Datenverarbeitung Aspekte des Datenschutzes an den Rand zu drängen. Daten sind zum Rohstoff des 21. Jahrhunderts geworden und werden zunehmend kommerziell, aber auch unter Sicherheitsaspekten in Echtzeit ausgewertet, wie die Spähaffäre angloamerikanischer Geheimdienste gezeigt hat. Ausufernde Datensammlungen, zum Beispiel im Bereich des Gesundheitswesens, und mächtige Analysewerkzeuge machen es immer leichter, einen Personenbezug herzustellen und selbst sensible Daten konkreten Personen zuzuordnen. Das Diktum des Bundesverfassungsgerichts im sog. Volkszählungsurteil vom 15. Dezember 1983, unter den (damaligen!) Bedingungen der Datenverarbeitung gäbe es kein belang-

loses Datum, gilt heute erst recht. Von daher steht die Politik jetzt vor der Wahl, ob die Spielregeln der Internetgesellschaft allein durch die technische Machbarkeit und die kommerzielle Verwertbarkeit der Daten determiniert werden sollen oder ob sie eigene Gestaltungsspielräume nutzt, die das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger wieder in den Mittelpunkt rücken. Datenschutz darf dabei nicht als Innovations- und Investitionsbremse verstanden werden, sondern muss in seiner europäischen Ausprägung zum Wettbewerbsvorteil werden. Davon ausgehend, dass die Bürgerinnen und Bürger den Wert der Privatsphäre weiterhin hoch schätzen werden, haben die Datenschutzbeauftragten des Bundes und der Länder bei ihrer Konferenz am 1./2. Oktober 2013 u. a. folgende Forderungen für die 18. Legislaturperiode aufgestellt:

- Die Bundesregierung sollte sich für eine Weiterentwicklung des Datenschutzrechts nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene einsetzen. In erster Linie geht es derzeit um eine Europäische Datenschutzreform auf hohem Niveau. Flankierend dazu - dies hat die aktuelle Spähaffäre vor Augen geführt - müssen völkerrechtliche Instrumente initiiert und weiterentwickelt werden.

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung stärker als Rechnung tragen. Wichtig ist dabei auch eine umfassende Kontrolle der Sicherheitsdienste. In diesem Zusammenhang ist auch an die Aussage des Bundesverfassungsgerichts zu erinnern, dass das Verbot einer Totalüberwachung der Freiheitswahrnehmung der Bürgerinnen und Bürger zur verfassungsrechtlichen Identität unseres Staates gehöre, für die sich die politisch Verantwortlichen im europäischen und internationalen Kontext einsetzen müssen.

- Im Bereich des Sozial- und Gesundheitswesens zeichnet sich ein zunehmender Wettbewerb mit einer wachsenden Vernetzung und Arbeitsteilung zwischen den Akteuren und der Auslagerung von technischen Dienstleistungen an Dritte ab, der besondere Risiken für das informationelle Selbstbestimmungsrecht mit sich bringt; die Gefahr von „gläsernen“ Patienten und Versicherten wächst. Dieser Wettbewerb darf jedoch nicht zu Lasten der Betroffenen gehen; vielmehr sind deren Privat- und Intimsphäre nachhaltig zu stärken.

- Schließlich haben die Datenschutzbeauftragten auch daran erinnert, dass die vom Bundesverfassungsgericht mit Verfassungsrang versehene Vertraulichkeit und Integrität informationstechnischer Systeme und elektronischer Kommunikation stärker zu fördern sei und der öffentliche Bereich hier mit gutem Beispiel vorangehen müsse, indem er beispielsweise flächendeckend eine Ende-zu-Ende-Verschlüsselung einsetzt.

Die Entschließungen der Datenschutzkonferenz sind in den Anhängen 19-21 nachzulesen.

Der Koalitionsvertrag von CDU/CSU und SPD für die 18. Legislaturperiode enthält aus Datenschutzsicht einige positive Ansätze. So werden in einem Abschnitt „Moderner Staat, innere Sicherheit und Bürgerrechte“ – offenkundig unter dem Eindruck der Spähaffäre – vor allem Maßnahmen der IT-Sicherheit in Aussicht gestellt. Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme solle mit Leben erfüllt werden, sichere Ende-zu-Ende-Verschlüsselung solle erheblich ausgebaut werden, Methoden der Anonymisierung, Pseudonymisierung und Datensparsamkeit müssten verbindlich werden. Ansonsten werden als Konsequenz aus der NSA-Affäre u. a. Nachverhandlungen zu Safe Harbor und SWIFT angekündigt. Diesen datenschutzfreundlichen Verheißungen stehen aber auch restaurative Elemente wie die (Wieder-)Einführung der Vorratsdatenspeicherung gegenüber.

1.5 Aus der Dienststelle

Die **Personalausstattung** meiner Dienststelle hat sich im Berichtszeitraum weiter positiv entwickelt, wenngleich naturgemäß nicht so sprunghaft wie durch die Zusammenlegung der beiden Datenschutzaufsichtsbehörden zum 1. April 2011. Im Zuge der Umressortierung waren damals 6,5 Stellen vom Innenministerium, wo die Aufsichtsbehörde für den nicht-öffentlichen Bereich bis dato angesiedelt war, in das neue Kapitel 0103 übertragen worden. Parallel dazu hatte der Landtag im Dritten Nachtrag 2011 drei weitere Neustellen zugewiesen, so dass die Dienststelle zu Beginn des Berichtszeitraums über 25,5 Stellen verfügte. Im Staatshaushaltsplan 2012 gingen je eine weitere Stelle des höheren Dienstes und des gehobenen Dienstes zu. Außerdem stellte der Landtag Mittel für die Abordnung von zwei weiteren Mitarbeitern zur Verfügung. Leider meldete sich daraufhin - trotz Unterrichtung aller Ministerien und des Rechnungshofs - nur ein Mitarbeiter des gehobenen Dienstes aus dem Geschäftsbereich des Ministeriums für Finanzen und Wirtschaft. Auch dieser Mitarbeiter wurde von seiner Behörde erst nach zähen Verhandlungen und zunächst nur für die Dauer von einem Jahr - mit dem Ziel der Versetzung - freigegeben. Dieser Widerstand ist nicht unverständlich, denn eine Behörde kann die Stelle eines abgeordneten Beamten für die Zeit der Abordnung nicht bzw. allenfalls mit befristet Beschäftigten besetzen; erschwerend kommen die Rahmenvorgaben zum Stellenabbau in der Landesverwaltung hinzu. Auf die Abordnungsstelle des höheren Dienstes bewarb sich trotz mehrfacher Anläufe seinerzeit sogar niemand. Neben dem Widerstand der entsendenden Dienststelle mag dies auch daran liegen, dass für gute Nachwuchskräfte - zumindest bisher - schwer abschätzbar ist, inwieweit eine Verwendung bei meiner Dienststelle für das eigene berufliche Fortkommen förderlich ist. Nach meinem Eindruck ist die personelle Durchlässigkeit der Landesverwaltung zwischen den Ressorts ohnehin nicht besonders ausgeprägt. Ein Wechsel zu meiner Dienststelle, die nicht unbedingt im Blickfeld der Personalreferenten der Ministerien liegt, mag insofern für grundsätzlich am Datenschutz interessierte Kandidaten ein Risiko darstellen. Das im Haushaltsplan 2012 angelegte „Abordnungsmodell“ war daher nur teilweise erfolgreich, was ich auch den Landtagsfraktionen mitteilte. Erfreulicherweise wurden daraufhin die Abordnungsmittel im Doppelhaushalt 2013/2014 in zwei Neustellen „umgewandelt“ (A 15 h. D.; A 13 g. D.). Dank der tatkräftigen Unterstützung des Justizministeriums konnte die Stelle des höheren Dienstes inzwischen doch noch im Wege der Abordnung mit einem hervorragend qualifizierten Staatsanwalt besetzt werden, der sich u. a. um die datenschutzrechtlichen Schnittstellen zwischen Justiz und Sicherheitsbehörden kümmert und von dessen Berufserfahrung wir besonders profitieren können. Um vergleichbare Verwendungen auch in Zukunft zu ermöglichen, sollte im Haushaltsplan in den Erläuterungen zum Stellenteil ein Hinweis angebracht werden, dass die Stellen des höheren Dienstes bei meiner Dienststelle - zumindest teilweise und vorübergehend - mit Richtern und Staatsanwälten im Wege der Abordnung besetzt werden können. Bezüglich des konkreten Falles geschah dies inzwischen im Zweiten Nachtrag zum Staatshaushaltsplan 2014. Zum Ende des Berichtszeitraums weist meine Dienststelle somit eine Personalausstattung von 29,5 Stellen, davon 24,0 Beamte und 5,5 Tarifbeschäftigte, auf. Insbesondere im Assistenz-, aber auch im Sachbearbeiterbereich ist eine weitere Verstärkung wünschenswert, um kein Missverhältnis zwischen „Häuptlingen“ und „Indianern“ entstehen zu lassen. Erfreulicherweise konnte meine Dienststelle im Berichtszeitraum weiterhin von der Abordnung einer Beamtin des höheren Polizeivollzugsdienstes und eines IT-Fachlehrers (zu 80%) profitieren, die zugleich zu einem Wissens- und Erfahrungsaustausch mit diesen großen Fachbereichen der Landesverwaltung beitrugen.

Ungeachtet der quantitativen Stellenentwicklung muss in Zukunft ein besonderes Augenmerk auf die **Durchlässigkeit** zwischen meiner Dienststelle und der übrigen Landesverwaltung gelegt werden, um eine auch qualitativ gute Personalausstattung der anspruchsvollen Querschnittsaufgabe Datenschutz sicherzustellen. Die europarechtlich gebotene Unabhängigkeit der Datenschutzaufsicht darf jedenfalls nicht in die personalpolitische Isolation führen und die Tätigkeit bei meiner Dienststelle

nicht zur beruflichen Sackgasse werden. Insofern kann der Zugang von Neustellen zu einer dauerhaften Qualitätsverbesserung nur dann beitragen, wenn es gelingt, für meine Mitarbeiterinnen und Mitarbeiter angemessene Anschlussverwendungen zu finden. Andernfalls besteht die Gefahr, dass gute Nachwuchskräfte den Wechsel zu meiner Dienststelle scheuen, weil sie für sich keine Perspektive der anschließenden beruflichen Weiterentwicklung sehen. Ich gebe allerdings zu, dass es dabei ggf. auch auf die eigene Wechselbereitschaft ankommt und dass das Stellenangebot wegen der Stelleneinsparungen in vielen Bereichen der Landesverwaltung derzeit überschaubar ist. Im Hinblick auf die nach § 26 Absatz 4 Satz 4 LDSG von der Landesregierung zu gewährleistende Einbeziehung meiner Mitarbeiterinnen und Mitarbeiter in den allgemeinen Personalaustausch der Landesverwaltung hatte ich schon im Sommer 2011 dem Staatsministerium vorgeschlagen, hierzu eine schriftliche Vereinbarung zu erarbeiten, wie sie in der Gesetzesbegründung vorgesehen worden war. Leider teilte mir der Amtschef des Staatsministeriums daraufhin unter Hinweis auf beamtenrechtliche Zwänge im Ergebnis nur mit, dass die vom Gesetzgeber vorgesehene Vereinbarung allenfalls deklaratorischen Charakter haben könne. Immerhin wurde mir zugesagt, dass ich mein Anliegen im Kreis der Personalreferenten vortragen könne, was dann auch geschah. Ich meine, dass hier eine aktive Unterstützung seitens der Landesregierung angebracht ist und diese die zeitweise Verwendung von Landesmitarbeitern bei meiner Dienststelle als Kompetenzgewinn auch im eigenen Interesse fördern sollte. Weder der Landesverwaltung noch den Bürgern noch mir ist mit reinen „Datenschutzkarrieren“ gedient. Ich habe deshalb vor, demnächst der Landesregierung eine entsprechende Vereinbarung vorzuschlagen, die einen regelmäßigen Personalaustausch vorsieht.

Im Bereich der **Sachmittel** wurde der durch die Stellenentwicklung bedingte, aber auch durch Projekte wie den neuen Internetauftritt entstandene Mehrbedarf im Haushalt berücksichtigt. Der Haushaltsansatz beträgt hier derzeit knapp 127.000 €.

Organisatorisch ist vor allem die bereits im letzten Tätigkeitsbericht angekündigte Bildung des neuen Referats „Technisch-organisatorischer Datenschutz, Medien, Internet, Telekommunikation, E-Government“ zum 1. Januar 2013 zu erwähnen, in dem auch zwei juristische Referentinnen tätig sind.

Die Entwicklung[24] der **Eingaben, Kontrollen und Beratungen** zeigt die nachstehende Übersicht, wobei - wie in den Vorjahren - allerdings zu berücksichtigen ist, dass die Anzahl der Eingaben und - bedingt - auch die der Beratungsfälle von uns nicht zu beeinflussen ist und von tatsächlichen Entwicklungen ebenso abhängt wie vom Medienecho auf echte oder vermeintliche „Datenschutzskandale“.

	2010	2011	2012	2013[25]
Eingaben				
- öffentl. Bereich	2.540	1.788	1.061	1.060
- nicht-öff. Bereich	-	1.033	1.455	1.666
Kontrollen				
- öffentl. Bereich	25	18	13	16
- nicht-öff. Bereich		-	9	11
Beratungen				
- öffentl. Bereich	712	880	1.054	977
- nicht-öff. Bereich		230	450	1.067

Zu den Kontrollmaßnahmen ist auch die arbeitsaufwändige Überprüfung von knapp 4400 Internetauftritten öffentlicher Stellen in Baden-Württemberg im Hinblick auf die Einbindung des Facebook-Like-Buttons im Jahr 2013 zu rechnen (vgl. Kapitel 11.2.3), die in den o. g. Zahlen nicht enthalten ist. Bei Außenterminen gingen Kontrolle

[24] Die Zahlen für den öffentlichen und den nichtöffentlichen Bereich können bis einschließlich 2011 nicht miteinander verglichen werden, da die Erfassungsmethoden der beiden Aufsichtsbehörden voneinander abwichen.
[25] teilweise hochgerechnet

und Beratung häufig ineinander über, was ebenso naheliegend wie sinnvoll ist. Insgesamt ist die Erarbeitung aussagekräftiger Kennzahlen aber noch ein offener Posten auf unserer Agenda. Eine gewisse Vereinfachung erhoffen wir uns hierbei mittelfristig durch die im Frühjahr 2013 begonnene Einführung eines neuen Registraturverfahrens, das auch bei zahlreichen Kommunen im Einsatz ist; ein in der Landesverwaltung verbreitetes anderes Verfahren hatte sich schlicht als zu teuer erwiesen. Die Arbeitsbelastung wird mittlerweile - wie bereits dargelegt - auch durch die zunehmende Zahl der eingehenden fremdsprachigen Dokumente, insbesondere der umfangreichen Arbeitspapiere und Stellungnahmen der Artikel-29-Gruppe, einschließlich ihrer Untergruppen, sowie durch Umfragen in- und ausländischer Datenschutzstellen und Forschungseinrichtungen beeinflusst. In Zukunft werden wir uns in Gremien auf nationaler und internationaler Ebene stärker engagieren müssen; bisher hat sich die Dienststelle aus Kapazitätsgründen hier traditionell vornehm zurückgehalten und anderen beispielsweise den Vorsitz in Datenschutzgremien oder die Mitwirkung in den Untergruppen der Artikel-29-Gruppe überlassen. Im Jahr 2013 haben wir immerhin den Vorsitz in der ad-hoc-AG Videoüberwachung der deutschen Datenschutzbeauftragten übernommen und zwei Sitzungen in Stuttgart durchgeführt.

Dank der Unterstützung des Justizministeriums ist meine Dienststelle inzwischen auch zur regulären Ausbildungsstelle in der Pflichtstation Verwaltung „befördert“ worden; bisher hatten wir hin und wieder Referendare nur in der Wahlstation. Die entsprechende Änderung der Juristenausbildungs- und Prüfungsordnung (JAPrO) ist am 7. Mai 2013 in Kraft getreten. Mittlerweile gibt es vereinzelt auch Anfragen wegen Praktika, z. B. von Studenten an (Fach-)Hochschulen.

2. Innere Sicherheit

2.1 Notwendige, freiwillige und unterlassene Änderungen des Polizeirechts

Das Polizeirecht des Landes ist weiterhin in Bewegung. Im Berichtszeitraum wurde das Polizeigesetz bereits zweimal geändert; eine weitere Änderung ist beabsichtigt. Anlässe waren teils hausgemacht (Polizeistrukturreform), teils den Vorgaben der Europäischen Union und des Bundesverfassungsgerichts geschuldet. Meine datenschutzrechtlichen Anregungen wurden teilweise aufgegriffen, teilweise aber auch verworfen; auch der im Dezember 2013 eingebrachte Gesetzentwurf bildet insoweit keine Ausnahme. Leider wurde der dringende Änderungsbedarf auch bezüglich einiger Forderungen nicht anerkannt, die prominente Vertreter der Regierungskoalition zu Oppositionszeiten noch selbst erhoben haben.

2.1.1. Gesetz zur Änderung des Polizeigesetzes und des Gesetzes zur Ausführung des Personenstandsgesetzes vom 20. November 2012 (LT-Drs. 15/2675)

Mit dem ersten Änderungsgesetz im Berichtszeitraum wurden gleich mehrere europäische Vorgaben umgesetzt. Dazu gehörte der sogenannte **Ratsbeschluss Prüm** (Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität), der in Baden-Württemberg bezüglich der Gefahrenabwehr in geltendes Recht zu überführen war, nachdem auf Bundesebene ein entsprechendes Umsetzungsgesetz bereits am 31. Juli 2009 (BGBl. I S. 2507) verkündet worden war. Der Ratsbeschluss Prüm hatte zum Ziel, Teile der Regelungen des Prümer Vertrages vom 27. Mai 2005 zwischen Deutschland, den Benelux-Staaten, Spanien, Frankreich und Österreich für alle Mitgliedsstaaten der EU verbindlich vorzuschreiben. Die Vorgaben für den Gesetzgeber des Landes betrafen dabei im Wesentlichen den automatisierten Austausch von DNA-Daten, Fingerabdrucksdaten und Daten aus Kraftfahrzeugregistern, den Austausch von Informationen im Zusammenhang mit Großveranstaltungen und den Austausch von Informationen über terroristische Gefährder. Die europarechtliche Vorgabe wurde im Polizeigesetz (PolG) im Wesentlichen durch eine neue Verweisungsnorm umgesetzt, die den Ratsbeschluss bei der polizeilichen Zusammenarbeit mit den Mitgliedsstaaten für anwendbar erklärt (§ 43c PolG neu).

Weiterhin wurde der Rahmenbeschluss 2006/960/JI des Rates über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der EU vom 18. Dezember 2006 umgesetzt. Zur Kritik insbesondere der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der im Rahmen der Umsetzung durch den Bund (Gesetz zur Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedsstaaten der Europäischen Union vom 21. Juli 2012, BGBl. I S. 1566) angehörten Experten an diesem auf eine Initiative Schwedens zurückgehenden Rahmenbeschluss (**„Stockholmer Programm“)** verweise ich auf die Darstellungen in früheren Tätigkeitsberichten (29. Tätigkeitsbericht, LT-Drs. 14/5500, S. 13, 17 ff.; 30. Tätigkeitsbericht, LT-Drs. S. 15/955, S. 34 f.). Trotz der Kritik war die europäische Vorgabe umzusetzen; der Landesgesetzgeber fügte hierzu die §§ 43a, 43b in das Polizeigesetz ein.

Schließlich setzte der Landesgesetzgeber den **Rahmenbeschluss 2008/977/JI** des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen einer polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, um, soweit dies erforderlich war. Auch insoweit hatte der Landesgesetzgeber nur einen geringen Entscheidungsspielraum.

Die Notwendigkeit, europäische Vorgaben in das Landesrecht zu überführen, konnte ich im Rahmen der Anhörung nicht bestreiten. Allerdings wies ich nochmals auf die Mängel der europäischen Rechtssetzung im Bereich der öffentlichen Sicherheit und Justiz - insbesondere ihre mangelnde Konsistenz - hin. Die Länder müssen künftig darauf achten, dass neue Initiativen schlüssiger aufeinander abgestimmt werden.

Mit dem Änderungsgesetz wurden noch weitere Neuerungen vorgenommen, gegen die keine Bedenken bestanden, weil sie im Wesentlichen Vorgaben des Bundesverfassungsgerichts umsetzten: In § 22 Absatz 1 Nr. 5 PolG wurde die überfällige Rechtsgrundlage für den Einsatz von Vertrauenspersonen zur Gefahrenabwehr geschaffen. Nachdem das Bundesverfassungsgericht die in § 113a des Telekommunikationsgesetzes (TKG) vorgesehene Vorratsdatenspeicherung von Verkehrsdaten durch die Telekommunikationsdienste mit Urteil vom 2. März 2010 - 1 BvR 256/08 u. a. - für verfassungswidrig erklärt hatte (vgl. hierzu 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 55) und eine Neuregelung der Vorratsdatenspeicherung nicht in Sicht war, regelt § 23a PolG nun die Erhebung von Verkehrsdaten bei den Telekommunikationsanbietern, die sowohl die polizeiliche Aufgabe der Gefahrenabwehr als auch die Zweckbestimmung der Telekommunikationsdaten beachtet. Ferner wurde in § 23 Absatz 8 PolG eine allgemeine Bestimmung zur Abfrage von Bestandsdaten bei Telekommunikationsanbietern eingefügt.

Allerdings gab es auch Anlass zur Kritik, insbesondere bei der weiteren Verankerung des sogenannten Mitzieheffekts in § 38 Absatz 5 PolG: Nach § 38 PolG darf die Polizei unter bestimmten Voraussetzungen personenbezogene Daten, die ihr im Rahmen von Ermittlungsverfahren bekannt wurden, zur vorbeugenden Bekämpfung von Straftaten speichern. Dabei muss sie innerhalb bestimmter Fristen regelmäßig prüfen, ob die weitere Speicherung zu diesem Zweck noch erforderlich ist. Bereits zuvor war in § 38 Absatz 5 Satz 1 PolG geregelt, dass die Prüffristen spätestens mit Ablauf des Jahres beginnen, in dem das letzte Ereignis erfasst worden ist, das zur Speicherung der personenbezogenen Daten geführt hat. Hierdurch entsteht der **„Mitzieheffekt“**, demzufolge spätere Eintragungen dazu führen, dass im Zeitpunkt der Eintragung eines neuen Ereignisses noch zulässigerweise gespeicherte Daten aus früheren Ermittlungsverfahren weiter gespeichert werden dürfen, selbst wenn das Aussonderungsprüfdatum früherer Erkenntnisse abgelaufen wäre. Dieser „Mitzieheffekt“ führt vielfach zu einer langen Speicherung von Alt- bis Uraltvorgängen, deren aktueller Nutzen nach meinen langjährigen Erfahrungen häufig zweifelhaft ist. Durch den Passus, dass bei weiteren Eintragungen zu derselben Person für alle Speicherungen gemeinsam diejenige Frist gelte, die als letzte endet, wird der Mitzieheffekt noch verstärkt; die Regelung wurde damit aus meiner Sicht in die verkehrte Richtung weiter ausgebaut. Meine Anregung im Gesetzgebungsverfahren, zur Vermeidung von „Datenfriedhöfen“ (vgl. hierzu schon 27. Tätigkeitsbericht 2006, LT-Drs. 14/650, S.44 ff.) stattdessen für die Speicherung von Daten aus Ermittlungsverfahren feste Löschroutinen einzuführen, also die Speicherung eines Vorganges von vornherein für einen festen Zeitraum vorzusehen und den Vorgang ungeachtet späterer Eintragungen im Regelfall zum Ablaufzeitpunkt zu löschen, wurde leider nicht aufgegriffen.

Ferner wurde in § 60 Absatz 4 des Polizeigesetzes eine Bestimmung aufgenommen, die eine Zuständigkeit des Polizeivollzugsdienstes neben den Gesundheitsämtern für die **Anordnung von Maßnahmen nach dem Infektionsschutzgesetz** begründete, wenn Tatsachen die Annahme rechtfertigen, dass eine Übertragung besonders gefährlicher Krankheitserreger auf eine andere Person stattgefunden hat, für diese daher eine Gefahr für Leib oder Leben bestehen könnte und die Kenntnis des Untersuchungsergebnisses für die Abwehr der Gefahr erforderlich ist. Durch den Verweis auf die (inzwischen vom Bundesgesetzgeber wieder abgeänderten) Bestimmungen der §§ 25 Absatz 1 und 26 Absätze 1 und 2 des Infektionsschutzgesetzes wurde dabei klargestellt, dass die erhobenen personenbezogenen Daten nur für Zwecke des Infektionsschutzgesetzes verwendet werden dürfen (vgl. § 26 Absatz 2 Satz 5 des Infektionsschutzgesetzes in der damaligen Fassung). Ich wies darauf hin, dass die Regelung die Gefahr berge, dass der Polizeivollzugsdienst aufgrund seiner Zuständigkeit für die Speicherung von Daten zur Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten nach § 38 Absatz 1 PolG das Untersuchungsergebnis zu einer betroffenen Person in den polizeilichen Auskunftssystemen speichern könnte. Deshalb empfahl ich zu regeln, dass sich die Zuständigkeit des Polizeivollzugsdienstes in der Anordnung der infektionsschutzrechtlichen Maßnahme erschöpfe, er jedoch keine Kenntnis vom Untersuchungsergebnis

erlangen dürfe. Meinem Anliegen wurde insoweit entsprochen, dass in der Gesetzesbegründung noch einmal deutlich erwähnt wurde, dass die erhobenen Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie erhoben wurden (und deshalb nicht zur Gefahrenabwehr gespeichert werden dürfen).

2.1.2 Änderungen durch das Gesetz zur Umsetzung der Polizeistrukturreform vom 23. Juli 2013 (LT-Drs. 15/2675)

Mit der **Polizeistrukturreform** wurde zum 1. Januar 2014 eine grundlegende Umorganisation des Polizeivollzugsdienstes vorgenommen. Insbesondere wurden die bisherigen vier Landespolizeidirektionen in den Regierungspräsidien mit den 37 Polizeipräsidien und Polizeidirektionen zu zwölf regional zuständigen Polizeipräsidien verschmolzen und unmittelbar dem Innenministerium nachgeordnet. Daneben wurden ein neues Präsidium Einsatz und als Einrichtung für den Polizeivollzugsdienst ein Präsidium Einsatz, Logistik, Service der Polizei gebildet. Das Landeskriminalamt und die Hochschule für Polizei blieben im Grundsatz bestehen; allerdings wird in der neuen Struktur eine Vielzahl von Aufgaben anderen Stellen als bisher zugeordnet. Die Polizeistrukturreform selbst hat erhebliche Auswirkungen auf die von ihr betroffenen Bediensteten. Die dazu notwendige Verarbeitung von Personaldaten wurde von meinen Mitarbeitern intensiv geprüft; hierzu und über sonstige Auswirkungen der Polizeistrukturreform auf den Datenschutz, insbesondere durch das neugeschaffene Präsidium Technik, Logistik, Service der Polizei, berichte ich in Kapitel 2.3.

Das Polizeistrukturreformgesetz selbst enthielt im Übrigen keine unmittelbar datenschutzrelevante Änderung des Polizeirechts. Die Änderungen des Polizeigesetzes betrafen im Wesentlichen zwangsläufige organisatorische Regelungen aufgrund der Umsetzung der Polizeistrukturreform.

Allerdings wurde im Rahmen der Strukturreform auch die Durchführungsverordnung zum Polizeigesetz (DVO PolG) geändert. In diesem Zusammenhang empfahl ich - aus meiner Sicht durchaus innerhalb der politischen Vorgabe, dass durch reformunabhängige Änderungen des Polizeirechts keine Verzögerung des Gesetzgebungsverfahrens zum Polizeistrukturreformgesetz entstehen dürften -, einzelne konkret formulierte Änderungen der Verordnung mit aufzunehmen. Meine Empfehlungen betrafen Verbesserungen der Bestimmungen über die Speicherung und Verarbeitung personenbezogener Daten zur vorbeugenden Bekämpfung von Straftaten und wären für den Alltag des Datenschutzes besonders wichtig gewesen. Insbesondere sollte zur Vorbeugung gegen unzulässige Datenabfragen jeder Zugriff auf die polizeilichen Auskunftssysteme - statt wie bisher nur jeder 50. Abruf - protokolliert werden und die Protokolldaten sollten auch bis zu einem Jahr (statt bislang nur für ein halbes Jahr) gespeichert bleiben. Meine Vorschläge wurden leider mit der Begründung abgelehnt, sie stünden nicht im Zusammenhang mit der Reform. Immerhin erklärte die Landesregierung, bei der nächsten Änderung der Verordnung meine Vorschläge prüfen zu wollen.

2.1.3 Geplante Änderungen im Polizeigesetz und im Landesverfassungsschutzgesetz

Anfang Dezember 2013 brachte die Landesregierung einen weiteren Gesetzentwurf zur Änderung des Polizeigesetzes (und des Landesverfassungsschutzgesetzes; zu den geplanten Änderungen des Landesverfassungsschutzgesetzes siehe Kapitel 2.4.1) in den Landtag ein (LT-Drs. 15/4421). Anlass für die abermalige Änderung ist die Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012, 1 BvR 1299/05, in der die Regelungen zur **Bestandsdatenabfrage** für teilweise verfassungswidrig erklärt wurden. Unter Bestandsdaten sind dabei nach § 3 Nummer 3 des Telekommunikationsgesetzes (TKG) Daten des Kunden eines öffentlich zugänglichen Telekommunikationsdienstes zu verstehen, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Hierzu gehören beispielsweise Anschlussnummern, der Name des Anschlussinhabers usw., aber auch Codewörter, deren Eingabe zur Nutzung erforderlich ist, und nach der Lesart mancher auch (dynamische) IP-Adressen. Das Bundesverfassungsgericht hatte entschieden, dass § 113 TKG für die Übermittlung von Auskünften über einfache Bestandsdaten - also Bestandsdaten

ohne Zugangscodes und IP-Adressen - von den Telekommunikationsdienstleistern an die Strafverfolgungs- und Gefahrenabwehrbehörden (ebenso wie an die Verfassungsschutzbehörden) ausreichend ist. Voraussetzung für eine zulässige Datenübermittlung sei allerdings, dass den genannten Behörden aufgrund der für sie gültigen Regelungen auch entsprechende Erhebungsbefugnisse zustünden; denn ähnlich wie beim Durchgang durch eine Doppeltür von jeder Seite eine Tür zu öffnen sei, bedürfe eine Datenübermittlung immer zweier Normen, einer Norm, die die Übermittlung durch die übermittelnde Stelle zulasse, und einer zweiten Norm, die die Erhebung durch die empfangende Stelle erlaube. Die seinerzeit bestehende Übermittlungsnorm für die Telekommunikationsanbieter sei außerdem dahingehend verfassungskonform auszulegen, dass Auskünfte über dynamische IP-Adressen nicht darunter fielen, denn derartige Auskünfte würden immer auch einen Eingriff in das Fernmeldegeheimnis darstellen und daher einer gesonderten Rechtsgrundlage bedürfen. Außerdem sei die bisherige Regelung insoweit verfassungswidrig, als sie Auskünfte über Zugangscodes unabhängig davon erlaube, ob den empfangenden Behörden überhaupt eine Befugnis zu deren Nutzung zukomme. Das Bundesverfassungsgericht gestand den Gesetzgebern und Behörden allerdings eine Übergangsfrist bis zum 30. Juni 2013 zu; bis zu diesem Zeitpunkt durften die genannten Behörden Auskünfte über den Inhaber dynamischer IP-Adressen sowie über Zugangscodes aufgrund der bisherigen Regelung verlangen und erhalten, sofern im Falle eines Auskunftsersuchens über Zugangscodes im Einzelfall eine Befugnis zu deren Nutzung vorlag.

Der **Bundesgesetzgeber** hat noch vor dem Ablauf der Übergangsfrist - am 20. Juni 2013 - ein Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft (BGBl. I S. 1602) in Kraft gesetzt, das die Auskünfte über den Inhaber dynamischer IP-Adressen und über Zugangscodes in Bezug auf die Datenübermittlung durch die Telekommunikationsdienste und in Bezug auf die Datenerhebung durch die Polizeien und Geheimdienste des Bundes neu regelte.

Dementsprechend war auch der **Landesgesetzgeber** gehalten, die Datenerhebung über IP-Adressen und Zugangcodes durch die zuständigen Landesbehörden - namentlich durch den Polizeivollzugsdienst und das Landesamt für Verfassungsschutz - neu zu regeln, soweit entsprechende Datenerhebungen für erforderlich erachtet werden (einfache Bestandsdatenauskünfte konnten durch den Polizeivollzugsdienst bereits aufgrund der Gesetzesänderung vom 20. November 2012 [s. o.] nach § 23a Absatz 9 PolG eingeholt werden). Die Landesregierung hat zwar im Laufe des Jahres 2013 mit den Arbeiten an einem Gesetzentwurf begonnen - und mich dankenswerter Weise früh zur Beratung hinzugezogen -, allerdings die bis zum 30. Juni 2013 gesetzte Frist des Bundesverfassungsgerichts zunächst verstreichen lassen, so dass derzeit weder der Polizeivollzugsdienst noch das Landesamt für Verfassungsschutz nach § 113 TKG Auskünfte über IP-Adressen oder über Zugangscodes verlangen dürfen.

Im Herbst 2013 hatte ich Gelegenheit, zum **Referentenentwurf des Innenministeriums** Stellung zu nehmen. Er griff im Bereich des Polizeirechts einige meiner Anregungen auf. Positiv hervorzuheben ist vor allem, dass Auskünfte über den Inhaber einer dynamischen IP-Adresse ebenso wie über Zugangcodes in materieller Hinsicht nur zur Abwehr bestimmter qualifizierter Gefahren (nämlich von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder einer gemeinen Gefahr) zugelassen werden. Die Forderung des Bundesverfassungsgerichts, aus einer Befugnisnorm zur Abfrage von Zugangscodes müsse klar hervorgehen, dass diese nur dann erhoben werden dürften, wenn auch die beabsichtigte Nutzung des Zugangscodes durch die Behörde zulässig sei, wurde durch eine nahezu wörtliche Übernahme der Formulierung des Bundesverfassungsgerichts erfüllt.

Kritik äußerte ich im Rahmen meiner Stellungnahme im Hinblick auf die förmlichen Voraussetzung dieser Abfragen: Entsprechend den Vorgaben des Bundesverfassungsgerichts sollten bei Erhebungen zum Inhaber von IP-Adressen die

rechtlichen und tatsächlichen Grundlagen - also die Subsumtion des Einzelfalls - aktenkundig gemacht werden; dies sollte meines Erachtens sowohl bei IP-Adressen-Abfragen als auch bei Auskunftsersuchen über Zugangscodes dadurch sichergestellt werden, dass beispielsweise nach dem Vorbild des § 20a Absatz 3 des nordrhein-westfälischen Polizeigesetzes eine schriftliche Anordnung des Behördenleiters gefordert wird, in der insbesondere die tragenden Erkenntnisse für das Vorliegen der konkreten qualifizierten Gefahr und die Begründung der Verhältnismäßigkeit der Maßnahme darzulegen sind. Ein weiterer Kritikpunkt ist aus meiner Sicht, dass bestimmte Nutzungsdaten nach § 15 des Telemediengesetzes (TMG) den Bestandsdaten i. S. des Telekommunikationsgesetzes gleichgestellt werden sollen, obwohl an die Erhebung von Nutzungsdaten meines Erachtens zumindest dieselben Anforderungen wie an die Erhebung von Verkehrsdaten i. S. des Telekommunikationsgesetzes gestellt werden sollten. Auch die vorgesehenen Regelungen zur Benachrichtigung der Betroffenen hielt ich vor dem Hintergrund der verfassungsgerichtlichen Rechtsprechung ebenfalls für verbesserungsbedürftig.

Meine Kritik fand teilweise Eingang in den nunmehr in den Landtag eingebrachten Gesetzentwurf. Insbesondere wurden die Regelungen zur Benachrichtigung der Betroffenen überarbeitet. An der Gleichsetzung von bestimmten Nutzungsdaten nach § 15 TMG mit Bestandsdaten will man dagegen - anders übrigens als im Geltungsbereich des Landesverfassungsschutzgesetzes - festhalten. Auch meinem Rat, die vom Bundesverfassungsgericht geforderten Dokumentationspflichten festzuschreiben, ist die Landesregierung in ihrem Gesetzentwurf nur für das Verfassungsschutzrecht, nicht aber für das Polizeirecht gefolgt. Eine Rechtfertigung für diese Unterschiede zwischen Polizei- und Verfassungsschutzrecht sehe ich nicht und hoffe, dass im Rahmen der Erörterungen im Landtag noch eine Harmonisierung auf dem jeweils datenschutzfreundlicheren Niveau erfolgen wird.

2.1.4 Der Sinneswandel im Polizeirecht

In den genannten Gesetzgebungsverfahren habe ich mehrfach weitere Änderungen des Polizeirechts empfohlen, die bisher leider unberücksichtigt blieben; diese betrafen vor allem die **automatische Kennzeichenerfassung** und die Regelungen zur **Verarbeitung von Daten zur vorbeugenden Bekämpfung von Straftaten**.

Die automatische Kennzeichenerfassung, bei der verdachtslos die amtlichen Kennzeichen aller an dem Gerät vorbeifahrenden Fahrzeuge erfasst und mit einem Fahndungsbestand abgeglichen werden, war bereits in früheren Tätigkeitsberichten thematisiert worden. Schon im Frühjahr 2004 hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Bedenken erhoben (vgl. 25. Tätigkeitsbericht, LT-Drs. 13/2650, Anhang 3, S. 180) und erneut in einer Entschließung vom Oktober 2005 (vgl. 26. Tätigkeitsbericht, LT-Drs. 13/4910, Anhang 5, S. 114). Im Jahr 2006 konnte ein ohne gültige Rechtsgrundlage geplanter Pilotversuch verhindert werden (27. Tätigkeitsbericht, LT-Drs. 14/650, S. 31). Und bei der Einfügung des § 22a PolG in das Polizeigesetz wurde wieder auf durchgreifende Bedenken gegen die Regelung hingewiesen (vgl. 29. Tätigkeitsbericht, LT-Drs. 14/5500, S. 36): Zum einen ist die Regelungskompetenz des Landesgesetzgebers fraglich, da diese für den Bereich der Strafverfolgung nach den Grundsätzen der konkurrierenden Gesetzgebung gemäß Artikel 72 Absatz 1 des Grundgesetzes dem Bund zusteht. Zum anderen ist die Regelung hinsichtlich des Mitteleinsatzes zu unbestimmt. Ob die verfassungsrechtlichen Vorgaben (vgl. Urteil des Bundesverfassungsgerichts zu den entsprechenden Regelungen in Hessen und Schleswig-Holstein vom 11. März 2008 - 1 BvR 2074/05 u. a.) eingehalten wurden, ist zweifelhaft; die Entscheidung über eine anhängige Verfassungsbeschwerde (1 BvR 2795/09) wegen des § 22a PolG steht noch aus.

Offen gesagt finde ich es erstaunlich, dass in der 15. Wahlperiode an der bisherigen Regelung der automatischen Kennzeichenerfassung festgehalten wird, obgleich es in der 14. Wahlperiode Änderungsanträge der damaligen Opposition gab (vgl. Änderungsanträge der Fraktion Bündnis 90/

Die Grünen, LT-Drs. 14/3475, S. 1 f., und der Fraktion der SPD, a. a. O., S. 5) und vor allem entsprechende Aussagen in der Ersten und Zweiten Lesung. So bezeichnete der heutige Innenminister seinerzeit die Regelung als „zu starken Eingriff in einem demokratischen Staat“, deren Geeignetheit angesichts der geringen Trefferquoten bei Erfahrungen anderer Länder in Frage stehe (Plenarprotokoll 14/52 vom 2. Oktober 2008, S. 3682 [3683 f.]; Plenarprotokoll 14/54 vom 6. November 2008, 3795 [3796]), und auch der Vertreter der Fraktion Bündnis 90/Die Grünen kritisierte die Regelung im Plenum als „überprüfungsbedürftig und … [im Hinblick auf das zitierte Urteil des Bundesverfassungsgerichts] bedenklich“ (Plenarprotokoll 14/52 vom 2. Oktober 2008, 3684 [3685 f.]; Plenarprotokoll 14/54 vom 6. November 2008, S. 3799). Eine praktische Notwendigkeit für die Maßnahme ist auch fünf Jahre nach dem Inkrafttreten der gesetzlichen Regelung nicht zu erkennen.

Ebenso wenig nachvollziehbar ist für mich die mangelnde Bereitschaft, die Regelungen zu einer überzogenen Speicherung von Daten zur vorbeugenden Bekämpfung von Straftaten zu überarbeiten. Die polizeilichen Auskunftssysteme leiden darunter, dass zahlreiche nicht erforderliche Daten gespeichert sind und - wie wir aus zahlreichen Eingaben wissen - viele Bürger belasten. Außer den bereits oben erwähnten Alt- und Uraltvorgängen gehören vor allem Bagatelldelikte dazu. Eine der Ursachen für die ausufernden Speicherungen ist die im Jahr 2008 entgegen den Empfehlungen meiner Dienststelle (s. hierzu bereits 29. Tätigkeitsbericht, LT-Drs. 14/5500, S. 36 ff.) und gegen die Stimmen der damaligen Opposition eingeführte Bestimmung des § 38 Absatz 2 PolG. Diese begründet eine Ausnahme von dem Grundsatz, dass Speicherungen zur vorbeugenden Bekämpfung von Straftaten nur dann zulässig sind, wenn tatsächliche Anhaltspunkte sowohl für den Verdacht, dass die betroffene Person eine Straftat begangen hat, als auch dafür vorliegen, dass die betroffene Person zukünftig eine Straftat begehen wird (vgl. § 38 Absatz 3 Satz 1 PolG), wobei sich solche Anhaltspunkte für eine Negativprognose insbesondere auch aus Art, Ausführung und Schwere der Tat, derer der Betroffene verdächtig ist, ergeben können. Abweichend hiervon erklärt die Bestimmung des § 38 Absatz 2 PolG bis zu einer Dauer von zwei Jahren die Speicherung, Veränderung und Nutzung der Daten bereits dann als erforderlich, wenn allein ein Tatverdacht besteht, ohne dass es auf das Bestehen von Anhaltspunkten für weitere künftige Straftaten des Betroffenen ankommen soll. Dies bewirkt, dass routinemäßig von der Polizei bearbeitete Ermittlungen für zwei Jahre gespeichert werden, bei denen der Tatverdacht nicht vollständig ausgeräumt wurde, selbst wenn es sich um Bagatelldelikte handelt und eine Wiederholungsprognose nicht gestellt werden kann. Ich halte nach wie vor diese Speicherungen für die vorbeugende Bekämpfung von Straftaten nicht für erforderlich; sie blähen den Umfang der polizeilichen Datensammlungen nur unnötig auf.

Auch hierzu kann ich nur unterstreichen, was der heutige Innenminister sowohl in der Ersten als auch in der Zweiten Lesung des damaligen Gesetzentwurfs zur Einfügung des § 38 Absatz 2 PolG äußerte (Plenarprotokoll 14/52 vom 2. Oktober 2008, S. 3682 [3683 f.]; Plenarprotokoll 14/54 vom 6. November 2008, 3795 [3796]): Die Neuregelung sei kaum geeignet, Straftaten zu verhindern, und stelle Betroffene unnötig zwei Jahre lang unter Generalverdacht. Mit ausufernder Datenspeicherung erreiche man letztendlich nichts anderes, als den Heuhaufen der Datenmenge immer mehr zu vergrößern, so dass die Nadel des Verbrechens hierbei immer schwerer zu finden sei. Seine Fraktion hatte damals den Antrag gestellt, von der Einfügung dieser Regelung abzusehen (LT-Drs. 14/3475, S. 6). Warum dennoch an der Regelung des § 38 Absatz 2 PolG festgehalten wird, bleibt mir ein Rätsel. Sollte der Sinneswandel mit der Übernahme des Ministeramts und dem starken Einfluss des Polizeivollzugsdienstes im Innenministerium zusammenhängen?

Weitere Anregungen zur Änderung des Polizeirechts habe ich im Rahmen des Gesetzgebungsvorhabens zur Polizeistrukturreform gegeben, mich dabei jedoch im Hinblick auf die Eilbedürftigkeit des Vorhabens auf kleine, aber datenschutzrechtlich bedeutsame Änderungen der Durchführungsverordnung zum Polizeigesetz (DVO PolG) beschränkt, die ohnehin durch das Polizeistrukturreformgesetz geändert wurde. Aber auch diese

wurden nicht berücksichtigt. Damit bleibt die ausführlichere Auswahlprotokollierung für die Zugriffe auf die polizeilichen Auskunftssysteme auf jeden 50. Fall beschränkt und wird nur für ein halbes Jahr gespeichert. Schon bei der Speicherdauer wäre eine Erhöhung auf ein Jahr geboten gewesen. Und die von mir angeregte Vollprotokollierung würde eine wirksamere Hürde zur Verhinderung unzulässiger Datenbankabfragen darstellen.

Ob die Regierungsfraktionen des Landtags die eigenen Vorschläge aus Oppositionszeiten aufgreifen werden, bleibt abzuwarten. Ich werde im Interesse der Bürgerrechte nicht zögern, sie immer wieder daran zu erinnern.

2.2 Datenverarbeitung durch Sicherheits- und Ordnungsbehörden

2.2.1 Der Polizeivollzugsdienst und seine Dateien

Für den Polizeivollzugsdienst des Landes ist die Nutzung der Auskunftssysteme auf Bundes- und Landesebene eine Selbstverständlichkeit. Rechtsgrundlagen dafür sind vor allem das Bundeskriminalamtsgesetz für die Verbunddateien und das Polizeigesetz für die Anwendungen im Land. Die auf diesen Bestimmungen basierenden Dateien unterliegen einem permanenten Änderungsprozess, der auch meine Dienststelle bei Beratungen, Stellungnahmen zu Änderungen oder im Zusammenhang mit Kontrollen und Eingaben fordert.

Schon im Jahr 2011 wurde ich darüber unterrichtet, dass sich in der bundesweiten Informationslandschaft der Polizei etwas ändern soll. Die jetzt noch bestehende Struktur auf der Ebene der am INPOL-Verbund teilnehmenden Polizeien des Bundes und der Länder soll hinsichtlich der Datenstrukturen und Standards für jeglichen Informationsaustausch vereinheitlicht werden. Dabei sollen für den polizeiexternen Datenaustausch die im Projekt „Deutschland-online“ entwickelten Standards als Orientierung für das „Informationsmodell Polizei (IMP)“ dienen und konzeptionell die Basis für alle polizeilichen Softwareanwendungen bilden.

Eine solche Anwendung wird der „Polizeiliche Informations- und Analyseverbund (PIAV)“ sein. Dieser Verbund soll langfristig die bisher bestehenden Meldedienste zwischen den Polizeien des Bundes und der Länder ersetzen. Dadurch sollen Zusammenhänge zwischen Taten und Tätern leichter hergestellt werden können, um die Polizeidienststellen in verschiedenen Ländern gezielter zu unterstützen und den derzeitigen finanziellen Aufwand für die INPOL-Fall-Dateien zu verringern. Als erste operative Pilotanwendung in PIAV wird derzeit der Bereich „Waffen/Sprengstoff“ entwickelt, der im Jahr 2015 in Betrieb gehen soll. Bis dahin soll noch ein Lastenheft erstellt werden, das mir noch zur datenschutzrechtlichen Bewertung zugehen wird. In einem Informationsgespräch wurde meinen Mitarbeitern zugesichert, dass die Rechtevergabe für die Nutzung sehr eng an den Aufgabenstellungen orientiert werde. Die Nutzung des Verbunds werde in dem Landesfallbearbeitungssystem erfolgen, aus dem auch die Daten angeliefert werden. Dabei sollen die datenschutzrechtlichen Anforderungen zur Speicherung personenbezogener Daten beachtet werden. Über die weitere Entwicklung werde ich erst im nächsten Tätigkeitsbericht berichten können.

Ein anderes Kapitel in der polizeilichen Datenverarbeitung ist die im Einzelfall erfolgende Speicherung von besonderen Hinweisen zu auffällig gewordenen Personen, die aus polizeilicher Sicht für den Fall eines Kontaktes mit dieser Person beim Einschreiten oder bei Ermittlungen hilfreich sein können. Der Katalog dieser „personengebundenen Hinweise (PHW)“ ist für die Verbunddateien einheitlich vorgegeben, für das jeweilige Landessystem, in Baden-Württemberg POLAS-BW, war gleichwohl beabsichtigt, noch weitere Merkmale zu verwenden. Das Innenministerium unterrichtete mich im Herbst 2012 mit der Bitte um Stellungnahme über die Streichung, die Beibehaltung und die Wiedereinführung bestimmter personengebundener Hinweise. Da zwei bestimmte Hinweise beibehalten werden sollten, bat ich um nähere Begründung, da diese im bundeseinheitlichen Katalog nicht mehr vorgesehen waren.

Besonders setzte ich mich mit dem Hinweis „Freitodgefahr“ auseinander, der im Landessystem wieder eingeführt werden sollte, nachdem er aufgrund einer Beanstandung meiner Amtsvorgängerin bereits im Jahr 1992 ausgesetzt worden war. Zum einen bezweifelte ich, dass damit die Wahrnehmung polizeilicher Aufgaben sachgerecht unterstützt werden kann. Zum anderen bedauerte ich, dass der aus wissenschaftlicher Sicht geeignetere Begriff „Suizidgefahr“ nicht verwendet wurde, allerdings hatte bereits der Bundesgesetzgeber in § 2 Absatz 1 Nummer 15 der BKA-Daten-Verordnung zur Ausführung von § 7 Absatz 3 des Bundeskriminalamtsgesetzes den Begriff „Freitodgefahr“ fixiert. Letztlich kritisierte ich noch die vorgesehene Speicherungsdauer von zwei Jahren, die nach Prüfung erneut vergeben werden kann. Auf die Erfüllung meiner Bitte, vor einer landesweiten Freigabe der PHW mir eine Stellungnahme zu meinen Anmerkungen zukommen zu lassen, warte ich allerdings seit über einem Jahr.

Bereits im 28. Tätigkeitsbericht (LT-Drs. 14/2050, S. 26 ff.) war die Verarbeitung erkennungsdienstlicher Unterlagen beim Bundeskriminalamt als unbefriedigend bezeichnet worden, weil dieses Amt nach Aufgabe des Besitzes an solchen Unterlagen durch die ursprünglich zuständige Landespolizei eine „Besitzübernahme“ erklärte und diese Daten als eigenen Bestand weiterspeicherte. Die auch vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gegenüber dem Bundesministerium des Innern vorgetragene Kritik führte inzwischen dazu, dass ein mehrere hunderttausend Fälle umfassender Bestand gelöscht wurde. Allerdings hat meine Dienststelle in Einzelfällen immer wieder festgestellt, dass die Polizeidienststellen im Land bei der Löschung der Daten aus erkennungsdienstlichen Behandlungen nicht immer konsequent das Bundeskriminalamt darüber unterrichteten, damit dieses die Daten ebenfalls in seiner eigenen Datei löschen konnte. Sofern diese gesonderte Information des Bundeskriminalamts durch eine verantwortliche Stelle nicht erfolgt, führt die Verknüpfung der INPOL-Zentraldatei mit dem Auskunftssystem POLAS-BW automatisch dazu, dass der betreffende Fall in einen anstehenden Löschwarnlauf nicht aufgenommen wird. Eine technische Lösung kann nach Aussage des Landeskriminalamts vom Bundeskriminalamt nur in Zusammenarbeit mit den anderen INPOL-Teilnehmern entwickelt werden, ein Zeithorizont konnte meiner Dienststelle nicht genannt werden. Bis dahin muss jede Polizeidienststelle im Land dafür sorgen, dass das Bundeskriminalamt von der Löschung im Land erfährt und seiner eigenen Löschpflicht nachkommen kann.

Letztlich hat auch die Polizeistrukturreform erhebliche Auswirkungen auf die Datenverarbeitung des Polizeivollzugsdienstes im Land. Die gesamte bisherige Struktur musste bis zum 1. Januar 2014 in die neue Struktur überführt werden. Da dies nicht in einer juristischen Sekunde von 41 Stellen auf nur noch 16 Stellen zum Jahreswechsel funktionieren kann, wurde meine Dienststelle von dem zuständigen Teilprojekt zur Umsetzung der Reform um Beratung gebeten. Dabei konnte eine Lösung gefunden werden, die zwar nicht ganz der reinen datenschutzrechtlichen „Lehre“ entsprach, aber unter Berücksichtigung der nur wenige Wochen umfassenden Übergangsphase und im Hinblick auf die ausdrückliche schriftliche Erinnerung an die datenschutzrechtliche Verpflichtung jedes einzelnen Beschäftigten hingenommen werden konnte. In gleicher Weise muss auch das bisherige Lagebildinformationssystem LABIS, mit dem sich meine Dienststelle zum ersten Mal im Jahr 2003 befasst hatte (24. Tätigkeitsbericht, LT-Drs. 13/2650, S. 19 ff.), vollkommen auf die neue Struktur umgestellt werden. Dies wurde meinen Mitarbeitern durch das Landeskriminalamt vorgestellt; soweit die bisherigen datenschutzrechtlichen Standards beibehalten werden, ist dieses aus meiner Sicht unproblematisch. Gleichzeitig unterrichtete das Landeskriminalamt noch über weitere Maßnahmen der IT-Sicherheit und über Handreichungen für die neuen Dienststellen, damit auch dort von Anfang an die inzwischen erreichten datenschutzrechtlichen Standards ohne Bruch erhalten werden können. Die in den letzten Monaten erkennbare konstruktive Zusammenarbeit bei der Klärung aktueller datenschutzrechtlicher Probleme lässt hoffen, dass diese in der neuen Struktur des Polizeivollzugsdienstes fortgesetzt wird, zumal die wichtigen Datenverarbeitungen in POLAS-BW, die Vorgangsbearbeitung ComVor, die Fallbearbeitung in CRIME und in den vielen anderen Anwendungen auf Bundes- und Landesebene sich nicht verändern.

2.2.2 Was der Tatort nicht zeigt - die Mitarbeiterdatenbank der Polizei

Es ist für einen Täter nahezu unmöglich, seine genetischen Spuren, also seine DNA, nicht am Tatort zu hinterlassen. Den Ermittlern am Tatort geht es ebenso. Um die Tatrelevanz einer genetischen Spur am Tatort beurteilen zu können, sind daher „berechtigte Spurenverursacher" auszuschließen. Hierzu können auch Einsatz- und Rettungskräfte, z. B. ein Notarzt, ein Feuerwehrmann, Spurensicherungsbeamte der Polizei oder Laborpersonal der forensischen Untersuchungsstellen gehören, die - trotz aller professionellen Schutzmaßnahmen - nach dem eigentlichen Tatgeschehen ihre Spuren direkt oder mittelbar hinterlassen haben.

Im April 2007 wurde eine 22-jährige Polizistin auf der Heilbronner Theresienwiese tödlich und ihr damals 24-jähriger Kollege mit einem Kopfschuss schwer verletzt. Am Streifenfahrzeug konnte eine DNA-Spur gesichert werden, die bereits vor, aber auch nach dieser Tat im Zusammenhang mit einer Vielzahl von weiteren Straftaten festgestellt wurde. Überprüfungen des Landeskriminalamtes Baden-Württemberg im März 2009 ergaben, dass das an verschiedenen Tatorten in Hessen, Rheinland-Pfalz, im Saarland, in Baden-Württemberg, Frankreich und Österreich aufgefundene DNA-Profil keiner Serientäterin, sondern einer Fabrikarbeiterin zuzuschreiben war, die an der Produktion von Spurensicherungs-Wattestäbchen beteiligt war. Vor diesem Hintergrund wurde in Baden-Württemberg noch im April 2009 ein Expertenkreis zur „Qualitätsicherung bei der DNA-Analyse" einberufen, der Lösungsansätze entwickeln sollte, um das Risiko der Fremdkontamination von Spuren und Spurensicherungsmaterialien künftig weitestgehend zu minimieren. Eine der Empfehlungen des Gremiums war es, eine sog. „Eliminationsdatenbank" mit den DNA-Identifizierungsmustern der mit der Spurensicherung beauftragten Personen anzulegen, um jede am Tatort aufgefundene DNA-Spur damit abgleichen zu können.

Auf Bundesebene befasste sich eine Bund-Länder-Projektgruppe „DNA-Standards" mit dem gleichen Thema. Auch die Innenministerkonferenz äußerte sich zu den „Mindeststandards zur Kontaminationsvermeidung und -erkennung im Zusammenhang mit der DNA-Spurensicherung und -untersuchung". Beide Gremien empfahlen ebenfalls Eliminationsdatenbanken für Labor- und Spurensicherungspersonal und darüber hinaus eine Datenbank mit DNA-Profilen von Mitarbeitern von Herstellerfirmen. In der Folge begann die Polizei in Baden-Württemberg mit dem Aufbau einer Mitarbeiterdatenbank-DNA Polizei (MADB-Polizei).

Aber darf das Land Baden-Württemberg als Dienstherr von seinen Mitarbeitern die Herausgabe der DNA-Muster verlangen und diese in eine Datei einstellen? Und wie kann der Dienstherr sicherstellen, dass ein Mitarbeiter der Polizei im sog. „Trefferfall" nicht automatisch für den Tatverdächtigen gehalten wird? In Österreich sind die Beamten z. B. gesetzlich zur Abgabe einer Speichelprobe und zur dauerhaften Speicherung des DNA-Codes verpflichtet. In Baden-Württemberg kann mangels einer solchen gesetzlichen Grundlage die Entscheidung nur beim Betroffenen selbst liegen: Zwar können im Einzelfall alle an einem Tatort befindlichen Personen aus strafprozessualen Gründen zur Abgabe einer DNA-Probe veranlasst werden, um Trugspuren auszuschließen. Wenn eine Datei, die in einem automatisierten Abrufverfahren i. S. des § 8 des Landesdatenschutzgesetzes (LDSG) die entsprechenden Daten dauerhaft vorhält, eingerichtet werden soll, so kann der Dienstherr keinen Mitarbeiter zur Abgabe einer Speichelprobe verpflichten. Selbst wenn es bei den zu speichernden DNA-Mustern „nur" um jene Abschnitte der DNA geht, die keine individuellen Erbinformationen, wie z. B. die Augen- oder Haarfarbe, enthalten, aber trotzdem unverwechselbar sind, so sind diese keine Beschäftigtendaten i. S. des § 36 LDSG. Denn zu diesen gehören nur solche, die für die Organisation des Dienstbetriebs erforderlich sind und die der Arbeitgeber deshalb einfordern darf.

Um deutlich zu machen, dass es sich bei der MADB-Polizei um eine völlig andere Dateianwendung der Polizei handelt, die weder den Bestimmungen des Polizeigesetzes noch denen der Strafprozessordnung unterfällt, wird sie zwar beim Landeskriminalamt, dort aber beim Kriminaltechnischen Institut (KTI), betrieben. Neben den DNA-

Proben von Mitarbeiterinnen und Mitarbeitern des KTI und der Polizei sind auch die der Handwerker und des Wartungspersonals gespeichert, die die technischen Geräte im Kriminaltechnischen Institut reparieren oder warten, mit denen die DNA-Proben analysiert werden. Denn die von diesen Personen möglicherweise verursachten Trugspuren müssen ebenfalls ausgeschlossen werden können.

Der einzige Weg, um eine solche Eliminationsdatenbank einrichten zu können, geht für die Polizei in Baden-Württemberg - auch aus meiner Sicht - über die schriftliche und informierte Einwilligung der Betroffenen nach § 4 Absatz 1 Nr. 2 i. V. m. Absätze 2 und 3 LDSG. Es ging aber nicht nur um den zukünftigen Ausschluss von Trugspuren. In einer weiteren Einwilligungserklärung konnten sich die Beschäftigten zu einem retrograden Abgleich der DNA-Identifizierungsmuster mit den in der forensischen DNA-Analyse-Datei gespeicherten DNA-Spuren einverstanden erklären. Auf dieser Grundlage sind tatsächlich Trugspuren aus früheren Fällen erkannt worden. Da ich Einwilligungen von Arbeitnehmern gegenüber ihrem Arbeitgeber aufgrund des immanenten Abhängigkeitsverhältnisses immer kritisch sehe, ist mir wichtig, dass jeder betroffene Polizeiangehörige ohne negative Folgen für seine weitere berufliche Tätigkeit die Einwilligung verweigern kann und dass die Möglichkeit besteht, die Einwilligung zu widerrufen.

Bei einem Kontrollbesuch im KTI konnten meine Mitarbeiter in alle datenschutzrechtlich relevanten Datenverarbeitungen Einblick nehmen und sich über die verwendeten Informationsblätter für die Mitarbeiter unterrichten lassen. Erkennbares Ziel - so wurde uns erläutert - sei vor allem gewesen, über die mit der Datenbank verbundenen Vorteile der Verbesserung der Qualität der Untersuchung von Tatortspuren zu informieren und gleichzeitig deutlich zu machen, dass mit der Verfahrensweise eine Entlastung der forensischen DNA-Analyse-Datenbank verbunden sei, wenn die Spuren tatort- und spurenberechtigter Personen dort nicht gespeichert werden müssten.
Das Berechtigungskonzept für die MADB-Polizei sieht streng voneinander abgegrenzte Zugriffsrechte vor, so dass nur die Administratoren völligen Einblick nehmen können, alle anderen Berechtigten aber nur für den unbedingt für sie notwendigen Umfang Zugriff haben. Für die Rollen „Personal“ und „Kurzprüfung“, die von besonderem Interesse sind, sind insgesamt 56 Berechtigte erfasst. Hierzu wurde verdeutlicht, dass gerade im Hinblick auf die Bereitschaft der betroffenen Personen eine möglichst weitgehende Trennung der Rollen angestrebt wird.

Auf der Ebene der Polizeidienststellen gibt es außerdem eine von den Beschäftigten als besonders vertrauenswürdig angesehene Person, die die Einwilligungen entgegennimmt und aufbewahrt sowie den Datensatz in der Datenbank erfasst.

Die Personendaten und die DNA-Muster werden getrennt gespeichert, so dass nur über den Anonymisierungscode eine Zuordnung zu einer bestimmten Person möglich ist. Für die eigentliche Analyse der DNA-Proben reichen daher Barcodes aus, die im KTI zur Ermittlung des DNA-Identifizierungsmusters durch das beauftragte Labor verwendet werden. Das Labor seinerseits nutzt beim Eingang der Probe ebenfalls einen Barcode zur Kennzeichnung, analysiert die Probe, vernichtet diese anschließend und überträgt das Ergebnis des Gutachtens in einen QR-Code neben dem Klartext. Die auf diese Weise übermittelten Ergebnisse werden vom KTI in die MADB-Polizei dem jeweiligen Anonymisierungscode zugespeichert, also völlig getrennt von den personenbezogenen Daten des betreffenden Probengebers.

Wie geschieht nun im Trefferfall? Zunächst erfolgt eine sog. „Kurzprüfung“ durch besonders berechtigte Personen. Die Plausibilität einer möglichen Kontamination wird anhand von Dienstplänen sowie räumlichen und zeitlichen Gegebenheiten geprüft. Wird eine Trugspur durch eine berechtigte Person festgestellt, so wird dies dem LKA in anonymisierter Form mitgeteilt. Die Trugspur wird also nicht in die forensische DNA-Analyse-Datei eingestellt.

Sollte sich ein Treffer nicht schlüssig begründen lassen, erfolgt eine intensive Prüfung durch eine spezielle Fallkonferenz. Erst wenn weitere Umstände bekannt werden, die den Anfangsverdacht einer Straftat begründen, sind der jeweilige

Dienststellenleiter und die Staatsanwaltschaft zu unterrichten. Seit der Einführung der MADB-Polizei gab es 110 Trefferfälle, die alle über die Kurzprüfung als Trugspur erkannt werden konnten.

Unter den beschriebenen Bedingungen habe ich die Mitarbeiterdatenbank letztlich als datenschutzrechtlich vertretbar akzeptiert. Der frühzeitig beteiligte Hauptpersonalrat der Polizei hatte - was mir angesichts der sensiblen Thematik wichtig war - zuvor ebenfalls seinen Segen dazu gegeben.

Mit der Mitarbeiterdatenbank können unnötige Datenerhebungen bei der Verfolgung falscher Ermittlungsansätze vermieden werden. Dem Grundsatz der Verhältnismäßigkeit wird dadurch Rechnung getragen, dass am Tatort aufgefundene Spuren nur mit den Referenzdaten der für den Tatort zuständigen Dienststelle sowie den Referenzdaten der zuständigen Labormitarbeiter abgeglichen werden, nicht jedoch mit dem Gesamtdatenbestand aller Beschäftigten. Außerdem wird im Trefferfall ein Stufenkonzept zur Plausibilitätsprüfung realisiert.

2.2.3 Drohen Drohnen? Überlegungen zur polizeilichen Videoüberwachung aus der Luft

Quadrocopter für rd. 300 €, Steuerung über das Smartphone: schon ist es möglich von oben in Nachbars Garten zu schauen. Für derartige, oft als „Drohnen“ bezeichnete Fluggeräte interessieren sich mittlerweile auch öffentliche Stellen. Sie können - allerdings in größerer und stärkerer, aber auch deutlicher teurerer Ausführung als die Angebote der Elektronikhändler - ggf. Aufklärungsmaßnahmen bei Einsätzen besser unterstützen als beispielsweise Helikopter. Bei einigen Länderpolizeien gibt es bereits Exemplare, die baden-württembergische Polizei verfügt wie viele andere Länderpolizeien darüber noch nicht. Gleichwohl wurde in einem Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Frage nachgegangen, wie die Videoüberwachung mittels „Drohnen“ datenschutzrechtlich zu bewerten ist.

In allen Polizeigesetzen der Länder gibt es Bestimmungen über den Einsatz von Geräten zur Videoüberwachung zum Zwecke der Gefahrenabwehr. In Baden-Württemberg regelt § 21 des Polizeigesetzes (PolG) die Anfertigung von offenen, also für jeden erkennbare Bildaufzeichnungen. In der Regelung sind die Voraussetzungen, insbesondere die Orte und die Kenntlichmachung der Anfertigung von Bildaufzeichnungen geregelt. Keine Aussage trifft das Gesetz dagegen zu der Technik, die die Videoaufnahmen ermöglicht. Damit können Orte mittels ferngesteuerten Videokameras überwacht werden, was eine Kennzeichnung des überwachten Bereichs erfordert; auf das Beispiel des Vorplatzes am Mannheimer Hauptbahnhof, dessen **Videoüberwachung** seit mehreren Jahren immer wieder in den Tätigkeitsberichten Thema war, darf ich verweisen. Soweit Polizeibeamte in Uniform mit Videokameras tätig werden, ist nach der gesetzlichen Regelung der Erkennbarkeit Genüge getan. Sobald ein Polizeihubschrauber mit einer entsprechenden Kennzeichnung über einem Gelände kreist, wird man zwar eine Videokamera nicht ohne weiteres erkennen, aber die Erfüllung der gesetzlichen Voraussetzungen der Kennzeichnung wird eher gegeben sein. Dieses dürfte bei „**Drohnen**“ anders sein, die aufgrund der elektrischen Antriebsart erheblich leiser und bei einer Flughöhe von 100 bis 150 Meter über Grund mit dem bloßen Auge kaum noch zu erkennen sind. Dies gilt dann erst recht für eine Kennzeichnung an dem Fluggerät. Insofern sind Videoaufnahmen mittels einer „Drohne“ eher als verdeckter Einsatz zur Anfertigung von Bildaufzeichnungen nach den Regelungen des § 22 PolG zu bewerten, es sei denn, der Einsatz erfolgt in einem begrenzten Bereich, der nach § 21 Absatz 5 PolG gekennzeichnet ist.

Auch die Regelungen des Luftverkehrsrechts helfen bei der Bewertung nicht unbedingt weiter. Nach § 1 Absatz 2 des Luftverkehrsgesetzes (LuftVG) gelten als Luftfahrzeuge unbemannte Fluggeräte einschließlich ihrer Kontrollstation, die nicht zu Zwecken des Sports oder zur Freizeitgestaltung betrieben werden; sie werden als unbemannte Luftfahrtsysteme definiert. Wenn die Polizei derartige Geräte für ihre Tätigkeit einsetzen würde, könnten verschiedene Regelungen des Luftverkehrsrechts gelten, sofern nicht die Aus-

nahmeregelung des § 30 LuftVG anwendbar ist. Diese setzt voraus, dass die Ausnahme zur Erfüllung der besonderen Aufgaben der Polizei unter Berücksichtigung der öffentlichen Sicherheit oder Ordnung erforderlich ist. Die Ausnahme kann in gleicher Weise bezüglich der Regelungen der Luftverkehrsordnung wirken, so dass Einschränkungen, die für nicht hoheitliche Betreiber von unbemannten Luftfahrtsystemen gelten, außer Acht bleiben können. So ist das Gebot in § 16 Absatz 4 der Luftverkehrs-Ordnung, dass bei einer Erlaubnis für die Nutzung des Luftraums zum Aufstieg unbemannter Luftfahrtsysteme die Vorschriften über den Datenschutz nicht verletzt werden dürfen, in der Praxis nur schwer zu überwachen. Beim Einsatz derartiger Fluggeräte durch die Polizei wird es auf die Beachtung der datenschutzrechtlichen Regelungen des Polizeigesetzes ankommen. Eine Kontrolle durch meine Dienststelle wäre allenfalls im Nachhinein und nicht während eines aktuellen Einsatzes denkbar.

Ob für den Einsatz unbemannter Luftfahrtsysteme zur Anfertigung von Bildaufzeichnungen eine gesetzliche Regelung in den Polizeigesetzen oder der Strafprozessordnung erforderlich ist, ist derzeit noch offen. Die weitere Entwicklung ist sorgfältig zu beobachten.

2.2.4 Zuverlässigkeitsprüfungen in allen Varianten

Schon in früheren Tätigkeitsberichten habe ich über die Praxis berichtet, bei Großveranstaltungen aller Art mit Hilfe von Akkreditierungsverfahren Personen, die dort Zutritt zu Sicherheitsbereichen erhalten sollen, auf ihre persönliche Zuverlässigkeit zu überprüfen. Hierfür gibt es nach wie vor keine gesetzliche Grundlage, sondern es wird auf eine Einwilligung des Betroffenen abgehoben, so dass dieser nur die Wahl zwischen einem Einverständnis zur Abfrage der polizeilichen und teilweise nachrichtendienstlichen Dateien oder der Ablehnung des Zutritts hat. Im Berichtszeitraum ist meine Dienststelle mit weiteren Spielarten dieser fragwürdigen Praxis konfrontiert worden, die von einer Großveranstaltung im Jahr 2013 bis zu einer Provinzposse reichten.

Herausragendes Ereignis waren in dieser Hinsicht die Feierlichkeiten zum **Tag der Deutschen Einheit** in Stuttgart am 2. und 3. Oktober 2013, die umfangreiche Sicherheitsmaßnahmen zum Schutz der Verfassungsorgane von Bund und Ländern erforderten. Soweit Bundesorgane betroffen sind, obliegt nach § 5 des Bundeskriminalamtsgesetzes dem Bundeskriminalamt der Personenschutz. Hierzu gehört auch die Verarbeitung personenbezogener Daten von Personen, die sich im Umfeld der zu schützenden Personen befinden. In Stuttgart beließ es das Bundeskriminalamt bei dieser eng umgrenzten Aufgabe; das Polizeipräsidium Stuttgart hatte den gesamten polizeilichen Einsatz zu verantworten. Die Akkreditierung von Personen, die in die festgelegten Sicherheitsbereiche Einlass erhalten sollten, hat dabei zum einen im Vorfeld die Abgabe entsprechender Einwilligungserklärungen zur Abfrage der polizeilichen und nachrichtendienstlichen Auskunftssysteme vorausgesetzt. Zum anderen erfolgte eine Überprüfung der eingeladenen Gäste an einer Zugangsschleuse beim Staatsakt in der Liederhalle. Soweit die Überprüfung im Vorfeld erfolgte, hatte das Polizeipräsidium die Aufgabe, die Erkenntnisse zu einer Person zu erheben, im „Trefferfall“ dieser Gelegenheit zu einer Stellungnahme binnen 14 Tagen zu geben, und dann das Staatsministerium darüber zu unterrichten, ob „Bedenken“ bestehen oder nicht. Danach hatte dieses zu entscheiden, ob die betreffende Person dann die Akkreditierung erhalten würde oder nicht.

In der Vorbereitung der Veranstaltungen wurde meine Dienststelle sehr frühzeitig durch das Polizeipräsidium Stuttgart nicht nur über die sonstigen Maßnahmen zur Sicherung der Veranstaltungsstätten unterrichtet, sondern gerade auch über das Akkreditierungsverfahren. Mein mehrfach geäußerter Wunsch, endlich eine gesetzliche Grundlage für Zuverlässigkeitsprüfungen bei derartigen Veranstaltungen zu schaffen, wurde vom Staatsministerium und vom Innenministerium unter Hinweis auf die vorhandenen Einwilligungserklärungen abgelehnt. Überzeugen kann mich diese Auffassung immer noch nicht, da z. B. das Polizeigesetz Bestimmungen für die Abwehr abstrakter, also eben nicht konkreter Gefahren enthält. Und eine Zuverlässigkeitsprüfung soll doch gerade klären, ob von irgendwelchen Personen im

sicherheitsempfindlichen Umfeld von Veranstaltungen Gefahren ausgehen könnten. So gesehen wäre eine gesetzliche Regelung, die die bisherige Praxis verfassungskonform regeln würde, besser als jede de facto erzwungene Einwilligung in die Abfrage polizeilicher oder auch anderer Auskunftssysteme, mit der eine Zweckänderung für die Nutzung der dabei abgerufenen Daten verbunden ist. Denn eine Person, die beispielsweise bei einer Veranstaltung als Servicekraft eingesetzt werden möchte, um dadurch etwas für den Lebensunterhalt zu verdienen, wird zu einer Einwilligungserklärung gezwungen, wenn sie nicht von vornherein auf einen Verdienst verzichten will.

Auf Nachfrage hat das Polizeipräsidium Stuttgart nach den Veranstaltungen zum Tag der Deutschen Einheit in Stuttgart mitgeteilt, dass insgesamt 2.524 Personen im Vorfeld überprüft wurden. Bedenken wurden gegen insgesamt 34 Personen geltend gemacht, eine Person wurde - da sie zur Festnahme ausgeschrieben war - gleich „aus dem Rennen“ genommen, die anderen Personen waren für folgende Tätigkeiten vorgesehen:

- Sicherheitsdienst: 25 Personen
- Catering: 6 Personen
- Veranstaltungsmanagement: 1 Person
- Pressevertreter: 1 Person

An den Einlassschleusen wurden während der Veranstaltungen 60 Personen kurzfristig akkreditiert, während 5 Personen abgewiesen bzw. aus dem Sicherheitsbereich verwiesen wurden, diese waren für folgende Tätigkeiten vorgesehen:

- Sicherheitsdienst: 2 Personen
- Catering: 2 Personen
- Pressevertreter: 1 Person

Von den Personen, die im Vorfeld überprüft wurden, erhielt nach Aussage des Staatsministeriums keine eine Akkreditierung, wenn das Polizeipräsidium Stuttgart dagegen Bedenken geäußert hatte. Rechtliche Schritte gegen die Versagung der Akkreditierung wurden ebenfalls nicht bekannt.

Eine andere Konstellation ergibt sich für den **Zutritt zu vom Polizeivollzugsdienst dienstlich genutzten Gebäuden und Grundstücken.** Die Polizei, insbesondere die Bereitschaftspolizei, verfügt über Anlagen, in denen nicht nur die Angehörigen des Polizeivollzugsdienstes und die Polizeianwärter Sport treiben können, sondern die auch sonstigen örtlichen Vereinen und Organisationen hierfür offen stehen. Außerdem muss für das Personal privater Dienstleister wie Handwerker, Reinigungsfirmen usw. der Zutritt zu Polizeigebäuden geregelt werden. Das Innenministerium hat für diese Fälle festgelegt, dass nicht dem Polizeivollzugsdienst oder den Polizeidienststellen angehörende Personen aus Sicherheitsgründen nur nach einer Zuverlässigkeitsüberprüfung aufgrund einer Einwilligungserklärung zugelassen werden können. Bei dieser Konstellation kann ggf. das Hausrecht die Rechtsgrundlage für eine entsprechende Überprüfung darstellen, wenngleich eine gesetzliche Regelung auch hier die Zweifel an der Nutzung der für andere Zwecke gespeicherten Daten leichter ausräumen könnte.

Seit Jahren beschäftigen sich die Datenschutzbeauftragten überdies mit der Frage, ob **Bewerber für den Polizeivollzugsdienst** im Rahmen einer Zuverlässigkeitsprüfung auch auf solche Informationen hin überprüft werden dürfen, die zur Gefahrenabwehr oder zur vorbeugenden Bekämpfung von Straftaten gespeichert wurden. Diese Datenspeicherungen, deren Zulässigkeit sich aufgrund des § 483 Absatz 3 der Strafprozessordnung (StPO) nach den polizeirechtlichen Vorschriften richtet, umfassen alle von der Polizei betriebenen Ermittlungsverfahren, selbst wenn diese später durch die Staatsanwaltschaft eingestellt wurden. Derartige Daten werden für eine Dauer zwischen zwei und zehn Jahren gespeichert, abhängig vom Alter des Täters bei Begehung der Tat, von dem strafrechtlichen Vorwurf und von weiteren tat- oder täterbezogenen Aspekten. Auch in den meisten anderen Ländern wird schon seit Jahren von Bewerbern für den Polizeivollzugsdienst die Abgabe einer Einwilligungserklärung verlangt, um Daten aus den polizeilichen Informationssystemen im Rahmen des Auswahlverfahrens nutzen zu können. Begründet wird dies vor allem mit dem Bedürfnis, in den Polizeivollzugsdienst nur solche Bewerber aufzunehmen, bei denen sich aus früheren Ermittlungsverfahren keine Persönlichkeitsmängel ergeben. Entscheidend ist für Bewer-

ber in diesem Zusammenhang vor allem, dass sie die Frage nach etwaigen Ermittlungsverfahren gegen sie richtig und vollständig beantworten. Fatal ist es nämlich, wenn diese Frage - unabhängig davon, ob wissentlich oder unwissentlich - verneint wird und aufgrund der Einwilligungserklärung beim Abruf der Auskunftssysteme dann doch eine „Jugendsünde“ oder ein sonstiger Bagatellvorgang zum Vorschein kommt. Denn dann spielt die Verfehlung selbst, gleichgültig warum das frühere Ermittlungsverfahren eingestellt wurde, keine Rolle mehr. Sondern die Bewerbung wird dann schon deshalb zurückgewiesen, weil unzutreffende Angaben gemacht wurden. Darauf wird auch bei der Einstellungsberatung oder bei Aushändigung der Bewerbungsbögen unmissverständlich schriftlich hingewiesen. Da die Akten über Bewerbungen fünf Jahre aufgehoben werden, bedeutet dies faktisch für diesen Zeitraum einen Ausschluss des Bewerbers von weiteren Bewerbungsverfahren.

Bewerbern für den Polizeivollzugsdienst kann deshalb nur dringend empfohlen werden, beim Landeskriminalamt Baden-Württemberg rechtzeitig vor der Abgabe einer Bewerbung einen Auskunftsantrag zu den möglicherweise gespeicherten Daten aus Ermittlungsverfahren zu stellen. Auf diese Weise kann jeder an dem Beruf Interessierte kostenlos erfahren, ob in Vergessenheit geratene „Kontakte“ mit der Polizei noch gespeichert sind und einer Bewerbung entgegen stehen könnten. Zur Beruhigung für die Betroffenen ist anzumerken, dass nicht jede „Jugendsünde“ oder Bagatelle den Weg in den Polizeivollzugsdienst versperren darf. Selbst „schwerwiegendere“ Verfehlungen sind nicht hinderlich, wie dem Beschluss des Verwaltungsgerichts Stuttgart vom 1. August 2008, Az. 3 K 1886/08, zu entnehmen ist. In diesem Fall war die Einstellung eines Strafverfahrens wegen unerlaubten Entfernens vom Unfallort wegen geringer Schuld und geringen Schadens dennoch für die Bereitschaftspolizei Anlass gewesen, den Bewerber erst gar nicht für die Eignungstests zuzulassen. Das Gericht hatte daraufhin im einstweiligen Rechtsschutzverfahren erhebliche Mängel bei dieser Entscheidung festgestellt. Die Chance für eine inhaltliche Abwägung und Entscheidung wird aber vertan, wenn schon die Frage nach früheren Ermittlungsverfahren nicht oder falsch beantwortet wird.

Eine weitere Fallkonstellation bildet die Überprüfung der **Zuverlässigkeit des Personals von Abschleppbetrieben**, wie sich aufgrund einer Umfrage meines bayerischen Kollegen ergab. Abschleppbetriebe werden von der Polizei bekanntlich häufig und rasch in Anspruch genommen, um Unfallstellen auf Straßen zu räumen, behindernd abgestellte Fahrzeuge zu beseitigen oder Fahrzeuge sicherzustellen. Eine Anfrage beim Innenministerium zur Praxis in Baden-Württemberg förderte Dienstanweisungen von zwei Landespolizeidirektionen zutage, die eine Vielzahl von Regelungen über die technische Erfüllung des Auftrags und die gewerberechtliche Zulässigkeit der Dienstleistung enthielten. Bemerkenswerterweise war auch ein Hinweis auf die Überprüfung der Zuverlässigkeit der Mitarbeiter derartiger Betriebe enthalten. Als Ergebnis einer Überprüfung der einzelnen Mitarbeiter sollte dem Betriebsinhaber nur mitgeteilt werden, ob und gegen wen Bedenken bestehen oder nicht, ohne diese Erkenntnisse näher zu erläutern. Wie die Praxis in anderen Dienstbezirken aussah, schien nach dem Antwortschreiben des Innenministeriums eher unklar, um nicht zu sagen beliebig zu sein. Von Bemühungen, den Umgang mit den personenbezogenen Daten der Inhaber und Mitarbeiter der Abschleppbetriebe landeseinheitlich zu regeln, war jedenfalls nichts zu merken.

Anlass zur Kritik gab auch die **Zuverlässigkeitsprüfung der Mitarbeiter von Sicherheitsdiensten durch Gaststättenbehörden** in einem Landkreis. Dort hatte man sich das grundsätzlich begrüßenswerte Ziel gesetzt, öffentliche Veranstaltungen im Hinblick auf den Jugendschutz, zur Vermeidung von Alkoholmissbrauch und sonstige negative Begleiterscheinungen künftig sicherer zu gestalten. Zu diesem Zweck hatten die Veranstalter einen Sicherheitsdienst zu verpflichten, der bei entsprechenden Verstößen oder sonstigen Störungen einschreiten sollte. Soweit so gut - der Hilferuf eines Betriebsinhaber eines Sicherheitsunternehmen machte jedoch deutlich, dass die Umsetzung in diesem Landkreis in wesentlichen Teilen weder verwaltungsverfahrensrechtlichen noch datenschutzrechtlichen Anforderungen ent-

sprach. Die zwischen Landratsamt, Gaststättenbehörden und Polizei abgesprochene und auch im Internet nachzulesende Vorgehensweise sah wie folgt aus:

Für eine Veranstaltung erhielt der dafür Verantwortliche von seiner Gaststättenbehörde eine Gestattung nach § 12 des Gaststättengesetzes, die unter anderem vorsah, dass „die eingesetzten Sicherheitsdienstmitarbeiter … namentlich (Name, Vorname, Geburtsdatum) 1 Woche vor Veranstaltungsbeginn dem örtlichen Polizeirevier zu benennen [sind].“ Dem Inhaber des Sicherheitsdienstes wurde die an den Veranstalter gerichtete Gestattung zur Kenntnisnahme übersandt, wobei er dann noch „insbesondere um **Beachtung und Erledigung der Ziff. 5** [Anmerkungen: u. a. vorstehend zitierte Regelung; Fettdruck im Original] dieser Gestattung“ gebeten wurde. Das zuständige Polizeirevier hat dann die Namen der Sicherheitsdienstmitarbeiter anhand der in den polizeilichen Auskunftssystemen verfügbaren Daten daraufhin „geprüft“, ob diese bei der Veranstaltung eingesetzt werden können oder nicht, und das Ergebnis der Gaststättenbehörde mitgeteilt.

Meine Mitarbeiter kamen nicht umhin, das Landratsamt als Initiator dieser Verfahrensweise daran zu erinnern, dass die Verwaltung nach Artikel 20 Absatz 3 des Grundgesetzes an Recht und Gesetz gebunden ist. Die Erforderlichkeit der Datenerhebungen und Datenübermittlungen zwischen Sicherheitsdienst, Polizeirevier und Gaststättenbehörde war nämlich weder aus den gaststättenrechtlichen noch aus den gewerberechtlichen oder polizeirechtlichen Bestimmungen herzuleiten. Außerdem war das informationelle Selbstbestimmungsrecht der Mitarbeiter des Sicherheitsdienstes völlig außer Acht gelassen worden. Dass außerdem die verwaltungsverfahrensrechtlichen Grundlagen bezüglich des Adressaten eines Verwaltungsaktes nicht beachtet wurden - wie ich zugunsten der Verfasser der Gestattungen unterstellten möchte -, rundete das Bild einer eigenwilligen Rechtsschöpfung in der Provinz ab.

Um die Rechtslage deutlich zu machen: Gaststättenrechtlich ist allein der Veranstalter verantwortlich. Ihm kann eine Gaststättenbehörde beispielsweise aufgeben, dass nur ein zuverlässiger Sicherheitsdienst mit entsprechend zuverlässigen Mitarbeitern die Ordnung auf der Veranstaltung zu gewährleisten hat. Hierfür kann sie vom Veranstalter entsprechende Nachweise zu dem von ihm engagierten Sicherheitsdienst fordern. Die in diesem Fall an den Inhaber des Sicherheitsdienstes gerichtete Aufforderung, eine Auflage gegenüber dem Veranstalter zu beachten und umzusetzen, passt nicht zum Adressaten einer Gestattung, also des Verwaltungsaktes. Zudem ist das Gewerberecht zu beachten:

Wer einen Sicherheitsdienst betreiben will, bedarf einer Erlaubnis nach § 34a der Gewerbeordnung (GewO). Danach müssen der Gewerbetreibende und das von ihm beschäftigte Personal zuverlässig sein und noch weitere Voraussetzungen erfüllen. Um die Zuverlässigkeit zu prüfen, kann die für die Erlaubnis zuständige Behörde unbeschränkte Auskünfte aus dem Bundeszentralregister zu dem Personal einholen und das Ergebnis der Überprüfung einschließlich der für die Beurteilung der Zuverlässigkeit erforderlichen Daten dem Gewerbetreibenden übermitteln. Um eben diese Bestimmungen ging es in der gesamten meiner Dienststelle geschilderten Problematik aber nicht.

Die Verpflichtung des Veranstalters, den von ihm engagierten Sicherheitsdienst zu verpflichten, die personenbezogenen Angaben der für den Einsatz vorgesehenen Beschäftigten dem zuständigen Polizeirevier zu übermitteln, damit dieses der Gaststättenbehörde übermitteln konnte, ob und ggf. welcher von diesen Beschäftigten nicht eingesetzt werden dürfe, krankte in vielerlei Hinsicht an rechtlichen Mängeln.

Zunächst gibt das Gaststättenrecht für eine derartige Regelung nichts her: Wenn ein Veranstalter einen Sicherheitsdienst benötigt, muss er sich darauf verlassen können, dass dieser nicht nur die Erlaubnis nach der Gewerbeordnung besitzt, sondern auch nur entsprechend zuverlässiges und fachkundiges Personal einsetzt. Wenn sich herausstellt, dass der Sicherheitsdienst diese Bedingungen nicht (mehr) erfüllt, hat seine Erlaubnisbehörde und nicht jede Gaststättenbehörde zu prüfen, ob die gewerberechtliche Erlaubnis widerrufen werden muss oder Einschränkungen bezüglich des Mitarbeitereinsatzes vorzunehmen sind.

Das Verlangen, die Mitarbeiterdaten dem zuständigen Polizeirevier zu übermitteln, damit dieses - durch Nutzung der Auskunftssysteme des Polizeivollzugsdienstes - dann der Gaststättenbehörde mitteilen kann, ob und ggf. welcher der Mitarbeiter nicht eingesetzt werden darf, war in datenschutzrechtlicher Hinsicht völlig verfehlt. Schon der Ansatz, die Zuverlässigkeit vor jedem Einsatz zu überprüfen, widerspricht der Gewerbeordnung. Für die Beteiligung des Polizeivollzugsdienstes - wie sie in anderen gesetzlichen Bestimmungen ausdrücklich enthalten ist (dazu später mehr) - ist nichts vorgesehen. Die einzige Bestimmung, die dem Polizeivollzugsdienst bezüglich des Sicherheitsdienstes ein Tätigwerden ermöglicht, ist § 10 der Verordnung der Landesregierung über Zuständigkeiten nach der Gewerbeordnung (GewO-ZuVO). Danach darf er prüfen, ob die erforderliche Erlaubnis nach § 34a GewO vorliegt. Auch insoweit ist von der Überprüfung der Mitarbeiter eines Sicherheitsdienstes nicht die Rede. Und dass der Inhaber des Sicherheitsdienstes über diese Erlaubnis verfügt, war in dem gesamten Komplex nie strittig.

Um die Daten der Mitarbeiter überhaupt erheben, den Abruf aus den Auskunftssystemen durchführen und der Gaststättenbehörde das „Ergebnis“ übermitteln zu können, gab es keine Rechtsgrundlage. Es lagen noch nicht einmal die nach § 4 Absatz 1 Nummer 2, Absätze 2 und 3 des Landesdatenschutzgesetzes (LDSG) notwendigen schriftlichen und - wegen der Zwecke der Abfrage - informierten Einwilligungen der Beschäftigten vor. Auch der Versuch, diesen Mangel über eine Erklärung des Inhabers zu „heilen“, dass er seine Mitarbeiter informiert habe, musste vor dem Hintergrund der eindeutigen gesetzlichen Regelung der Rechte der Betroffenen als untauglich scheitern. Damit waren die Datenerhebung auf Veranlassung der Gaststättenbehörde und die Übermittlung an das Polizeirevier rechtswidrig. Das Polizeirevier konnte anhand der übermittelten personenbezogenen Daten feststellen, ob in den Auskunftssystemen Vorgänge zu den Mitarbeitern gespeichert waren. Ob es darüber hinaus auf den entsprechenden Aktenrückhalt möglicherweise zugreifen konnte, war für meine Dienststelle nicht erkennbar. Die Übermittlung an die Gaststättenbehörde habe sich, so eine Stellungnahme des zuständigen Polizeireviers, in dem Ausgangsfall nicht auf Details aus den polizeilichen Datensammlungen zu dem einzelnen Mitarbeiter bezogen, sondern in den Fällen mit Datenspeicherungen nach einer Bewertung des Inhalts dann eine entsprechende Aussage beinhaltet, wenn aus Sicht der Polizei dessen Zuverlässigkeit und Geeignetheit für die zu übernehmende Aufgabe nicht gegeben gewesen sei. Wenn ein Revier darauf hinweist, dass ein Sicherheitsdienst auch Personal einsetzt, das nicht den Anforderungen entspricht, dann rechtfertigt dieses keinesfalls die geschilderte Vorgehensweise. Stattdessen müsste der Polizeivollzugsdienst bei negativen Erkenntnissen zum Einsatz eines Sicherheitsdienstes die zuständige Erlaubnisbehörde nach § 7 GewOZuVO darüber informieren, damit diese ihre rechtlichen Möglichkeiten prüfen kann.

Aufgrund unserer Beratung wurde der Internetauftritt des Landratsamtes inzwischen korrigiert und die bisherige Verfahrensweise aufgegeben. Nach Presseberichten soll der zuständige Ausschuss des Kreistags bedauert haben, dass diese „bewährte“ Praxis eingestellt werden musste. Dazu kann ich nur feststellen: „Nicht jeder Zweck heiligt die Mittel.“ Im Übrigen gibt es durchaus geeignete und vor allem rechtsstaatliche Wege, Missstände zu verhindern oder zu beseitigen, man muss sie nur suchen und gehen.

Aufgrund trauriger Anlässe ist die **Zuverlässigkeitsprüfung von Waffenbesitzern** in den letzten Jahren verschärft und detailliert geregelt worden, was auch aus rechtsstaatlichen Gründen zu begrüßen ist. Im Unterschied zu anderen Regelungsmaterien enthält das Waffengesetz (WaffG) schon seit Jahren eine einschlägige Bestimmung in § 5 Absatz 5:

> Die zuständige Behörde hat im Rahmen der Zuverlässigkeitsprüfung folgende Erkundigungen einzuholen:
> 1. die unbeschränkte Auskunft aus dem Bundeszentralregister;
> 2. die Auskunft aus dem zentralen staatsanwaltschaftlichen Verfahrensregister hinsichtlich der in Absatz 2 Nr. 1 genannten Straftaten;
> 3. die Stellungnahme der örtlichen Polizeidienststelle, ob Tatsachen bekannt sind, die Bedenken gegen die Zuverlässigkeit begründen; die örtliche Polizeidienststelle schließt in ihre Stellungnahme

das Ergebnis der von ihr vorzunehmenden Prüfung nach Absatz 2 Nr. 4 ein.
Die nach Satz 1 Nr. 2 erhobenen personenbezogenen Daten dürfen nur für den Zweck der waffenrechtlichen Zuverlässigkeitsprüfung verwendet werden.

§ 5 Absatz 2 des Waffengesetzes bestimmt u. a. Folgendes:

Die erforderliche Zuverlässigkeit besitzen in der Regel Personen nicht, die
a) wegen einer vorsätzlichen Straftat,
b) wegen einer fahrlässigen Straftat im Zusammenhang mit dem Umgang mit Waffen, Munition oder explosionsgefährlichen Stoffen oder wegen einer fahr lässigen gemeingefährlichen Straftat,
c) wegen einer Straftat nach dem Waffengesetz, dem Gesetz über die Kontrolle von Kriegswaffen, dem Sprengstoffgesetz oder dem Bundesjagdgesetz
zu einer Freiheitsstrafe, Jugendstrafe, Geldstrafe von mindestens 60 Tagessätzen oder mindestens zweimal zu einer geringeren Geldstrafe rechtskräftig verurteilt worden sind oder bei denen die Verhängung von Jugendstrafe ausgesetzt worden ist, wenn seit dem Eintritt der Rechtskraft der letzten Verurteilung fünf Jahre noch nicht verstrichen sind,
……
innerhalb der letzten fünf Jahre mehr als einmal wegen Gewalttätigkeit mit richterlicher Genehmigung in polizeilichem Präventivgewahrsam waren,
…….

In der Allgemeinen Verwaltungsvorschrift zum Waffengesetz vom 5. März 2012 (BAnz Jg. 64, Nr. 47a) wird zu § 5 WaffG noch ergänzend ausgeführt:

§ 5 Absatz 5 enthält eine Regelung zu den Erkenntnisquellen, die nach Bundesrecht verpflichtend bei der Zuverlässigkeitsprüfung heranzuziehen sind. Diese Regelung nennt die nutzbaren Erkenntnisquellen nicht abschließend. Beispielsweise bietet sich ergänzend zur Anfrage bei der örtlichen Polizeidienststelle im Einzelfall eine Anfrage bei der zuständigen Landesbehörde für Verfassungsschutz nach dort vorhandenen Erkenntnissen im Hinblick auf Unzuverlässigkeitsgründe an.
Die Anfrage der Waffenbehörde bei der örtlichen Polizei nach § 5 Absatz 5 Satz 1 Nummer 3 kann auch über eine übergeordnete Polizeidienststelle (z. B. LKA) erfolgen. Sie stellt auf die Abfrage vorhandener Erkenntnisse ab. Dies sollte im Anschreiben an die Polizei mit aufgenommen werden.

Baden-Württemberg sieht sich im Vergleich zu anderen Ländern besonderen Herausforderungen gegenüber: Von über 570 Waffenbehörden im Bundesgebiet sind allein 148 im Land beheimatet. Die Zuständigkeit für das Waffenrecht ist nach der Verordnung der Landesregierung zur Durchführung des Waffengesetzes im Wesentlichen den Kreispolizeibehörden zugewiesen worden. Kreispolizeibehörden sind nach § 62 Absatz 3 PolG die Unteren Verwaltungsbehörden. Dazu gehören nach § 15 des Landesverwaltungsgesetzes neben den Stadt- und Landkreisen die Großen Kreisstädte sowie auf Antrag die Verwaltungsgemeinschaften mit mehr als 20.000 Einwohnern.

Um den Aufwand bei den Zuverlässigkeitsprüfungen zu verringern, wurde für die Waffenbehörden der Zugang zu einem **„Online-Sicherheits-Portal (OSIP)“** des Landes eingerichtet. Über dieses Portal können die Waffenbehörden direkt abrufen, ob zu einem Antragsteller oder Waffenbesitzer Erkenntnisse vorliegen oder nicht. In letzterem Fall können sie dann direkt den Vorgang weiterbearbeiten. Bei Erkenntnissen werden die Polizeidienststellen bezüglich ihrer Stellungnahme für die anfragende Waffenbehörde vom Landeskriminalamt unterrichtet. Damit ergänzt dieses Abrufverfahren das automatisierte Abrufverfahren, welches auch für die Waffenbehörden beim Bundesamt für Justiz bezüglich des Bundeszentralregisters und des zentralen staatsanwaltschaftlichen Verfahrensregisters eingerichtet wurde.

Die Regelungen zum Waffenrecht zeigen, dass die Nachfrage nach Informationen zur Zuverlässigkeit einer Person in datenschutzrechtlich einwandfreier Weise bei der zuständigen Stelle erfüllt werden kann. Inwieweit die eingerichteten automatisierten Abrufverfahren nicht zuletzt nach der Umsetzung des Nationalen Waffenregistergesetzes von den Waffenbehörden in Übereinstimmung mit den gesetzlichen Regelungen genutzt werden, werden meine Mitarbeiter in den nächsten Monaten kontrollieren.

2.2.5 Das Nationale Waffenregister

Deutschland hat im Vergleich zu anderen Staaten ein relativ restriktives Waffengesetz. Gleichwohl konnte dieses Gesetz nicht verhindern, dass es immer wieder zur Begehung von Straftaten mit Waffen kam, die auch in Baden-Württemberg unvorstellbares Leid über viele Mitbürgerinnen und Mitbürger gebracht haben. Es ist allerdings nicht zu verkennen, dass die Dunkelziffer des illegalen Waffenbesitzes beträchtlich ist und es daher auch eine Vielzahl von Waffen in der Hand von Nichtberechtigten gibt, von denen keine Waffenbehörde etwas erfährt. Gleichwohl haben es die Europäische Union und nachfolgend der Bundesgesetzgeber für erforderlich gehalten, ein computergestütztes Waffenregister einzurichten, in dem Lieferanten sowie Erwerber und Besitzer von Waffen erfasst werden.

Am 15. Juni 2012 hat der **Bundesrat** dem Gesetz zur Errichtung eines Nationalen Waffenregisters (Nationales-Waffenregister-Gesetz - NWRG) und der Verordnung zur Durchführung des Nationalen-Waffenregister-Gesetzes (NWRG-Durchführungsverordnung - NWRG-DV) zugestimmt und damit die Grundlage für die seit geraumer Zeit laufenden Anstrengungen zur Realisierung des zentralen Registers beim Bundesverwaltungsamt geschaffen (vgl. zur Vorgeschichte 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 55). Dieser Teil des Projekts „Deutschland-online“ sollte sogar noch erheblich vor dem von der Europäischen Union vorgegebenen Termin (31. Dezember 2014) in Betrieb gehen. Im September 2012 wurde meine Dienststelle über die Aufnahme des Probebetriebs in einigen Waffenbehörden unterrichtet. Im Sommer 2013 standen dann die zum automatisierten Abruf berechtigten Stellen im Land fest: 148 Waffenbehörden, insgesamt 42 Dienststellen des Polizeivollzugsdienstes sowie das Landesamt für Verfassungsschutz. Nachdem nun alle diese Stellen im Nationalen Waffenregister online tätig sind, wird meine Dienststelle in den nächsten Monaten einige Waffenbehörden genauer unter die Lupe nehmen.

Das **Nationale Waffenregister** ist beim Bundesverwaltungsamt eingerichtet, wo es am 2. Januar 2013 in Betrieb ging. Nach der ersten Auswertung befanden sich in der Bundesrepublik Deutschland zum damaligen Zeitpunkt rd. 5,5 Mio. Waffen legal in der Hand von rd. 1,4 Mio. Privatbesitzern.

Da die Abrufberechtigungen für das Register zahlenmäßig sehr begrenzt sind und die Schutzmaßnahmen höher als üblich angesetzt wurden, dürfte ein Missbrauch der Daten nur aufgrund bewusster Missachtung aller rechtlichen Vorgaben eintreten. Beschwerden oder Probleme sind meiner Dienststelle jedenfalls bisher nicht bekannt geworden.

2.3 Die Polizeistrukturreform - auch eine Herausforderung für den Datenschutz

Kurz nach der Bildung der Landesregierung im Jahr 2011 wurden Pläne bekannt, den Polizeivollzugsdienst in seiner Struktur grundlegend zu reformieren. Begründet wurde dies mit Aufgabenveränderungen und absehbaren finanziellen Engpässen. Die mit Beginn 2014 in Kraft tretende Strukturreform hat auch meine Dienststelle intensiv beschäftigt.

Im Januar 2012 wurden die von einer polizeiinternen Projektgruppe erarbeiteten Eckpunkte der neuen Struktur bekannt. Zusammengefasst wird die bisherige - zumeist drei Ebenen umfassende - hierarchische Polizeistruktur auf eine zweistufige Organisation reduziert. Dazu werden auf der unteren Ebene 37 Polizeidirektionen aufgelöst und mit den bisherigen vier Landespolizeidirektionen (Abteilungen in den Regierungspräsidien auf der Mittelebene) zu 12 regionalen Polizeipräsidien zusammengeführt. Daneben werden landeseinheitlich wahrzunehmende Aufgaben des Polizeivollzugsdienstes zukünftig von dem Präsidium Einsatz und dem Landeskriminalamt wahrgenommen. Für die Personalgewinnung sowie die Aus- und Weiterbildung wird die Hochschule für Polizei zuständig sein. Das neu gebildete Präsidium Technik, Logistik, Service Polizei soll sich um die Aufgaben der polizeilichen Informations-, Kommunikations- und Einsatztechnik und die damit verbundenen Logistik- und Serviceaufgaben kümmern. Bei diesem Präsidium wird auch der Polizeiärztliche Dienst konzentriert. Anzumerken ist, dass sowohl die Hochschule als auch das

Präsidium Technik, Logistik, Service der Polizei keine Polizeidienststellen, sondern Einrichtungen für den Polizeivollzugsdienst sein werden.

Die völlige Umgestaltung der bisherigen Polizeistruktur hat nicht nur erhebliche Auswirkungen auf die Beschäftigten des Polizeivollzugsdienstes und des Nichtvollzugsdienstes, selbst wenn auf der Ebene der Polizeireviere alles beim alten bleiben soll. Auch durch die Verschiebung von Aufgabenwahrnehmungen ergeben sich etliche Fragen, die den Datenschutz nicht aussparen. Über einige Punkte wird hier berichtet.

2.3.1 Das Interessenbekundungsverfahren (IBV) - der Datenschutz zwischen Organisations- und Personalinteressen

Um eine möglichst sozialverträgliche Umsetzung aller Beschäftigten im Rahmen der Strukturreform zu erreichen, empfahl die Projektgruppe ein sog. Interessenbekundungsverfahren (IBV), bei dem die Beschäftigten ihre Verwendungswünsche einbringen können. Seit Oktober 2012 haben Mitarbeiter meiner Dienststelle den Prozess intensiv begleitet. Dabei war von vornherein klar, dass es für das IBV keine gesetzliche Grundlage gab und aus zeitlichen Gründen auch nicht geben würde. Allerdings wurden die Angehörigen des höheren Polizeivollzugsdienstes, soweit sie auf Funktionsstellen geführt wurden, in einem gesonderten Verfahren ihren neuen Aufgaben zugewiesen.

Die Polizeistrukturreform in einem Personalkörper mit immerhin weit über 30.000 Personen umzusetzen, wäre zwar nach den beamten- und tarifrechtlichen Grundlagen auch ohne Beteiligung der einzelnen Beschäftigten denkbar gewesen. Damit wäre aber das Risiko verwaltungsgerichtlicher Verfahren verbunden gewesen, die für die gesamte Reform vor allem wegen des engen Zeitplans hätten kritisch werden können. Daher wurde ein **Interessenbekundungsverfahren (IBV)** geschaffen, um Wünsche und wesentliche Probleme der Beschäftigten für ihre zukünftige Verwendung zu erfahren und soweit wie möglich berücksichtigen zu können. Dies erforderte aber die Bereitschaft der Beschäftigten, sich an dem Verfahren zu beteiligen, wobei es entscheidend auf dessen Rahmenbedingungen ankam. Diese betrafen zum einen die Beteiligung der Personalräte und zum anderen die Verwendung höchstpersönlicher Informationen der Beschäftigten ausschließlich durch die jeweils involvierten Projektverantwortlichen. Schon früh zeigte sich, dass die Beteiligungsrechte der Personalvertretung nach dem Landespersonalvertretungsgesetz in einem solchen Verfahren nur in sehr engen Grenzen zum Tragen kommen konnten. Daher kam es in der nach § 4 LDSG notwendigen Einwilligungserklärung eines jeden Beschäftigten, der sich am IBV beteiligen wollte, für die Verarbeitung seiner personenbezogenen Daten darauf an, über alle Einzelheiten des Verfahrensganges genau informiert zu werden. Denn gerade die Wünsche für oder die Bedenken gegen eine bestimmte Verwendung und die entsprechenden persönlichen Gründe hierfür waren nicht aus den Personalakten erkennbar. Daher war die Sicherstellung der Vertraulichkeit solcher Angaben ein herausragender Aspekt, dem erfreulicherweise durch die Verantwortlichen große Aufmerksamkeit gewidmet wurde.

Im IBV hatten die Beschäftigten, von denen immerhin etwa die Hälfte von dem Angebot der Beteiligung Gebrauch machte, in einer ersten Phase Gelegenheit, in einem sicheren Online-Verfahren die aus ihrer Sicht erforderlichen Angaben in den zur Verfügung gestellten Online-Formularen zu machen. Erst nach dem Abschluss dieser Phase konnten die personalverwaltenden Stellen auf die Daten zugreifen und dann die Daten der vorgesehenen und interessierten Beschäftigten zunächst ohne Angabe besonderer persönlicher Gründe für die jeweiligen Projekte (die zukünftigen Dienststellen und Einrichtungen) zur Verfügung stellen. Die Projekte hatten entsprechend den zahlenmäßigen Vorgaben für die Sollstärke der neuen Dienststellen und Einrichtungen zu überprüfen, ob die benannten Beschäftigten in der Konzeption berücksichtigt werden konnten. Unterstützt wurden die Beschäftigten, aber auch die Projektverantwortlichen von besonderen Ansprechpartnern, die beratend zu allen Fragen im Zusammenhang mit dem IBV zur Verfügung standen. Ehe die Projektverantwortlichen zu dem Vorschlag Änderungswünsche äußerten, wurden diese in Personalkommissionen, denen als sachverständige Mitglieder Per-

sonalvertreter aus allen bisherigen Dienststellen angehören konnten, erörtert. Nach den Sitzungen der Personalkommissionen wurden die Änderungen den personalverwaltenden Stellen vorgetragen, die dann überprüfen konnten, ob sie realisierbar waren. Wenn dieses nicht möglich erschien, war vorgesehen, die besonderen persönlichen Gründe im Rahmen einer weiteren Sitzung der Personalkommission auf Projektebene vorzutragen. Aus der meinen Mitarbeitern bei den Kontrollbesuchen bei drei Projekten bekannt gewordenen Verfahrensweise wurde deutlich, dass die Personalkommissionen in der ersten Anhörung zwar Kenntnis von den Wünschen für die Verwendung und die Ablehnung einer bestimmten Verwendung erlangten, die Unterlagen aber stets bei den Projekten verblieben. Für die zweite Anhörung der Personalkommissionen hatten sich die Projektverantwortlichen weitere, die Individualinteressen der Beschäftigten besonders berücksichtigende Verfahrensweisen überlegt, um möglichst wenige sensitive Daten bekannt geben zu müssen. Diese wurden aber nach unseren Informationen nicht benötigt, was auch daran lag, dass schon während der ersten Phase - in Absprache mit meiner Dienststelle - die ursprünglich nicht zur Bekanntgabe vorgesehenen Wohnanschriften einbezogen wurden, so dass damit wesentliche soziale Aspekte für die Zuordnung, vor allem die Entfernung zwischen Wohnung und Arbeitsstelle, berücksichtigt werden konnten. Für den Fall, dass nicht alle Zuweisungen - auch zwischen den Projekten - nicht einvernehmlich geklärt werden konnten, war eine Clearingkommission beim Innenministerium vorgesehen. Ein angedachter Kontrollbesuch bei dieser konnte dann „mangels Masse“ entfallen. Letztlich waren nur zwei Fälle übriggeblieben. Danach begann dann die Arbeit der personalverwaltenden Stellen zur Umsetzung der Beschäftigten einschließlich der dafür vorgesehenen Beteiligung der Personalvertretungen.

Bei der technischen Durchführung des IBV musste ebenfalls Neuland beschritten werden. Für die Erhebung der Daten wurde eine Web-Anwendung entwickelt, auf die jeder Mitarbeiter aus dem Netzwerk der Polizei zugreifen konnte. Die Authentisierung erfolgte, indem dem Mitarbeiter eine E-Mail mit einem Verweis auf die entsprechende Intranetseite zugesandt wurde. Um die Möglichkeit der Änderung der eingegebenen Daten zu eröffnen, wurde nach der ersten Anmeldung ein Benutzerkonto angelegt. Die Mitarbeiter konnten sich dann mit Benutzerkennung und Passwort an der Anwendung anmelden. Die personalverwaltenden Stellen arbeiteten mit einer erweiterten Version der Anwendung direkt mit diesen Datenbeständen, wohingegen die Projekte Kopien der Daten anfertigten. Die Ergebnisse der Personalkommissionen mussten in das landesweite Verfahren eingepflegt werden. Die Kopien der Daten wurden entweder mit einem Tabellenkalkulationsprogramm und vereinzelt auch mit einer Kooperationsplattform weiter verarbeitet. Hinsichtlich der Stellen, die mit Tabellenkalkulationsprogrammen arbeiteten, hatte das Querschnittsprojekt beim Innenministerium eine Handreichung zur Verfahrensweise vorgegeben. Bei den Informationsbesuchen haben meine Mitarbeiter den Eindruck gewonnen, dass man sich hinsichtlich der Gewährleistung der Vertraulichkeit der mitunter brisanten Sozialdaten Mühe gegeben hatte. Die Anzahl der Mitarbeiter, die auf die Daten zugreifen konnten, wurde so klein wie möglich gehalten. Die Daten waren auf eigenen Laufwerken gespeichert. Der Zugriff auf die dort gespeicherten Dateien war durch Zugriffsrechte eingeschränkt. Was jetzt noch aussteht, ist die Löschung nach dem Inkrafttreten der Reform zum 1. Januar 2014, was meine Dienststelle zu gegebener Zeit überprüfen wird.

Die rechtzeitige und fortwährende Beteiligung meiner Dienststelle bei der Realisierung des IBV hat nach meinem Eindruck sowohl den Interessen der Beteiligten als auch der Umsetzung gedient. Das gewählte Verfahren mit einer detaillierten informierten Einwilligung hat für Akzeptanz gesorgt. Die Polizei des Landes hat sich der datenschutzrechtlichen Verantwortung gestellt, die mit der Verarbeitung der zahlreichen hochsensiblen Daten ihrer Beschäftigten verbunden war. Dass im Rahmen des IBV die teilweise nicht konsistenten Grundlagen der Personalstammdaten aktualisiert werden konnten und nach der Umsetzung des Personals auf die neuen Dienstposten entsprechend ergänzt werden, war ein weiterer wichtiger Nebeneffekt, der in Zusammenarbeit mit meiner Dienststelle erreicht wurde.

2.3.2 Profitiert der Datenschutz von der Strukturreform?

Die regionalen Polizeipräsidien, das Präsidium Einsatz und auch die Einrichtungen für die Polizei erhalten im Zuge der Polizeistrukturreform auf der Leitungsebene besondere Rechtsreferate, die - nicht zuletzt im Hinblick auf die selbstständige Vertretung bei rechtlichen Auseinandersetzungen - große Bedeutung gewinnen dürften. Für den Datenschutz werden sie ebenfalls zuständig sein, was insbesondere bei den Dienststellen, die über Datenstationen verfügen - also den regionalen Polizeipräsidien und dem Landeskriminalamt - im Hinblick auf ihre Funktion als „verantwortliche Stelle“ für die Speicherung von personenbezogenen Daten Betroffener von Bedeutung sein wird. Eine gewisse Neuorientierung für die Kontroll- und Beratungstätigkeit meiner Dienststelle wird die Folge sein.

Nach der bisherigen Aufgabenverteilung war das **Landeskriminalamt** für meine Dienststelle in vielen Fällen die entscheidende Anlaufstelle, unabhängig davon, ob es um Einzeleingaben Betroffener oder um grundsätzliche Fragen der Datenverarbeitung der Polizei ging. Künftig wird sich das Landeskriminalamt zwar um Auskünfte an Betroffene oder Anfragen meiner Dienststelle zu Einzelfällen weiterhin kümmern und die fachlichen Anforderungen an die Datenverarbeitung stellen, jedoch nicht mehr für die gesamte Datenverarbeitung zuständig sein. Die Entwicklung der Verfahren, die Nutzerverwaltung der polizeilichen Datenverarbeitung, das polizeiinterne Informationsangebot „Polizei-online“ und weitere Aufgaben, die unter Technik, Logistik und Service fallen, sind nach § 70 Absatz 2 Nr. 2 des PolG i. V. m. §§ 19, 20 der Verordnung zur Durchführung des Polizeigesetzes der neuen Einrichtung für den Polizeivollzugsdienst, dem **Präsidium Technik, Logistik, Service der Polizei**, zugewiesen.

Ein erhöhter Aufwand dürfte in bestimmten Fällen bei Kontrollen entstehen, zum Beispiel bei Prüfung der Frage, von welchem Arbeitsplatz der Polizei bestimmte Daten abgerufen wurden und ob dies fachlich erforderlich war. Jeder Account ist im sog. Active Directory (AD) hinterlegt, so dass anhand der Protokolldatenbank festgestellt werden kann, von welchem Rechner welcher Beschäftigte welche Daten abgerufen hat. Dies ist bei Nachforschungen, ob die Nutzung der gespeicherten Daten rechtmäßig erfolgte, von Bedeutung. Die Prüfung der fachlichen Notwendigkeit erfolgt dann in Abstimmung mit der verantwortlichen Stelle, ggf. bei fachaufsichtlichen Fragen unter Einschaltung des Landeskriminalamts. Aufwändiger werden künftig auch Besprechungen über fachliche Anforderungen, deren Umsetzung in den Datenverarbeitungsprogrammen und über die für die Nutzung erforderlichen Dienstanweisungen, da dann im Regelfall das jeweilige Präsidium und das Landeskriminalamt vertreten sein müssen.

Ein weiteres Augenmerk ist darauf zu richten, dass das Präsidium Technik, Logistik, Service der Polizei die Aufgaben für die jeweils verantwortlichen Stellen des Polizeivollzugsdienstes nur im Rahmen einer Auftragsdatenverarbeitung nach § 7 LDSG erfüllen kann, wofür entsprechende Vereinbarungen zu treffen sind. Außerdem gelten im Verhältnis zwischen den Polizeidienststellen und diesem Präsidium nicht mehr die Regeln des Polizeigesetzes für die Speicherung, Nutzung und Übermittlung von Daten durch Dienststellen des Polizeivollzugsdienstes. Vielmehr gilt für die eigene Tätigkeit dieses Präsidiums das Landesdatenschutzgesetz, wie sich der Begründung zu Artikel 13 Nummer 5 des Gesetzes zur Umsetzung der Polizeistrukturreform entnehmen lässt:

> Die Einordnung des Präsidiums Technik, Logistik, Service der Polizei als Einrichtung für den Polizeivollzugsdienst bringt zum Ausdruck, dass die Aufgaben des Präsidiums nicht dem Bereich der polizeilichen Vollzugshandlungen zuzurechnen sind, es vielmehr in erster Linie Unterstützungsleistungen für die gesamte Polizei des Landes erbringt (LT-Drs. 15/3496, S. 56).

Diese andersartige Stellung ist daher künftig in vielerlei Hinsicht, insbesondere für den Fall von Übermittlungen von Polizeidienststellen an das Präsidium zu beachten.

Die mit der Umsetzung der Polizeistrukturreform verbundenen Auswirkungen auf die tägliche Arbeit meiner Dienststelle werden sich - positiv und negativ - erst nach einer Eingewöhnungsphase herauskristallisieren. Langfristig kann eine Verankerung der Aufgabenbereiche Recht und Datenschutz im Leitungsbereich der regionalen Polizeipräsidien nur von Vorteil sein. Von einem Zauber, der nach Hermann Hesse bekanntlich jedem Anfang innewohnt, möchte ich allerdings nicht sprechen.

2.4 Der Verfassungsschutz in schwerer See

2.4.1 Verfassungswidrige Zustände im Verfassungsschutzrecht noch immer nicht behoben

Im März 2014 jährt sich zum zehnten Mal die Entscheidung des Bundesverfassungsgerichts zum sog. großen Lauschangriff (Urteil vom 3. März 2004 - 1 BvR 2378/98 u. a.). Darin hatte das Bundesverfassungsgericht festgestellt, dass die damalige Regelung der akustischen Wohnraumüberwachung in der Strafprozessordnung in wesentlichen Teilen verfassungswidrig war. Im Verfassungsschutzrecht unseres Landes ist das Urteil immer noch nicht umgesetzt worden.

Das **Bundesverfassungsgericht** hatte an der damaligen strafprozessualen Regelung insbesondere kritisiert, der Gesetzgeber habe dem Schutz des Kernbereichs privater Lebensgestaltung nicht genügend Rechnung getragen und die insoweit verfassungsrechtlich gebotenen Überwachungs-, Erhebungs- und Verwertungsverbote sowie Verfahrenssicherungen nicht hinreichend konkretisiert. Es ist völlig unstreitig, dass diese Rechtsprechung auch auf das Verfassungsschutzrecht zu übertragen ist. Es ist auch unbestritten, dass die derzeitige Regelung des Landesverfassungsschutzgesetzes (LVSG) in § 6 Absatz 3 nicht mehr verfassungskonform ist. Die **Landesregierung** hatte spätestens mit der Novellierung des Polizeigesetzes im Jahr 2008 zugestanden, dass die Entscheidung des Bundesverfassungsgerichts auch im Bereich der Gefahrenabwehr Platz greift, und deswegen die entsprechende Regelung in § 23 PolG den verfassungsrechtlichen Anforderungen angepasst (siehe hierzu LT-Drs. 14/3165, S. 53). In der Folgezeit räumte die Landesregierung auch ein - u. a. in der Stellungnahme zu meinem 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 57), in dem ich die Untätigkeit des Landesgesetzgebers kritisiert hatte -, dass die Regelung in § 6 Absatz 3 LVSG nicht den Anforderungen des Bundesverfassungsgerichts entspreche. Außerdem kündigte sie geradezu generös an, das Innenministerium werde mich „zu gegebener Zeit“ an der Erarbeitung der Neuregelung beteiligen.

Die Zeit ist schon lange reif für eine entsprechende Änderung; spätestens jetzt wäre auch die Gelegenheit hierfür gegeben. Denn die Landesregierung hat Anfang Dezember 2013 einen Entwurf zur Änderung des Landesverfassungsschutzgesetzes (und des Polizeigesetzes; s.o.) in den Landtag eingebracht (LT-Drs. 15/4421). Anlass hierfür war zwar nicht die Wohnraumüberwachung, sondern die Entscheidung des Bundesverfassungsgerichts über die Bestandsdatenauskunft vom 24. Januar 2012 - 1 BvR 1299/05. Darin hatte das Bundesverfassungsgericht festgestellt, dass die bisherigen Regelungen zur Bestandsdatenauskunft bei verfassungskonformer Auslegung Abfragen bei Telekommunikationsdienstleistern über den Inhaber von IP-Adressen nicht zulassen und dass die bisherige Regelung verfassungswidrig sei, soweit sie die Abfrage von Zugangscodes zu Speichermedien zulasse. Zur Korrektur der Regelungen über die Bestandsdatenauskunft hatte das Gericht den Gesetzgebern des Bundes und der Länder eine Übergangsfrist bis zum 30. Juni 2013 zugebilligt, die inzwischen – ohne rechtzeitige Umsetzung in Baden-Württemberg - abgelaufen ist (siehe hierzu ausführlich Kapitel 2.1.3).

Das Innenministerium hat zwar meine Dienststelle erfreulich früh bei der Erarbeitung eines Referentenentwurfs zur Bestandsdatenauskunft beteiligt. Ich hatte daraufhin erneut eine Anpassung des Landesverfassungsschutzgesetzes auch in Bezug auf die Vorschriften über die Wohnraumüberwachung (§ 6 Absatz 3 LVSG) angemahnt, denn der Referentenentwurf enthielt hierzu wiederum keine Aussage. Zur Begründung führt die Landesregierung im Hinblick auf meine Stellungnahme zum

Referentenentwurf an, die Gesetzesnovelle bezwecke ausschließlich die rechtskonforme Regelung der Bestandsdatenabfrage. Weitergehende Änderungen des Landesverfassungsschutzgesetzes blieben einer späteren Novellierung vorbehalten. Weiterhin stellt die Landesregierung klar, dass das Landesamt für Verfassungsschutz derzeit keine Maßnahmen nach § 6 Absatz 3 LVSG durchführe (LT-Drs. 14/4421, S. 17 f.).

Die hartnäckige **Verweigerungshaltung der Landesregierung** ist mir unbegreiflich. Da das Landesamt für Verfassungsschutz nunmehr schon seit Jahren keine verfassungskonforme Wohnraumüberwachung vornehmen kann und in der Begründung des aktuellen Gesetzentwurfs (LT-Drs. 15/4421, S. 18) auch eingeräumt wird, dass keine entsprechenden Maßnahmen durchgeführt würden, muss inzwischen die Frage gestattet sein, ob dieser gravierende Grundrechtseingriff überhaupt erforderlich ist. Wenn dem nicht so ist, dann kann die Vorschrift auch gleich ganz gestrichen werden.

Meine Stellungnahme zum Referentenentwurf führte im Bereich der Bestandsdatenauskunft immerhin zu folgenden Änderungen des Regierungsentwurfs:

- Der Referentenentwurf hatte noch keine besonderen formellen Voraussetzungen für die Einholung von Auskünften über IP-Adressen und über Zugangscodes vorgesehen. Auf meinen Hinweis, dass das Bundesverfassungsgericht (1 BvR 256/08 vom 2. März 2010, Absatz Nummer 261) bestimmte Dokumentationspflichten begründete, wurde nunmehr immerhin bestimmt, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren aktenkundig zu machen sind. Meine weitergehende Anregung, zur Sicherstellung der Dokumentation eine Anordnung des Leiters des Landesamtes für Verfassungsschutz oder seines Vertreters (vgl. § 5a Absatz 4 Satz 2 LVSG) zu verlangen, wurde hingegen nicht aufgegriffen.

- Auf meinen Hinweis auf die entsprechenden verfassungsgerichtlichen Anforderungen (BVerfG, 1 BvR 256/08 vom 2. März 2010, Absatz Nummer 263) wurden Regelungen zur Benachrichtigung der Betroffenen aufgenommen.

- Die Neuregelung soll nunmehr - ebenso wie die Neuregelung der Bestandsdatenauskunft im Polizeirecht - nach fünf Jahren evaluiert werden.

Meine Kritik, dass die Neuregelung mit besserer Systematik in das bestehende Gesetz einzufügen wäre und dass nach den Anforderungen des Bundesverfassungsgerichts die Voraussetzungen für eine IP-Adressen-Abfrage dahingehend einzuschränken sind, dass auch bei nachrichtendienstlichen Erhebungen eine „auf Anhaltspunkte im Tatsächlichen gestützte konkrete Gefahr“ vorliegen muss (BVerfG, 1 BvR 256/08 vom 2. März 2010, Absatz Nummer 261), wurde dagegen von der Landesregierung - u. a mit Hinweis auf das Wesen des Verfassungsschutzes - nicht aufgegriffen. Insoweit hoffe ich auf weitere Verbesserungen im Verlauf des Gesetzgebungsverfahrens.

2.4.2 Terrorismusabwehr im Spannungsfeld von kollektivem Sicherheitsdenken und individuellen Freiheitsrechten

Das „Trennungsgebot“ zwischen Polizei und Verfassungsschutz ist seit Jahren Gegenstand der politischen und fachlichen Diskussion Im 27. Tätigkeitsbericht 2006 (LT-Drs. 14/650, S. 10) und im 28. Tätigkeitsbericht (LT-Drs. 14/2050, S. 12) hatte mein Vorgänger das „Gemeinsame-Dateien-Gesetz“ kritisiert, welches zur Verbesserung der Terrorismusabwehr eine Verknüpfung von Dateien der Nachrichtendienste auf Bundes- und Landesebene mit denen der Polizeien u. a. in einer „Antiterrordatei“ regelte. Das zunächst bis zum Januar 2012 zeitlich befristete Gesetz für diese Datei wurde nach einigem Hin und Her auf Bundesebene bis zum Jahre 2017 verlängert. Eine bereits im Jahr 2007 erhobene Verfassungsbeschwerde (1 BvR 1215/07) hat im April 2013 zu einem Urteil des Bundesverfassungsgerichts geführt, das viele der datenschutzrechtlichen Bedenken gegen die Antiterrordatei bestätigte. Allerdings wurde zugleich das vielfach postulierte Trennungsgebot zwischen Nachrichtendiensten und Polizeien zu einem „Trennungsprinzip“ umgewandelt.

Es ist leider inzwischen „Tradition“: Sicherheitsgesetze werden vor allem mit dem Anspruch gemacht, dass es dem Schutz der Freiheit und der Bürger diene, wenn die Sicherheitsbehörden möglichst viel von möglichst vielen wissen. Dass der betroffene Bürger hiervon nicht viel mitbekommen soll, versteht sich fast von selbst. Wie der gegenseitige Informationsaustausch von Nachrichtendiensten und Polizeien des Bundes und der Länder - über die eigenen Datenbanken hinaus - aussehen sollte, war § 2 des Antiterrordateigesetzes (ATDG) zu entnehmen:

> Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Abs. 1 in der Antiterrordatei zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die Daten sich beziehen auf
> 1. Personen, die
>   a) einer terroristischen Vereinigung nach §129a des Strafgesetzbuchs, die einen internationalen Bezug aufweist, oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Abs. 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland oder
>   b) einer Gruppierung, die eine Vereinigung nach Buchstabe a unterstützt, angehören oder diese unterstützen,
> 2. Personen, die rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten, befürworten oder durch ihre Tätigkeiten vorsätzlich hervorrufen,
> 3. Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in Nummer 1 Buchstabe a oder in Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind (Kontaktpersonen), oder
> 4. a) Vereinigungen, Gruppierungen, Stiftungen oder Unternehmen,
>   b) Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse, Telekommunikationsendgeräte, Internetseiten oder Adressen für elektronische Post, bei denen tatsächliche Anhaltspunkte die Annahme begründen, dass sie im Zusammenhang mit einer Person nach Nummer 1 oder Nummer 2 stehen und durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können,
>
> und die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland erforderlich ist. Satz 1 gilt nur für Daten, die die beteiligten Behörden nach den für sie geltenden Rechtsvorschriften automatisiert verarbeiten dürfen.

Schon im Rahmen der Gesetzgebung hatten die Datenschutzbeauftragten des Bundes und der Länder an den unbestimmten Begriffen dieser Regelung scharfe Kritik geäußert. Über eine erste Kontrolle durch meine Dienststelle im Jahr 2007 wurde im 28. Tätigkeitsbericht (LT-Drs. 14/2050, S. 12 ff.) umfassend berichtet, soweit es die uns auferlegte Verschwiegenheitsverpflichtung zuließ; auch andere Kollegen überprüften die Umsetzung in ihren Ländern bzw. bei den Sicherheitsbehörden des Bundes. Die Ergebnisse der Kontrollen flossen später in Stellungnahmen an das **Bundesverfassungsgericht** zu der dort anhängigen Verfassungsbeschwerde ein. Als das Bundesverfassungsgericht 2012 einen Termin zur mündlichen Verhandlung anberaumte, habe ich zur Vorbereitung sowohl beim **Landeskriminalamt** als auch beim **Landesamt für Verfassungsschutz** weitere Kontrollbesuche durchgeführt.

Dabei stellte sich rasch heraus, dass es nicht nur für meine Dienststelle, sondern selbst für die zu kontrollierenden Stellen schwierig war, bei dem für die Antiterrordatei zuständigen **Bundeskriminalamt** Protokolldaten in einer aussagekräftigen Form und in vertretbarer Zeit zu erhalten. Diese Probleme habe ich - wie auch schon der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - in einer weiteren Stellungnahme an das Bundesverfassungsgericht deutlich gemacht. Vor allem war die Verantwortung für die Protokolldatenbank sehr unbefriedigend geregelt. Diese Datenbank steht beim Bundeskriminalamt, das allein dafür auch verantwortlich ist; damit unterliegt sie eigentlich vollumfänglich der Kontrolle des Bundesbeauftragten. Da aber auch die Protokolldaten der Länderbehörden enthalten sind, war das Bundeskriminalamt der Auffassung, dass der Bundesbeauftragte insoweit keine Kontrolle durchführen dürfe. Für die Landesbeauftragten für den Datenschutz ergab sich aufgrund des jeweiligen

Landesgesetzes hingegen keine Kontrollkompetenz für diese Datenbank beim Bundeskriminalamt. Und aus der Ferne ließen sich die Protokolldaten nicht praktikabel überprüfen.

Nach Vorlage der - zugegebenermaßen außerordentlich aufwändig zusammenzuführenden - Protokolldaten sowie der Auflistung der von den verantwortlichen Stellen im Land gespeicherten Daten führte ich bei beiden Stellen also Kontrollbesuche durch. Dabei stellte sich beim Landeskriminalamt heraus, dass die Protokolldaten nicht nur schon gelöschte Fälle enthielten, sondern darüber hinaus auch Fälle, deren Speicherung nicht erklärt werden konnte. Der Aufwand für die nur stichprobenartigen Kontrollen war dabei in manchem Einzelfall kaum zu bewältigen, da eine zusammenfassende Begründung für die Speicherung in der Antiterrordatei in den Unterlagen nicht vorhanden war. Für eine Kontrolle wäre es hilfreich, wenn ein aussagekräftiger Bericht die wesentlichen Erkenntnisse aus den mitunter vielen Ordnern zu der betreffenden Person zusammenfasst und ggf. die weiteren Fundstellen aufführt. Dieser Anregung will das Landeskriminalamt zukünftig Rechnung tragen.

Zu den „Kontaktpersonen“ nach § 2 Satz 1 Nummer 3 ATDG wurde mir vom Landeskriminalamt erläutert, dass es nur die sogenannten „dolosen“ Kontaktpersonen speichere. Auf die nach der Gesetzesbegründung mögliche Speicherung „undoloser“ Kontaktpersonen, also von Personen, die keine Kenntnis von dem Terrorismusbezug der ihnen bekannten Personen haben, habe man von vornherein verzichtet. Außerdem wies das Landeskriminalamt darauf hin, dass es die Berechtigung weiterer acht Polizeidienststellen, Abrufe in der Antiterrordatei zu tätigen, in Kürze widerrufen werde.

Beim Landesamt für Verfassungsschutz konzentrierte ich mich ebenfalls auf die von dort eingespeicherten „Kontaktpersonen“. Die Speicherung erfolgte durch Setzen eines Merkers im nachrichtendienstlichen Informationssystem NADIS. Zu mehreren Personen prüfte ich die Voraussetzungen vertieft, bei einer dieser Personen waren Erkenntnisse aus einer Telefonüberwachung eingeflossen.

Schon der Fragenkatalog des Bundesverfassungsgerichts und der Verlauf der mündlichen Verhandlung am 6. November 2012 ließen erahnen, dass die Antiterrordatei in der bisherigen Form nicht mehr lange Bestand haben dürfte. Ebenso waren Folgen für die Rechtsextremismusdatei zu erwarten, die aufgrund der im Zuge der Ermittlungen zum „Nationalsozialistischen Untergrund (NSU)“ erkannten Defizite in der Zusammenarbeit von Nachrichtendiensten und Polizeien durch das „Rechtsextremismus-Datei-Gesetz (RED-G)“ nach dem Strickmuster der Antiterrordatei kurzfristig neu errichtet worden war.

So kam es dann auch. Das Urteil des Ersten Senats vom 24. April 2013, 1 BvR 1215/07 (vgl. http://www.bundesverfassungsgericht.de/entscheidungen/rs20130424_1bvr121507.html) bestätigte zwar, dass die Antiterrordatei in ihren Grundstrukturen mit der Verfassung vereinbar sei, dass aber der darin vorgenommene Informationsaustausch gesteigerten verfassungsrechtlichen Anforderungen unterliege. Aus den tangierten Grundrechten folge zudem ein **„informationelles Trennungsprinzip“** (also nicht mehr „Trennungsgebot“), das den Austausch nur ausnahmsweise zulasse. Im Übrigen wurden erhebliche gesetzliche Konkretisierungen und - wichtig für die Datenschutzbeauftragten - eine wirksame Aufsicht gefordert.

Zu dem Urteil sind in den einschlägigen Fachzeitschriften zahlreiche Beiträge veröffentlicht worden, auf die ich hier nicht eingehe, Das Landeskriminalamt und das Landesamt für Verfassungsschutz haben nach dem Urteil und einer entsprechenden Information durch das Bundesministerium des Innern jedenfalls folgende **Konsequenzen** gezogen:

- Beide Stellen haben alle Personen, die den Personengruppen nach § 2 Satz 1 Nummer 1b) und Nummer 3 ATDG zugeordnet waren, gelöscht. Alle „Unterstützer“ und „Kontaktpersonen“, die bei meinen Kontrollbesuchen gespeichert waren, sind inzwischen gelöscht, also auch nicht verdeckt nach § 4 ATDG gespeichert, wie es das Bundesverfassungsgericht unter bestimmten Voraussetzungen für möglich hielt.

- Bezüglich der Personen, die nach § 2 Satz 1 Nummer 1a) bzw. Nummer 2 ATDG gespeichert sind, hat sich im Ergebnis keine signifikante Änderung ergeben, auch wenn einige der im Zeitpunkt meiner Kontrollbesuche gespeicherten Datensätze zwischenzeitlich gelöscht wurden.

- Soweit das Bundesverfassungsgericht die Unvereinbarkeit der Bestimmungen festgestellt hatte, als Daten durch Grundrechtseingriffe in das Telekommunikationsgeheimnis bzw. die Unverletzlichkeit der Wohnung erhoben und offen gespeichert wurden, teilte eine Stelle mit, dass sie keine entsprechenden Datenerhebungen vorgenommen hatte. Die andere wies darauf hin, dass sie keine Grunddaten (§ 3 Absatz 1 Nummer 1a) ATDG) gespeichert habe, die aus solchen Eingriffen stammten, und daher diese auch nicht verdeckt nach § 4 ATDG speichern müsse.

Da das Landeskriminalamt die Berechtigung der acht Polizeivollzugsbehörden, auf die Antiterrordatei zugreifen zu können, bereits im Oktober 2012 zurückgenommen hatte, betraf die Feststellung des Gerichts, dass § 1 Absatz 2 ATDG mit dem Grundrecht auf informationelle Selbstbestimmung mangels Bestimmtheit der Zahl und der fachlichen Betroffenheit der möglichen abrufberechtigten Stellen unvereinbar sei, das Land praktisch nicht mehr. Bemerkenswert war in diesem Zusammenhang die Mitteilung des Landeskriminalamts, dass sich das Abrufverhalten bezüglich der in der Antiterrordatei gespeicherten Daten in der Zeit nach meiner Kontrolle nicht wesentlich verändert habe. Nach meiner Kontrolle wurden Ansichten der „erweiterten Grunddaten“, welche nach § 4 ATDG beschränkt oder verdeckt gespeichert werden können, weder vom Landeskriminalamt bei anderen Dienststellen noch von anderen Dienststellen bei diesem angefordert.

Vorbehaltlich der noch nicht vorliegenden Protokolldaten dürfte die Zahl der Abrufe nach dem Urteil sehr stark zurückgegangen sein, weil aufgrund von Vorgaben des Bundesministeriums des Innern von Anfang Mai 2013 zunächst nur noch Abrufe im sog. Eilfall nach § 5 Absatz 2 ATDG zulässig sind. Zu derartigen Eilfällen teilten mir die beiden Stellen im Land - ebenfalls unter dem Vorbehalt der Protokolldatenauswertung - mit, dass es keine solchen Abrufe im Land gegeben habe.

Das Bundesverfassungsgericht hat - entsprechend der Einschätzung der Datenschutzbeauftragten - auch die datenschutzrechtlichen **Kontrollmöglichkeiten** nach § 10 ATDG für unzureichend gehalten. Kurz gesagt sah es das Gericht im Interesse eines effektiven Schutzes der Rechte von Betroffenen als notwendig an, dass auch auf Seiten der Datenschutzbeauftragten eine Zusammenarbeit zur wirksamen Kontrolle der Antiterrordatei erfolgt und diese sich untereinander wechselseitig zur Wahrnehmung ihrer Kontrollbefugnisse ermächtigen können sollen. Für diese Kontrollaufgabe ist eine geeignete Regelung im Gesetz erforderlich, das Gericht sah eine „Nachbesserungspflicht“ auf Seiten des Gesetzgebers.

Die „normalen“ Abrufe aus der Antiterrordatei dürften entsprechend den Vorgaben des Bundesverfassungsgerichts auf Bundesebene vorerst völlig gestoppt sein. Der 18. Deutsche Bundestag wird sich alsbald mit gesetzlichen Änderungen des Antiterrordateigesetzes, aber auch mit den Auswirkungen auf die Rechtsextremismusdatei befassen müssen, der vergleichbare verfassungsrechtlich angreifbare Regelungen zugrunde liegen. Für die Datenschutzbeauftragten wird sich je nach künftigem Regelungsinhalt und technischer Umsetzung dann die Frage stellen, wie die vom Gericht geforderte verstärkte Kontrolle ausgeübt werden kann. Hierfür werden ggf. Personalverstärkungen unumgänglich sein.

2.4.3 Die Neustrukturierung des nachrichtendienstlichen Informationssystems NADIS

Im Juni 2013 wurde das neue nachrichtendienstliche Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder nach mehrmaligen Verschiebungen in Betrieb genommen (vgl. auch 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 77). Nunmehr ist die papierlose Bearbeitung von Dokumenten möglich, jedoch regelt das zugrunde liegende Bundesverfassungsschutzgesetz dazu (noch) keine näheren Einzelheiten. Bisher erschloss das Informationssystem

als Indexdatei den Aktenrückhalt. Jetzt können die Verfassungsschutzbehörden auf die zu einem Vorgang gehörenden Unterlagen elektronisch zugreifen, ohne dass die jeweils verantwortliche Stelle zuvor um Übermittlung gebeten werden muss. Außerdem hat die Umstellung dazu geführt, dass die Amtsdatei des Landesamtes für Verfassungsschutz, die losgelöst vom Bundessystem betrieben wird, nun auf dieser Systembasis vom Bundesamt für Verfassungsschutz gehostet wird.

Die Entwicklung des neuen nachrichtendienstlichen Informationssystems **NADIS** lief - wie bereits im letzten Tätigkeitsbericht dargestellt - weitgehend an den Landesbeauftragten für den Datenschutz vorbei. Im Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde zwar regelmäßig über den Stand der Entwicklung informiert, wirkliche Einflussmöglichkeiten ergaben sich hierdurch jedoch nicht, weil auf die Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die beim Bundesamt betriebene Zentraldatei verwiesen wurde. Nun ist das System im aktiven Betrieb und ich werde mir bei passender Gelegenheit genauer zeigen lassen, welche Veränderungen dieser Umstieg zur Folge hat. Denn schon im Vorfeld der Neuausrichtung auf Bundesebene wollte das Landesamt für Verfassungsschutz wissen, wie es seine bisherige Amtsdatei auf derselben technischen Basis wie das Bundessystem führen könne. Hierbei spielten auch wirtschaftliche Gründe eine Rolle, denn das Landesamt speichert in seiner Amtsdatei ohnehin nur Daten, die auch die Voraussetzungen nach dem Bundesverfassungsschutzgesetz für NADIS erfüllen. Der einzige Unterschied zwischen Bundes- und Landesrecht besteht darin, dass im Bund Daten zu Personen erst ab dem vollendeten 16. Lebensjahr gespeichert werden dürfen, während im Land die Altersgrenze bei 14 Jahren liegt.

Das entscheidende Rechtsproblem bei der fachlich „Hosting“ genannten Führung der Amtsdatei des Landesamtes durch das Bundesamt liegt nach meiner Auffassung in den rechtlichen Grundlagen. Während die Ämter - nicht nur in Baden-Württemberg - argumentieren, diese Dateiführung unterliege den Amtshilferegelungen des § 1 Absatz 3 des Bundesverfassungsschutzgesetzes, habe ich - wie auch meine Kollegen in anderen Ländern - die Auffassung vertreten, es handele sich um eine **Auftragsdatenverarbeitung**, die das Bundesamt für das Landesamt erbringe. Da das Landesverfassungsschutzgesetz insoweit keine vom Landesdatenschutzgesetz abweichende Regelung enthält, wäre das Landesamt als öffentliche Stelle des Landes verpflichtet, die Auftragsdatenverarbeitung nach dem Grundsatz, dass die Verwaltung an Recht und Gesetz gebunden ist, mit dem Bundesamt zu vereinbaren. Das Bundesamt wollte sich aber offensichtlich nicht auf derartige Vereinbarungen einlassen, die zu einer - auf den jeweiligen Datenbestand eines Landesamtes beschränkten - Kontrollkompetenz auch der Landesbeauftragten für den Datenschutz geführt hätten. Inwieweit mir adäquate Kontrollmöglichkeiten im Landesamt eröffnet werden, wird sich zeigen.

Meine rechtlichen Bedenken und das Angebot zu weiteren Gesprächen wurden leider nicht aufgegriffen. Eine Änderung des Landesverfassungsschutzgesetzes zur rechtlichen Fundierung des neuen Verfahrens ist mir bisher auch nicht bekannt geworden.

2.4.4 Auskunft nach dem Landesverfassungsschutzgesetz

Wie bei jeder anderen Behörde kann ein Betroffener auch beim Landesamt für Verfassungsschutz den Antrag stellen, ihm Auskunft zu seinen dort gespeicherten Daten zu geben. In Abweichung von den allgemeinen Regelungen des Landesdatenschutzgesetzes sind dabei aber Besonderheiten zu beachten, die im Ergebnis nicht unbedingt dazu führen, dass ein Betroffener etwas für ihn wirklich Wichtiges erfährt.

§ 13 des Landesverfassungsschutzgesetzes (LVSG) regelt das „wozu“, „wie“ und „wann“ einer Auskunftserteilung an einen Betroffenen. Dieser hat in seinem Antrag zunächst auf einen konkreten Sachverhalt hinzuweisen und sein besonderes Interesse an einer **Auskunft** darzulegen. Grundsätzlich gilt, dass das Amt nicht verpflichtet ist, über die Herkunft der Daten, die Empfänger von Übermittlungen und den Speicherungszweck et-

was mitzuteilen. Die weitaus größeren Hindernisse werden aber in Absatz 2 aufgeführt:

Die Auskunftserteilung unterbleibt, soweit
1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,
2. durch die Auskunftserteilung Quellen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamtes für Verfassungsschutz zu befürchten ist,
3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Die Entscheidung trifft der Behördenleiter oder ein von ihm besonders beauftragter Mitarbeiter.

Häufig enthält die - ggf. nur teilweise - Ablehnung einer Auskunft, die nicht unbedingt begründet werden muss, den Hinweis, dass sich der Betroffene an meine Dienststelle wenden kann, was hin und wieder auch geschieht. In der Regel wird eine entsprechende Anfrage dann zum Anlass genommen, die zu dem Betroffenen beim Landesamt gespeicherten Daten einer stichprobenartigen Durchsicht zu unterziehen. Anschließend wird mit dem Amt ggf. erörtert, ob die weitere Speicherung überhaupt noch erforderlich ist oder ob nicht doch die eine oder andere Erkenntnis dem Betroffenen mitgeteilt werden kann. Den Betroffenen muss ich in diesem Zusammenhang häufig daran erinnern, dass ich die Fachlichkeit der Speicherung - also die inhaltlich richtige Anwendung der Regelungen des Gesetzes - nur eingeschränkt überprüfen kann und dass die Verarbeitung seiner personenbezogenen Daten durch das Landesamt für Verfassungsschutz daher datenschutzrechtlich nicht zu beanstanden gewesen sei. Weitere Einzelheiten darf ich in den meisten Fällen nicht mitteilen, da ich selbst nach § 27 Absatz 2 des Landesdatenschutzgesetzes zur Verschwiegenheit verpflichtet bin und meine Mitteilung an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand des Landesamts zulassen darf. Dieser unbefriedigende „Kanzleitrost“ ist aufgrund der weit gefassten Regelungen des Landesverfassungsschutzgesetzes leider häufig kaum zu vermeiden.

Allerdings bin ich nicht immer mit der Verfahrensweise des Amtes zufrieden. Als ich in einem Fall anregte, bestimmte Daten könnten doch gelöscht und der Betroffene über die Löschung und den Inhalt informiert werden, wurde mir gegenüber dieses abgelehnt. Als der Betroffene wegen der Auskunftsverweigerung dann ein verwaltungsgerichtliches Verfahren anstrengte, wurden die Inhalte der gelöschten Datensätze sehr schnell mitgeteilt. Bei dieser Verfahrensweise fühle ich mich in meiner Aufgabenstellung nicht ernst genommen.

3. Justiz

3.1 Europäische Ermittlungsanordnung

Auf europäischer Ebene wird eine Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese soll die grenzüberschreitende Strafverfolgung erleichtern.

Die **Europäische Ermittlungsanordnung (EEA)** wird zu einer weitgehenden gegenseitigen Anerkennung von Ermittlungsentscheidungen zwischen den Mitgliedstaaten führen: Die von einer zuständigen Behörde eines Mitgliedstaats (Anordnungsstaat) getroffene Ermittlungsentscheidung ist von einem anderen Mitgliedstaat (Vollstreckungsstaat) zu vollstrecken. Da mit der Richtlinie keine einheitlichen Verfahrensgarantien geschaffen werden, zwischen den nationalen Strafverfahren aber erhebliche Unterschiede bestehen und in der Europäischen Union auch kein einheitliches und ausreichendes Datenschutzniveau besteht, wirft die gegenseitige Anerkennung von Ermittlungsanordnungen Probleme auf. Wenn der Anordnungsstaat z. B. niedrigere Schutzstandards aufweist als der Vollstreckungsstaat, könnte es dazu kommen, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre. Die Europäische Ermittlungsanordnung könnte damit zu einer Absenkung der Schutzstandards bei strafprozessualen Maßnahmen führen.

Um zu verhindern, dass eine gegenseitige Anerkennung von Entscheidungen der Mitgliedstaaten zu Lasten des Grundrechtsschutzes und damit auch des Datenschutzes geht, ist es daher nötig, Mindeststandards für Strafverfahren festzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher in einer Entschließung vom 21./22. März 2012 gefordert, dass die Europäische Ermittlungsanordnung in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden muss, das die Grundrechte der Bürgerinnen und Bürger gewährleistet (vgl. Anhang 2).

Nach meinen Informationen wurde Ende November 2013 im Trilog zwischen den beteiligten europäischen Gremien eine Einigung über eine Europäische Ermittlungsanordnung erzielt. Danach sind die Möglichkeiten eines Vollstreckungsstaates, eine Ermittlungsanordnung zurückzuweisen, insbesondere soweit die eigenen Grundrechtsstandards nicht gewahrt werden, gegenüber dem ursprünglichen Entwurf verbessert worden. Zum Datenschutz wurde auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 verwiesen und der Zugang zu den Daten allein auf autorisierte Personen beschränkt. Ob damit alle aus Sicht des Datenschutzes erforderlichen Sicherungen eingebaut wurden, wird sich in der praktischen Umsetzung nach der für den Februar 2014 erwarteten Schlussabstimmung im Europäischen Parlament zeigen.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen.

3.2 Schuldnerverzeichnis im Internet

Seit dem 1. Januar 2013 können die bisher bei den Amtsgerichten geführten Schuldnerverzeichnisse über ein zentrales und länderübergreifendes Internetportal eingesehen werden. Das Schuldnerverzeichnis für jedes Land wird nun von einem zentralen Vollstreckungsgericht geführt, in Baden-Württemberg vom Amtsgericht Karlsruhe.

Grundlage für die Schaffung dieses Internetportals ist das Gesetz zur Sachaufklärung in der Zwangsvollstreckung vom 29. Juli 2009 (BGBl. I 2009 S. 2258), das am 1. Januar 2013 in Kraft getreten ist und das die Informationsbeschaffung des Gläubigers in der Zwangsvollstreckung verbessern und die Führung der Schuldnerverzeichnisse der Länder modernisieren soll. Die Ausgestaltung der damit wesentlich erleichterten Einsichtsmöglichkeit in das **Schuldnerverzeichnis** wurde vom Bundesministerium der Justiz durch Rechtsverordnung - die Schuldnerverzeichnisführungsverordnung vom 26. Juli 2012 (BGBl. I 2012 S. 1654), gültig seit 1. Januar 2013 - geregelt.

Wie bereits in meinem letzten Tätigkeitsbericht erwähnt (LT-Drs. 15/955, S. 79 f.), begegnete der erste Verordnungsentwurf des Bundesministeriums der Justiz erheblichen datenschutzrechtlichen Bedenken: So war dort z. B. vorgesehen, dass bereits nach Eingabe des Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Land eingerichtet sind, hätte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner erhalten, deren Kenntnis sie nicht benötigt.

Nachdem die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 7. Februar 2012 (vgl. Anhang 1) gefordert hatte, dass bei der Internetabfrage die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen ist, um so dafür Sorge zu tragen, dass möglichst nur diejenige Person angezeigt wird, auf die sich der Abfragezweck bezieht, wurde der Verordnungsentwurf in diesem Punkt erheblich nachgebessert:

Nach der seit dem 1. Januar 2013 geltenden Schuldnerverzeichnisführungsverordnung hat die anfragende Person zunächst mindestens Familien- und Vornamen oder die Firma des Schuldners, den Sitz des zuständigen Vollstreckungsgerichts oder den Wohnort des Schuldners oder den Ort, an dem der Schuldner seinen Sitz hat, einzugeben. Sind nach Eingabe dieser Daten mehrere Datensätze (mehrere Schuldner) vorhanden, ist zusätzlich zu den genannten Angaben das Geburtsdatum des Schuldners einzugeben. Ergibt auch diese Abfrage mehrere Ergebnisse, hat der Nutzer zusätzlich den Geburtsort des Schuldners einzugeben.

Die in der Schuldnerverzeichnisführungsverordnung geregelte Ausgestaltung der Internetabfrage stellt im Vergleich zum ersten Verordnungsentwurf aus datenschutzrechtlicher Sicht eine erhebliche Verbesserung dar.

3.3 Quellen-Telekommunikationsüberwachung im Ermittlungsverfahren - Kontrollbesuch bei einer Staatsanwaltschaft

Im Rahmen eines Kontrollbesuchs bei einer Staatsanwaltschaft haben sich Mitarbeiter meiner Dienststelle mit den mehrere tausend Seiten umfassenden Akten zu einem Verfahren befasst, in dem aufgrund einer Vielzahl von richterlichen Beschlüssen verschiedene verdeckte Ermittlungsmaßnahmen, darunter auch Maßnahmen der **Quellen-Telekommunikationsüberwachung**, angeordnet worden waren.

Wegen der gem. § 2 Absatz 3 des Landesdatenschutzgesetzes auf die Verwaltungsangelegenheiten der Gerichte beschränkten Kontrollkompetenz meiner Dienststelle, die auf die grundgesetzlich garantierte richterliche Unabhängigkeit zurückzuführen ist, haben meine Mitarbeiter diese richterlichen Beschlüsse selbstverständlich nicht kontrolliert. Da staatsanwaltschaftliche Ermittlungsmaßnahmen jedoch auch insoweit meiner Kontrollbefugnis unterliegen, als sie sich auf Antragstellungen gegenüber dem Ermittlungsrichter beziehen, haben meine Mitarbeiter im Rahmen der Kontrolle auch die Anträge der Staatsanwaltschaft auf verdeckte Ermittlungsmaßnahmen geprüft.

In einigen der staatsanwaltschaftlichen Anträge ging es um die Zulassung der Überwachung und die Aufzeichnung der gesamten - auch verschlüsselten - Telekommunikation, die über die vom Beschuldigten genutzten informationstechnischen Systeme geführt wurde. Die Anträge der Staatsanwaltschaft, die zu vollzogenen richterlichen Beschlüssen geführt haben, haben sich dabei ausschließlich auf die Überwachung der laufenden Telekommunikation und auf solche Veränderungen am informationstechnischen System beschränkt, die für die Überwachung der Telekommunikation unerlässlich waren.

Die Überwachung der verschlüsselten Telekommunikation ist nur durch eine Quellen-Telekommunikationsüberwachung möglich (die von der Online-Durchsuchung zu unterscheiden ist; vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 35 ff.; 29. Tätigkeitsbericht, LT-Drs. 14/5500, S. 13)). Hierzu muss auf dem Computer der zu überwa-

chenden Zielperson eine entsprechende Software installiert werden, die auf die Daten der laufenden Kommunikation (Internet-Telefonie, E-Mail-Verkehr, Nachrichtenaustausch in sozialen Netzwerken) zugreift und diese an die jeweilige Ermittlungsbehörde weiterleitet, bevor die Daten verschlüsselt werden bzw. nachdem sie entschlüsselt worden sind.

Strittig ist, ob die Vorschriften in der Strafprozessordnung (StPO) zur Telekommunikationsüberwachung auch auf Maßnahmen der Quellen-Telekommunikationsüberwachung anwendbar sind. Aus der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (BVerfGE 120, 274 ff.) ergibt sich, dass Maßnahmen im Rahmen einer Quellen-Telekommunikationsüberwachung nur dann als alleiniger Eingriff in das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) zu bewerten und damit als Telekommunikationsüberwachungsmaßnahmen einzuordnen sind, wenn durch rechtliche Vorgaben und technische Vorkehrungen sichergestellt ist, dass sich diese Maßnahmen auf die laufende Kommunikation beschränken. Meines Erachtens bedeutet die Forderung des Bundesverfassungsgerichts nach rechtlichen Vorgaben, dass die vorhandenen Rechtsgrundlagen der Strafprozessordnung für Eingriffe in das Fernmeldegeheimnis (v. a. die §§ 100a, 100b StPO, auf die sich die Anträge der Staatsanwaltschaft stützten) keine hinreichende bereichsspezifische Ermächtigungsgrundlage darstellen. Denn eine Quellen-Telekommunikationsüberwachung kann über den Eingriff der herkömmlichen Telekommunikationsüberwachung hinaus zusätzlich die Integrität eines IT-Systems beeinträchtigen. Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits früher die Auffassung vertreten, dass die Quellen-Telekommunikationsüberwachung ebenso wie die Online-Durchsuchung (bisher) nicht in der Strafprozessordnung geregelt sei und dass Schutzvorkehrungen nur im Rahmen von Gerichtsbeschlüssen auf der Grundlage der §§ 100a, 100b StPO nicht ausreichten (vgl. Entschließung vom 16./17. März 2011, Anhang 16 zum 30. Tätigkeitsbericht, LT-Drs. 15/955). Da Ermittlungsrichter jedoch eine abweichende Meinung vertreten, sind staatsanwaltschaftliche Anträge auf Erlass eines richterlichen Beschlusses nach den §§ 100a, 100b StPO zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung von mir nicht zu beanstanden, soweit die Voraussetzungen der genannten Vorschriften vorliegen und in diesen Anträgen sichergestellt wird, dass sich die beantragte Überwachung auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt und Zugriffe auf Festplatten und andere Speichermedien ausgeschlossen werden.

Die erwähnten Anträge der Staatsanwaltschaft, die sich ausdrücklich auf die Überwachung der laufenden Telekommunikation beschränkten, entsprachen den von der Rechtsprechung aufgestellten Anforderungen. Zur Konkretisierung des - lediglich abstrakt eingegrenzten - Antragsgegenstandes bietet es sich jedoch an, die Programme bzw. Programmsysteme, die ausgeleitet werden sollen, in den Beschlussanträgen explizit zu nennen. Nach den meiner Dienststelle vorliegenden Informationen ist dies deshalb möglich, weil Maßnahmen der Quellen-Telekommunikationsüberwachung regelmäßig eine Telekommunikationsüberwachung vorausgeht, aus der sich einerseits die Notwendigkeit einer Quellen-Telekommunikationsüberwachung und andererseits auch das Wissen ergibt, welche Programme ausgeleitet werden müssen.

Aufgrund der Kontrolle ergab sich außerdem, dass es im Rahmen der Quellen-Telekommunikationsüberwachung des Beschuldigten auch zu Ausleitungen von Telekommunikation bei Einsatz des Laptops des Beschuldigten im Ausland gekommen war. Hierzu wurde uns erklärt, es habe im Voraus nicht ermittelt werden können, wo sich der Beschuldigte zum Zeitpunkt der Aufzeichnung von Gesprächen aufhalten werde. Diese im Ausland durchgeführte Datenerhebung erfolgte jedoch ohne Rechtsgrundlage. Die Quellen-Telekommunikationsüberwachung hätte ab dem Zeitpunkt der Ausreise bzw. dem Zeitpunkt, zu dem die Strafverfolgungsbehörden von dieser Kenntnis erlangt haben, bis zur Wiedereinreise eingestellt werden müssen.

Dass nicht bekannt gewesen sei, wann sich der Beschuldigte im Ausland aufhält, ist für mich nicht nachvollziehbar. Anhand einer IP-Adresse eines

Rechners kann zwar keine Aussage zum Standort eines Rechners getroffen werden. Es bestehen jedoch technische Möglichkeiten, den Standort eines Rechners, der der Quellen-Telekommunikationsüberwachung unterliegt, näherungsweise zu lokalisieren. Im konkreten Fall dürfte außerdem bereits aufgrund der sonstigen Ermittlungsmaßnahmen bekannt gewesen sein, wann sich der Beschuldigte ins Ausland begeben und wie lange er sich dort aufhalten wird, so dass die Möglichkeit bestanden hätte, auf die Aufzeichnung der im Ausland geführten Gespräche zu verzichten. Ich habe die Staatsanwaltschaft über meine Auffassung informiert und gebeten, in künftigen Fällen entsprechend zu verfahren.

Nachdem auch der Generalbundesanwalt - wie aus einer Antwort der Bundesregierung auf eine Kleine Anfrage im Bundestag[26] hervorging - die Auffassung vertrat, dass § 100a StPO keine ausreichende Rechtsgrundlage für eine Quellen-Telekommunikationsüberwachung biete, kann ich als Fazit nur die Forderung wiederholen, in der neuen Legislaturperiode des Deutschen Bundestages eine für derartige Eingriffe in die Integrität informationstechnischer Systeme geeignete präzise Bestimmung zu treffen. Damit würde die in dem vorstehenden Fall festgestellte Anwendung des § 100a StPO der Vergangenheit angehören, wenn es gelingt, durch eine differenzierte Regelung zur technischen Durchführung derartiger Maßnahmen eine datenschutzrechtlich eindeutige Grundlage zu schaffen.

3.4 Teilprivatisierung im Justizvollzug

Im Berichtszeitraum haben Mitarbeiter meiner Dienststelle einen Kontroll- und Informationsbesuch bei der einzigen Justizvollzugsanstalt in Baden-Württemberg durchgeführt, die teilprivatisiert betrieben wird. Gegenstand dieser Kontrolle war u. a. die datenschutzrechtliche Bewertung der Kooperation zwischen der Justizvollzugsanstalt und dem privaten Dienstleister.

Rund 40% der Dienstleistungen in dieser **Justizvollzugsanstalt** wurden per Vertrag einem privaten Unternehmen übertragen. Die Zuständigkeit dieses privaten Dienstleisters ist auf Tätigkeiten im Vollzug beschränkt, denen kein Eingriffscharakter gegenüber Inhaftierten zukommt. Hierzu zählen z. B. die Beschäftigung der Gefangenen in Arbeits/-Werkbetrieben, die Versorgung der Gefangenen (Küche, Wäsche, Gefangeneneinkauf, Telefonie), die schulische und berufliche Ausbildung einschließlich der Arbeitstherapie und Tätigkeiten in der Lohnbuchhaltung, der Arbeitsverwaltung, aber auch im medizinischen, sozialen und psychologischen Dienst. Der Vertrag mit dem privaten Dienstleister läuft allerdings Ende Mai 2014 aus. Nach diesem Zeitpunkt sollen alle Aufgabenfelder wieder staatlich betrieben werden.

Eine Teilübertragung von Vollzugsaufgaben an Dienstleister ist nach dem am 1. Januar 2010 in Kraft getretenen Ersten Buch des Justizvollzugsgesetzbuches (JVollzGB I) möglich. Auch die Vorgängergesetze enthielten entsprechende Vorschriften. Das Erste Buch des Justizvollzugsgesetzbuchs enthält auch Regelungen für die Datenverarbeitung nach einer Übertragung von Vollzugsaufgaben. § 54 Absatz 1 JVollzGB I, der § 28 Absatz 1 des bis zum 31. Dezember 2009 geltenden Justizvollzugsdatenschutzgesetzes entspricht, erlaubt z. B., dass der Stelle, an die Aufgaben übertragen worden sind, die personenbezogenen Daten übermittelt werden dürfen, die für die Aufgabenerledigung erforderlich sind. Die Erledigung von Aufgaben durch Mitarbeiter des privaten Dienstleisters in der Justizvollzugsanstalt ist als **Funktionsübertragung** im datenschutzrechtlichen Sinn ausgestaltet. Dies hat zur Folge, dass der private Dienstleister nicht nur als unselbstständiger „verlängerter Arm“ für die Justizvollzugsanstalt tätig wird, sondern als verantwortliche Stelle i. S. des Landesdatenschutzgesetzes (LDSG). Der private Dienstleister ist aus datenschutzrechtlicher Sicht damit - obwohl seine Mitarbeiter in der Justizvollzugsanstalt tätig sind und z. T. die gleichen Arbeiten erledigen wie Mitarbeiter der Justizvollzugsanstalt - nicht der Justizvollzugsanstalt zuzurechnen. Er ist vielmehr „Dritter“ i. S. des § 3 Absatz 5 LDSG. Dies führt dazu, dass Zugriffe der in der Justizvollzugsanstalt tätigen Mitarbeiter des privaten Dienstleisters auf

[26] vgl. Antwort vom 22. November 2012, http://dipbt.bundestag.de/dip21/btd/17/115/1711598.pdf

Gefangenendaten datenschutzrechtlich teilweise anders zu bewerten sind als Zugriffe, die von Mitarbeitern der Justizvollzugsanstalt vorgenommen werden. Nimmt z. B. ein Mitarbeiter der Justizvollzugsanstalt Einblick in eine Gefangenenpersonalakte, stellt dies eine Datennutzung dar, deren Zulässigkeit sich nach den §§ 34 ff. JVollzGB I bestimmt. Nimmt dagegen ein Mitarbeiter des privaten Dienstleisters - der datenschutzrechtlich dieser anderen Stelle zuzurechnen ist - Einblick in eine solche Akte, stellt dies eine Datenerhebung dar, auf die die §§ 54 Absatz 3, 31 JVollzGB I Anwendung finden.

Obwohl die Zulässigkeit ein und derselben datenschutzrelevanten Tätigkeit - je nachdem, ob sie von einem Mitarbeiter der Justizvollzugsanstalt oder einem Mitarbeiter des privaten Dienstleisters erledigt wird - u. U. nach verschiedenen Vorschriften zu prüfen ist, dürfte man dennoch häufig zu identischen Ergebnissen gelangen. Eine pauschale Gleichsetzung der Tätigkeit von Mitarbeitern der Justizvollzugsanstalt mit der von Mitarbeitern des privaten Dienstleisters ist aus datenschutzrechtlicher Sicht damit aber nicht möglich, wie das nachfolgende Beispiel zeigt:

In der Justizvollzugsanstalt wird für die Verarbeitung insbesondere der personenbezogenen Daten der Gefangenen ein EDV-Fachverfahren (IS-Vollzug) eingesetzt. Von der Fragestellung ausgehend, welche personenbezogenen Daten der Gefangenen für die Erledigung einer bestimmten Vollzugsaufgabe erforderlich sind, wurden die Zugriffsberechtigungen für IS-Vollzug ausschließlich nach der Zuständigkeit der handelnden Personen vergeben und nicht danach, ob eine bestimmte Aufgabe von einem Mitarbeiter der Justizvollzugsanstalt oder einem solchen des privaten Dienstleisters erledigt wird. Da die Mitarbeiter des privaten Dienstleisters im Verhältnis zur Justizvollzugsanstalt Dritte im datenschutzrechtlichen Sinne sind, ist die Vorgehensweise, diesen Zugriffe auf IS-Vollzug einzuräumen, als Übermittlung durch ein automatisiertes Abrufverfahren zu bewerten. Ein solches liegt vor, wenn die speichernde Stelle (Justizvollzugsanstalt) einer anderen Stelle (dem privaten Dienstleister) die Berechtigung einräumt, aus einem Datenbestand bestimmte, festgelegte Datenarten über ein Endgerät selbstständig abzurufen und die Daten über Datennetze zu empfangen. Im Gegensatz hierzu liegt bei Zugriffen von Mitarbeitern der Justizvollzugsanstalt auf EDV-Systeme der Justizvollzugsanstalt keine automatisierte Übermittlung durch Abruf vor, da diese Zugriffe datenschutzrechtlich nicht als Übermittlung bzw. Erhebung, sondern als Nutzung einzustufen sind.

Eine Rechtsgrundlage, die es erlauben würde, Mitarbeiter des privaten Dienstleisters in ein automatisiertes Übermittlungs- und Abrufverfahren einzubeziehen, existiert jedoch nicht. Die Stellen, die an einem automatisierten Abrufverfahren beteiligt werden können, sind in § 52 JVollzGB I ausdrücklich benannt. Dienstleister, denen im Rahmen einer Funktionsübertragung Aufgaben übertragen worden sind, sind im Katalog des § 52 JVollzGB I jedoch nicht enthalten, obwohl davon auszugehen ist, dass die in der Justizvollzugsanstalt praktizierte Vorgehensweise bereits vorgesehen war, als die Vorschrift bzw. entsprechende Vorgängervorschriften geschaffen worden sind. Ich gehe davon aus, dass die im Katalog des § 52 JVollzGB I fehlende Nennung von Dienstleistern i. S. v. § 54 JVollzGB I auf ein Versehen zurückzuführen ist. Da das Justizministerium durch Verordnung weitere Beteiligte an automatisierten Übermittlungs- und Abrufverfahren benennen kann, ist dieser Mangel behebbar.

Werden einer privaten Stelle im Wege einer Funktionsübertragung Vollzugsaufgaben übertragen, kann die Tätigkeit von Mitarbeitern dieser privaten Stelle in der Justizvollzugsanstalt in datenschutzrechtlicher Hinsicht nicht pauschal mit der Tätigkeit von Mitarbeitern der Justizvollzugsanstalt selbst gleichgesetzt werden.

3.5 Adressangaben von Zeugen in der Anklageschrift

Nach § 200 Absatz 1 Satz 3 StPO sind Zeuginnen und Zeugen in der Anklageschrift als Beweismittel mit ihrem Wohnort oder Aufenthaltsort anzugeben. Im zweiten Halbsatz von Satz 3 ist ausdrücklich geregelt, dass es der Angabe der vollständigen Anschrift nicht bedarf.

*Der durch das **Zweite Opferrechtsreformgesetz** vom 29. Juli 2009 (BGBl. I S. 2280) neu gefasste Satz 3 des § 200 Absatz 1 SPO dient dem Zeugenschutz. Bis zum Inkrafttreten dieser Änderung war als Regelfall noch die Nennung des Wohnorts und der Wohnanschrift vorgesehen. Obwohl die derzeit geltende Fassung des § 200 Absatz 1 Satz 3 StPO bereits vor einigen Jahren in Kraft getreten ist, scheint es immer wieder vorzukommen, dass in Anklageschriften die vollständige Anschrift von Zeugen genannt wird So hat mich im Berichtszeitraum die Eingabe eines Bürgers erreicht, der von einem Amtsgericht eine Ladung zur Vernehmung als Zeuge in einer Strafsache erhalten hatte. Der im Verfahren Angeschuldigte, der wegen einer Körperverletzung bereits vorbestraft gewesen sei, habe den Zeugen - unter Hinweis darauf, dass er aufgrund eines Schreibens der Staatsanwaltschaft wisse, wo der Zeuge wohne - dazu veranlassen wollen, zu seinen Gunsten auszusagen.*

Die zuständige Staatsanwaltschaft hat sich meiner Dienststelle gegenüber dahingehend geäußert, dass die Anschrift des Zeugen in der Anklageschrift enthalten gewesen sei, die dem Angeschuldigten vom zuständigen Gericht zugestellt worden sei. Zwar regele die Strafprozessordnung, dass es der Angabe der vollständigen Anschrift nicht bedürfe. Von der Angabe der Anschrift sehe die Staatsanwaltschaft ohne das Vorliegen besonderer Gründe jedoch nicht grundsätzlich ab. Im Einzelfall könne die Benennung der Anschrift eines Zeugen aus Gründen des Zeugenschutzes unterbleiben. Im vorliegenden Fall habe jedoch kein Anlass für einen besonderen Zeugenschutz bestanden.

Diese von der zuständigen Staatsanwaltschaft geschilderte Vorgehensweise kehrt das durch das Zweite Opferrechtsreformgesetz in § 200 StPO aufgenommene Regel-Ausnahmeverhältnis in sein Gegenteil um. Dem Wortlaut der Vorschrift ist eindeutig zu entnehmen, dass grundsätzlich die bloße Angabe des Wohnorts oder des Aufenthaltsorts ausreicht und die Angabe der Wohnanschrift nicht erforderlich ist. Auch den Beratungen zum Zweiten Opferrechtsreformgesetz ist zu entnehmen, dass die Neufassung des § 200 Absatz 1 StPO darauf abzielte, im Interesse des Zeugenschutzes die Nichtaufnahme der ladungsfähigen Anschrift eines Zeugen in der Anklageschrift als ausdrückliche gesetzliche Regelung einzuführen.

Aus Gründen des Zeugenschutzes ist in Anklageschriften grundsätzlich auf die Angabe der vollständigen Anschrift von Zeugen zu verzichten.

4. Steuern und Statistik

4.1 Die Elektronischen LohnSteuerAbzugs-Merkmale (ELStAM)

Derzeit wird die Lohnsteuerkarte in Papierform durch ein elektronisches Verfahren ersetzt. Dabei werden die elektronischen Lohnsteuerabzugsmerkmale (**ELStAM**) aller Arbeitnehmer in Deutschland vom Bundeszentralamt für Steuern (BZSt) auf der Grundlage des § 39e des Einkommensteuergesetzes (EStG) gespeichert und zum Abruf durch berechtigte Arbeitgeber bereitgehalten. Bei den Merkmalen handelt es sich insbesondere um die Steuerklasse, die Zahl der Kinderfreibeträge, die Freibeträge und Merkmale für den Kirchensteuerabzug.

Welche datenschutzrechtlichen Risiken dabei auftreten können, hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits in einer Entschließung vom 24. Juni 2010 aufgezeigt (vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, Anhang 9). Aus datenschutzrechtlicher Sicht ist insbesondere Wert darauf zu legen, dass nur berechtigte Arbeitgeber die Daten ihrer jeweiligen Arbeitnehmer abrufen. Missbräuchliche Abrufe, etwa aus reiner Neugier, müssen verhindert oder zumindest erschwert werden. Zum Schutz seiner Daten kann jeder betroffene Arbeitnehmer mit verhältnismäßig geringem Aufwand selbst beitragen. Dazu muss er natürlich wissen, welche Rechte er überhaupt hat. Zu diesem Zweck wurde vom Arbeitskreis „Steuern“ der Konferenz der Datenschutzbeauftragten von Bund und Ländern ein entsprechendes **Merkblatt** entwickelt, welches diese Rechte im Einzelnen beschreibt und das über die Internetseite meiner Dienststelle abgerufen werden kann (http://www.baden-wuerttemberg.datenschutz.de/elstam/).

Zudem habe ich mich kürzlich an das Ministerium für Finanzen und Wirtschaft Baden-Württemberg gewandt und um Informationen über die Nutzung der ELStAM durch die Finanzverwaltung des Landes gebeten. Dabei geht es mir neben der Frage nach der datenschutzrechtlichen Verantwortung insbesondere darum, ob Maßnahmen des technischen und organisatorischen Datenschutzes ergriffen wurden, um Abrufe durch unbefugte Arbeitgeber zu verhindern. Inzwischen erfuhr ich auch, wie nach Ansicht des Bundesministeriums der Finanzen die weitere Umsetzung datenschutzrechtlicher Maßnahmen aussehen soll. Danach ist geplant, ab Januar 2015 eine vollständig automatisierte Überprüfung von Abrufen einzuführen; die bis dahin weitergeführte manuelle Überprüfung habe bisher allerdings keine Missbrauchsfälle, also unbefugte Abrufe, zu Tage gefördert.

4.2 Zensus und Haushaltsstatistiken

In meinem 30. Tätigkeitsbericht konnte ich erfreulicherweise feststellen, dass der Zensus 2011 ohne wesentliche Datenschutzmängel über die Bühne gegangen war. Die inzwischen von kommunaler Seite erhobenen Widersprüche gegen die Zensusergebnisse ändern an dieser datenschutzrechtlichen Einschätzung nichts. Denn Anlass war hier der aus den Zensusergebnissen in vielen Fällen ablesbare „Einwohnerschwund“ und die damit einhergehenden finanziellen Nachteile. Datenschutzrechtlich interessanter ist jetzt der Blick voraus.

Eine Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder hat - gestützt auf die Erfahrungen mit dem **Zensus 2011** - Eckpunkte für den nächsten Zensus formuliert, der nach den Vorgaben der Europäischen Union voraussichtlich im Jahr 2021 stattfinden soll. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat im Mai 2013 „Eckpunkte für eine datenschutzgerechte Volkszählung“ veröffentlicht, die in seinem Internetangebot unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/EckpunktepapierZensus2021.pdf?__blob=publicationFile abrufbar sind.

Solche Eckpunkte können nur eine erste Positionsbestimmung darstellen, da sich bis 2021 noch viel ereignen kann. Neben dem rasanten technischen Fortschritt könnte beispielsweise auch das Projekt zur **Weiterentwicklung des Systems der Haushaltsstatistiken** in Deutschland von Bedeutung sein, über das mich das Statistische Landesamt Baden-Württemberg im Sommer 2013 frühzeitig informiert hat. Dieses Projekt wurde

2012 vom Statistischen Bundesamt initiiert und wird von diesem zusammen mit den Statistischen Ämtern der Länder betrieben.

Der zentrale Gedanke bei der Neuausrichtung des Systems der Haushaltsstatistiken ist ein Gesamtsystem, bei dem ab dem Jahr 2017 die bisher weitgehend unabhängig voneinander durchgeführten Haushaltsstatistiken, beispielsweise der **Mikrozensus** (die „kleine Volkszählung“), die **Arbeitskräfteerhebung der Europäischen Union** (Labor Force Survey), die **Statistik über Einkommen und Lebensbedingungen der Bevölkerung in der Europäischen Union** (Leben in Europa / EU-SILC), die **EU-Erhebung zur Nutzung von Informations- und Kommunikationstechnologien in privaten Haushalten** (IKT) und **freiwillige Erhebungen** nach § 7 des Bundesstatistikgesetzes, als Module einer gemeinsamen Erhebung realisiert werden. Das neue System der Haushaltsstatistiken soll auf einer gemeinsamen Zufallsstichprobe basieren. Wie bei der derzeitigen Mikrozensusstichprobe soll auch zukünftig ein Prozent der Wohnbevölkerung befragt werden. Insgesamt wollen die Statistikbehörden die Qualität und die Aussagekraft der Haushaltsstatistiken verbessern, Redundanzen vermeiden und auf den wachsenden Bedarf an Statistikdaten schnell und flexibel reagieren können. Bürgerinnen und Bürger sollen dabei möglichst gering belastet werden.

Auch wenn sich das Projekt in einem relativ frühen Stadium befindet und viele Details noch auszuarbeiten sind, ist erkennbar, dass eine Umsetzung etliche datenschutzrechtliche Fragen aufwerfen wird, unabhängig von den Erwartungen an einen Zensus 2021.

4.3 Zentrale Informations- und Annahmestellen bei Finanzämtern

Mehrere Bürger haben im Berichtszeitraum moniert, dass sie bei ihrem Finanzamt wegen Umbauarbeiten ihre Steuerangelegenheiten mit einem Sachbearbeiter in einem Raum besprechen mussten, in dem sich noch weitere Sachbearbeiter und ratsuchende Bürger befanden hätten. Kein Wunder, dass diese Bürger unerbetene Mithörer befürchteten und das Steuergeheimnis in Gefahr sahen.

Zum Hintergrund: Die Finanzämter gehen nach und nach dazu über, sog. **Zentrale Informations- und Annahmestellen (ZIA)** einzurichten. In mehr oder weniger geräumigen Großraumbüros werden dabei Wartebereiche und Sachbearbeiterarbeitsplätze eingerichtet, wo Auskünfte gegeben, Anträge entgegen genommen und weitere Tätigkeiten ausgeführt werden, die in Anwesenheit des Bürgers vorgenommen werden können oder müssen. Die ganze Aktion geht auf einen Erlass des Finanzministeriums aus dem Jahr 1997 zurück.

Bei aller berechtigten Entrüstung ist allerdings im Auge zu behalten, dass in den Finanzämtern des Landes die sog. Sachbearbeiterregistratur geführt wird. Das heißt, dass die Steuerakten nicht in einer zentralen Registratur, sondern im Büro des jeweiligen Sachbearbeiters aufbewahrt werden. Wer in der Vergangenheit in einem Finanzamt je zum Büro des Steuersachbearbeiters vorgedrungen ist, wird sich vielleicht an die mit Akten überfüllten Aktenschränke auf dem Flur oder im Büro erinnern. Vor diesem Hintergrund sind die Überlegungen der Finanzverwaltung, den Bürger aus den Amtszimmern der Steuersachbearbeiter fernzuhalten, nicht von vornherein abwegig, sondern unter Berücksichtigung des Steuergeheimnisses nachvollziehbar.

Die Schaffung neuer „Begegnungszonen“ zwischen Bürger und Steuersachbearbeiter darf aber nicht dazu führen, dass die datenschutzrechtlichen Vorschriften für personenbezogene Steuerdaten nicht mehr gewährleistet sind. Daher sind an zentrale Informations- und Annahmestellen folgende Anforderungen zu stellen:

- Die Finanzämter müssen sicherstellen, dass die zwischen Sachbearbeiter und Bürger geführten Gespräche vertraulich sind. Dazu sollten die Räumlichkeiten in einen Wartebereich und einen Bearbeitungsbereich unterteilt sein, etwa durch besondere Trennwände (z. B. mit Milchglasscheiben, Jalousien oder Vorhängen) oder durch eine entsprechende Anordnung der Schalter.

- Es sollten weitere Vorkehrungen getroffen werden, dass Dritte die Gespräche zwischen dem Bürger und dem Sachbearbeiter nicht mithören können. Der Wartebereich sollte in genügend großer Entfernung von den Arbeitsplätzen dieser Sachbearbeiter liegen, so dass die Gespräche an den Annahmeplätzen nicht mitgehört werden können. Das bedeutet, dass Gesprächsgeräusche hingenommen werden können, wenn sich dadurch nicht der Inhalt der Gespräche erschließt. Im Bereich der Annahme ist auch auf einen ausreichenden Abstand der einzelnen Arbeitsplätze untereinander zu achten. Wenn mehrere Annahmeplätze eingerichtet sind, sollten die Sitzmöglichkeiten für die Bürger so platziert werden, dass sie sich gegenseitig den Rücken zukehren. Wenn eine ausreichende Entfernung nicht eingehalten werden kann, müssen andere geeignete Maßnahmen des Schallschutzes ergriffen werden.

- Ferner sollten die zwischen dem Sachbearbeiter und dem Bürger geführten Gespräche unbeobachtet erfolgen können. Wartebereich und Annahmebereich sollten dann optisch getrennt werden, wenn der Annahmebereich vom Wartebereich aus eingesehen werden kann und der Bürger nicht mit dem Rücken zum Wartebereich sitzt. Innerhalb des Annahmebereichs sollten die Abstände zwischen den Arbeitsplätzen so groß sein, dass Dritte nicht lesen können, was in den Akten steht. Die Anordnung der Sitzgelegenheiten sollte so gewählt werden, dass die Bürger nicht einander zugewandt sitzen.

- Unverzichtbar ist weiterhin, dass dem Bürger, dem die beschriebenen Maßnahmen nicht ausreichen, eine Möglichkeit eröffnet wird, sein Anliegen gänzlich unbeobachtet, ungestört und unbeeinträchtigt vortragen zu können. Hierzu ist bei den Zentralen Informations- und Annahmestellen ein separater Besprechungsraum in unmittelbarer Nähe vorgesehen. Der Bürger sollte auf die mögliche Nutzung dieses Diskretionsraumes mindestens durch gut sichtbare Hinweisschilder hingewiesen werden.

- Abschließend ist darauf hinzuweisen, dass die betreffenden Sachbearbeiter durch entsprechende Schulungen für die Belange des Datenschutzes zu sensibilisieren sind.

Diese Anforderungen sind in dem einleitend genannten Erlass, auf den sich die Finanzämter berufen, zwar interpretationsfähig formuliert worden. Die Prüfung der Eingaben hat aber in allen von meiner Dienststelle aufgegriffenen Fällen bisher keinen Grund zu einer förmlichen Beanstandung ergeben.

5. Kommunales

5.1 Kontrolle und Beratung - beides ist wichtig

Eine wichtige Aufgabe meiner Dienststelle ist es, die Verarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen in Baden-Württemberg zu kontrollieren. Dabei kann ich mir selbst ein Bild von den Verhältnissen vor Ort machen und ggf. einschreiten. Die Erfahrungen bei der Fallbearbeitung und bei Kontrollen zeigen mir aber, dass die Beratung eine zunehmende Bedeutung gewinnt und auch gewinnen sollte.

Dies wurde im Berichtszeitraum insbesondere im kommunalen Bereich deutlich. Ich hatte meine Mitarbeiter gebeten, dort einen Schwerpunkt zu setzen und vermehrt **Beratungs- und Kontrollbesuche** bei verschiedenen Kommunen durchzuführen. Schon nach wenigen Terminen zeigte sich, dass in der kommunalen Praxis teilweise gravierende datenschutzrechtliche Wissenslücken vorhanden sind. Zum Teil waren sich die Gesprächspartner nicht bewusst, in wie vielen Situationen ihrer täglichen Arbeit sie es mit personenbezogenen Daten zu tun haben. Dadurch waren sie auch nicht in der Lage, qualifiziert zu prüfen, ob die jeweilige Datenverarbeitung datenschutzrechtlich überhaupt zulässig ist.

Wenn es schon an datenschutzrechtlichen Grundkenntnissen fehlt, führt es nicht weiter, allein auf Kontrolle zu setzen. Denn die Kontrolle erfolgt typischerweise im Nachhinein, also dann, wenn „das Kind bereits in den Brunnen gefallen ist“. Besser ist es selbstredend, wenn es erst gar nicht zu solchen Rechtsverstößen kommen würde. Deshalb halte ich eine verstärkte Beratung der Kommunen für sinnvoll. Diese Beratungsaufgabe könnte etwa von den kommunalen Aufsichtsbehörden, beispielsweise von Landratsämtern oder Regierungspräsidien wahrgenommen werden. Daneben sehe ich aber auch mein Amt zunehmend gefordert. Durchaus denkbare Beratungsmaßnahmen stoßen in meiner Dienststelle allerdings an kapazitative Grenzen. In manchen Fällen hätten die Kommunen zudem auch selbst zu einer effizienteren Beratung beitragen können, indem sie den relevanten Sachverhalt vollständig darstellen und sich zunächst - ggf. in Abstimmung mit dem behördlichen Datenschutzbeauftragten und/oder dem Rechtsamt - eine eigene Rechtsmeinung bilden. Manche Kommunen haben es sich insoweit zu leicht gemacht und sind auf meine Dienststelle mit allgemeinen Prüfungsanfragen oder der Bitte um rechtliche Begutachtung zugekommen. Bei allem Verständnis dafür, dass Datenschutzfragen nicht gerade zum kommunalen Standardprogramm gehören mögen, wäre ich doch dankbar, wenn die verantwortlichen Stellen sich auch ihrer eigenen Verantwortung in Datenschutzangelegenheiten stärker bewusst werden.

Dabei verkenne ich nicht, dass die kommunale Landschaft recht bunt ist. Je größer eine Kommune und je größer ihre Verwaltungskraft ist, desto eher verfügt sie über einen formal bestellten behördlichen Datenschutzbeauftragten oder zumindest über Mitarbeiter, die sich fachbereichsübergreifend mit datenschutzrechtlichen Fragen befassen. Nach Möglichkeit sollte jede Kommune einen behördlichen Datenschutzbeauftragten bestellen, selbst wenn sie derzeit hierzu nicht verpflichtet ist. Für mehrere kleinere Gemeinden könnte dies ggf. auch ein Sachberarbeiter des Landratsamtes koordinierend übernehmen. Das Land sollte endlich dem Beispiel anderer Länder folgen und dies im Landesdatenschutzgesetz verpflichtend einführen.Mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung werden voraussichtlich ohnehin strengere Anforderungen gelten, auf die sich die Kommunen rechtzeitig einstellen sollten.

Beratungen und Kontrollen wurden im Berichtszeitraum aus unterschiedlichen Gründen durchgeführt:

- So ist beispielsweise eine Stadt in Nordbaden in Zusammenhang mit einem anstehenden innerstädtischen Entwicklungsprojekt auf mein Amt mit der Bitte um Beratung zugekommen, erfreulicherweise, bevor die Datenverarbeitung begann. Hierdurch können nachträgliche Beschwerden, Kontrollen und Beanstandungen vermieden werden.

- Beratungs- und Kontrollbesuche wurden auch durchgeführt, wenn schon aus den angeforderten Stellungnahmen hervorging, dass es an datenschutzrechtlichen Grundkenntnissen mangelte. In solchen Fällen haben meine Mitarbeiter vor Ort datenschutzrechtliche Grundlagen über den konkreten Anlass hinaus vermittelt.

- Zudem fanden Beratungs- und Kontrollbesuche statt, um bestimmte Verfahren oder Bereiche zu prüfen, in denen es substanzielle Änderungen gab (wie die Einführung des elektronischen Personenstandsregisters oder des neuen Personalausweises). Grundlegende datenschutzrechtliche Mängel waren aber hier erfreulicherweise nicht zu vermelden.

5.2 Gespräche mit den Kommunalen Landesverbänden und kommunalen Praktikern über Veröffentlichungen durch Kommunen

Ein Schwerpunkt bei den Beratungs- und Kontrollbesuchen waren kommunale Veröffentlichungen; hier bestehen bei vielen Kommunen nicht unerhebliche Unklarheiten.

Um die immer wieder erkennbare Diskrepanz zwischen den datenschutzrechtlichen Anforderungen einerseits und der kommunalen Praxis andererseits zu verringern, bin ich mit den Kommunalen Landesverbänden, die ihrerseits Vertreter der kommunalen Praxis hinzugezogen haben, in einen konstruktiven Dialog eingetreten. Zwar dauern die seit Februar 2013 geführten Gespräche noch an, jedoch gibt es bereits erste wichtige Ergebnisse:

*Hinsichtlich kommunaler Veröffentlichungen von Bildern (keine bewegten Bilder wie in Videos) hat meine Dienststelle eine **Handreichung** für die Kommunen erarbeitet und mit der kommunalen Seite abgestimmt. Sie ist seit Dezember 2013 auch im Internetauftritt meiner Dienststelle abrufbar (Themen A-Z/Kommunales)[27].*

Wesentliche datenschutzrechtliche Anforderungen ergeben sich in diesem Zusammenhang aus §§ 22 bis 24 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG). Das in diesen Vorschriften geregelte **Recht am eigenen Bild** schützt das Persönlichkeitsrecht der Betroffenen insbesondere dadurch, dass Bildnisse grundsätzlich nur mit Einwilligung des Abgebildeten veröffentlicht werden dürfen. Ausnahmen, die in der kommunalen Praxis eine wichtige Rolle spielen, ergeben sich insbesondere aus § 23 Absatz 1 KunstUrhG. Beispielsweise dürfen Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben, nach § 23 Absatz 1 Nr. 3 KunstUrhG ohne Einwilligung veröffentlicht werden. Soweit eine Einwilligung erforderlich ist, halte ich gewisse Erleichterungen hinsichtlich der Form für denkbar, die aus datenschutzrechtlicher Sicht hingenommen werden können.

Einige Kommunen sind auch daran interessiert, **Film- und Tonaufnahmen aus Sitzungen ihrer Gremien im Internet** zu veröffentlichen, beispielsweise als sog. Live-Stream. Dass dabei schwierige datenschutzrechtliche Anforderungen zu beachten sind, hatte ich bereits in meinem 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 118) aufgezeigt. Da eine entsprechende Änderung der Gemeindeordnung noch aussteht, habe ich zusammen mit den Kommunalen Landesverbänden Lösungsmöglichkeiten auf der Grundlage des bestehenden Rechts erörtert, soweit es um eine Veröffentlichung durch die Kommunen selbst geht. Auf dieser Grundlage wollen derzeit die Stadt Konstanz und die Gemeinde Seelbach in Zusammenarbeit mit meiner Dienststelle in Pilotprojekten datenschutzkonforme Lösungen entwickeln. Die Stadt Konstanz strebt dabei eine sog. „Podcast-Lösung“ an, wonach Bürgerinnen und Bürger ab dem Tag nach der Sitzung über die Tagesordnung gezielt Filmbeiträge zur jeweiligen Gemeinderatssitzung im Internet abrufen können. Diese Beiträge sollen von der Stadt im Rahmen der Zusammenstellung auf ihre Datenschutzkonformität geprüft werden. Die Gemeinde Seelbach beabsichtigt, einen (quasi) Live-Stream von öffentlichen Gemeinderatssitzungen mit 90 Sekunden Zeitversatz anzubieten. Durch den Zeitversatz

[27] http://www.baden-wuerttemberg.datenschutz.de/kommunales/

besteht die Gelegenheit, datenschutzrechtlich problematische Passagen zu stoppen oder auszublenden. Bis Anfang 2014 sollten zunächst die rechtlichen, technischen und organisatorischen Fragen geklärt und anschließend in der konkreten Umsetzung erprobt werden.Sobald eine datenschutzkonforme Lösung erarbeitet worden ist, können die Kommunen online gehen.

5.3 Die Bettensteuer und der Datenschutz

Seit wenigen Jahren wird vielerorts diskutiert, ob Städte und Gemeinden eine örtliche Steuer auf Gästeübernachtungen in Beherbergungsbetrieben erheben dürfen bzw. sollen. Dabei stellen sich auch datenschutzrechtliche Fragen.

Sie heißt Bettensteuer, Beherbergungssteuer, Übernachtungssteuer, Übernachtungsabgabe oder gar Kulturförderabgabe. In jedem Fall geht es um dasselbe, nämlich um die Erschließung einer weiteren Einnahmequelle durch die Erhebung einer örtlichen **Abgabe auf Übernachtungen in Beherbergungsbetrieben**. Dass Kommunen nach den Bestimmungen des jeweiligen Kommunalabgabengesetzes (KAG) örtliche Verbrauchs- und Aufwandssteuern erheben dürfen, ist weithin bekannt. Und dass der Phantasie bei der Suche nach Steuertatbeständen kaum Grenzen gesetzt sind, zeigt die regelmäßig wiederkehrende Diskussion um die Einführung von Abgaben für das Halten von Pferden oder Katzen. Kein Wunder, dass finanziell notleidende Kommunen auch Übernachtungsgäste zur Kasse bitten wollen. Allerdings hatte das **Bundesverwaltungsgericht** am 11. Juli 2012 in zwei Fällen (9 CN 1.11 und 9 CN 2.11) kommunale Satzungen für unwirksam erklärt, die keine Differenzierung nach dem Anlass der Reise vorsahen. Das Gericht befand nämlich, dass die örtliche Aufwandssteuer nur auf privat veranlasste entgeltliche Übernachtungen, nicht aber auf solche erhoben werden dürfe, die beruflich zwingend erforderlich sind. Mit der Erhebung einer Bettensteuer ist daher unweigerlich die Frage verbunden, von wem und wie die Information, ob eine Übernachtung **privat oder beruflich veranlasst** ist, einzuholen ist.

Mir ist bisher erst eine Stadt in Baden-Württemberg bekannt, die konkret die Einführung einer Bettensteuer plant und bereits Einnahmen hieraus in Höhe von immerhin einer Million Euro in ihrem Haushalt ab 2014 vorgesehen hat. In der im Oktober 2013 beschlossenen „Übernachtungssteuersatzung“ dieser Stadt ist vorgesehen, dass **Steuerschuldner der Betreiber des Beherbergungsbetriebs** ist. Der Gast seinerseits muss - wenn er die Bettensteuer vermeiden will - eine Erklärung abgeben, dass seine Beherbergung „ausschließlich beruflichen Zwecken“ diene und diesen Reisezweck auch belegen. Laut Satzung kommt als Nachweis eine Bescheinigung des Arbeitgebers oder Dienstherrn in Betracht, bei Selbständigen ggf. eine „amtlich vorgeschriebene Eigenbescheinigung“. Die Nachweise sind auf Anforderung der Stadt vollständig im Original vorzulegen und - wie auch weitere Belege zur Steuerpflicht - für die Dauer von vier Kalenderjahren aufzubewahren. Falls die berufliche Veranlassung der Beherbergung geltend gemacht wird, so sind die Gäste und deren Arbeitgeber, bei Selbständigen oder gesetzlichen Vertretern von juristischen Personen u. a. die Geschäftspartner, verpflichtet, Auskunft über die „berufliche Notwendigkeit der Beherbergung“ zu geben. Auch einen Außendienst zur Prüfung der Steuerpflicht vor Ort sieht die besagte Satzung vor. Um weitere Schlupflöcher zu schließen, werden in der städtischen Satzung auch Hotel- und Zimmervermittlungsagenturen sowie „Dienstleistungsunternehmen ähnlicher Art“ verpflichtet, die zur Besteuerung erforderlichen Angaben bei Bedarf zu liefern, beispielsweise in welchem Umfang und zu welchen Preisen in dem fraglichen Betrieb entgeltliche Beherbergungsleistungen erbracht wurden. Offenbar scheint die Stadt hier im Vorgriff auf die erst ab 1. Januar 2014 geltende Satzung tätig geworden zu sein, denn bereits im November 2013 beschwerte sich eine große, in Baden-Württemberg beheimatete Internetbuchungsplattform für Privatunterkünfte darüber, dass die Stadt von ihr schon die Übermittlung aller Vermieterdaten gefordert habe. Damit stand sie nach Presseberichten nicht alleine da, denn die Stadt soll ähnliche Anfragen an über 30 weitere Buchungsplattformen gerichtet haben.

Ich wage die Prognose, dass der mit der Bettensteuer verbundene Aufwand - sowohl auf Seiten der Stadt als auch auf Seiten der Hotelbetreiber - erheblich sein wird. Außerdem werden die geradezu inquisitorischen **Recherche- und Nachweispflichten** in Grenzfällen sicher noch für manchen Ärger sorgen. Man stelle sich etwa die Berechnung der Bettensteuer für den Geschäftsführer einer mittelständischen GmbH vor, der zusammen mit seiner Frau zu einem Geschäftstermin anreist und auch das anschließende Wochenende in der Stadt verbringen will, womöglich mit seinem Geschäftspartner am Samstag zeitweise auf dem Golfplatz. Will die Stadt dann nachforschen, ob dabei auch über Geschäftliches gesprochen wurde? Was ist mit dem Studenten, der in den Semesterferien regelmäßig seine Studentenbude einem auswärts wohnenden Freund gegen eine „Unkostenbeteiligung“ für ein paar Tage überlässt? Kein Wunder, dass auch die Stimmung im Gemeinderat bei der Beschlussfassung über die Satzung gemischt war und bereits eine von Verbandsseite unterstützte Musterklage gegen die kommunale Satzung im Gespräch ist. Auftrieb erhielt der Widerstand gegen die örtliche Bettensteuer zuletzt durch mehrere Entscheidungen des Oberverwaltungsgerichts (OVG) Münster vom 23. Oktober 2013 (14 A 314 bis 317/13), das in zweiter Instanz die Beherbergungsabgabensatzung der Stadt Dortmund für nichtig erklärte. Denn hier war die Satzung ähnlich abgefasst wie in der baden-württembergischen Stadt; auch hier sollten die Hoteliers nachforschen, ob eine Übernachtung beruflichen Zwecken dient. Die Argumentation des **OVG Münster** bezieht sich zwar auf das Kommunalabgabenrecht, wirkt sich aber indirekt auch auf die datenschutzrechtliche Zulässigkeit der mit der Bettensteuer verbundenen Datenerhebungen aus, denn hierfür wäre eine gültige (abgabenrechtliche) Rechtsgrundlage Voraussetzung: Nach Ansicht des Gerichts müsse sich eine Gemeinde bei der Entscheidung, wer Steuerschuldner sein soll, an die Grundentscheidungen des Kommunalabgabenrechts halten, das nur erlaube, einen Steuerschuldner zu bestimmen, der in einer besonderen rechtlichen und wirtschaftlichen Beziehung zum Steuergegenstand steht und einen maßgeblichen Beitrag zur Verwirklichung des Steuertatbestandes leistet. Das sei beim Hotelier zwar hinsichtlich des Merkmals der Beherbergung der Fall, nicht aber für das eigentlich steuerbegründende Merkmal, nämlich den privaten Zweck der Übernachtung. Nur wem die Erfüllung des Steuertatbestands zugerechnet werden könne, dürfe auch zum Steuerschuldner bestimmt werden. Der Inhaber des Beherbergungsbetriebs könne daher allenfalls - ähnlich wie bei der Kurtaxe - zum Steuerentrichtungspflichtigen bestimmt werden, der beim eigentlich Steuerpflichtigen, dem Gast, die Steuer einzuziehen und an die Stadt abzuführen hat. Eine analoge Anwendung des für die Kurtaxe einschlägigen § 43 KAG kommt jedoch nicht in Betracht, so dass es in Baden-Württemberg insoweit noch eine gesetzliche Regelungslücke gibt.

Ob auch die Satzung der baden-württembergischen Stadt von den Gerichten gekippt wird, bleibt abzuwarten. Maßgeblich werden dabei voraussichtlich die dargestellten abgabenrechtlichen, nicht die datenschutzrechtlichen Gesichtspunkte sein, denn das OVG Münster hat gleichzeitig klargestellt, dass das hier für die Beherbergungsbetriebe einschlägige Bundesdatenschutzgesetz der Erhebung und Weiterleitung der Erklärungen und Nachweise über den beruflichen Charakter einer Übernachtung nicht entgegenstehe, weil die kommunale Abgabensatzung grundsätzlich eine tragfähige Rechtsgrundlage i. S. v. § 4 Absatz 1 BDSG darstelle. Aus datenschutzrechtlicher Sicht würde ich es natürlich begrüßen, wenn auf die mit der Erhebung der Bettensteuer verbundene „Schnüffelei“ verzichtet werden könnte; andererseits verkenne ich nicht die wirtschaftlichen Zwänge der Stadt. Aber selbst wenn die Gültigkeit der Satzung von den Gerichten eines Tages bestätigt werden sollte, sollten Aufwand und Ertrag zu gegebener Zeit noch einmal unvoreingenommen überprüft werden.

Die erwähnte Internetbuchungsplattform hat sich übrigens geweigert, dem vorzeitigen Auskunftsverlangen der Stadt nachzukommen. Ob sie nach Inkrafttreten der Satzung dazu verpflichtet ist, halte ich rechtlich für fraglich, denn die Vorschrift des § 93 der Abgabenordnung (AO), auf die die kommunale Satzung verweist, sieht vor, dass andere Personen als die Beteiligten erst dann zur Auskunft verpflichtet werden sollen, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. Die Stadt

hat daher zunächst alle anderen Mittel auszuschöpfen, beispielsweise private Zimmervermieter über die Medien auf eine Anmelde- und Steuerpflicht hinzuweisen, bevor sie Dritte zu „Hilfssheriffs“ macht. Wie die Stadt allerdings die bei den zahlreichen internationalen Buchungsplattformen registrierten Gastgeber von Privatunterkünften ausfindig machen will, wird noch spannend zu beobachten sein. Zum Glück - wegen des Aufwands auch für die Stadt - ist wenigstens das beliebte „Couchsurfing“ kostenlos und damit „bettensteuerfrei“; immerhin sind nach einem Bericht einer örtlichen Tageszeitung schon knapp 4000 Bürger der Stadt bei der einschlägigen Internetplattform als Gastgeber registriert.

Die Erhebung der Bettensteuer ist auch eine Herausforderung für den Datenschutz. Im Interesse der Datensparsamkeit sollte darauf verzichtet werden.

5.4 Die Neuregelung des Bundesmeldegesetzes - kaum verabschiedet, schon wieder repariert

In meinen beiden letzten Tätigkeitsberichten bin ich bereits auf das neue Bundesmeldegesetz eingegangen. Nun könnte man denken, was lange währt, wird endlich gut. Jedoch war es bis zur Verabschiedung des neuen Bundesmeldegesetzes noch ein weiter und aus Sicht des Datenschutzes nicht immer guter Weg. Leider wurde im Gesetzgebungsverfahren dem Datenschutz in einigen Punkten nicht hinreichend Rechnung getragen. Damit wurden Chancen zur Stärkung des informationellen Selbstbestimmungsrechtes vertan.

Am 28. Juni 2012 beschloss der Deutsche Bundestag das neue **Bundesmeldegesetz** und sorgte damit - zu Recht - für große Kritik in der Öffentlichkeit. Anlass war weniger, dass nur wenige Abgeordnete an der zunächst kaum beachteten abendlichen Blitzabstimmung (während des Europameisterschaftsspiels Deutschland gegen Italien) teilnahmen, sondern vor allem der Inhalt, soweit es um **Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels** ging. Denn insoweit beschloss der Bundestag überraschend nur eine **Widerspruchsmöglichkeit** (statt der von der Bundesregierung ursprünglich vorgesehenen **Einwilligungslösung**). Diese Änderung, die eine deutliche Schwächung des Persönlichkeitsrechts vieler zu Gunsten wirtschaftlicher Interessen weniger dargestellt hätte, war aus der Sicht des Datenschutzes völlig inakzeptabel. Kein Wunder, dass dieser Ansatz in der Öffentlichkeit auf großes Unverständnis stieß. Deshalb bat ich auch umgehend das für das Meldewesen zuständige Innenministerium Baden-Württemberg, sich im Bundesrat bzw. im Vermittlungsausschuss dafür einzusetzen, dass die vom Bundestag beschlossene Änderung nicht zum Tragen kommt und stattdessen die ursprünglich vorgesehene datenschutzgerechtere Einwilligungslösung Gesetzeskraft erlangt. Die Fraktionsvorsitzenden im Landtag verständigte ich ebenfalls und bat sie um Unterstützung. Auch die Datenschutzbeauftragten von Bund und Ländern sprachen sich vehement gegen die vorgesehene Widerspruchslösung aus (vgl. Entschließung vom 22. August 2012**,** Anhang 7). Bundesweit meldeten sich zudem kommunale Vertreter zu Wort und erklärten, die Städte und Gemeinden hätten nicht die Absicht, zu Datenhändlern zugunsten kommerzieller Unternehmen zu werden.

Erfreulicherweise stieß ich im Innenministerium und im Landtag auf breite Unterstützung, wie sich auch in einer Plenardebatte am 11. Juli 2012 zeigte. Der Bundesrat rief im weiteren Verlauf des Gesetzgebungsverfahrens den Vermittlungsausschuss an, der daraufhin einen Kompromissvorschlag vorlegte, welcher vom Bundestag am 28. Februar und vom Bundesrat am 1. März 2013 angenommen wurde. Auch die Bundesregierung zeigte unter dem Eindruck der Kritik Einsicht und empfahl die Ablehnung des von den Regierungsfraktionen veränderten Entwurfs, was auch nicht alle Tage vorkommt. Nach dem neuen Bundesmeldegesetz, das am 1. Mai 2015 in Kraft treten und damit das Melderechtsrahmengesetz und die Meldegesetze der Länder ablösen wird, sind nun Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels nur mit Einwilligung des Betroffenen möglich. Doch leider sind auch Chancen zur Stärkung des informationellen Selbstbestimmungsrechts im Meldewesen vergeben worden:

- Die erst vor wenigen Jahren abgeschaffte **Mitwirkungspflicht des Wohnungsgebers** bei der Anmeldung des Mieters wird wieder eingeführt. Abgeschafft wurde diese seinerzeit unter anderem mit der Begründung, erfahrungsgemäß sei die Zahl der Scheinmeldungen zu vernachlässigen. Es ist nicht ersichtlich, dass sich dies zwischenzeitlich geändert hat.

- Die **Widerspruchsmöglichkeit** bei der Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs wurde abgeschafft. Die aktuelle Debatte, wie Daten im Internet für andere, aus Sicht des Betroffenen nicht gewünschte Zwecke verwendet werden, unterstreicht wieder einmal, mit welchen Gefahren und Risiken Internetübermittlungen grundsätzlich verknüpft sind. Vor diesem Hintergrund sollte das informationelle Selbstbestimmungsrecht des Betroffenen nicht weiter geschwächt werden. Eine Auskunft auf nichtelektronischem Wege sollte ausreichen, wenn dies der von der Auskunft Betroffene wünscht.

- Die **Hotelmeldepflicht** wurde nicht abgeschafft, obwohl es sich hier aus Sicht des Datenschutzes um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste werden somit wohl weiterhin als potentielle Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt.

Mit der **Hotelmeldepflicht** bzw. den besonderen Meldescheinen habe ich mich im Berichtszeitraum auch aufgrund mehrerer Eingaben von Betroffenen und im Zusammenhang mit Presseanfragen befasst. Dabei habe ich festgestellt, dass einige baden-württembergische Polizeidienststellen von Beherbergungsbetrieben forderten, Daten aus Meldescheinen elektronisch aufzubereiten und in dieser Form an die Polizei zu übermitteln. Dies halte ich nicht für zulässig, denn der **Polizeivollzugsdienst** darf nach den derzeit noch geltenden Vorschriften lediglich die Übermittlung der Meldescheine (im Original) verlangen. Der geradezu ultimativ vorgetragene Wunsch dieser Polizeidienststellen nach elektronischer Unterstützung durch die Hotelbetriebe steht überdies in auffälligem Gegensatz zu Informationen aus anderen Teilen des Landes, wonach die Polizei sich dort allenfalls gelegentlich oder anlassbezogen für Hotelmeldescheine interessiere. Eine unterschiedliche Verfahrensweise der Polizei wurde mir übrigens auch vom Landesverband des Hotel- und Gaststättengewerbes bestätigt.

Nach dem Inkrafttreten des Bundesmeldegesetzes wird der Polizeivollzugsdienst nur noch das Recht haben, **Einsicht in die Meldescheine** zu nehmen. Die im Landesmeldegesetz bislang vorgesehene Pflicht zur Herausgabe der Meldescheine wurde nach der Gesetzesbegründung vom Gesetzgeber bewusst nicht übernommen. Hier gelten künftig die bereichsspezifischen Regelungen zur Beschlagnahme oder Sicherstellung. Es besteht somit **künftig keine Verpflichtung für Beherbergungsbetriebe mehr, Meldescheine an Polizeidienststellen zu übermitteln**. Dies würde bei Beherbergungsbetrieben außer der gesetzlich vorgeschriebenen Aufbewahrung der Meldescheine eine zusätzliche, rechtlich jedoch nicht erforderliche weitere Datenverarbeitung bedeuten. Dem Innenministerium Baden-Württemberg habe ich aus gegebenem Anlass bereits meine Rechtsauffassung hierzu mitgeteilt und um Beachtung gebeten. Im Hinblick auf die neue Rechtslage sollte die Polizei überzogene Praktiken abstellen. Welche skurrile Geschichten die Realität bislang schreibt, zeigt der folgende Fall:

Vor kurzem meldete sich bei mir ein Hotelgast, der in einer Großstadt des Landes in seinem Hotelzimmer frühmorgens überraschend Besuch von mehreren Polizeibeamten erhalten hatte. Der Hotelgast, der zugegebenermaßen einen häufig vorkommenden Namen trug, war jedoch nicht der gesuchte Straftäter, dem der Einsatz galt. Als der Gast einige Zeit später erneut in dem Hotel nächtigte, wiederholte sich der Polizeieinsatz. Da der Petent sich nicht erklären konnte, wie die Polizei auf ihn gekommen war, erkundigte er sich bei der Hotelrezeption und erfuhr zu seiner Überraschung, dass das Hotel auf Verlangen der Polizei jeden Abend alle an diesem Tag von den Gästen ausgefüllten Hotelmeldescheine an die örtliche Polizeidienststelle faxen oder per E-Mail versen-

den müsse. Da der Hotelmeldeschein keine Rubrik für den Geburtsort aufwies, der nach der Vorgabe der Polizeidienststelle in der Liste auch nicht vorgesehen war, die gesuchte Person denselben Namen trug und zu allem Überfluss auch noch dasselbe Geburtsdatum wie unser Hotelgast aufwies, wurde die Verwechslung erst während des Polizeieinsatzes durch einen Blick in die Identitätspapiere festgestellt. Ein dritter Hotelaufenthalt des Petenten verlief übrigens ungestört, da das Hotel die Übermittlung seiner Daten an die Polizei inzwischen eingestellt hatte.

Auch mich verblüffte diese Geschichte. Zwar gehört es zu den Aufgaben des Polizeivollzugsdienstes, reisende Straftäter aufzuspüren. Dazu kann ggf. auch die Überprüfung von Gästen in Beherbergungsbetrieben gehören. Aber dass heute noch ein „Schleppnetz“ wie in den Hochzeiten der RAF-Fahndung der 1970er Jahre über das Land geworfen wird, verwundert denn doch. Wenn so eine Aktion überhaupt Sinn machen sollte, dann müssten ja eigentlich auch die anderen Hotelbetriebe der Stadt allabendlich die Hotelmeldescheine an die Polizei übermitteln und dies nicht nur in einer Gemeinde, sondern im ganzen Land. Den damit verbundenen Aufwand auf Seiten der Polizei kann man nur erahnen. Dass in einer städtischen Polizeidienststelle jemand allabendlich nichts anderes zu tun hat, als Hotelmeldescheine mit Fahndungslisten abzugleichen, hatte ich mir bis zu dieser Eingabe nicht vorstellen können. Der inzwischen eingegangenen Stellungnahme der Polizeidienststelle war übrigens zu entnehmen, dass der geschilderte Übermittlungsweg vor einigen Jahren mit Vertretern des Hotel- und Gaststättengewerbes auf freiwilliger Basis verabredet worden sei, aber nicht einmal die Hälfte der Betriebe an dem Verfahren teilnahm. Ob dieses Fahndungsinstrument wirklich geeignet ist, wage ich zu bezweifeln.

Nebenbei bemerkt: Es ist dem Hotelgast nach seinem ersten Erlebnis mit der Polizei hoch anzurechnen, dass er im Hotel stets seinen richtigen Namen angab. Erfahrungsgemäß überprüfen Hotels anhand der Identitätspapiere nicht, wen sie da tatsächlich vor sich haben. Hierzu sind sie nach gegenwärtiger wie nach künftiger Rechtslage nur bei Ausländern verpflichtet, was aus meiner Sicht eine gewisse Diskriminierung darstellt.

Im Hinblick auf das 2015 in Kraft tretende Bundesmeldegesetz sollten überzogene Praktiken der Polizei im Umgang mit Hotelmeldescheinen bald abgestellt werden.

6. Verkehr

6.1 Das intelligente Auto und der Datenschutz

Das Internet hält auf breiter Front nicht nur in Smartphones und mobilen Computern Einzug, es erobert auch das Kraftfahrzeug. Internetkonzerne wie Google widmen sich in Kalifornien bereits dem autonom fahrenden Fahrzeug und auch hiesige Premiumhersteller statten ihre Fahrzeuge mit modernen Assistenz- und Kommunikationssystemen aus und widmen sich der Vernetzung der Fahrzeuge untereinander oder mit der Infrastruktur am Straßenrand. Die Europäische Union hat diesen Trend aufgegriffen und ein Regelwerk für intelligente Verkehrssysteme entwickelt, das zugleich zu mehr Verkehrssicherheit beitragen soll. Da intelligente Verkehrssysteme eine Vielzahl von durchaus personenbeziehbaren und damit grundrechtsrelevanten Daten speichern können, droht der Datenschutz im wahrsten Sinne des Wortes unter die Räder zu geraten, wenn die rechtlichen Rahmenbedingungen nicht alsbald geklärt werden.

Schon heute verfügen unsere Kraftfahrzeuge vielfach über **Assistenzsysteme**, die den Fahrer unter Zuhilfenahme von Informations- und Kommunikationstechnologien bei der Steuerung des Fahrzeugs unterstützen: Antiblockiersysteme verhindern ein zu starkes Blockieren der Räder bei Bremsmanövern, der Bremsassistent verstärkt die Bremskraft bei Gefahrbremsungen, der Notbremsassistent leitet bei Gefahr vorbeugend eine Notfallbremsung und weitere Sicherheitsmaßnahmen ein, der Abstandsregeltempomat hilft, den Abstand zum vorausfahrenden Fahrzeug zu optimieren und Auffahrunfälle zu vermeiden, automatische Einparkhilfen steuern das Fahrzeug wie von Geisterhand in die vom Einparkassistenten selbst ausgemessene Parklücke usw. Aber Forschung und Entwicklung bleiben hier nicht stehen. Zwei - miteinander zusammenhängende - Trends lassen sich ausmachen: Die Assistenzsysteme sollen so weiter ausgebaut werden, dass sich das Fahrzeug in Zukunft *autonom*, ohne Steuerung durch einen Menschen, sicher fortbewegen kann. Und das Auto soll zum anderen mehr und mehr Kontakt mit seiner Umwelt aufnehmen, mit ihr - mit anderen Fahrzeugen („car2car“), aber auch mit der Infrastruktur der Straßen („car2infrastructure“), insgesamt also „car2x“ - *kommunizieren*: Auf diese Weise sollen die Fahrzeuge frühzeitig über die auf der geplanten Strecke befindlichen Baustellen, Ampeln und ähnliche Hindernisse informiert werden; und vorausfahrende oder entgegenkommende Fahrzeuge sollen Straßenzustände und Verkehrssituationen, beispielsweise Vollbremsungen, glatte Fahrbahnen, aber auch Staus und zähfließenden Verkehr, den übrigen hiervon betroffenen Verkehrsteilnehmern frühzeitig übermitteln, damit diese ihr Fahrverhalten darauf einrichten können. Das Autofahren soll durch autonom gesteuerte und kommunizierende Fahrzeuge bequemer, sicherer und flüssiger werden.

Aktuell wurde in Hessen von August 2012 an im Rahmen des von der Bundesregierung und dem Land Hessen geförderten Forschungsvorhabens **„Sichere intelligente Mobilität - Testfeld Deutschland“** (abgekürzt: **SIM^{TD}**), das von einem Konsortium aus Automobilherstellern, Automobilzulieferern, Kommunikationsunternehmen und Forschungsinstituten betrieben wird, über sechs Monate lang ein Feldversuch mit 123 Fahrzeugen, die mit einer kombinierten WLAN- und Mobilfunk-Technik zum Zwecke der car-2-x-Kommunikation ausgestattet waren, im öffentlichen Verkehrsraum durchgeführt. Das im Rahmen des Projekts zu erarbeitende Datenschutzkonzept ist bislang leider noch nicht veröffentlicht worden. Im Sommer 2013 vollbrachte die Daimler AG - und auch die meisten anderen Hersteller forschen an ähnlichen Systemen - auf den Spuren der historischen Fahrt von Bertha Benz über ca. 100 km eine Testfahrt mit einem autonom fahrenden Pkw der S-Klasse.

Die **Europäische Union** treibt die Entwicklung zu autonomen und vernetzten Fahrzeugen ihrerseits voran: Im Jahr 2006 hat die Kommission **die Initiative Intelligentes Fahrzeug** (Intelligent Car Initiative) ins Leben gerufen und darin die bereits damals bestehende eSafety Initiative integriert. Ein Ergebnis dieser Initiativen war die am 7. Juli 2010 erlassene **Richtlinie 2010/40/EU** zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern. Im Berichtszeitraum

wurde sie durch das **Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVSG)** vom 11. Juni 2013 in nationales Recht umgesetzt (BGBl. I 2013 S. 1553). Ziel der Richtlinie ist es, dass ein Mitgliedstaat der Europäischen Union ein „Intelligentes Verkehrssystem“ an den in der Richtlinie aufgeführten Spezifikationen ausrichtet, damit die Systeme innerhalb Europas kompatibel sind. Das nur sechs Paragraphen umfassende IVSG sieht in § 5 eine Ermächtigung für das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) vor, durch Rechtsverordnung mit Zustimmung des Bundesrats die Anforderungen an intelligente Verkehrssysteme in vorrangigen Bereichen zu regeln. Bislang liegen nach meinen Informationen aber noch keine entsprechenden Konkretisierungen vor, jedenfalls nicht hinsichtlich der datenschutzrechtlichen Rahmenbedingungen.

Als eines der ersten Intelligenten Systeme soll nach dem Willen der Europäischen Union der automatische **Notruf „eCall“** eingeführt werden. Dieses System soll im Falle eines Autounfalls automatisch durch den auslösenden Airbagsensor und über das Mobilfunknetz die örtlich zuständige Notrufabfragestelle informieren, wobei die Positionsdaten des Unfallautos übertragen und eine Sprechverbindung zwischen dem Fahrzeug und der Notrufabfragestelle aufgebaut werden soll. Mit delegierter Verordnung vom 26. September 2012 Nr. 305/2013 hat die Kommission die Spezifikationen für die Infrastruktur der Notrufabfragestellen festgelegt, die bis zum 1. Oktober 2015 einzurichten sind; am 13. Juni 2013 hat die Europäische Kommission außerdem ihren Vorschlag für eine EU-Verordnung über die Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeugen vorgestellt.

Auch die Bundesrepublik unterstützt die Entwicklung: Im Juni 2013 unterzeichnete das BMVBS ein Abkommen mit den Verkehrsministern der Niederlande und Österreichs. Danach sollen ab 2015 erstmals auf dem Korridor Rotterdam-Frankfurt a.M.-Wien intelligente Verkehrssysteme eingeführt werden. Baustellensperranhänger für temporäre Baustellen sollen mit Modulen ausgestattet werden, die ihre aktuelle Position und die Spurführung an der Baustelle den teilnehmenden Fahrzeugen frühzeitig mitteilen („Baustellenwarnung“). Außerdem sollen die teilnehmenden Fahrzeuge die von ihnen erfassten Verkehrslageinformationen mit ihrer genauen Position in eine Verkehrsleitzentrale übermitteln („Verkehrslageerfassung“), so dass den übrigen Verkehrsteilnehmern ein genaues und aktuelles Verkehrslagebild mitgeteilt werden kann.

Die geschilderten Entwicklungen werfen in datenschutzrechtlicher Hinsicht zahlreiche - teilweise bislang ungeklärte - Fragen auf:

- Schon heute werden in den Speichermedien der elektronischen Steuerungselemente eines Kraftfahrzeugs unzählige Daten gespeichert, z. B. über Geschwindigkeiten, Bremsbetätigungen, Beschleunigungen oder Blinkerbetätigungen, Füllstände, Betätigung des Lichts und vieles mehr. Diese Fahrzeugdaten, die primär den störungsfreien und sicheren Fahrbetrieb gewährleisten und Reparaturen sowie die Wartung des Fahrzeugs erleichtern sollen, sind jedenfalls dann personenbezogen, wenn sie einer Person zugeordnet werden können, z. B. wenn das Fahrzeug nur von einer Person genutzt wird oder die Nutzung anhand der konkreten Fahrzeit nachvollzogen werden kann, beispielsweise weil es zu einem Unfall gekommen ist und der Fahrer zur Unfallzeit feststeht. Wenn bei einem Werkstattbesuch die Daten ausgelesen werden, kann in diesem Fall die Werkstatt zahlreiche Einzelheiten über das Fahrverhalten des Nutzers erfahren. Angesichts des hohen Technisierungsgrades wird kaum ein Fahrzeugnutzer eine konkrete Vorstellung davon haben, was alles in seinem Fahrzeug gespeichert ist. Um wenigstens einen Mindeststandard an Transparenz der Speichervorgänge sicherzustellen, haben die deutschen Datenschutzaufsichtsbehörden im Februar 2012 unter Leitung des Bayerischen Landesamts für Datenschutzaufsicht zusammen mit dem Verband der Automobilindustrie (VDA) eine **Muster-Information** entwickelt, die insbesondere in die Betriebsanleitungen der Fahrzeuge aufgenommen werden soll. Der Wortlaut dieser Erklärung ist auf der Internetseite des bayerischen Landesamts

nachzulesen (http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Muster-Information_Fahrzeugdatenspeicher.pdf).

- Mit der Einführung weiterer Assistenzsysteme als Vorstufe zum autonomen Fahren nimmt die Menge an gespeicherten Daten zu. Zugleich werden mit der Vernetzung der Fahrzeuge Kommunikationswege eröffnet, über die von außen auf die erfassten Daten des Fahrzeugs zugegriffen werden kann und soll. An diesen Daten bestehen aber unterschiedliche Interessen: Nicht nur für den Rettungsdienst kann es von Bedeutung sein, wo sich das Fahrzeug befindet, wie stark der Aufprall war usw. Für die gespeicherten Daten interessieren sich beispielsweise auch Versicherungen, die im Falle eines Unfalles den genauen Unfallablauf rekonstruieren wollen - oder die schon im Vorfeld ihre Tarife nach Art und Weise der konkreten Nutzung des Fahrzeuges, insbesondere Zeit und Ort der Nutzung und Fahrweise, staffeln wollen („pay as you drive“). Die Kfz-Hersteller haben ein Interesse an den Daten, um die Sicherheit der Assistenzsysteme zu überprüfen und sie ggf. zu verbessern. Die Werkstatt hat ein Interesse, den Kunden dadurch an sich zu binden, dass sie ihn auf verbesserungswürdige Zustände des Fahrzeugs anhand der aktuellen Daten aufmerksam macht und so Wartungsaufträge generiert. Selbst ein Fahrzeugvermieter oder ein Arbeitgeber als Fahrzeughalter können ein Interesse an den gespeicherten Fahrzeugdaten haben. Erst recht wird dies auf einen Unfallgegner und auf die Polizei im Falle eines Unfalles zutreffen. Die Daten beziehen sich dabei u. U. nicht nur auf den Fahrer des Fahrzeugs. Viele Assistenzsysteme erfassen - beispielsweise mittels Kameras - Daten der übrigen Verkehrsteilnehmer; insoweit ist es jedenfalls ausgeschlossen, diese situationsabhängige Datenverarbeitung auf eine Einwilligung zu stützen.

Wenn die Fahrzeuge miteinander oder mit der Straßeninfrastruktur kommunizieren, ist stets die Frage zu stellen, ob die ausgetauschten Daten einen Personenbezug haben müssen. Die Daten müssen allerdings - auch wenn sie an sich nur kumuliert benötigt werden - schon aus Sicherheitsgründen belastbar sein; Hackerangriffen und unabsichtlichen Störungen ist vorzubeugen. Das bedingt aber nach dem Stand der Technik, dass den übermittelten Daten Absenderkennungen beigefügt werden müssen. Auch aus anderen Gründen wird es bei vielen Anwendungen erforderlich sein, die Daten - jedenfalls vorübergehend - bestimmten Fahrzeugen sowie Zeit und Ort zuzuordnen und damit Daten mit Personenbezug zu verarbeiten. Dies gilt selbst dann, wenn die Daten möglicherweise pseudonymisiert werden können. Mit der Aussage in einer Pressemitteilung des Projekts SIM^{TD}, die Fahrzeugdaten würden nur „in anonymisierter Form übermittelt“ und es würden „zum Schutz der Informationen Verschlüsselungstechnologien eingesetzt“, ist die Frage noch nicht beantwortet, ob personenbeziehbare Daten erhoben werden und auf welcher Rechtsgrundlage dies erfolgen soll. Für die Verarbeitung bedarf es deshalb konkreter Rechtsgrundlagen; die Frage nach der verantwortlichen Stelle ist zu beantworten, und vor allem ist der Grundsatz der Datensparsamkeit zu beachten. Der Gefahr, dass unbeobachtetes Fahren letztlich nicht mehr möglich sein könnte, ist unbedingt vorzubeugen.

An der aktuellen Fachdiskussion hat sich meine Dienststelle im Berichtszeitraum bei verschiedenen Veranstaltungen beteiligt. Nach meinem Eindruck ist bislang vor allem die technische Seite intelligenter Verkehrssysteme in den Blick genommen worden. Wenn die hochfliegenden Zukunftsvisionen verwirklicht werden sollen, dann müssen sie bald mit der notwendigen datenschutzrechtlichen Bodenhaftung versehen werden. Wir werden uns weiter in diesem wichtigen Themenfeld engagieren.

6.2 Kontrollbesuch bei der Zentralen Bußgeldstelle des Regierungspräsidiums Karlsruhe - das Verfahren OWi 21

Die Verarbeitung personenbezogener Daten in Ordnungswidrigkeitenverfahren sorgt immer wieder für datenschutzrechtliche Beschwerden. Eine Vielzahl von Bußgeldbehörden im Land nutzt dabei das Verfahren „OWi 21“, das meine Mitarbeiter

im Berichtszeitraum näher unter die Lupe genommen haben. Dafür war besonders die Zentrale Bußgeldstelle beim Regierungspräsidium Karlsruhe geeignet, da dort alle Verkehrsordnungswidrigkeiten verfolgt werden, die auf den Bundesautobahnen im Land begangen werden. Um das Ergebnis vorweg zu nehmen: Die in unzähligen Gerichtsverfahren erreichte Reife dieses Verfahrens hat auch aus Sicht des Datenschutzes keinen Anlass zu einer durchgreifenden Kritik ergeben.

Zur Verfolgung festgestellter Verkehrsordnungswidrigkeiten auf den Autobahnen leiten die zuständigen Polizeidienststellen die bei Geschwindigkeitsmessungen und Abstandsverstößen gewonnenen Bilddaten der Zentralen Bußgeldstelle zu. Die Daten sind auf dem Datenträger verschlüsselt gespeichert. In der Zentralen Bußgeldstelle werden die Daten entschlüsselt und auf einem lokalen Server gespeichert. Bei einer ersten Prüfung werden diejenigen Ordnungswidrigkeiten selektiert, die weiterverfolgt werden, weil der Fahrzeughalter an Hand des unzweifelhaft erkennbaren Kraftfahrzeugkennzeichens ermittelt werden kann. Mit den Bilddaten dieser Messungen wird in **„OWi 21“** jeweils eine elektronische Akte angelegt. Auf diese Akten können alle Sachbearbeiter zugreifen. Die Sachbearbeiter ermitteln den Halter des Kraftfahrzeugs und übermitteln diesem dann entweder einen Anhörungsbogen, der bei geringfügigeren Verstößen das Angebot der Zahlung eines Verwarnungsgeldes vorsieht, oder einen Zeugenfragebogen. Für die Entscheidung, welcher der Bögen im Programm auszuwählen ist, ist der aus den Bilddaten gewonnene Eindruck über das Geschlecht des Fahrzeugführers bedeutsam. Wenn dieses mit dem Geschlecht des Halters übereinstimmt, wird dem Fahrzeughalter ein Anhörungsbogen zugesandt. Er hat dann die Möglichkeit, sofern er die Ordnungswidrigkeit nicht begangen hat, den verantwortlichen Fahrer ggf. zu veranlassen, ein angebotenes Verwarnungsgeld zu bezahlen oder den Anhörungsbogen auszufüllen und zurückzusenden. Stimmt nach dem Bild das Geschlecht des Fahrzeugführers nicht mit dem Geschlecht des Halters überein, erhält der Halter einen Zeugenfragebogen, in dem er unter Hinweis auf sein mögliches Zeugnisverweigerungsrecht aufgefordert wird, den ordnungswidrig handelnden Fahrer zu nennen. Sobald der verantwortliche Fahrzeugführer feststeht und sein Verstoß nicht mit einem Verwarnungsgeld geahndet werden konnte, wird diesem ein Bußgeldbescheid zugestellt. Da diese Verfahrensweise nach dem Ordnungswidrigkeitengesetz vorgesehen ist und somit eine Rechtsgrundlage vorliegt, kann dies datenschutzrechtlich nicht bemängelt werden.

Die Bilddaten und weitere Daten (Datum der Geschwindigkeitsmessung, Datum der letzten Eichung des Geräts, Eignungsnachweis des Gerätebedieners etc.) werden von der Zentralen Bußgeldstelle in der Regel für die Dauer von zwei Jahren gespeichert. Eine frühere Löschung, etwa zeitnah nach der Erledigung eines Vorgangs, kommt nach Mitteilung der Zentralen Bußgeldstelle nicht in Betracht, weil die kompletten Bildreihen bereitgehalten werden müssen, um sie bei einem Einspruch gegen einen Bußgeldbescheid auf Verlangen dem zuständigen Gericht vorlegen zu können. Dies sei erforderlich, damit sich ein Gericht mit der Frage befassen kann, ob eine Bildreihe, einschließlich eines konkret umstrittenen Bildes, ordnungsgemäß mit zugelassenen Geräten und anerkannter Methodik erstellt wurde. Diese Vorgehensweise der Zentralen Bußgeldstelle bei der Speicherung der Bilddaten ist aus datenschutzrechtlicher Sicht letztlich zulässig.

Das Verfahren „OWi 21“ wird von der Kommunalen Informationsverarbeitung Baden-Franken (KIVBF) im Auftrag der Zentralen Bußgeldstelle und von Kommunen im Land betrieben. Die mit der Programmiersprache Java implementierte Anwendung basiert auf einer zweistufigen Systemarchitektur, d. h. die Benutzer greifen auf einen Web-Server zu, der die Daten auf einem nachgelagerten Datenbankserver abspeichert oder abruft. Bei der Zentralen Bußgeldstelle greifen die Sachbearbeiter mit ungefähr 75 bis 80 PCs auf die Anwendung zu.

In technischer Hinsicht haben sich bei der Kontrolle folgende Sachverhalte ergeben, die datenschutzrechtlich zu hinterfragen waren:

- Innerhalb des Verfahrens „OWi 21“ können alle Sachbearbeiter auf alle elektronischen Akten zugreifen. In einer Historie wird zu je-

dem Fall vermerkt, wann welcher Mitarbeiter welche Eingaben getätigt hat. Als Begründung wurde uns bei der Kontrolle genannt, dass der Zugriff organisatorisch nicht anders realisiert werden könne, da bei der Stelle viele Teilzeitkräfte beschäftigt seien, die sich gegenseitig vertreten können müssten. Außerdem sei bei Verkehrsordnungswidrigkeiten nur eine Verfolgungsverjährungsfrist von drei Monaten vorgesehen, die es bisweilen erfordere, bei Abwesenheit des betreffenden Sachbearbeiters schnell reagieren zu können.

- Während der Kontrolle erschien ein Fehlerdialog, der besagte, dass ein Datensatz mit gleichem Schlüssel bereits vorhanden sei. Diese Meldung lässt darauf schließen, dass das Programm noch gewisse algorithmische Unzulänglichkeiten hat. Die Fehlermeldung wurde kopiert und an das zuständige Rechenzentrum weitergeleitet.

- Bei einer Erörterung des Verfahrens mit dem Produktverantwortlichen des Kommunalen Rechenzentrums hat sich ergeben, dass die Fälle der Zentralen Bußgeldstelle und der kommunalen Bußgeldstellen in einer Datenbanktabelle gespeichert werden. Der Zugriff auf die Daten wird durch sog. Datenbanksichten gesteuert. Damit jede dieser Stellen nur auf die von ihr zu verarbeitenden personenbezogenen Daten zugreifen kann, wird als Selektionskriterium die Kennung der Dienststelle verwendet. Zwar ist diese Methode der Speicherung und des Zugriffs weit verbreitet und wird von Datenbanksystemen zuverlässig unterstützt, datenschutzfreundlicher wäre es aber gewesen, die personenbezogenen Daten mindestens in unterschiedlichen Tabellen oder in getrennten Datenbanken für jede Bußgeldstelle zu speichern. Der Nachteil bei der Verwendung von Datenbanksichten, um Zugriffsbeschränkungen zu realisieren, besteht darin, dass logisch zu trennende Datenbestände in einem zentralen und damit datenschutzrechtlich schwieriger zu kontrollierenden Datenbestand gespeichert werden. Zur Implementierung von Zugriffsbeschränkungen verfügen Datenbanksysteme über andere Mechanismen. Im Gegensatz zum Bundesdatenschutzgesetz regelt das Landesdatenschutzgesetz das Trennungsgebot jedoch nicht. Die Verarbeitung war daher nicht zu beanstanden.

Ungeachtet der genannten kleineren Kritikpunkte ist festzuhalten, dass das Verfahren „OWi 21“ einen hohen sicherheitstechnischen Reifegrad und insgesamt ein zufriedenstellendes datenschutzrechtliches Niveau aufweist. Selbst wenn dies manchen Beschwerdeführern nicht gefallen mag: Bußgeldbescheide würden selbst durch datenschutzrechtliche Mängel nicht unwirksam.

6.3 Datenschutz auf der Autobahn - die temporäre Seitenstreifenfreigabe auf der A 8

Die nahezu täglich auftretenden Staus auf den Autobahnen und Bundesstraßen im Ballungsgebiet Mittlerer Neckar zehren an den Nerven der Autofahrerinnen und Autofahrer. Schnelle Abhilfe durch einen entsprechenden Straßenausbau ist mangels finanzieller Mittel nicht in Sicht. Deshalb hat das Ministerium für Verkehr und Infrastruktur durch die Landesstelle für Straßentechnik eine für Spitzenverkehrszeiten anderenorts bereits eingeführte Alternative einrichten lassen. Die Kapazität könnte in jeder Fahrtrichtung um 25 - 33% erhöht werden, wenn der Seitenstreifen zu Zeiten hoher Straßenauslastung vorübergehend für den fließenden Verkehr freigegeben würde. Auch der Datenschutz spielte dabei eine Rolle.

Mitte 2011 informierte das Ministerium meine Dienststelle über die Absicht, auf der Bundesautobahn A 8 zwischen dem Autobahnkreuz Stuttgart und der Anschlussstelle Stuttgart-Möhringen eine sog. **temporäre Seitenstreifenfreigabe** einzurichten. Dafür sei es notwendig, auf dem gesamten Streckenbereich im Abstand von 800m hochauflösende, schwenk- und zoomfähige Kameras zu installieren. Denn die Freigabe des Seitenstreifens dürfe nur erfolgen, wenn sich dort keine Personen, Fahrzeuge, Fahrzeugteile oder sonstige Hindernisse befänden. Die hohe Auflösung der Kameraobjektive und die Zoom-Funktion würden benötigt, um z. B. zwischen einer Papiertüte und einem Metallgegenstand unterscheiden zu können. Die Freigabe selbst erfolge durch telematisch gesteuerte Wechselverkehrszeichen der Stre-

ckenbeeinflussungsanlage. Während der Freigabe sei die Prüfung auf Hindernisfreiheit regelmäßig zu wiederholen; hierzu würde neben der wiederholten Kontrolle der Videobilder durch das Personal der Straßenverkehrszentrale auch eine Software zur maschinellen Bildauswertung zum Einsatz kommen. Das Ministerium räumte dabei ein, dass von der Videobeobachtung angesichts der erforderlichen Auflösung der Kameras auch personenbezogene Daten (beispielsweise individualisierbare Personen oder Kfz-Kennzeichen) erfasst würden. Allerdings sei eine solche Erfassung nicht Ziel der Videoeinrichtung.

Die Erhebung personenbezogener Daten durch **Videotechnik** bedarf auch dann einer Rechtsgrundlage, wenn die Erhebung nicht gezielt vorgenommen wird, sondern nur aus technischen Gründen gleichsam als Nebenprodukt zur Erreichung eines von den personenbezogenen Daten unabhängigen Ziels - hier der sicheren Freigabe des Seitenstreifens - erfolgt. Eine solche Rechtsgrundlage gibt es nicht. Insbesondere kommt die Regelung des § 20a LDSG nicht in Betracht. Diese Vorschrift betrifft die Zulässigkeit von Videoanlagen zum Personen- und Objektschutz vor bestimmten Gefahren an bestimmten Orten - insbesondere in oder in der Nähe von „öffentlichen Einrichtungen“ oder „sonstigen baulichen Anlagen öffentlicher Stellen“. Die Regelung war hier jedoch nicht einschlägig. Denn eine Straße ist weder eine „öffentliche Einrichtung“ noch eine „bauliche Anlage“ in diesem Sinne; dies war den Verfassern des Gesetzentwurfs zur Einführung der Bestimmung des § 20a LDSG im Jahr 2010 bewusst (LT-Drs. 14/7313, S. 18). Ferner wurde seitens meiner Dienststelle deutlich gemacht, wenn zur Zielerreichung nicht an personenbezogene Daten (hier an die Videoaufnahmen individuell erkennbarer Personen und von Kfz-Kennzeichen) angeknüpft werden müsse, die Erforderlichkeit ihrer Verarbeitung besonders zu prüfen sei.

In intensiven Gesprächen meiner Dienststelle mit der Straßenverkehrszentrale bei der Landesstelle für Straßentechnik konnte eine Änderung des Ablaufs in Form eines zweistufigen Prüfverfahrens erreicht werden: Vor der temporären Freigabe eines Seitenstreifens wird nunmehr in einem ersten Schritt ein sogenannter Grobscan durchgeführt. Dabei wird dem Operator der Zentrale in einem technikgeführten Prüfprozess der Seitenstreifen zunächst kameraweise mit reduzierter Bildqualität angezeigt. Bei diesem Vorgang können große Gegenstände, zum Beispiel Fahrzeuge, Personen oder Tiere, erkannt werden, die Aufnahmen sind jedoch aufgrund der geringen Bildqualität in aller Regel ohne Personenbezug. Falls der Seitenstreifen sich dabei als nicht frei erweist, wird der Prozess abgebrochen, ohne dass Bilddaten weiter gespeichert werden. Nur dann, wenn der Seitenstreifen beim Grobscan frei erscheint, wird er noch in einem zweiten Kameradurchlauf mit hoher Bildqualität überprüft, um möglicherweise kleinere, aber gefährdende Gegenstände auf dem Seitenstreifen zu erkennen. Durch den vorgelagerten Grobscan und einen laufenden Bildabgleich im Hintergrund ist hierbei aber weitgehend sichergestellt, dass keine Personen oder größere Gegenstände mit Personenbezug mehr erfasst werden. Nur in sehr unwahrscheinlichen Fällen ist es denkbar, dass personenbezogene Daten erhoben werden, beispielsweise wenn ein markantes Kraftfahrzeug mit einem Werbeaufdruck, der auf eine natürliche Person hinweist, auf dem Seitenstreifen liegengeblieben ist. Ob es datenschutzrechtlich zulässig ist, Aufnahmen von derartigen Kraftfahrzeugen ohne Rechtsgrundlage anzufertigen, ist in Fachkreisen umstritten. Ich betone ausdrücklich, dass sich die Beurteilung derartiger datenschutzrechtlicher Grenzfälle grundsätzlich am Einzelfall ausrichtet.

Nur bei Freigabe des Seitenstreifens erfolgt eine Speicherung zu Dokumentationszwecken. Außerdem wird die Landesstelle auf eine wiederholte Überprüfung während des Laufs der Seitenstreifenfreigabe verzichten, da diese ohnehin nur erfolgt, wenn und solange der Verkehr so dicht fließt, dass ein Hindernis auf dem Seitenstreifen zur sofortigen Stockung führen würde.

Meine Mitarbeiter haben das Verfahren inzwischen in der Straßenverkehrszentrale überprüft und sich davon überzeugt, dass die abgesprochenen Rahmenbedingungen eingehalten werden.

6.4 Die intelligente Straße wird noch intelligenter - das Projekt BLIDS auf der B 27

Um Staus zu vermeiden und den Individualverkehr auf öffentliche Verkehrsmittel umzulenken, wollte das Verkehrsministerium in einem Pilotprojekt die Verkehrsteilnehmer mit Hilfe von Informationen über die aktuelle Reisezeit zum Umsteigen bewegen. Dazu sollte an der Bundesstraße 27 (B 27) die Reisezeit der Autofahrer ermittelt, mit der Fahrtzeit öffentlicher Verkehrsmittel verglichen und das Ergebnis den Autofahrern am Besten schon vor Fahrtantritt über moderne Kommunikationskanäle mitgeteilt werden.

Die regelmäßig überlastete B 27 südlich von Stuttgart wurde bereits vor vielen Jahren mit einer **Streckenbeeinflussungsanlage** und von dem damaligen Verkehrsminister daraufhin mit dem schmückenden Prädikat **„intelligente Straße“** versehen. Geholfen hatte diese Maßnahme wegen des permanenten Verkehrszuwachses wenig. Nun sollte die Straße samt der Verkehrsteilnehmer noch intelligenter werden. Konkret sah die Konzeption des Verkehrsministeriums bzw. der Projektpartner vor, an sechs Stellen entlang der B 27 zwischen Aichtal und Leinfelden-Echterdingen mit leistungsfähigen Detektoren im Sekundentakt die **Bluetooth-Adressen** von verbindungsbereiten Geräten, die in den vorbeifahrenden Kraftfahrzeugen mitgeführt werden (z. B. Mobiltelefone, Navigationsgeräte usw.), zu erheben. Dabei wäre jedes Gerät im Umkreis von bis zu 200 Metern von den Detektoren erfasst worden. Diese Daten sollten anschließend anonymisiert werden. Wenn ein Bluetooth-Gerät von zwei oder mehr Detektoren erfasst worden wäre, wäre dies an den anonymisierten Daten erkennbar gewesen. Aus den Zeitstempeln hätte man eine Zeitdifferenz für die Strecke zwischen den Messpunkten und aus einer Menge von Zeitdifferenzen eine durchschnittliche Reisezeit zwischen den Standorten der Detektoren errechnen können. Das von einer österreichischen Firma entwickelte Verfahren nannte sich BLIDS®, eine Abkürzung für **BL**uetooth Based traff**I**c **D**ata collection **S**ystem.

Im Verlauf der von uns erbetenen datenschutzrechtlichen Beratung ergab sich Folgendes:

- Die Regelungen in § 4 des Landesdatenschutzgesetzes (LDSG) sind einschlägig. Danach ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Vorschrift die Verarbeitung erlaubt oder der Betroffene eingewilligt hat. Bei den von dem System erfassten Bluetooth-Adressen handelt es sich um personenbezogene Daten. Zwar sind die Adressen zunächst den einzelnen Geräten und nicht unmittelbar einer Person zugewiesen. Aus der Zugehörigkeit der Geräte zu den sie nutzenden Personen ergibt sich jedoch mittelbar ein Personenbezug. Im Falle personenbezogener Daten stellt die genannte Bestimmung des Landesdatenschutzgesetzes nicht darauf ab, welcher Art die Verarbeitung ist. Insbesondere sind sowohl die Erhebung als auch die anschließende Anonymisierung von personenbezogenen Daten Verarbeitungen, für die es einer **Rechtsgrundlage** bedarf. Die Einholung einer Einwilligung des jeweiligen Gerätebesitzers dürfte offensichtlich nicht realistisch sein. Eine Vorschrift, welche die Verarbeitung erlaubt, konnten weder meine Mitarbeiter ausfindig machen, noch sah sich das Ministerium für Verkehr und Infrastruktur in der Lage, eine solche Vorschrift zu nennen. Ich empfahl daher dem Verkehrsministerium, zunächst eine gesetzliche Grundlage für eine derartige Verarbeitung zu schaffen.

- Außerdem war zu berücksichtigen, dass bei der geplanten Vorgehensweise möglicherweise Bluetooth-Adressen von Geräten erhoben und verarbeitet werden, die von Fußgängern, Radfahrern oder Anwohnern (in der Nähe der Straße) mitgeführt werden. Diese Daten wären für den Zweck der Reisezeitermittlung von Kraftfahrzeugen völlig ungeeignet. Ganz abgesehen davon dürfte eine Erhebung und Verarbeitung dieser Daten nach den §§ 13 und 15 LDSG nicht erfolgen. Die Eignung für einen bestimmten Zweck ist ein zentrales Kriterium einer datenschutzrechtlich zulässigen Erhebung und Verarbeitung personenbezogener Daten. Insofern dürfte eine zu schaffende gesetzliche Grundlage die Erhebung und Verarbeitung von für den eigentlichen Verarbei-

tungszweck ungeeigneten personenbezogenen Daten nicht erlauben, selbst wenn rechtlich und tatsächlich darauf abgestellt würde, die Menge der fälschlicherweise erhobenen und verarbeiteten personenbezogenen Daten minimal zu halten.

- Aber selbst wenn diese juristischen Hürden nicht bestehen würden, zeigte die beabsichtigte Vorgehensweise auch hinsichtlich des technischen Datenschutzes Schwächen. Zu hinterfragen war insbesondere die vorgesehene Anonymisierung personenbezogener Daten. Diese muss mit Algorithmen durchgeführt werden, die als hinreichend sicher gelten. Damit Bluetooth-Adressen von Geräten der die Strecke befahrenden Pendler nicht täglich durch das gleiche anonyme Datum abgebildet werden, sollte neben der Bluetooth-Adresse auch eine täglich neu zu generierende Zufallszahl in den Anonymisierungsalgorithmus einbezogen werden. Bei der Prüfung hat sich herausgestellt, dass zur Erzeugung dieser Zufallszahlen ein Zufallszahlengenerator verwendet werden sollte, der für kryptographische Anwendungen nicht geeignet ist. Ich habe empfohlen, den Algorithmus durch einen anderen zu ersetzen, dessen Zufallszahlen von besserer Qualität sind und dessen Nutzung den Telekommunikationsunternehmen für ihre Anwendungen von der Bundesnetzagentur vorgeschrieben wird.

  Damit jeder Detektor zu einer Bluetooth-Adresse das gleiche anonyme Datum errechnet, muss die Zufallszahl täglich an alle Detektoren übertragen werden. Die Übertragung sollte verschlüsselt erfolgen. Auch hier waren die Darstellungen im Konzept nicht wasserdicht. Zum einen war nicht klar, ob die Übertragung über ein privates oder ein öffentliches Netzwerk erfolgt. Außerdem war nicht dargetan, dass die Zufallszahl, die in den Detektoren wieder im Klartext vorliegen muss, dort nicht „zurückgewonnen“ werden kann.

  Hinzu kam, dass die sog. Systemarchitektur, also die einzelnen Systemkomponenten und deren Zusammenwirken, gewisse Defizite hatte. Da bei dem Verfahren, wie sich später herausstellte, über das öffentliche Internet kommuniziert werden sollte, wäre eine **verschlüsselte Übertragung** unabdingbar gewesen. Für die Verschlüsselung sollte die Softwareplattform OpenSSL genutzt werden. Dagegen ist zunächst nichts einzuwenden, da die Programme von vielen Anwendern genutzt werden und einen gewissen Reifegrad erreicht haben. Zur anscheinend unvermeidlichen Fehlerbeseitigung sollten sog. Patches zeitnah und bedauerlicherweise auch relativ häufig bereitgestellt werden. Das alles nutzt aber nichts, wenn man in der Konzeption Wert darauf legt, dass die Software eines Detektors als Ganzes „eingefroren“ und dann nur durch Neuinstallation verändert werden kann. Die Folge davon ist, dass man ein System betreibt, bei dem die Verschlüsselungssoftware vermutlich nicht fehlerfrei ist und die Fehler nicht beseitigt werden können, wenn sie erkannt werden. Diese Konstellation ist nicht erstrebenswert . Deshalb habe ich empfohlen, dafür zu sorgen, dass Verbesserungen bezüglich der Softwaresicherheit jederzeit auf den jeweiligen Systemen vorgenommen werden können.

Das Verkehrsministerium hat mir aufgrund der genannten Kritikpunkte mitgeteilt, dass es meine Empfehlungen aufgreifen und das Verfahren vorerst nicht weiter verfolgen wolle. Insgesamt zeigt auch dieses Beispiel, dass für die überall propagierten intelligenten Verkehrssysteme alsbald tragfähige Rechtsgrundlagen geschaffen werden sollten.

Im Oktober 2013 verkündete die Landesstelle für das Straßenwesen in einer Pressemitteilung, dass man die Reisezeit entlang der B 27 über das Internet abrufen könne (http://www.svz-bw.de/verkehrslage.html). Auf Nachfrage erhielt ich die Auskunft, dass die Reisezeitendaten von einem privaten Anbieter gekauft werden. Meines Wissens werden derartige Informationen von Navigationsgeräte-Herstellern und Telekommunikationsunternehmen angeboten. Ob hierbei datenschutzrechtlich alles mit rechten Dingen zugeht, wird noch zu prüfen sein.

7. Gesundheit und Soziales

7.1 Das Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten

Informationspflicht des Arztes, Dokumentation der Behandlung, Einsicht in die Patientenakte - diese und weitere wichtige Aspekte der Patientenversorgung regelt das am 26. Februar 2013 in Kraft getretene Gesetz zur Verbesserung der Rechte der Patientinnen und Patienten (Patientenrechtegesetz), BGBl. I S. 277 ff. Es bildet die rechtliche Grundlage für die Beziehung zwischen einem Patienten und seinem behandelnden Arzt oder Psychotherapeuten.

Es ist natürlich nicht so, dass Patienten in der Vergangenheit ohne Rechte waren. Allerdings waren die Rechte der Patienten im Verhältnis zu Ärzten und Krankenhäusern traditionell „Richterrecht“ und zudem in verschiedenen Gesetzen in verschiedenen Rechtsbereichen teilweise lückenhaft geregelt. Mit dem **Patientenrechtegesetz** werden nunmehr die bisher richterrechtlich entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts gesetzlich im Bürgerlichen Gesetzbuch (BGB) in einem neuen Untertitel „Behandlungsvertrag“ (§§ 630a bis 630h) kodifiziert. Patienten sollen ihre Rechte konzentriert in einem Gesetz nachlesen können; substantiell wesentlich Neues wurde damit jedoch nicht geschaffen.

Auch die gesetzlichen Krankenkassen wurden in dem neuen Gesetz in die Pflicht genommen. So sind Kranken- und Pflegekassen verpflichtet, ihre Versicherten bei der Durchsetzung von Schadensersatzansprüchen zu unterstützen (§ 66 des Fünften Sozialgesetzbuchs - SGB V). Entscheidet eine Krankenkasse über einen Antrag auf Leistung nicht innerhalb von festgelegten Fristen, muss sie dem Versicherten den Grund mitteilen. Unterlässt sie dies, gilt der Antrag als genehmigt. Zuvor muss der Versicherte der Krankenkasse allerdings eine angemessene Frist setzen (§ 13 Absatz 3a SGB V). Versicherte können außerdem ihre Teilnahmeerklärung am Hausarztmodell zwei Wochen nach deren Abgabe schriftlich gegenüber der Krankenkasse ohne Angabe von Gründen widerrufen (§§ 73b, 73c, 140a SGB V).

Schwerpunkt des Gesetzes ist die Kodifizierung des Behandlungs- und Arzthaftungsrechts. Aus datenschutzrechtlicher Sicht sind folgende Regelungen erwähnenswert:

- § 630c Absatz 2 bis 4 BGB behandelt die **Informationspflichten** der Behandelnden. Diese müssen ihre Patienten umfassend über die für die Behandlung wichtigen Umstände (z. B. Diagnose, voraussichtliche gesundheitliche Entwicklung, Therapie) informieren und aufklären. Die Informationspflicht besteht nur dann nicht, soweit dies ausnahmsweise aufgrund besonderer Umstände entbehrlich ist. Das Gesetz nennt exemplarisch die unaufschiebbare Behandlung und den Verzicht des Patienten auf Aufklärung.

  Weiterhin hat der Behandelnde den Patienten auf Nachfrage oder zur Abwendung gesundheitlicher Verfahren zu informieren, wenn für ihn Umstände erkennbar sind, die die Annahme eines Behandlungsfehlers begründen. Diese Informationspflicht gilt auch für Umstände, die einen eigenen oder fremden Behandlungsfehler begründen.

- Nach § 630d BGB muss der Behandelnde vor der Durchführung einer medizinischen Maßnahme die **Einwilligung des Patienten** einholen. Bei Einwilligungsunfähigkeit, beispielsweise weil der Patient aufgrund seines Zustandes nicht in der Lage ist, die Tragweite seiner Entscheidung abzusehen, muss ein hierzu Berechtigter (Vormund, Betreuer, gesetzlicher Vertreter, rechtgeschäftlich Bevollmächtigter) einwilligen. Auch Minderjährige können, abhängig von ihrem Alter und ihrer Verstandesreife, nicht ohne ihre Eltern bzw. Sorgeberechtigten über die Behandlung entscheiden. Eine Einwilligung ist nur dann nicht erforderlich, wenn eine **Patientenverfügung** nach § 1901a BGB vorliegt, die die geplante Behandlung gestattet oder untersagt, oder wenn die Einwilligung für eine unaufschiebbare Maßnahme nicht rechtzeitig eingeholt wer-

den kann, sie aber dem mutmaßlichen Willen des Patienten entspricht.

- Die Einwilligung ist allerdings nur wirksam, wenn der Patient rechtzeitig, umfassend und verständlich aufgeklärt wurde (§ 630e BGB). Dazu muss der Behandelnde den Patienten sämtliche für die Einwilligung wesentlichen Umstände (beispielsweise Art, Umfang, Durchführung, zu erwartende Folgen und spezifische Risiken der Maßnahme sowie ihre Notwendigkeit, Dringlichkeit, Eignung und Erfolgsaussichten) aufzeigen.
  Die **Aufklärung** muss mündlich erfolgen, ergänzend kann auf Unterlagen Bezug genommen werden, die dem Patienten in Kopie ausgehändigt werden müssen.

- Der Behandelnde ist gem. § 630f BGB verpflichtet, alle für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und Ergebnisse in einer sog. **Patientenakte** zu dokumentieren. Dazu gehören beispielsweise die Erhebung der Krankengeschichte, Diagnosen, Untersuchungen und deren Ergebnisse und Befunde, medikamentöse Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Aufklärungen und Einwilligungen sowie Arztbriefe. Die Patientenakte kann in Papierform oder elektronisch geführt werden.
  Neu ist die Verpflichtung, die Patientenakte „in unmittelbarem zeitlichen Zusammenhang“ mit der Behandlung zu führen. Neu ist außerdem die Verpflichtung, bei Berichtigungen und Änderungen von Eintragungen in der Patientenakte den ursprünglichen Inhalt erkennbar zu lassen sowie den Zeitpunkt der Berichtigung und Änderung erkennbar zu machen. Bei elektronischer Aktenführung ist eine manipulationssichere Software zu verwenden.

- § 630g BGB regelt das Recht des Patienten auf Einsichtnahme in das Original seiner Patientenakte. Der Patient muss wissen, wie mit seiner Gesundheit umgegangen wurde, welche Daten sich dabei ergeben haben und wie die Prognose aussieht. Das Begehren des Patienten auf **Akteneinsicht** hat der Arzt unverzüglich, d. h. ohne schuldhaftes Zögern zu erfüllen.

Die Akteneinsicht darf nur in besonderen Ausnahmefällen verweigert werden:

- Der Arzt kann die Einsichtnahme (ganz oder teilweise) verweigern, wenn erhebliche therapeutische Gründe dagegen sprechen, d. h. wenn zu befürchten ist, dass der Patient durch die Einsichtnahme erheblichen gesundheitlichen Schaden nehmen kann. Grundsätzlich hat jedoch der Patient das Recht, eigenverantwortlich über die Frage zu entscheiden, wie viel er wissen möchte. Verweigert der Arzt die Einsichtnahme, muss er konkrete und substantielle Anhaltspunkte hierfür vorbringen und die für und gegen die Einsichtnahme sprechenden Gründe gegeneinander abwägen.

- Niederschriften über persönliche Eindrücke und subjektive Wahrnehmungen des Arztes müssen dem Patienten grundsätzlich offenbart werden. Über ein begründetes Interesse des Arztes an der Nichtoffenbarung solcher Aufzeichnungen ist, in Abwägung mit dem Persönlichkeitsrecht des Patienten, im Einzelfall zu entscheiden.

- Der Arzt hat die Einsichtnahme auch dann zu verwehren, wenn und soweit in die Dokumentationen Informationen über dritte Personen eingeflossen sind, die ihrerseits schutzwürdig sind.

Die Einsichtnahme in die Patientenakte muss an dem Ort erfolgen, an dem sich die einzusehenden Unterlagen oder Dokumente befinden. Liegt ein wichtiger Grund vor, kann der Patient die Einsichtnahme an einem anderen Ort fordern. Der Patient hat das Recht, Abschriften von der Patientenakte zu verlangen. Abschriften können von einem Text, von elektronischen Dokumenten oder auch in Form von Dateien in elektronischer Form angefertigt werden. Die Kosten hat der Patient zu tragen.

Auch Angehörige und Erben haben ein Einsichtsrecht in die Patientenakte. Erben müssen vermögensrechtliche Interessen geltend machen. Gleiches gilt für die nächsten Angehörigen, soweit sie immaterielle Interessen vorbringen. Angehörige und Erben haben allerdings nur dann ein Einsichtsrecht, wenn der ausdrückliche oder mutmaßliche Wille des Patienten der Einsichtnahme nicht entgegensteht.

Wenngleich das Patientenrechtegesetz nur wenig Neues enthält, so wurde damit doch ein Schritt in die richtige Richtung getan, weitere müssen nun folgen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung „Patientenrechte müssen umfassend gestärkt werden“ vom 23. Mai 2012 frühzeitig auf die aus datenschutzrechtlicher Sicht nicht ausreichenden Regelungen hingewiesen (vgl. Anhang 5). Leider hat der Gesetzgeber diese Forderungen bislang weder im Patientenrechtegesetz noch an anderer Stelle berücksichtigt.

7.2 Das Krebsfrüherkennungs- und registergesetz des Bundes - was wird aus dem Krebsregister Baden-Württemberg?

Das am 9. April 2013 in Kraft getretene Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (Krebsfrüherkennungs- und registergesetz - KFRG), BGBl. I S. 617 ff., verpflichtet die Länder zur flächendeckenden Einführung klinischer Krebsregister.

Krebskranke Menschen, Leistungserbringer, Kostenträger, Forschungseinrichtungen und politische Entscheidungsträger sind auf zuverlässige Auskünfte über die Qualität der onkologischen Versorgung angewiesen. Klinische **Krebsregister** leisten einen wichtigen Beitrag zur Darstellung der onkologischen Versorgungsqualität, zur onkologischen Qualitätsberichterstattung und zur Schaffung von Qualitätstransparenz in der onkologischen Versorgung. Allerdings weisen gerade die bereits existierenden klinischen Krebsregister keine einheitliche Qualität auf. Dies betrifft sowohl die Frage der Aufgaben der klinischen Krebsregister, der Meldepflichten oder -rechte der Ärzte, der Mitwirkungsrechte der Patienten (Einwilligung oder Widerspruch) als auch die technisch-organisatorische Ausgestaltung.

7.2.1 Das Krebsfrüherkennungs- und -registergesetz (KFRG)

Das KFRG schafft die rechtlichen und finanziellen Rahmenbedingungen für die Errichtung und den Betrieb flächendeckender und einheitlicher klinischer Krebsregister in den Ländern (§ 65c des Fünften Sozialgesetzbuchs - SGB V). Es regelt ihre maßgeblichen Aufgaben, zum Beispiel welche Art von Daten für welche Funktionen der klinischen Krebsregister benötigt werden, wer diese Daten wem auf welchen Wegen und mit welchen Unterlagen zu melden hat, und legt Grundanforderungen fest, z. B. die flächendeckende und möglichst einheitliche und vollzählige Erfassung der Daten der an Krebs erkrankten Menschen.

Krankenkassen fördern den Betrieb klinischer Krebsregister, indem sie einmalig für jede verarbeitete Meldung über eine Tumorneuerkrankung eine fallbezogene Krebsregisterpauschale zahlen. Voraussetzung für die Förderung ist, dass das klinische Krebsregister bestimmte organisatorische und infrastrukturelle Mindestanforderungen erfüllt. Diese Fördervoraussetzungen sind vom Spitzenverband Bund der Krankenkassen im Benehmen mit den Ländern zu beschließen und von den klinischen Krebsregistern zu erfüllen.

Die für die Einrichtung und den Betrieb der klinischen Krebsregister notwendigen Bestimmungen einschließlich datenschutzrechtlicher Regelungen bleiben dem jeweiligen Landesrecht vorbehalten. Damit lässt das KFRG Gestaltungsspielraum für länderspezifische Lösungen unter Berücksichtigung bestehender Strukturen.

Die Arbeitsgruppen der Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden haben eine länderoffene Arbeitsgruppe eingerichtet, die

die Aufgabe hat, **Musterelemente für die Landesgesetzgebung** bis Ende 2013 zu erarbeiten. Dabei spielte vor allem auch das Thema Datenschutz eine bedeutende Rolle. Erfreulicherweise konnte eine Beteiligung der Datenschutzbeauftragten des Bundes und der Länder in der Arbeitsgruppe erreicht werden.

7.2.2 Das Landeskrebsregister heute

In Baden-Württemberg wurden bereits mit dem **Landeskrebsregistergesetz** (LKrebsRG) vom 13. März 2006, GBl. S. 54, und der **Krebsregisterverordnung** vom 20. März 2009, GBl. S. 157, die gesetzlichen Voraussetzungen für die Errichtung eines Krebsregisters geschaffen und dieses in den vergangenen Jahren stufenweise aufgebaut. Um die an das Krebsregister gemeldeten persönlichen Daten bestmöglich schützen zu können, wurden drei räumlich, organisatorisch und personell voneinander getrennte Einrichtungen geschaffen: die Vertrauensstelle - angesiedelt bei der Deutschen Rentenversicherung Baden-Württemberg -, die Klinische Landesregisterstelle - betrieben durch die Baden-Württembergische Krankenhausgesellschaft - und das epidemiologische Krebsregister - eingerichtet beim Deutschen Krebsforschungszentrum in Heidelberg.

Keines dieser Register erhält Einblick in den vollständigen gemeldeten Datensatz, sondern lediglich in die Daten, die zur jeweiligen Aufgabenerfüllung erforderlich sind. So überprüft die Vertrauensstelle die elektronisch übermittelten Datensätze (Angaben zur Person) der meldenden Stellen (Ärzte, Zahnärzte, Pathologen, Tumorzentren, Onkologische Schwerpunkte, Gesundheitsämter und sonstige Einrichtungen, die ein eigenes Krebsregister führen) auf Vollständigkeit und Schlüssigkeit und verschlüsselt alle Angaben zur Person. Sie hat zu keinem Zeitpunkt Einblick in die medizinischen Daten. Die Klinische Landesregisterstelle überprüft die von der Vertrauensstelle übermittelten medizinischen Daten und verarbeitet diese für die onkologische Qualitätssicherung in der Krebsbehandlung. Die epidemiologischen Daten werden an das epidemiologische Krebsregister weitergeleitet und bevölkerungsbezogen ausgewertet. Klinisches und epidemiologisches Krebsregister erhalten, entsprechend ihrer Aufgabenstellung, medizinische Daten, haben jedoch keinen Zugang zu den personenbezogenen Daten.

Das Landeskrebsregistergesetz sieht eine landesweite Meldepflicht vor. Der Patient ist über die Meldung zu unterrichten und darüber aufzuklären, dass er der weiteren Verarbeitung seiner Daten durch Vertrauensstelle, klinisches und epidemiologisches Krebsregister widersprechen kann.

Das heute in Baden-Württemberg etablierte Krebsregister mit seinen komplexen Sicherungsvorkehrungen der Daten auf dem Weg von der meldenden Stelle zur Vertrauensstelle, zwischen den Registerteilen und in den Datenbankdateien der verschiedenen Registerbereiche verschaffen dem Register ein hohes Maß an Datensicherheit. Weitere Details zu den wesentlichen datenschutzrechtlichen Eckpunkten können im 29. Tätigkeitsbericht (vgl. LT-Drs. 14/5500, S. 86) nachgelesen werden.

7.2.3 Was passiert mit dem bestehenden Krebsregister?

Das Sozialministerium geht davon aus, dass die in § 65c SGB V festgelegten Aufgaben der klinischen Krebsregister in Baden-Württemberg auf der Grundlage des LKrebsRG vom **Krebsregister Baden-Württemberg** bereits weitestgehend wahrgenommen werden, Struktur und Organisation deshalb weitestgehend **beibehalten** werden können. Welche Auswirkungen und Anpassungen im Einzelnen erforderlich sind, könne erst nach Vorliegen der konkreten Fördervoraussetzungen abschließend beurteilt werden.

Die frühzeitige Erkennung und Verbesserung der Behandlung von Krebserkrankungen ist zweifellos außerordentlich wichtig. Die datenschutzkonforme Nutzung der bei der Krebserkrankung anfallenden medizinischen Daten zu diesem Zweck ist in Baden-Württemberg mit dem heutigen Krebsregister und den bestehenden Regelungen gewährleistet. Gemeinsames Ziel muss es sein, bei der Anpas-

sung des LKrebsRG an das KFRG darauf zu achten, dass das Krebsregister Baden-Württemberg die ihm gesetzlich übertragenen Aufgaben auch zukünftig unter Beachtung angemessener datenschutzrechtlicher Anforderungen erfüllen kann, das Datenschutzniveau insgesamt darf sich aber keinesfalls verschlechtern.

Datenschutzrechtlich problematisch sehe ich derzeit vor allem die im großen Umfang - im Gegensatz zum LKrebsRG - vorgesehene Speicherung und Übermittlung von Patientendaten in Klartextform. Insoweit wird noch intensiv zu diskutieren sein, für welche Aufgaben personenidentifizierende Daten wirklich unerlässlich sind. Auch die Fragen, ob Ärzte verpflichtet sind, Patientendaten an das Krebsregister zu melden, ob Patienten der Verarbeitung ihrer gemeldeten Daten widersprechen können oder ob eine Meldung nur mit Einwilligung der Betroffenen zulässig und ob die Weitergabe von Patientendaten an Krankenkassen zu Abrechnungszwecken erforderlich ist, bedürfen einer kritischen Betrachtung.

Meine Dienststelle wird die Umsetzung des neuen Gesetzes kritisch begleiten und darauf dringen, dass der bestehende hohe Datenschutzstandard weiterhin erhalten bleibt.

7.3 Die Pseudonymisierung von Krebsregisterdaten

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 des Bundeskrebsregisterdatengesetzes (BKRG) **pseudonymisiert** gespeichert. Als Pseudonyme werden sog. **Kontrollnummern** verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Das bisher genutzte Verfahren für die Pseudonymisierung von Krebsregisterdaten ist rd. 20 Jahre alt. Ich bin - zusammen mit meinen Kollegen von Bund und Ländern - der Auffassung, dass das damals entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen den durch mehrere Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.
- Auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat seine Empfehlungen mittlerweile überarbeitet und empfiehlt weder den Einsatz der sog. Hashfunktion MD-5 noch die Verschlüsselungsfunktion IDEA.

Diese Entwicklungen machen es erforderlich, die **Regeln** zur Bildung der Kontrollnummern zu **überarbeiten**. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, bei denen Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat einen entsprechenden Anforderungskatalog formuliert.

Mit ihrer Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern“ vom 13./14. März 2013 (vgl. Anhang 13, mit Anforderungskatalog des AK Technik) fordert die Datenschutzkonferenz die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für

den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Absatz 3 BKRG festgelegt werden.

Ich halte eine Umstellung sämtlicher Verschlüsselungsverfahren mit vertretbarem Aufwand für möglich und zumutbar. Eine gesetzliche Grundlage für eine Entschlüsselung der Personenchiffrate in einem Zwischenschritt zwecks Umschlüsselung ist für das Krebsregister Baden-Württemberg leider nicht gegeben. Vielmehr verbietet § 10 Absatz 3 des Landeskrebsregistergesetzes (LKrebsRG) die Verwendung des Schlüssels zu diesem Zweck. Der Schlüssel darf nur von der Vertrauensstelle in den in diesem Gesetz abschließend aufgezählten Fällen für die jeweiligen Zwecke verwendet werden.

Meine Dienststelle wird die Umsetzung der neuen und verbesserten Verfahren für die Bildung von Kontrollnummern zur Pseudonymisierung beim Krebsregister Baden-Württemberg aufmerksam verfolgen.

7.4 Orientierungshilfe Krankenhausinformationssysteme (OH KIS)

Im 30. Tätigkeitsbericht (LT-Drs. 12/5740, S. 96 f.) hatte ich über die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossene „Orientierungshilfe Krankenhausinformationssysteme“ (OH KIS) berichtet und die Krankenhausbetreiber aufgefordert, schnellstmöglich die Umsetzung der Orientierungshilfe anzugehen. Was hat sich seither getan?

7.4.1 Fortschreibung der OH KIS

Grundsätzlich wird die **Orientierungshilfe** von allen Seiten als eine für alle Bundesländer geltende einheitliche Messlatte begrüßt, die, auf den Klinikalltag bezogen, datenschutzrechtliche Anforderungen konkretisiert. Sie hat sowohl bei den Krankenhausträgern als auch bei den Herstellern der Software eine längst überfällige intensive und teilweise kontroverse **Diskussion** angestoßen. Es liegt in der Natur der Sache, dass etliche Punkte breite Zustimmung gefunden haben, andere von vielen zunächst kritisch gesehen wurden. Die von der Deutschen Krankenhausgesellschaft zunächst erhobenen inhaltlichen Bedenken konnten inzwischen ausgeräumt werden. Gleichwohl bedarf die Orientierungshilfe einer **Weiterentwicklung**, die die Erfahrungen der Prüftätigkeit der Datenschutzaufsichtsbehörden und die technische Weiterentwicklung, vor allem aber auch die von Krankenhausbetreibern und Herstellern geäußerten Kritikpunkte, berücksichtigt. Die Datenschutzaufsichtsbehörden arbeiten derzeit an der Fortschreibung der Orientierungshilfe.

Die Orientierungshilfe soll nicht völlig neu geschrieben werden. Vorgesehen ist, einzelne Anforderungen zu modifizieren bzw. inhaltlich zu präzisieren, andere Anforderungen werden gestrichen und neue aufgenommen. Da die Orientierungshilfe ein Konsenspapier war und auch bleibt, ist dieser Prozess entsprechend zeitaufwändig.

Exemplarisch möchte ich an dieser Stelle nur einige **Änderungen** nennen, die nach derzeitigem Stand beabsichtigt sind:

- Der als „Normative Eckpunkte“ überschriebene Teil I der Orientierungshilfe soll zur Klarstellung künftig als „Rechtliche Rahmenbedingungen“ bezeichnet werden, Notfallzugriffe sollen als Sonderzugriffe qualifiziert werden.
- Der aktive Hinweis auf das den Patienten zustehende Widerspruchsrecht bei der Aufnahme hinsichtlich der Hinzuziehung von Vorbehandlungsakten war von Anfang an umstritten. Kritisch gesehen wurde vor allem das Haftungsrisiko der Ärzte und des Krankenhauses, wenn wegen fehlender Informationen Patienten evtl. sogar fehlerhaft behandelt werden. Diese Anforderung soll jetzt gestrichen werden. Die Widerspruchsmöglichkeit der Patienten selbst bleibt davon unberührt.
- Ein Verfahren soll dann als „mandantenfähig“ gelten, wenn Patientendaten mandantenbe-

zogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können (siehe hierzu auch Orientierungshilfe Mandantenfähigkeit - Version 1.0 vom 11. Oktober 2012 - http://www.baden-wuerttemberg.datenschutz.de/orientierungshilfen-merkblatter/mandantenfahigkeit).

Die fortgeschriebene Orientierungshilfe wird voraussichtlich Frühjahr 2014 zur Verfügung stehen und kann dann auf meiner Homepage www.datenschutz-baden-wuerttemberg.de abgerufen werden. Dort sind bereits heute Materialien zur Orientierungshilfe veröffentlicht.

7.4.2 Handreichung der Deutschen Krankenhausgesellschaft (DKG)

Die Anpassung der eingesetzten Krankenhausinformationssysteme an die Orientierungshilfe stellt für die Krankenhäuser eine große Herausforderung dar, die erheblich Zeit und Arbeitskräfte bindet. Vor allem kleinere Krankenhäuser stoßen dabei schnell an Grenzen. Dies hat auch die **Deutsche Krankenhausgesellschaft (DKG)** erkannt und beschlossen, den Krankenhäusern **Arbeitshilfen** an die Hand zu geben, die bei der praktischen Umsetzung der Orientierungshilfe als Hilfestellung dienen sollen.

Die „Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme“ enthalten die im Krankenhaus erforderlichen bzw. sinnvollen organisatorischen Konzepte (Rollen- und Berechtigungskonzept, Protokollierung, Zugriffsbeschränkungen auf Patientendaten, Löschen von Patientendaten). Außerdem werden Themen, wie die Einbeziehung der Verschlüsselung von Daten oder Schutzmaßnahmen für besondere Patientengruppen (VIP, Mitarbeiter als Patient) behandelt sowie Mustervorlagen für die Teilkonzepte „Sperren/Auslagern von Daten“ und „Löschen von Patientendaten“ den Krankenhäusern an die Hand gegeben. Die Hinweise sollen auch den KIS-Herstellern bei der Erstellung noch fehlender Systemfunktionen und darauf basierender Standardeinführungskonzepte zur Orientierung dienen.

Es handelt sich bei den Umsetzungshinweisen der DKG gegenwärtig um ein Arbeitspapier, dessen inhaltliche Abstimmung in den Fachausschüssen und Unterarbeitsgruppen bereits vorgenommen wurde, das aber noch abschließend von den zuständigen Gremien beschlossen werden muss. Sobald dies formell erfolgt ist, werden die Hinweise auch auf meiner Homepage abrufbar sein.

7.4.3 Umsetzung der Orientierungshilfe auf Landesebene

Bei Krankenhäusern und Herstellern von KIS-Systemen besteht nach wie vor großer Handlungsbedarf hinsichtlich der datenschutzkonformen Ausgestaltung der eingesetzten Systeme. Viele Krankenhäuser befinden sich inzwischen mitten im Umsetzungsprozess, viele Krankenhäuser - dies haben zahlreiche Informations- und Beratungsgespräche, die meine Dienststelle im Berichtszeitraum geführt hat, bestätigt - fühlen sich angesichts des Umfangs und der Komplexität der Orientierungshilfe überfordert und schieben deshalb die Umsetzung auf die lange Bank.

Selbstverständlich biete ich grundsätzlich allen Krankenhäusern im Rahmen meiner Beratungsfunktion meine Unterstützung an. Dass ich im Hinblick auf die Vielzahl der meiner Zuständigkeit unterfallenden Krankenhäuser nicht in der Lage bin, mit jedem einzelnen Krankenhaus in einem geordneten Prozess die notwendigen Maßnahmen zu klären, liegt auf der Hand. Aufgrund dieser Schwierigkeiten unterstütze ich die Krankenhäuser bei der Umsetzung der Orientierungshilfe durch verschiedene **Maßnahmen auf Landesebene**.

Eine auf meine Initiative **zusammen mit der Baden-Württembergischen Krankenhausgesellschaft (BWKG) gebildete Arbeitsgruppe** hat Anfang 2012 ihre Arbeit aufgenommen. Der Arbeitsgruppe gehören, neben Vertretern der BWKG und Mitarbeitern meiner Dienststelle, auch IT-Spezialisten und Datenschutzbeauftragte einiger baden-württembergischer Krankenhäuser an. Dieser

Praxisbezug war mir wichtig und hat sich als außerordentlich wertvoll erwiesen.

Ziel der gemeinsamen Arbeit ist es, konkrete Umsetzungsprobleme zu eruieren und daraus Handlungsanleitungen zu entwickeln, die von den Krankenhäusern unter Berücksichtigung der finanziellen Mittel stufenweise umgesetzt werden sollen. Die Arbeitsgruppe hat dazu eine **Checkliste** entwickelt, die als Einstiegshilfe in die Umsetzung gedacht ist. Sie soll dem Krankenhaus an Hand wichtiger und exemplarischer Fragen zu wesentlichen Themenbereichen eine Analyse des Ist-Zustandes und des Handlungsbedarfs ermöglichen. Damit gewinnt das Krankenhaus sowohl einen Überblick über den Status Quo als auch über den daraus resultierenden Handlungsbedarf, der dann in einen konkreten Maßnahmenplan umgesetzt werden sollte.

Die Checkliste bringt Kernforderungen der Orientierungshilfe in eine überschaubare Form. Sie gliedert sich in die Themenkomplexe „Rollen- und Berechtigungskonzept“, „Protokollierungskonzept“, „Auswertung von Protokollierungen/Reporting“, „Sperr- und Löschkonzept“ und „Sicherheitskonzept“. Für jeden Themenkomplex werden zentrale Fragen formuliert, die vom Krankenhaus durchgearbeitet werden sollen. Die Checkliste nimmt eine unverbindliche Wertung vor, welcher Handlungsbedarf als besonders dringlich anzusehen ist und gibt damit Hilfestellung bei der Priorisierung der einzelnen umzusetzenden Maßnahmen.

Die Checkliste soll den Einstieg in die Umsetzung der Anforderungen der Orientierungshilfe erleichtern, kann aber keinesfalls die Orientierungshilfe ersetzen. Das Abarbeiten der Checkliste zeigt den Krankenhäuser den bestehenden Handlungsbedarf auf, gibt aber keine konkreten Handlungshilfen. Die Handreichung der Deutschen Krankenhausgesellschaft gibt hier wertvolle Hinweise.

Die Arbeitsgruppe hat im Juni 2013 in einer ganztägigen **Fachtagung** die Handreichung der DKG und die Checkliste vorgestellt. An der Veranstaltung nahmen Vertreterinnen und Vertreter von zahlreichen baden-württembergischen Krankenhäusern und Rehakliniken teil. Sowohl die Handreichung als auch die Checkliste wurden von den Teilnehmern übereinstimmend als notwendige und geeignete Hilfestellungen begrüßt.

Die Tagungsunterlagen können auf der Internetseite meiner Dienststelle abgerufen werden.[28]

7.4.4 Umsetzung an einem Referenzkrankenhaus

Erfreulicherweise hat sich ein Krankenhaus in Baden-Württemberg (Referenzkrankenhaus) bereit erklärt, zusammen mit Mitarbeitern meiner Dienststelle den Umsetzungsstand der in der Orientierungshilfe beschriebenen Anforderungen in seinem eigenen Krankenhausinformationssystem unter Berücksichtigung der bestehenden technischen Gegebenheiten und praktischen Abläufe zu überprüfen, den daraus resultierenden Handlungsbedarf sowohl für den Klinikbetreiber als auch den oder die Systemhersteller festzustellen und umzusetzen. Außerdem sollen die Handreichung der DKG und die Checkliste zur Orientierungshilfe auf ihre Praxistauglichkeit untersucht werden.

In verschiedenen Sitzungen wurde die Checkliste, unter Einbeziehung der Handreichung der DKG, durchgearbeitet und dabei die in der Orientierungshilfe enthaltenen Anforderungen mit der im Referenzkrankenhaus bestehenden Situation verglichen. Dabei hat sich gezeigt, dass mit der gegenwärtig betriebenen IT-Lösung die vorgegebenen Anforderungen zum Großteil bereits erfüllt werden. Dies betrifft beispielsweise das Sicherheitskonzept, das Rollen- und Berechtigungskonzept sowie die Protokollierung und das Reporting.

Gleichwohl besteht Nachbesserungsbedarf hinsichtlich einzelner in der Orientierungshilfe enthaltener Anforderungen, insbesondere beim Sperr- und Löschkonzept sowie bei der Archivierung von Protokolldaten.

Das Krankenhaus wird in den kommenden Monaten die notwendigen Anpassungen an die Vorgaben vornehmen. Soweit Vorgaben derzeit noch nicht umgesetzt sind, liegt dies teilweise daran,

[28] *http://www.baden-wuerttemberg.datenschutz.de/kis-fachtagung-19-juni-2013/*

dass entsprechende Funktionen herstellerseitig noch nicht oder nicht im erforderlichen Umfang zur Verfügung stehen (z. B. Sperren und Löschen von Daten). Der den Systemhersteller betreffende Handlungsbedarf soll daher mit diesem erörtert werden, um die notwendigen Maßnahmen ebenfalls schnellstmöglich umzusetzen.

Checkliste und Handreichung der DKG haben sich nach Einschätzung des Referenzkrankenhauses als hilfreich erwiesen. Die vorgeschlagenen Änderungen wird die Arbeitsgruppe prüfen.

Auch wenn der Umsetzungsprozess noch lange nicht abgeschlossen ist, bin ich der Auffassung, dass sich die Zusammenarbeit zwischen dem Referenzkrankenhaus und meiner Dienststelle bereits jetzt für beide Seiten gelohnt hat. Das Referenzkrankenhaus hat auf der Basis der bestehenden datenschutzrechtlichen Vorgaben und der Orientierungshilfe, unter Einbeziehung der weiteren Hilfestellungen, das aktuelle Datenschutzniveau des von ihm betriebenen Krankenhausinformationssystems beschrieben und die sich daraus ergebenden Verbesserungen festgestellt. Meine Dienststelle hat wertvolle Erfahrungen für die Umsetzung der Orientierungshilfe sowie für den Einsatz der Handreichung der DKG und der Checkliste gesammelt.

Eine wichtige Erkenntnis war, dass insbesondere die Hersteller endlich den Nutzern der Krankenhausinformationssysteme datenschutzgerechte Lösungen anbieten müssen - und zwar nicht als kostenpflichtiges Extra, sondern als gesetzeskonforme Basisausstattung. Es ist hoffentlich nur eine Frage der Zeit, bis die Kunden bzw. deren Verbände von den System-Herstellern diese Bereitstellung ebenfalls einfordern und die Hersteller erkennen, dass „Datenschutz made in Germany“ ein Verkaufsargument ist.

Meine Dienststelle wird den Umsetzungsprozess in den Krankenhäusern weiterhin aufmerksam begleiten.

7.5 Datenschutz im Krankenhaus

Datenschutz ist für ein Krankenhaus heutzutage unerlässlich. Patienten erwarten zu Recht, dass ihre Daten dort gut aufgehoben sind.

Gesundheitsdaten geben Auskunft über seelische und körperliche Leiden, Eigenschaften und gesundheitliche Dispositionen und sind deshalb besonders sensibel, weshalb jede unbefugte Offenbarung dieser Daten strafbar ist. Es ist daher von höchster Bedeutung, dass Krankenhausmitarbeiter und -verwaltung die vom Gesetzgeber vorgegebenen Grenzen für den Umgang mit Patientendaten sorgfältig beachten.

Welche Auswirkungen ein unsachgemäßer Umgang mit Patienten haben kann, haben im Berichtszeitraum zwei Vorfälle gezeigt, die auch bundesweit in den Medien für Schlagzeilen sorgten.

7.5.1 Der Verlust von Patientendaten

Ein Kreiskrankenhaus meldete uns den Verlust von zur Archivierung vorgesehenen Datensicherungsbändern, auf denen sämtliche Patientendaten (Name, Adresse, Geburtsdaten, Arztkorrespondenz, Befunde u. a.) von rd. 200.000 bis 300.000 Patienten gespeichert waren. Passiert war Folgendes: Ein EDV-Mitarbeiter sollte nach der routinemäßigen nächtlichen Datensicherung die Sicherungsbänder in den Tresor einschließen, der sich in einem anderen Teil des Gebäudes befand. Sicherungsbänder und Tresorschlüssel legte er dazu in einen Karton. Auf dem Weg zum Tresorraum erhielt er über sein Handy mehrere Anfragen wegen Computerproblemen, die teilweise schnell erledigt werden mussten. Er ging daher nicht sofort zum Tresorraum, sondern erledigte auf dem Weg dorthin die anstehenden Aufträge. Stunden später, als sich der Mitarbeiter an seinen ursprünglichen Auftrag - das Einschließen der Sicherungsbänder im Tresor - erinnerte, war der Karton mit den Bändern und dem Schlüssel verschwunden.

Nachforschungen ergaben, dass der Mitarbeiter den Karton vermutlich an einer öffentlich zugänglichen Laderampe auf einem Tisch abgestellt und

dort vergessen hatte. Was dann mit den Bändern und dem Schlüssel passierte, konnte bis heute nicht geklärt werden. Im günstigsten Fall wurden die Bänder als Müll entsorgt. Nicht auszuschließen ist natürlich, dass eine Person Bänder und/oder Schlüssel an sich genommen und die auf den Bändern gespeicherten Daten auch eingesehen hat. Allerdings ist zum Auslesen der Daten ein spezielles Bandlesegerät erforderlich. Weder die Sicherungsbänder noch die darauf gespeicherten Daten noch der Tresorschlüssel sind wieder aufgetaucht. Auch die staatsanwaltschaftlichen Ermittlungen blieben ergebnislos.

Der Verlust von Patientendaten in einem so großen Umfang ist sicherlich der „Super-GAU“ für jedes Krankenhaus. Unsere erste Vermutung, dass wohl kaum allein das fahrlässige Verhalten eines Mitarbeiters für das Abhandenkommen der Daten verantwortlich sein kann, sondern durch fehlende technische und organisatorische Randbedingungen begünstigt wurde, hat sich nicht bestätigt. Allerdings war bedenklich, dass der Vorfall erst nach acht Tagen der EDV-Leitung zur Kenntnis gelangte.

Das Krankenhaus hatte bereits vor dem Abhandenkommen der Sicherungsbänder eine interne Verfahrensanweisung „Ablauf Datensicherung“ eingeführt. Diese Verfahrensanweisung regelte detailliert, wie die Datensicherungen im Klinikum durchgeführt und organisiert werden. Nicht explizit geregelt war allerdings der Transport der Bänder vom Serverraum zum Tresor.

Als unmittelbare Konsequenz aus dem Vorfall wurde unmittelbar nach dessen Bekanntwerden die Verfahrensanweisung verschärft. Zusätzlich aufgenommen wurde ein Passus, der die tägliche Bandsicherung und Lagerung der Bänder im Tresor regelt. Danach müssen die Datensicherungsbänder von dem verantwortlichen EDV-Mitarbeiter auf direktem Wege vom Serverraum zum Datensicherungstresor verbracht werden. Sie dürfen auf dem Weg zwischen Serverraum und Tresorraum auf keinen Fall aus der Hand gegeben, irgendwo abgestellt oder zwischengelagert werden. Der Tresorschlüssel ist stets örtlich getrennt von den Datensicherungsbändern aufzubewahren. Er muss immer direkt an der Person (z. B. in der Hosentasche) aufbewahrt werden und darf keinesfalls aus der Hand gegeben werden. Sollte eine Unterbrechung des Transports unabdingbar sein, weil eine Anfrage eingeht, muss zunächst der Transport der Datensicherungsbänder ordnungsgemäß abgeschlossen werden, bevor auf die Supportanfrage reagiert wird. Neu aufgenommen wurde auch eine Vorschrift zur Verschlüsselung der Datensicherungsbänder, die, soweit technisch realisierbar, zumindest für einen Teil der im Klinikum gespeicherten Patientendaten vorgesehen ist. Weiterhin wurde ein neues Datensicherungskonzept entwickelt, so dass im Folgejahr die bestehende Bandsicherung sowie die damit verbundenen Transportwege entfallen.

Der Vorfall zeigt einmal mehr, wie leicht aus einer kleinen Störung der Routine eine umfassende Datenpanne entstehen kann. Die im Nachgang getroffenen Maßnahmen hätte man sich bereits im Vorfeld gewünscht. Verschlüsselung gehört dabei genauso zum Grundhandwerkszeug wie die regelmäßige Dokumentation und Kontrolle von Datensicherung und Datentransporten zur Qualitätssicherung ggf. nach dem 4-Augen-Prinzip. Schließlich kann immer etwas schiefgehen und menschliches Versagen ist nie gänzlich auszuschließen.

Da das Krankenhaus umgehend alle erforderlichen Maßnahmen (Meldung des Vorfalls bei meiner Dienststelle, Strafanzeige, Benachrichtigung der betroffenen Patienten durch Anzeigen in zwei überregionalen Tageszeitungen, Austausch des Tresorschlosses, Verschärfung der Verfahrensanweisung) ergriffen und nach meinen Feststellungen bereits vor dem Vorfall Regelungen zur Datensicherung getroffen hat, habe ich davon abgesehen, die Einleitung eines Bußgeldverfahrens beim zuständigen Regierungspräsidium Karlsruhe zu beantragen. Das Regierungspräsidium seinerseits hielt die Einleitung eines Verfahrens ebenfalls für nicht geboten.

7.5.2 Die Entsorgung von Patientenakten durch einen externen Dienstleister

„Schlamperei mit Patientenakten“: Mit dieser und ähnlichen Schlagzeilen berichteten die Medien über eine weitere Datenpanne, von der zwar deutlich weniger Patienten betroffen waren, die aber

erst durch den äußerst nachlässigen Umgang des Krankenhauses mit Patientenakten ermöglicht wurde.

Meine Nachforschungen ergaben, dass das Krankenhaus sog. Röntgentaschen ehemaliger Patienten mit Röntgenaufnahmen und Röntgenbefunden, die in angemieteten Kellerräumen außerhalb des Klinikgeländes gelagert wurden, in einer auf drei Tage angelegten Aktion entsorgen wollte. Mit der Entsorgung wurde ein Recycling- und Entsorgungsbetrieb beauftragt, der die zum Abtransport bereitstehenden Röntgentaschen in dem externen Lager abholen, zum Sitz des Unternehmens transportieren und dort entsorgen sollte. Der allein arbeitende Mitarbeiter der Entsorgungsfirma deponierte zunächst die auszusondernden Taschen in offenen Gitterboxen, die er auf einen vor dem Gebäude abgestellten Lkw lud. Bei jedem Gang in den Keller blieb die Laderampe des Lkw offen und unbeaufsichtigt und damit auch für jedermann zugänglich. Es kam wie es kommen musste: Ein Passant beobachtete das Geschehen, entnahm aus einer Gitterbox vier Röntgentaschen und spielte diese dem SWR zu.

Wegen des steigenden Kostendrucks im Gesundheitswesen suchen Krankenhäuser nach Möglichkeiten, wie sie die Kosten verringern und das Krankenhauspersonal entlasten können. Immer öfter entscheiden sie sich daher dafür, Teile ihrer Datenverarbeitung an externe Dienstleister zu übertragen. Dies betrifft vor allem Schreibarbeiten, Mikroverfilmung, Digitalisierung und Archivierung von Patientenunterlagen, aber auch die Aktenvernichtung. Aus der Sicht des Datenschutzes verbinden sich mit solchen Maßnahmen deutliche Risiken für den Patienten. Schließlich liegt es auf der Hand, dass das Einbeziehen privater Dritter in Verwaltungsabläufe eines Krankenhauses dazu führen kann, dass sensibelste Daten der betroffenen Patienten Personen zur Kenntnis gelangen, die nicht in das vertrauliche Arzt-Patienten-Verhältnis eingebunden sind.

Vorliegend hatte sich das Krankenhaus wenig Gedanken darüber gemacht, ob und unter welchen Voraussetzungen eine Aktenvernichtung durch ein privates Unternehmen zulässig ist und welche technischen und organisatorischen Maßnahmen dabei zu beachten sind. Offensichtlich wurde davon ausgegangen, mit der mündlichen Beauftragung des Dienstleisters sei jegliche Verantwortung auf diesen übergangen.

Überhaupt scheint das Krankenhaus dem Dienstleister fast grenzenloses Vertrauen entgegengebracht zu haben: So hatte das Krankenhaus die zur Vernichtung vorgesehenen Röntgentaschen zwar in Kartons mit Deckeln bereitgestellt, diese wurden aber nicht zugeklebt. Dem Mitarbeiter der Entsorgungsfirma wurde sogar der Schlüssel für das externe Lager ausgehändigt, dieser hatte damit ungehindert Zugang zu allen dort gelagerten Patientenunterlagen. Während der gesamten Aktion befand sich kein Krankenhausmitarbeiter im Lager, eine Kontrolle oder Beaufsichtigung fand zu keinem Zeitpunkt statt. Dem Krankenhaus war auch nicht bekannt, ob die Vernichtung evtl. durch ein Subunternehmen erfolgen sollte - die vorgelegten Unterlagen wiesen darauf hin. Die vom Krankenhaus ausgesonderten Unterlagen wurden nicht erfasst und damit war und ist auch nicht nachvollziehbar, welche Akten dem Archiv entnommen werden sollten bzw. entnommen wurden. Die Überprüfung, welche der bereitgestellten Röntgentaschen im Hinblick auf zu beachtende Aufbewahrungsfristen tatsächlich zu entsorgen waren, wurde dem Dienstleister überlassen. Dieser sollte anhand des Geburtsdatums der Patienten entscheiden, welche Akten ggf. wieder dem Archiv zugeführt werden sollten.

Bereits im 21. Tätigkeitsbericht 2000, LT-Drs. 12/5740, S. 25, hat mein Amtsvorgänger datenschutzkonforme Möglichkeiten einer Aktenvernichtung durch private Firmen dargestellt. Danach kann die Aktenvernichtung folgendermaßen erfolgen:

- Der Auftragnehmer, also der Dienstleister, vernichtet die Unterlagen im Krankenhaus und unter Aufsicht von Krankenhauspersonal; der Einsatz mobiler Vernichtungsanlagen ist schon heute keine Seltenheit mehr.

- Die zu vernichtenden Unterlagen werden in einem verschließbaren Behältnis gesammelt und dem Unternehmen zur Vernichtung übergeben. Dabei ist sicherzustellen, dass vor der

eigentlichen Vernichtung, insbesondere während des Transports, nicht auf die Unterlagen zugegriffen werden kann. Dies ist beispielsweise nicht sichergestellt, wenn dem Fahrer des Transportfahrzeugs der Schlüssel für das Behältnis ausgehändigt wird. Um hier die erforderliche Sicherheit zu gewährleisten, muss der Transport von einem Mitarbeiter des Krankenhauses begleitet werden. Dessen Aufgabe muss es auch sein, die eigentliche Vernichtung zu kontrollieren und dabei darauf zu achten, dass während des Vernichtungsvorgangs keine Akten unbefugt gelesen werden.

Das Krankenhaus hat zwar eingeräumt, der Entsorgungsfirma zu sehr vertraut zu haben, ist aber nach wie vor der Meinung, den datenschutzrechtlichen Anforderungen genügt zu haben. Künftige Vernichtungsaktionen sollen vordringlich auf dem Klinikgelände vorgenommen werden, auf jeden Fall würde ein Klinikmitarbeiter den Prozess bis zu Vernichtung begleiten. Was das konkret bedeutet, hat die Klinik bislang offen gelassen und wird mit meiner Dienststelle noch intensiv zu diskutieren sein.

Das Problem der Aktenvernichtung war leider nicht der einzige Punkt, über den sich das Krankenhaus keine Gedanken machte. Im Zuge meiner Nachforschungen musste ich feststellen, dass die Klinik grundsätzlich, zumindest seit dem Jahr 2009, keine Patientendaten löschte. Das Krankenhaus war der Auffassung, auch nach Ablauf der einschlägigen Aufbewahrungsfristen bestehe keine Pflicht zur Löschung von Patientendaten. Eine Löschung/Vernichtung erfolgte daher bislang allenfalls wegen bestehender Platzprobleme. Ungeachtet der Tatsache, dass diese Auffassung geltendem Recht widerspricht, überraschte sie auch deshalb, weil interne Leitlinien zum Datenschutz die Datenlöschung sehr wohl vorsahen. Da davon auszugehen ist, dass sowohl im zentralen Krankenhausarchiv als auch im externen Lager eine Vielzahl von Akten aufbewahrt werden, die längst hätten vernichtet werden müssen bzw. in den nächsten Jahren nach und nach zu vernichten sind, muss das Krankenhaus schnellstens ein Verfahren implementieren, mit dessen Hilfe die zu vernichtenden Akten/Unterlagen ermittelt und einer geordneten Vernichtung zugeführt werden können. Ein erster wichtiger Schritt erfolgte mit der Erstellung einer Archivordnung, die allerdings noch nachzubessern ist - so fehlen bislang gerade die Bestimmungen für die Entsorgung von Papierakten.

Das Fehlen einer Archivordnung wurde bei einem Ortstermin im Zentralarchiv und im externen Archivlager offenkundig. Der Schlüssel für das externe Archiv wurde bis zum Besuch meiner Mitarbeiter nur in einem nicht abschließbaren Schrank zwischen Kondensmilch und Würfelzucker aufbewahrt. Ein Schlüsselbehälter war nicht vorhanden, eine Schlüsselverwaltung, z. B. in Form eines Schlüsselausgabebuchs, fand ebenfalls nicht statt.

Auch die Aufbewahrung des Archivguts im externen Lager ließ zu wünschen übrig. Beim Betreten des Archivs fiel ein gekipptes Fenster auf, wodurch das Archivgut sowohl Witterungseinflüssen als auch möglichem Nagetierbefall ausgesetzt war. In den Gängen und zwischen den Schiberegalen standen eine Vielzahl von sog. Europaletten mit Kartons, in denen noch einzusortierende Patientenakten und Röntgentaschen aufbewahrt wurden. Einige Paletten standen zudem komplett im Fluchtweg zum Notausgang. Viele in den Regalen befindliche Unterlagen wurden in offenen Kartons über die eigentliche Füllhöhe hinaus aufgestapelt aufbewahrt. Nach Angaben der Klinik wurde das Archivgut inzwischen in die Regale verbracht und die Fluchtwege wurden freigeräumt.

Auf Anraten meiner Mitarbeiter wurde eine aktuelle Brandschutzbegehung durchgeführt. Brände stellen für ein Archiv die größte Bedrohung dar, aber Wasserschäden zählen zu den häufigsten Schadensarten in Archiven, sogar wenn man von Sekundärschäden durch Löschwasser und andere Löschmittel absieht. Archivgut sollte daher in Schutzumschläge und Archivkartons verpackt werden, welche einen guten Schutz bei Wasserschäden, Bränden und physischen Belastungen bieten. Für Anforderungen an die Aufbewahrung von Archiv- und Bibliotheksgut bietet die DIN ISO 11799 umfassende Hinweise. Diese Norm ist eine Empfehlung, wird aber durch Eintragung in Ausschreibungen zur Pflicht. Zu beachten ist außer-

dem, dass bei Rechtsstreitigkeiten immer auf der Basis des aktuellen technischen Standes - also der entsprechenden Norm - geurteilt wird.

Aufgrund der schwerwiegenden Versäumnisse des Krankenhauses hat das Regierungspräsidium Karlsruhe ein Ordnungswidrigkeitenverfahren eingeleitet.

7.6 Babygalerien

Immer mehr Krankenhäuser veröffentlichen auf sog. Babygalerien im Internet Bilder der bei ihnen geborenen Kinder. Viele Eltern nehmen dieses Angebot gerne in Anspruch, um schnell und ohne großen Aufwand Verwandten und Freunden ein Bild ihres Kindes zukommen lassen zu können. Dies ist unter datenschutzrechtlichen Aspekten dann unbedenklich, wenn die Eltern, in Kenntnis möglicher Konsequenzen, einer Veröffentlichung der Bilder im Internet zugestimmt haben.

Im Berichtszeitraum haben sich mehrere Eltern bei meiner Dienststelle darüber beschwert, dass Geburtsdaten und Bilder ihres neugeborenen Kindes nicht nur auf der Homepage des Krankenhauses veröffentlicht wurden, sondern auch auf anderen Internetseiten abrufbar waren. Die Eltern hatten zwar in eine Veröffentlichung auf der Babygalerie des Krankenhauses mündlich oder schriftlich eingewilligt, nicht jedoch auf weiteren, ihnen nicht bekannten Internetseiten.

Die Krankenhäuser veröffentlichen Bilder Neugeborener nach meinen Feststellungen mit Vornamen, Geburtsdatum, Geburtsgröße und Geburtsgewicht des Kindes, darüber hinaus teilweise auch mit dem Nachnamen des Kindes und/oder den Vornamen der Eltern. Gegen eine Veröffentlichung solcher Babybilder ist nichts einzuwenden, sofern eine wirksame Einwilligungserklärung der Eltern vorliegt.

Eine wirksame Einwilligung setzt voraus, dass das Krankenhaus die Betroffenen zuvor über die vorgesehene Datenverarbeitung hinreichend informiert. Konkret müssen die Eltern wissen, welche Daten des Kindes und/oder der Eltern zusammen mit welchen Bildern ins Internet gestellt und wann diese in der Babygalerie wieder gelöscht werden sollen. Ebenso wichtig ist es, die Eltern darüber zu informieren, dass mit der Veröffentlichung im Internet weltweit unbekannte Dritte legal auf Bilder und Geburtsdaten zugreifen und diese für eigene Zwecke nutzen können. Legal deshalb, weil es sich insoweit um allgemein zugängliche Daten handelt, die unter den Voraussetzungen des § 28 Absatz 1 Satz 1 Nummer 3 des Bundesdatenschutzgesetzes (BDSG) auch durch (unbekannte) Dritte für eigene Geschäftszwecke erhoben, gespeichert, verändert, übermittelt oder genutzt werden dürfen. Dies dürfte den meisten Eltern nicht bewusst sein. Auch sollten Eltern darüber aufgeklärt werden, dass sie von Dritten aufgrund der zusammen mit dem Babybild veröffentlichten Daten ggf. identifiziert werden können. Denkbar wäre dann durchaus, dass Eltern bspw. (ungewollt) gezielt mit bestimmten Produkten beworben oder gar zu Hause besucht werden. Generell sollte das Krankenhaus davon absehen, Daten zu veröffentlichen, die eine Identifizierung der Eltern ermöglichen (z. B. Nennung des kompletten Nachnamens, der Angabe des Wohnortes oder Teilen davon). Der eigentliche Zweck der Veröffentlichung, nämlich Verwandten und Freunden das freudige Ereignis schnell mitteilen zu können (und gleichzeitig auch für das Krankenhaus zu werben), dürfte in der Regel auch ohne Angabe dieser Daten erreicht werden können.

Die Einwilligung sollte, im Interesse aller Beteiligten, schriftlich eingeholt werden, um im Streitfall nachvollziehen zu können, ob die Eltern tatsächlich eine Einwilligung erteilt haben bzw. das Krankenhaus zulässigerweise Babybilder veröffentlicht hat.

7.7 Datenschutz in Pflegestützpunkten und Pflegeeinrichtungen

7.7.1 Kontrollbesuch bei einem Pflegestützpunkt

Im 30. Tätigkeitsbericht (LT-Drs. Nr. 15/955, S. 107 ff.) habe ich über die datenschutzrechtlichen Startprobleme bei den Pflegestützpunkten berichtet. Strittig war dabei bis zuletzt die Frage, welche Daten die Pflegestützpunkte aufgrund ge-

setzlicher Befugnisse verarbeiten dürfen und ob und in welchem Umfang darüber hinaus eine datenschutzrechtliche Einwilligung der Hilfesuchenden in die Verarbeitung ihrer Daten erforderlich ist. Die Landesarbeitsgemeinschaft Pflegestützpunkte e.V. (LAG) erklärte sich schließlich dazu bereit, bis auf Weiteres auf das Einholen einer Einwilligungserklärung bei den Hilfesuchenden zu verzichten. Im Gegenzug habe ich mich dazu bereit erklärt, für den Fall, dass aufgrund der Erfahrungen der Pflegestützpunkte konkrete Datenverarbeitungsvorgänge benannt werden können, die nach Auffassung der Pflegestützpunkte und der LAG nur mit Einwilligung der Betroffenen rechtmäßig vorgenommen werden können, die Frage einer Einwilligungserklärung erneut zu prüfen.

Vor diesem Hintergrund haben sich Mitarbeiter meiner Dienststelle im Berichtszeitraum über den praktischen Umgang mit Daten der Hilfesuchenden im Rahmen eines Kontrollbesuchs bei einem Pflegestützpunkt informiert. Dabei stellte sich heraus, dass der Landkreistag Baden-Württemberg die Pflegestützpunkte in Baden-Württemberg in einem Rundschreiben über die mit mir erzielte Einigung informiert und darum gebeten hatte, dem Landkreistag Beratungsvorgänge zu melden, „die aufgrund ihrer Komplexität und der im Beratungsprozess zu beteiligenden Institutionen, einschließlich der dabei vorzunehmenden Datentransfers, ggf. doch eine Einwilligungserklärung notwendig machen könnten“.

Ungeachtet dessen verwendete der Pflegestützpunkt zum Zeitpunkt des Kontrollbesuchs die von der LAG entwickelte Einverständniserklärung, die nach meiner Auffassung datenschutzrechtlichen Anforderungen nicht genügt. Beratungsvorgänge, die im Einzelfall eine Einwilligungserklärung erforderlich gemacht haben, konnte der Pflegestützpunkt allerdings nicht benennen. Vielmehr drängte sich meinen Mitarbeitern der Eindruck auf, dass sich die Mitarbeiter des Pflegestützpunktes aus Unsicherheit und um „auf der sicheren Seite“ zu sein, im Einzelfall für oder gegen die Einholung einer Einwilligungserklärung entscheiden. Dem Bedürfnis der Hilfesuchenden nach Transparenz und Nachvollziehbarkeit hinsichtlich der durch den Pflegestützpunkt vorgenommenen Verarbeitung personenbezogener Daten wird damit nicht Genüge getan.

Ich habe dem Pflegestützpunkt empfohlen, auf das Einholen von Einwilligungserklärungen vorläufig zu verzichten und dem Landkreistag in Frage kommende Beratungsvorgänge zu melden. Diese Vorgehensweise empfehle ich an dieser Stelle sämtlichen in Baden-Württemberg eingerichteten Pflegestützpunkten. Wegen der in Frage stehenden Notwendigkeit von Einwilligungserklärungen und um das weitere Vorgehen abzustimmen, habe ich mich erneut an die LAG gewandt.

Ungeklärt war lange Zeit auch, wer bzw. welche Stelle verantwortliche Stelle i. S. des § 3 Absatz 3 LDSG ist (Pflegestützpunkt, Träger des Pflegestützpunkts, geschäftsführender Träger). Das Ministerium für Arbeit und Sozialordnung, Familie, Frauen und Senioren Baden-Württemberg und die LAG haben sich darauf verständigt, dass landeseinheitlich stets der geschäftsführende Träger des Pflegestützpunktes verantwortliche Stelle sein soll.

Der von meiner Dienststelle kontrollierte Pflegestützpunkt, der eine zentrale Pflegestützpunktstelle sowie weitere dezentrale Standorte umfasst, teilte diese Auffassung nicht. Nach dort vertretener Ansicht sei jeder Standort selbst verantwortliche Stelle, da die Standorte nur für sich selbst Daten erheben, verarbeiten und nutzen würden und ein Datenaustausch zwischen den Standorten nicht stattfinde. Gleichwohl wird davon ausgegangen, dass es sich um einen und nicht um mehrere Pflegestützpunkte handle. Dies entspricht nicht dem Interesse der Hilfesuchenden an einer klar definierten Anlaufstelle, soweit es um die Verantwortung im Umgang mit ihren Daten geht.

Ich habe den Pflegestützpunkt gebeten, sich wegen dieser Problematik an die LAG zu wenden. Der LAG habe ich empfohlen, die Pflegestützpunkte erneut explizit darüber zu unterrichten, welche Stelle - ggf. landeseinheitlich - verantwortliche Stelle sein soll.

Meine Mitarbeiter haben im Rahmen des Kontrollbesuchs im Übrigen keine schwerwiegenden datenschutzrechtlichen Mängel in dem Pflegestütz-

punkt vorgefunden. Insgesamt konnte festgestellt werden, dass der Umgang mit personenbezogenen Daten auf eine verantwortungsvolle und gewissenhafte Art und Weise erfolgte.

Meine Dienststelle wird wegen der datenschutzrechtlichen Anforderungen mit der LAG weiterhin im Gespräch bleiben und die weitere Entwicklung aufmerksam verfolgen.

7.7.2 Kontrollbesuche bei Pflegeeinrichtungen

Wer in einem Pflegeheim lebt, ist in besonderem Maße auf die Hilfe und Fürsorge anderer angewiesen. Unvermeidlich erlangen die Mitarbeiterinnen und Mitarbeiter dieser Einrichtungen auch Kenntnis von sensiblen Daten über die Gesundheit und Lebensumstände der Heimbewohner und teilweise auch über deren Angehörige. Die datenschutzrechtlichen Anforderungen werden leider nicht immer beachtet, wie Kontrollen ergeben haben.

Wie sich bei den Kontrollen in Alten- und Pflegeheimen gezeigt hat, waren sich die Einrichtungen ihrer Verantwortung durchaus bewusst. Eine der besuchten Einrichtungen konnte bereits eine umfassende EDV-gestützte Bewohnerverwaltung und Pflegedokumentation vorweisen. Erfreulich war dort insbesondere die passgenaue Berechtigungsstruktur, bei der nur diejenigen auf die Dokumente zugreifen können, die diese zur Erfüllung ihrer Aufgaben benötigen. Gleichwohl bestand umfangreicher Nachbesserungsbedarf; teilweise waren sogar geltende gesetzliche Bestimmungen nicht bekannt:

- Die überprüften Pflegeeinrichtungen hatten entweder gar keinen betrieblichen Datenschutzbeauftragen bestellt oder eine Person mit dieser Aufgabe betraut, deren hauptamtliche Aufgaben mit denen des Datenschutzbeauftragten nicht zu vereinbaren waren.

  Bei den Pflegeeinrichtungen hängt die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten von der Größe der Stelle und der Zahl der mit der Verarbeitung personenbezogener Daten beschäftigten Arbeitnehmer ab (§ 4f Absatz 1 BDSG). Dieser muss zudem fachkundig und zuverlässig sein (§ 4f Absatz 2 BDSG); Interessenkonflikte mit anderen hauptamtlichen Aufgaben des Datenschutzbeauftragten sind auszuschließen.

- Keine der Einrichtungen verfügte über ein Verfahrensverzeichnis, das den gesetzlichen Anforderungen entspricht, obwohl jede Daten verarbeitende nicht-öffentliche Stelle ihre Verfahren automatisierter Datenverarbeitungen in einer Gesamtübersicht über die im Einsatz befindlichen Verarbeitungsverfahren darstellen muss (§§ 4d, 4e BDSG).

- Wenn ein Heim beabsichtigt, Bewohnerdaten an Stellen außerhalb des Heims zu übermitteln und Informationen über die Bewohner bei externen Stellen einzuholen, so wird üblicherweise bereits im Rahmen des Heimvertrags das Einverständnis der Heimbewohner zu etwaigen Datenübermittlungen eingeholt (z. B. Datenweitergabe an behandelnde Ärzte, Krankenhäuser und Therapeuten). Nach § 4a BDSG muss der Betroffene aber zuvor über die Tragweite seiner Einwilligung aufgeklärt werden, um dem Grundrecht auf informationelle Selbstbestimmung gerecht zu werden. Es genügt daher nicht, beim Abschluss eines Heimvertrags vorab und pauschal für alle denkbaren Fälle der Datenweitergabe eine Einwilligungserklärung einzuholen.

  Die von den Heimen verwendeten Erklärungen waren viel zu allgemein und pauschal gehalten. So war für die Heimbewohner weder ersichtlich, welche Ärzte welche Informationen dem Heim übermitteln, welchen Mitarbeitern diese Informationen zur Verfügung stehen dürfen noch welche personenbezogenen Daten das Heim an Ärzte oder andere Stellen zu welchem Zweck übermitteln darf. Soweit die Heimbewohner in verschiedene Datenverarbeitungsvorgänge einwilligen sollen, empfiehlt es sich, die einzelnen Vorgänge einzeln in einer Erklärung darzustellen oder für die einzelnen Vorgänge separate Einwilligungs- und Schweigepflichtentbindungserklärungen zu

verwenden. Außerdem sollte dem Heimbewohner die Möglichkeit eingeräumt werden, auch nur einzelnen Datenverarbeitungsvorgängen zuzustimmen.

Die Einwilligungs- und Schweigepflichtentbindungserklärungen sollten überdies deutlich hervorgehoben werden, damit diese nicht im Gesamtvertragstext untergehen. Dies lässt sich am ehesten durch ein separates, als Anlage zum Heimvertrag beigefügtes, besonders zu unterzeichnendes Formular erreichen.

- Noch nicht abschließend geklärt werden konnte, wie lange die Pflegeheime die personenbezogenen Daten der Bewohner aufzubewahren haben.
  Personenbezogene Daten sind grundsätzlich zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die derzeit vorgesehene Aufbewahrungsdauer von generell zehn Jahren erscheint mir zu lang und ist von den Einrichtungen an Hand der zu beachtenden Aufbewahrungs- und Dokumentationsfristen zu überprüfen.

- Auch Heime gehen zunehmend dazu über, bestimmte Tätigkeiten durch externe Firmen in Form einer Auftragsdatenverarbeitung erledigen zu lassen (beispielsweise Fernwartung oder Betrieb der gesamten Server in Form eines IT-Outsourcings).

  Der Auftraggeber einer Auftragsdatenverarbeitung ist für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich (§ 11 Absatz 1 BDSG). Um dieser Verantwortung gerecht zu werden, hat er den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und ihm einen schriftlichen Auftrag zu erteilen, in dem Festlegungen u. a. 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.

  Bei der Vertragsgestaltung ist deshalb darauf zu achten, dass die erforderlichen technischen und organisatorischen Maßnahmen sich nicht nur in einem allgemeinen Hinweis auf den Datenschutz erschöpfen, sondern präzise regeln, welche Maßnahmen im Einzelnen notwendig sind. Der von einem Pflegeheim vorgelegte Vertrag war insoweit nicht ausreichend.

- Darüber hinaus waren Mängel festzustellen, die bereits in vergangenen Tätigkeitsberichten wiederholt angesprochen wurden: Offene Türen und Fenster bei unbesetzten Büros in sensiblen Bereichen mit Publikumsverkehr, mangelhafte Konfiguration von Multifunktionsgeräten (Kopierer als Scanner, Faxgerät und Netzwerkdrucker) sowie unzureichende Schreddermöglichkeiten (siehe hierzu Kapitel 11.3).

Auch Pflegeeinrichtungen müssen sich datenschutzkonform verhalten und die typischen Mängel alsbald abstellen.

7.8 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Im 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 176 f.) habe ich darüber berichtet, dass sich der Düsseldorfer Kreis dafür eingesetzt hat, die Einwilligungs- und Schweigepflichtentbindungserklärung für die Verbraucher transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) wurde deshalb eine für alle deutschen Versicherer gültige „Mustererklärung“ mit Hinweisen zu deren Verwendung erarbeitet (Beschluss des Düsseldorfer Kreises vom 17. Januar 2012, vgl. Anhang 22). Die neue Einwilligungs- und Schweigepflichtent-

bindungserklärung wird seit Januar 2013 von den Versicherungen eingesetzt.

Die Mustererklärung kann auf meiner Homepage abgerufen werden.[29]

7.9 Verrechnungsstellen und Forderungen für ärztliche Privatpatienten-Leistungen

Viele Ärzte lassen die Rechnungen für die Behandlung von Privatpatienten von Privatärztlichen Verrechnungsstellen erstellen. Eine gesetzliche Grundlage, die es erlauben würde, allgemein personenbezogene Daten oder gar die Behandlungs- und Untersuchungsdaten an Privatärztliche Verrechnungsstellen zu übertragen, gibt es nicht. Sofern der Patient nicht in die Datenübertragung eingewilligt hat, liegt eine strafbare Geheimnispflichtverletzung vor.

Wenn ein Arzt Daten über einen Patienten an eine Verrechnungsstelle weitergibt, damit diese seine Leistungen abrechnet und ggf. auch geltend macht, ist u. a. Folgendes zu beachten:

Der betroffene Patient muss, bevor er darüber entscheidet, ob er einer Weitergabe seiner Daten durch einen Arzt an eine Verrechnungsstelle zustimmt, eine zutreffende Vorstellung darüber haben, ob beim Einschalten der Verrechnungsstelle sein Arzt für seine Daten datenschutzrechtlich verantwortlich bleibt oder ob etwa die Verrechnungsstelle datenschutzrechtlich verantwortlich wird. Nur dann kann er eine rechtswirksame Erklärung abgeben. Maßgeblich ist, ob die Verrechnungsstelle (ggf. hinsichtlich bestimmter Punkte) ausschließlich nach den Weisungen und in der Verantwortung des Arztes oder ob sie in eigener Verantwortung tätig wird. Wer inwieweit datenschutzrechtlich verantwortlich ist, ist auch entscheidend dafür, wem gegenüber der Patient ein Recht z. B. auf Auskunft hat. In einem uns vorgetragenen Fall hatten zunächst beide beteiligten Stellen (sowohl die ärztliche Stelle als auch die Verrechnungsstelle) behauptet, die andere Stelle sei datenschutzrechtlich verantwortlich, schließlich sah sich dann doch noch eine der Stellen als datenschutzrechtlich verantwortlich an.

Der betroffene Patient muss auch eine zutreffende Vorstellung darüber haben, zu welchen Zwecken die Daten an welche Stelle(n) weitergegeben werden sollen. Dazu gehört grundsätzlich auch, unter welchen Voraussetzungen welche Stelle welche Arten von personenbezogenen Daten wie verarbeitet und verwendet.

Um künftig nicht in jedem Fall offenkundige Wissenslücken schließen zu müssen, ist eine Abstimmung hinsichtlich der datenschutzrechtlich einschlägigen Fragen mit der Landesärztekammer und der Landeszahnärztekammer vorgesehen.

Es ist grundsätzlich auch möglich, Privatzahnärztliche Verrechnungsstellen mit dem Einzug zahnärztlicher Honorarforderungen zu betrauen.

Der Patient muss, bevor er darüber entscheidet, ob er einer Weitergabe seiner Daten durch einen Arzt an eine Verrechnungsstelle zustimmt, eine entsprechende Vorstellung davon haben, wer welche Daten wozu bekommen soll.

7.10 Wann müssen Arztpraxen einen betrieblichen Datenschutzbeauftragten bestellen?

Die gesetzliche Pflicht nach § 4f Absatz 1 BDSG, einen betrieblichen Datenschutzbeauftragten zu bestellen, greift grundsätzlich immer dann, wenn zehn oder mehr Mitarbeiter/innen in einer öffentlichen oder nicht-öffentlichen Stelle (z. B. einem Unternehmen, einem Verein) - so auch in einer Arztpraxis - regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten betraut sind. Thematisiert wird nun, ob Arztpraxen unabhängig von der Mitarbeiterzahl - also auch unterhalb der Schwelle von zehn Mitarbeitern - zur Bestellung verpflichtet sind, da es dort vornehmlich um die Verarbeitung von Patienten- bzw. Gesundheitsdaten, also um besondere personenbezogene Daten i. S. des § 3 Absatz 9 BDSG geht,

[29] http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Beschluss-des-D%C3%BCsseldorfer-Kreises-vom-17.-Januar-2012-Einwilligungs-und-Schweigepflichtentbindungserkl%C3%A4rung-in-der-Versicherungswirtschaft.pdf

deren Bearbeitung besondere Risiken für das Persönlichkeitsrecht der Betroffenen aufweist und diese Datenverarbeitung somit der Vorabkontrolle unterliegen würde (§ 4f Absatz 1 Satz 6 BDSG i. V. m. § 4d Absatz 5 Satz 2 Nr. 1 BDSG). Um also besondere Risiken für die Rechte und Freiheiten durch die beabsichtigte automatisierte Verarbeitung festzustellen und ggf. auszuschließen, ist deren Rechtmäßigkeit vor der Inbetriebnahme durch die verantwortliche Stelle zu prüfen. Die Pflicht zur Durchführung einer Vorabkontrolle der Datenverarbeitung führt dazu, dass ein betrieblicher Datenschutzbeauftragter zu bestellen ist, unabhängig von der Zahl der mit Verarbeitung personenbezogener Daten befassten Mitarbeiter.

Dem ist indes bei der vorliegenden Fallkonstellation nicht so: Bei Arztpraxen entfällt im Normalfall die Pflicht zur Vorabkontrolle nach § 4d Absatz 5 Satz 2. Halbsatz BDSG, da im Regelfall ein Behandlungsvertrag nach § 630a BGB zwischen dem Arzt (oder dem Krankenhaus) und dem Patienten vorliegt, die Erhebung und Verarbeitung der Patienten- und Gesundheitsdaten also zur Durchführung dieses Rechtsgeschäfts i. S. v. § 28 Absatz 1 Satz 1 Nr. 1 BDSG erfolgt. Teilweise liegt auch eine ausdrückliche Einwilligung des Patienten zur Datenverarbeitung nach § 4a BDSG vor.

Da somit regelmäßig keine Pflicht zur Vorabkontrolle besteht, entfällt für Arztpraxen auch die - von der Mitarbeiterzahl unabhängige - Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. Die Bestellpflicht greift demnach im Regelfall erst ab zehn Mitarbeitern, § 4f Absatz 1 Satz 4 BDSG. Die Pflichten nach dem Bundesdatenschutzgesetz sind dann nach § 4g Absatz 2a BDSG vom Leiter der verantwortlichen Stelle, also z. B. dem Praxisinhaber, wahrzunehmen. Selbstverständlich kann jede Arztpraxis in diesem Falle auf freiwilliger Basis einen internen oder externen Datenschutzbeauftragten bestellen[30].

[30] Unser Merkblatt zum Thema „Der betriebliche Beauftragte für den Datenschutz“ finden Sie hier: *http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/03/Der-betriebliche-Beauftragte-für-den-Datenschutz.pdf*

7.11 Clearingstelle für Apotheken

Der Landesapothekerverband Baden-Württemberg e.V. plant ein Clearingverfahren für Rezepte für die Hilfsmittelversorgung.

Bei dem Verfahren geht es um das **Clearing von Hilfsmittelrezepten**. Anlass ist u. a. die Komplexität des Hilfsmittelmarktes mit zahlreichen Hilfsmittelverträgen und unterschiedlichen Abrechnungsformen (Vertragspreise, Genehmigungsgrenzen, Pauschalen) bei den Krankenkassen. Dem Landesapothekerverband geht es auch darum, seine Mitglieder zu unterstützen und die gesamten Prüfungen bei „unklaren“ Rezepten zu übernehmen. Die zum Versorgen der Patienten notwendigen Genehmigungen der Krankenkassen sollen einfacher und schneller eingeholt werden können. Meine Dienststelle hat den Landesapothekerverband dabei beraten.

Das Clearingverfahren stellt sich im Wesentlichen wie folgt dar: Die Apotheke erfasst Verordnungsdaten elektronisch. Dann wird zunächst über eine Datenbank elektronisch geprüft, ob die auf den Rezepten beruhenden, bei der Krankenkasse einzureichenden Kostenvoranschläge genehmigungsfähig sind. Erhält der Apotheker die gewünschte Information nicht aus dieser Datenbank, werden der Clearingstelle beim Landesapothekerverband bestimmte Daten aus dem Kostenvoranschlag zur einzelfallbezogenen Prüfung und Beratung der Apotheke zugeleitet. Die Clearingstelle soll (über eine Bildschirmansicht) ausschließlich folgende Daten erhalten: Das Bild des Verordnungsfeldes (mit dem Verordnungsgegenstand, der Diagnose und der Pharmazentralnummer), die vom System erzeugte interne Vorgangsnummer, den Status der Verordnung (etwa genehmigt), das Alter und das Geschlecht des Versicherten, das verordnete Hilfsmittel, den Namen der Krankenkasse (mit Kassennummer), die Telefonnummer und die Faxnummer des Hilfsmittel-Competence-Centers der Krankenkasse, das Verordnungsdatum, die Diagnose, die verordnete Leistung und ggf. den Verordnungszeitraum. Nur dann, wenn es im Verlauf des Clearingprozesses für den Bearbeiter notwendig werden sollte, kurzfristig mit der Apotheke Kontakt aufzunehmen, soll er nach Eingabe eines „definierten Grundes“ zusätzlich die

entsprechenden Daten (Apothekenname, Apotheken-Institutionskennzeichen, Ort, Telefonnummer und Faxnummer) einblenden können. Im Hintergrund des Clearingprozesses sollen Daten und Ergebnisse protokolliert werden. Anhand dieser wird der Apothekerverband das Einblenden der Apothekendaten prüfen. In Anbetracht dessen gehe ich davon aus, dass die Clearingstelle beim Landesapothekerverband von den erhaltenen Daten nicht auf den betroffenen Patienten oder den verordnenden Arzt schließen kann und damit insoweit keine personenbezogenen Daten verarbeiten wird.

Der Landesapothekerverband hat damit ein Verfahren erarbeitet, das den datenschutzrechtlichen Anforderungen genügt.

7.12 ELENAs Nachkommen

Im letzten Tätigkeitsbericht konnte ich das Aus für das ELENA-Verfahren verkünden. Seitdem hat sich wieder Einiges getan: Das ELENA-Verfahren musste abgewickelt werden, insbesondere waren die schon gespeicherten Daten zu löschen. Außerdem gibt es mittlerweile zwei Nachfolgeprojekte: OMS (Optimiertes Meldeverfahren in der sozialen Sicherung) und BEA (Bescheinigungen elektronisch annehmen).

Fast gleichzeitig mit dem Erscheinen meines letzten Tätigkeitsberichts im Dezember 2011 ist das Gesetz zur Aufhebung von Vorschriften zum E-LENA-Verfahren in Kraft getreten (vgl. auch 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 109 ff.). Bereits drei Tage nach Inkrafttreten des Gesetzes hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) den Datenbankhauptschlüssel vernichtet. Mit diesem digitalen Schlüssel war der Zugriff auf die verschlüsselt gespeicherten Entgeltdaten von mehr als 35 Millionen Arbeitnehmern möglich gewesen. Im Anschluss daran haben sowohl die Datenstelle der Träger der Rentenversicherung, bei der die „Zentrale Speicherstelle“ eingerichtet war, als auch die Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung als ehemalige „Registratur Fachverfahren“ Löschverfahren entwickelt, die den Sicherheitsstandards für die Löschung staatlicher Geheimnisse entsprechen. Die Löschung ist unter Aufsicht des BfDI und des Bundesamts für die Sicherheit in der Informationstechnik (BSI) durchgeführt worden, so dass die Daten nun auch physikalisch nicht mehr vorhanden sind (vgl. 24. Tätigkeitsbericht des BfDI 2011-2012, BT-Drs. 17/13000, S. 61).

Aus dem ELENA-Verfahren sind nun zwei Nachfolgeprojekte entstanden und zwar OMS (Optimiertes Meldeverfahren in der sozialen Sicherung) und BEA (Bescheinigungen elektronisch annehmen).

Bei dem **Projekt OMS** - bei dem der BfDI einbezogen ist - soll insbesondere aufgrund der im ELENA-Verfahren gewonnenen Erkenntnisse geprüft werden, ob bestehende Verfahren im Melde-, Bescheinigungs- und Antragswesen im Bereich der sozialen Sicherung optimiert und vereinfacht werden können. In der ersten Phase des Projekts wurde zunächst die Vielzahl der Melde-, Bescheinigungs- und Antragsverfahren - auch in datenschutzrechtlicher Hinsicht - erfasst und beschrieben. Beispiele für solche Verfahren sind *Meldeverfahren für sozialversicherungspflichtige Beschäftigte* (jeder in der Kranken-, Pflege-, Renten- oder Arbeitslosenversicherung versicherungspflichtige Beschäftigte muss vom Arbeitgeber der zuständigen Krankenkasse gemeldet werden), *Arbeitsbescheinigungen für Arbeitnehmer, die aus einem Beschäftigungsverhältnis austreten und arbeitslos werden* (in der Arbeitsbescheinigung bescheinigt der Arbeitgeber alle Tatsachen, die für die Entscheidung über den Anspruch auf Arbeitslosengeld oder Übergangsgeld erheblich sein können), oder *Antragsverfahren im Zusammenhang mit der Entsendung von Arbeitnehmern ins Ausland* (der Arbeitgeber beantragt in diesem Fall bei dem zuständigen Versicherungsträger in Deutschland eine Bescheinigung zur Weitergeltung der deutschen Sozialversicherungsvorschriften).

In der nächsten Phase des Projekts, die derzeit noch läuft, werden für diese Verfahren in Arbeitsgruppen - es gibt auch eine Arbeitsgruppe „Informationssicherheit und Datenschutz“ - Optimierungsvorschläge geprüft. Viele Optimierungsvor-

schläge sind datenschutzrechtlich unbedenklich. Problematisch sehe ich den Vorschlag, eine *zentrale* Datenannahmestelle einzurichten. Auch wenn mangels Kenntnis von Einzelheiten eine abschließende datenschutzrechtliche Bewertung dieses Vorschlags derzeit nicht möglich ist, ist das Gefährdungspotential bei zentralen Datenpools grundsätzlich größer als bei dezentralen Stellen.

Bei dem **Projekt BEA** - auch hier ist der BfDI beteiligt - geht es darum, dass Arbeitgeber Arbeitsbescheinigungen für Arbeitnehmer, die aus einem Beschäftigungsverhältnis austreten und arbeitslos werden, und Nebeneinkommensbescheinigungen künftig auch *elektronisch* an die Bundesagentur für Arbeit übermitteln können sollen. Der Arbeitgeber übermittelt die Daten über eine verschlüsselte Verbindung an die Bundesagentur für Arbeit.

Der Arbeitgeber kann wählen, ob er die Bescheinigung elektronisch übermittelt oder in Papierform erstellt. Der Arbeitnehmer kann der elektronischen Übermittlung der Bescheinigung widersprechen.

Das Gesetz zur Neuorganisation der bundesunmittelbaren Unfallkassen, zur Änderung des Sozialgerichtsgesetzes und zur Änderung anderer Gesetze, welches die gesetzlichen Grundlagen für die Umsetzung des Projekts enthält, ist am 24. Oktober 2013 verkündet worden; die Vorschriften traten am 1. Januar 2014 in Kraft.

Die Datenschutzbeauftragten des Bundes und der Länder werden die geplanten Projekte weiter im Auge behalten und beobachten, ob die von der Bundesregierung selbst erklärte Absicht, dass der Aspekt des Datenschutzes Priorität habe, auch verwirklicht wird.

7.13 Datenschutz im Jobcenter

Viele Eingaben im Berichtszeitraum betrafen den Datenschutz in Jobcentern. Außerdem war meine Dienststelle auch wieder bei Jobcentern zu Besuch, um diese in Fragen des Datenschutzes zu beraten und die Einhaltung des Datenschutzes vor Ort zu kontrollieren.

1. Aufbewahren von Personalausweiskopien
Gegenstand von Eingaben und Thema bei Kontrollen ist häufig die Frage, ob es zulässig ist, dass Jobcenter (ungeschwärzte) Kopien des Personalausweises von Leistungsbeziehern in der Akte aufbewahren.

Bei Anträgen auf Leistungen zur Sicherung des Lebensunterhalts nach dem Zweiten Buch des Sozialgesetzbuchs müssen dem Jobcenter die erforderlichen Unterlagen vorgelegt werden, um das Vorliegen der Anspruchsvoraussetzungen feststellen zu können. Dies schließt die Überprüfung der Identität ein. Zur Kontrolle der Personalien können Mitarbeiter der Jobcenter daher die Vorlage eines gültigen Passes oder Personalausweises verlangen. Die Angaben im Antrag, insbesondere die aktuelle Wohnanschrift, müssen mit den Daten des Personalausweises übereinstimmen. Zur Identifizierung und zur Aufgabenerfüllung des Jobcenters ist eine Kopie des Dokuments in der Akte aber grundsätzlich nicht erforderlich. Vielmehr dürfte regelmäßig ein dort oder auf dem Antragsformular anzubringender Vermerk darüber genügen, dass sich der Antragsteller durch Personalausweis oder sonstige Ausweispapiere ausgewiesen hat. Gegebenenfalls kann außerdem vermerkt werden, dass die im Antrag angegebenen Angaben mit denen auf dem Personalausweis übereinstimmen. In diesem Zusammenhang ist zu berücksichtigen, dass der Personalausweis personenbezogene Daten - z. B. die Seriennummer - enthält, deren Kenntnis - und erst recht deren Speicherung - für die Erfüllung der Aufgaben des Jobcenters nicht erforderlich ist.

Von einem Jobcenter wurde meiner Dienststelle gegenüber vorgetragen, dass die Aufbewahrung einer Kopie des Personalausweises in der Akte des jeweiligen Leistungsbeziehers erforderlich sei, um zu verhindern, dass ein Sachbearbeiter des Jobcenters einen fiktiven Fall anlegt, um Geldleistungen auf ein bestimmtes Konto zu transferieren; ohne Ausweiskopie könne nicht sicher belegt werden, ob die besagte Person überhaupt existiert. Es gebe bundesweit zahlreiche Betrugsfälle, die durch solche Sicherheitslücken geradezu begünstigt würden.

Ich gehe davon aus, dass es andere Möglichkeiten gibt, einen entsprechenden Betrug *durch Sachbearbeiter des Jobcenters* zu verhindern. Datenverarbeitungen auf Kosten der Antragsteller dürften zu diesem Zweck nicht erforderlich sein. Hierfür spricht auch, dass andere Sozialleistungsträger keine Personalausweiskopien von Antragstellern in ihren Akten aufbewahren.

2. Anforderung von Kontoauszügen
Nach der Rechtsprechung des Bundessozialgerichts ist die Anforderung der Kontoauszüge, jedenfalls der letzten drei Monate, bei der Beantragung von Leistungen nach dem Zweiten Buch des Sozialgesetzbuchs auch ohne konkreten Verdacht des Leistungsmissbrauchs zulässig (vgl. Urteil des Bundessozialgerichts vom 19. September 2008, Az. B 14 AS 45/07 R, und Urteil des Bundessozialgerichts vom 19. Februar 2009, Az. B 4 AS 10/08 R, sowie 29. Tätigkeitsbericht, LT-Drs. 14/5500, S. 100 f.).

Die Obliegenheit, Kontoauszüge vorzulegen, gilt allerdings nicht in vollem Umfang für die *Ausgabenseite*, d. h. für die Frage, wofür der Leistungsbezieher seine Mittel verwendet. Eine Einschränkung ergibt sich hier für *besondere Arten personenbezogener Daten*. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Geschützt ist die Geheimhaltung des Verwendungszwecks bzw. des Empfängers der Überweisung. Dementsprechend dürfen etwa Angaben über Gewerkschaftsbeiträge, Spenden an Kirchen oder an politische Parteien hinsichtlich des Empfängers, nicht aber der Höhe, geschwärzt werden. Lediglich für den Fall, dass sich aus den insoweit geschwärzten Kontoauszügen eines Leistungsbeziehers ergibt, dass in auffälliger Häufung oder Höhe Beträge überwiesen werden, ist nach Auffassung des Bundessozialgerichts im Einzelfall zu entscheiden, inwieweit ausnahmsweise doch eine Offenlegung auch des bislang geschwärzten Adressaten gefordert werden kann.

Das Bundessozialgericht hat in seinem Urteil vom 19. September 2008 ausgeführt, dass die Jobcenter hinsichtlich der Möglichkeiten der Schwärzung der Adressaten auf der Ausgabenseite bereits bei ihrem Mitwirkungsbegehren *hinweisen* müssen.

Obwohl es das Urteil des Bundessozialgerichts inzwischen schon seit über fünf Jahren gibt, musste ich im Berichtszeitraum feststellen, dass noch immer nicht alle Jobcenter einen solchen Hinweis erteilen. Die betroffenen Jobcenter haben, nachdem sie von meiner Dienststelle über die Rechtslage informiert wurden, erklärt, künftig einen entsprechenden Hinweis geben zu wollen.

3. Fehlender Hinweis auf die Freiwilligkeit von Angaben
Personen, die Leistungen nach dem Zweiten Buch des Sozialgesetzbuchs beantragen, müssen eine Vielzahl von Angaben machen, damit ihnen Leistungen bewilligt werden. Manche dieser Angaben sind aber *freiwillig*, z. B. die Telefonnummer und die E-Mail-Adresse des Antragstellers. Im Zehnten Buch des Sozialgesetzbuchs ist geregelt, dass das Jobcenter bei der Datenerhebung *auf die Freiwilligkeit von Angaben hinweisen* muss.

Aufgrund einer Eingabe wurde bekannt, dass bei einem Jobcenter ein solcher Hinweis bei der Erhebung von Telefonnummer und E-Mail-Adresse nicht erfolgte.Auf entsprechenden Hinweis meiner Dienststelle hat das Jobcenter den Antrag unverzüglich überarbeitet.

4. Zu weit gehender Gesundheitsfragebogen
Jobcenter haben die Eignung und Leistungsfähigkeit ihrer Kunden im Beratungs- und Vermittlungsprozess zu berücksichtigen. Bei gesundheitlichen Beschwerden, die Auswirkungen auf die Erwerbsfähigkeit haben, erstellen (u. a.) die Gesundheitsämter des jeweiligen Land- bzw. Stadtkreises ärztliche Gutachten zur Eignung bzw. Leistungsfähigkeit. In diesem Zusammenhang werden die Kunden aufgefordert, einen Gesundheitsfragebogen auszufüllen. Hierbei werden zwangsläufig Angaben über die Gesundheit erhoben, welche - wie oben ausgeführt - zu den besonderen Arten personenbezogener Daten gehören und daher besonders schützenswert sind. In einem von einem Gesundheitsamt verwendeten Fragebogen wurden aber so viele sensible Angaben erfragt, dass die Datenerhebung meiner Meinung nach weit über das Maß des Erforderlichen

hinausging: So sollte der Leistungsbezieher dem Gesundheitsamt alle „durchgemachten“ bedeutsamen Erkrankungen mitteilen, ferner Operationen, Unfälle, Krankenhausaufenthalte und Sanatoriums- und Kuraufenthalte (jeweils mit Jahr, Dauer und Grund) nennen und erklären, ob und ggf. weswegen und bei wem er zurzeit in ärztlicher oder psychotherapeutischer Behandlung ist. Weiter sollte der Betroffene angeben, ob und ggf. welche Arzneimittel er regelmäßig nimmt, ob und ggf. welche Drogen er nimmt bzw. in der Vergangenheit genommen hat, ob und ggf. wie viel er raucht, ob und ggf. wie viel und welche Art von Alkohol (Bier, Wein, Spirituosen) er trinkt und ob und ggf. wie viel Sport er in welcher Sportart treibt. Neben den Angaben zu seiner eigenen Gesundheit sollte der Kunde auch Auskunft zur Gesundheit seiner Verwandten erteilen: In dem Fragebogen wurde erhoben, ob bei Eltern und Geschwistern Bluthochdruck, Nervenkrankheiten oder sonstige bedeutsame Erkrankungen aufgetreten sind; außerdem, woran und in welchem Alter Eltern, Großeltern und Geschwister des Leistungsbeziehers verstorben sind.

Das betroffene Gesundheitsamt hat zwar meiner Dienststelle mitgeteilt, dass sämtliche Fragen im Gesundheitsfragebogen *freiwillig* beantwortet werden könnten. Dies widersprach aber den Ausführungen auf der schriftlichen „Einladung zur ärztlichen Untersuchung“, der zufolge das Datenblatt *vollständig ausgefüllt zur Untersuchung mitgebracht werden muss*.

Immerhin hat das betroffene Gesundheitsamt aufgrund der Anfrage meiner Dienststelle sofort die Fragebögen und Informationen überarbeitet und dem aktuellen Stand der Unterlagen bei der Bundesagentur für Arbeit angeglichen.

7.14 Benötigt das Sozialamt MDK-Gutachten?

Wer pflegebedürftig ist, aber die Pflegekosten weder durch die Leistungen der Pflegekasse bzw. der privaten Pflegeversicherung noch aus eigenem Einkommen oder Vermögen bestreiten kann, hat ggf. einen Anspruch auf Sozialhilfe. Welche Informationen aber benötigt das Sozialamt, um über diesen Anspruch entscheiden zu können?

Aufgrund von Eingaben bei meiner Dienststelle wurde bekannt, dass ein Sozialamt in Verfahren der Hilfe zur Pflege (eine Leistungsart der Sozialhilfe) von Betroffenen die Vorlage des „Gutachtens zur Feststellung der Pflegebedürftigkeit gemäß dem Elften Buch des Sozialgesetzbuchs“ des Medizinischen Dienstes der Krankenversicherung (MDK-Gutachten) verlangt. Der MDK erstellt dieses Gutachten im Auftrag der *Pflegekassen*.

Das betroffene Sozialamt hat meiner Dienststelle mitgeteilt, dass es das MDK-Gutachten benötige, um entscheiden zu können, ob die Pflege *ambulant, teilstationär oder stationär* zu erbringen sei. Dies kann zu unterschiedlichen Kosten führen.

In § 62 des Zwölften Buchs des Sozialgesetzbuchs (Sozialhilfe) ist geregelt, dass die Entscheidung der *Pflegekasse* über das Ausmaß der Pflegebedürftigkeit auch der Entscheidung des Sozialamts im Rahmen der Hilfe zur Pflege zu Grunde zu legen ist, soweit sie auf Tatsachen beruht, die bei beiden Entscheidungen zu berücksichtigen sind. Vorliegend stellt sich also die Frage nach der Reichweite der Bindungswirkung der von der Pflegekasse getroffenen Entscheidung. Nach Auffassung des betroffenen Sozialamts und des Sozialministeriums Baden-Württemberg erstreckt sich die Bindung auf die Feststellung der Pflegebedürftigkeit und die Einstufung in eine bestimmte Pflegestufe, nicht aber auf die richtige Pflegeart (ambulant, teilstationär oder stationär). Diese Einschätzung wird auch von meiner Dienststelle geteilt. Aufgrund dessen hat der Sozialhilfeträger die Befugnis, selbst zu prüfen, welche Pflegeart er gewährt (ambulant, teilstationär oder stationär), und ist nicht an das Ergebnis der Pflegekasse oder des MDK gebunden. Für diese Prüfung darf das Sozialamt auch die erforderlichen personenbezogenen Daten erheben.

Aus Sicht des Datenschutzes ist es daher grundsätzlich nicht zu beanstanden, wenn das Sozialamt von dem Betroffenen bzw. dessen gesetzlichem Vertreter die Vorlage des MDK-Gutachtens verlangt, in dem sich auch Ausführungen dazu befinden, ob die häusliche Pflege in geeigneter Weise sichergestellt ist und ob vollstationäre Pflege erforderlich ist. Allerdings ist fraglich, ob dazu das gesamte MDK-Gutachten - das Formulargut-

achten umfasst 14 Seiten und enthält eine Vielzahl besonders schützenswerter Angaben über die Gesundheit - benötigt wird oder ob es nicht ausreicht, das Gutachten nur auszugsweise vorzulegen bzw. in dem Gutachten Schwärzungen vorzunehmen. Von letzterem gehe ich gegenwärtig aus. Deswegen hat sich meine Dienststelle mit dem Sozialministerium in Verbindung gesetzt. Von dort wurde uns mitgeteilt, dass eine nur begrenze Einsichtnahme des Sozialamts in das MDK-Gutachten nicht in Betracht komme. Die hierfür genannten Gründe haben mich bislang nicht überzeugt.

Ich werde weiter den Kontakt mit dem Sozialministerium suchen, um eine datenschutzfreundlichere Praxis in diesem sensiblen Bereich zu erreichen.

8. Datenschutz in Kindertageseinrichtungen und Schulen

8.1 Datenschutz in Kindertageseinrichtungen

8.1.1 Broschüre zum Datenschutz in Kindertageseinrichtungen

Welche Daten dürfen in Kindertageseinrichtungen erhoben werden? Wann brauche ich eine Einwilligung der Eltern? Was muss beim Datenschutz überhaupt beachtet werden? Für die Beschäftigten in Kindertageseinrichtungen ergeben sich häufig schwierige Fragen beim Umgang mit den - teilweise sehr sensiblen - Daten der ihnen anvertrauten Kinder. Eine unter meiner Mitwirkung erarbeitete Broschüre des Kultusministeriums will hier Abhilfe schaffen.

Das Kultusministerium Baden-Württemberg hat im September 2012 - in Zusammenarbeit mit den Kommunalen Landesverbänden, den kirchlichen und sonstigen freien Trägerverbänden, den Datenschutzbeauftragten der Kirchen sowie mit meiner Dienststelle - die **Broschüre „Datenschutz in Kindertageseinrichtungen - zum Schutz des Kindes“** herausgegeben. Die Broschüre soll das Datenschutzbewusstsein stärken und den an der frühkindlichen Bildung Beteiligten Antworten auf praktische Fragen zum Datenschutz geben, z. B. darauf, welche Daten in Kindertageseinrichtungen erhoben werden dürfen, wann eine Einwilligung der Eltern erforderlich ist, wann Fotos, Ton- und Videoaufzeichnungen zulässig sind oder unter welchen Voraussetzungen Dritte von der sog. Entwicklungsdokumentationen eines Kindes Kenntnis erlangen dürfen. Sie enthält in einem Serviceteil auch Kopiervorlagen für Einwilligungserklärungen. Diese Broschüre soll anhand der Rückmeldungen über Erfahrungen in der Praxis fortgeschrieben werden.

Das Kultusministerium hat die Broschüre inzwischen in unterschiedlichen Sprachen herausgegeben und an alle Kindertageseinrichtungen und Träger versandt. Sie ist in Papierform beim Kultusministerium Baden-Württemberg (Thouretstraße 6, 70173 Stuttgart, Postfach 10 34 42, 70029 Stuttgart, Telefon: 0711/279-0, Fax: 0711-279-2810, poststelle@km.kv.bwl.de) oder über das „Kindergartenportal des Kultusministeriums Baden-Württemberg“ unter http://www.kindergarten-bw.de/,Lde/826424 zu beziehen.

Die Broschüre „Datenschutz in Kindertageseinrichtungen“ ist eine praktikable Hilfe bei Fragen zum Datenschutz. Ihr ist eine breite Beachtung zu wünschen.

8.1.2 Der Rechtsanspruch auf einen Platz in einer Kindertageseinrichtung und der Datenschutz

Der Anspruch auf frühkindliche Förderung für Kinder, die das erste Lebensjahr vollendet haben, soll nach Meinung mancher Stellen ein weitreichendes Verarbeiten von Daten über die Kinder und die Sorgeberechtigten nach sich ziehen.

Dieser Anspruch besteht seit dem 1. August 2013. Er ist in § 24 Absatz 2 Satz 1 des Achten Buchs des Sozialgesetzbuchs (SGB VIII) geregelt. Davor hatten lediglich Kinder vom vollendeten dritten Lebensjahr bis zum Schuleintritt Anspruch auf den Besuch einer Tageseinrichtung.

Ein Kind, das das erste Lebensjahr vollendet hat, hat bis zur Vollendung des dritten Lebensjahres Anspruch auf frühkindliche Förderung in einer Tageseinrichtung oder in Kindertagespflege.

Vielfach werden für die Anmeldung der Kinder zentrale Verfahren eingesetzt, so auch bei einem Träger der öffentlichen Jugendhilfe, auf den ich aufmerksam gemacht wurde. Der Träger verwendete einen Vordruck für das Anmelden bzw. Vormerkenlassen für einen Kinderbetreuungsplatz, auf dem folgende Angaben erfragt wurden:

- Sorgeberechtigte: Name, Anschrift und Geburtsdatum, (Verwandtschafts-)Verhältnis zum Kind, Angabe, ob der Sorgeberechtigte mit dem Kind als alleiniger Erziehungsberechtigter in einem Haushalt lebt und wenn ja: ob er beschäftigt ist bzw. wenn nein: ob beide Erziehungsberechtigte beschäftigt sind, ob ein oder kein Erziehungsberechtigter be-

schäftigt ist sowie wenn beschäftigt: Umfang der Berufstätigkeit,
- Bedarf: gewünschtes Aufnahmedatum, gewünschte Betreuungsart (Kleinkind, Kindergartenkind, Schulkindbetreuung oder Kindertagespflege) und gewünschte Betreuungszeit (Regelbetreuung, verlängerte Öffnungszeit oder Ganztagsbetreuung) und
- gewünschte Einrichtungen/Betreuungsplätze in der Kindertagespflege: Prioritäten 1 - 3 und (optional) Grund dafür.

Bei solchen Verfahren ist datenschutzrechtlich klar danach zu unterscheiden, welche konkreten Zwecke bzw. Aufgaben jeweils (zulässigerweise) verfolgt werden, etwa

- das Feststellen der Gesamtzahl der Kinder, die einen Platz wollen (also ohne dass Kinder mehrfach erfasst werden - sei es wegen fehlerhafter Angaben beim Erfassen oder wegen gleichzeitiger Anmeldung in mehreren Einrichtungen),
  - mit Blick auf den Anspruch nach § 24 Absatz 2 Satz 1 SGB VIII oder
  - mit Blick auf andere Ansprüche oder Betreuungsarten oder
- das Entscheiden über die Vergabe eines Platzes in einer bestimmten Einrichtung.

Auf Grundlage der vorliegenden Angaben ist für uns derzeit noch nicht hinreichend deutlich, dass ein Erheben aller genannten personenbezogenen Daten durch den örtlichen Träger der öffentlichen Jugendhilfe auf einer Rechtsgrundlage beruht und deswegen datenschutzrechtlich zulässig ist. Fraglich ist auch, ob die Kenntnis aller genannten Daten zur Erfüllung seiner Aufgaben (aus § 24 Absatz 2 Satz 1 SGB VIII) erforderlich ist. So genügt es z. B. nicht, wenn die Kenntnis insoweit lediglich günstig oder hilfreich ist und das vielleicht nur in seltenen Ausnahmefällen.

Ein zentrales Verfahren bei der Zuteilung von Plätzen in Kindertageseinrichtungen halte ich nicht von vornherein für datenschutzrechtlich unzulässig. Insoweit ist es zunächst Sache der datenschutzrechtlich verantwortlichen Stellen, etwa des örtlichen Trägers der öffentlichen Jugendhilfe, im Einzelnen zu prüfen und darzustellen, auf welcher Rechtsgrundlage (Rechtsvorschrift oder Einwilligung) welche Stelle welche Datenarten zu welchen konkreten Zwecken benötigt und verarbeiten soll. Dazu wird es auch notwendig sein, dass die verantwortlichen Stellen ein belastbares Konzept erarbeiten, wie das Vormerken bzw. Anmelden in der Praxis Schritt für Schritt unter Beteiligung welcher Stellen rechtmäßig ablaufen soll. Auch wird danach zu unterscheiden sein, welche Fallgestaltungen es gibt und welche Datenarten in welchen Fallgestaltungen wozu erforderlich sind. Eine Klarstellung durch die verantwortlichen Stellen ist weiterhin geboten. Ich stehe mit den kirchlichen Datenschutzbeauftragten in Kontakt, die sich ebenfalls um Lösungen bemühen. Eine Koordinierung durch das Kultusministerium wäre - ähnlich wie bei der Zusammenarbeit für die Broschüre über den Datenschutz in Kindertageseinrichtungen - sinnvoll.

Ein zentrales Verfahren zum Anmelden bzw. Vormerkenlassen für einen Kinderbetreuungsplatz wirft einige datenschutzrechtliche Fragen auf, die bald geklärt werden sollten.

8.2 Datenschutz an Schulen

Im 29. Tätigkeitsbericht (LT-Drs. 14/5500, S. 64 f.) hatte ich kritisch über die datenschutzrechtliche Situation an öffentlichen Schulen des Landes Baden-Württemberg berichtet. Im 30. Tätigkeitsbericht (LT-Drs. 15/955, S. 87) konnte ich bereits einige Verbesserungen vermelden, die auf Initiativen des Kultusministeriums zurückgingen. Inzwischen haben sich weitere Fortschritte ergeben.

Viele Anfragen von Schulleiterinnen und Schulleitern, Lehrerinnen und Lehrern, aber auch von Eltern zeigen, dass es bei der Auslegung der für Schulen geltenden datenschutzrechtlichen Vorschriften und deren praktischer Umsetzung nach wie vor zu Schwierigkeiten kommt. Dies liegt nicht zuletzt daran, dass längst Internet, Computer und Netzwerke, Schulverwaltungs-, Stundenplan- oder Zeugnisprogramme sowie Lernplattformen Einzug in den Schulalltag gehalten haben. Die Wahrung der Persönlichkeitsrechte aller am Schulleben Beteiligten beim Umgang mit neuen Medien und

neuen Verfahren stellt die Schulen immer wieder vor neue Herausforderungen.

8.2.1 Datenschutzrechtliche Zusammenarbeit mit ausgewählten Schulen

Im Jahr 2012 hat meine Dienststelle in Absprache mit dem Kultusministerium eine **Kooperation** mit zwei Schulen im Mittleren Neckarraum begonnen, bei der es darum geht, relevante Datenschutzfragen exemplarisch aufzuarbeiten und für andere Schulen Musterlösungen („Best Practice“) bereitzustellen. Ausgewählt wurden eine Grundschule und eine große Berufliche Schule, um das breite Spektrum der Schullandschaft abzudecken.

Diese Zusammenarbeit hat sich zu einem wertvollen und praxisnahen Instrument für die Weiterentwicklung des Datenschutzes an Schulen entwickelt, von dem auch andere Schulen künftig im Land profitieren können. Einige Beispiele mögen dies belegen:

8.2.2 Verfahrensverzeichnis

In der Vergangenheit musste ich wiederholt Verfahrensverzeichnisse von Schulen bemängeln, weil diese ganz überwiegend unvollständig, inhaltlich nicht korrekt oder gar völlig inhaltsleer waren.

Seit Sommer 2012 unterstützt das Kultusministerium die Schulen bei der Erstellung der Verfahrensverzeichnisse durch ein neues, webbasiertes Verfahren namens **"Verfahrensverzeichnis-Online-BW" (VV-Online-BW)**, zu dem jede Schule einen Zugangscode erhalten hat. Zur Einführung wurden zunächst umfangreiche, mit meiner Dienststelle abgestimmte Hilfetexte und "Leitfragen" in VV-Online-BW integriert. Zudem wurden zwei Mustervorlagen für die beiden Verfahren "Amtliche Schuldaten – Baden-Württemberg" (ASD-BW) und "Schulverwaltungsprogramm Baden-Württemberg" (SVP-BW) zur Verfügung gestellt. Außerdem wurden zum Verfahrensverzeichnis umfangreiche Erläuterungen in Hilfetexten erarbeitet. Inzwischen wurde auch ein Muster für das Verfahren „Kompetenzanalyse Profil AC“, über dessen Problematik ich bereits im 29. Tätigkeitsbericht (LT-Drs. 14/5500, S. 64 f.) berichtet hatte, entwickelt.

Im Rahmen der Zusammenarbeit mit der Beruflichen Schule wurde geprüft, ob die derzeit den Schulen zur Verfügung stehenden Hilfen des Kultusministeriums ausreichen, um das Verfahrensverzeichnis, den gesetzlichen Anforderungen entsprechend, erstellen zu können. Dabei hat sich gezeigt, dass es nicht genügt, den Schulen nur Verfahrensmuster als Hilfestellung anzubieten. Das Kultusministerium bietet deshalb mittlerweile Fortbildungen für die behördlichen Datenschutzbeauftragten an den Schulen und für Schulleitungen an.

Die **Fortbildungsveranstaltungen** für behördliche Datenschutzbeauftragte behandeln das Führen eines Verfahrensverzeichnisses und die Nutzung des Verfahrens VV-Online-BW detailliert (siehe http://lehrerfortbildung-bw.de/sueb/recht/fb/). Die Fortbildungsveranstaltungen für Datenschutzbeauftragte an Schulen gehen ebenfalls näher auf die Erstellung eines Verfahrensverzeichnisses mit Hilfe der Plattform VV-Online-BW ein. Die Erstellung des Verfahrensverzeichnisses für das Unterrichtsnetz bzw. für die schulische Moodle-Installation wird dagegen im Rahmen der Fortbildungen für Netzwerkberaterinnen und -berater bzw. Moodle-Administratorinnen und -Administratoren behandelt (vgl. http://lehrerfortbildung-bw.de/netz/muster/verfahrensverzeichnis und http://lehrerfortbildung-bw.de/sueb/recht/ds_neu/verfahren/verz.htm).

Um bewerten zu können, ob die Schulen mit dem Programm VV-Online-BW zurecht kommen und die angebotenen Fortbildungen die datenschutzrechtlichen Grundlagen ausreichend vermitteln, begleiten und unterstützen meine Mitarbeiter die eingangs genannten Schulen bei der Erstellung des Verfahrensverzeichnisses. Unsere Verbesserungsvorschläge zu VV-Online-BW hat das Kultusministerium in das Programm eingearbeitet.

8.2.3 Schulverwaltungsprogramm

Derzeit verwenden viele Schulen das „Landeseinheitliche Schulverwaltungsprogramm Baden-Württemberg“ (SVP) zur Verwaltung der Lehrer- und Schülerdaten. Dieses Programm ist nach Auffassung des Kultusministeriums der erste Schritt zu

einem landeseinheitlichen Standard. Als nächster Schritt soll in den nächsten Jahren das Programm „Amtliche Schulverwaltung Baden-Württemberg“ (ASV-BW) an allen Schulen eingeführt werden.

Auch eine der mit uns zusammenarbeitenden Schulen setzt dieses **Schulverwaltungsprogramm** ein. Allerdings haben meine Mitarbeiter bei näherem Hinsehen einige Defizite entdeckt. So können derzeit in diesem Programm Daten zwar gesperrt, aber nicht gelöscht werden. Das ist datenschutzrechtlich natürlich nicht hinnehmbar und soll sich nach Angaben des Kultusministeriums bald ändern: Im neuen Programm ASV-BW, das zum Schuljahr 2014/2015 an allen Schulen verpflichtend eingeführt werden soll, wird nicht nur ein Sperren, sondern auch ein (automatisiertes) Löschen von Daten möglich sein. Geplant ist auch die eigentlich überfällige Hinterlegung eines Rechte- und Rollenkonzepts. Damit kann sichergestellt werden, dass den einzelnen Nutzern nur die erforderlichen personenbezogenen Daten zugänglich sind. Die Schülerdaten einer Klasse dürfen z. B. nur den in dieser Klasse unterrichtenden Lehrern sichtbar sein.

Da das Programm ASV-BW mit dem Programm ASD-BW, das schulübergreifenden Verwaltungszwecken und statistischen Zwecken dient, verbunden ist, ist noch zu klären, welche personenbezogenen Daten dabei übertragen werden.

8.2.4 Datenverarbeitung im Auftrag

Im Zuge der Zusammenarbeit mit der Beruflichen Schule erfuhr ich, dass in Zukunft die bei der Schule anfallenden personenbezogenen Daten außerhalb der Schule beim Schulträger automatisiert verarbeitet werden sollen. Dazu muss der Auftragnehmer nach § 7 LDSG datenschutzrechtlich beauftragt werden.

Diese Konstellation ist an Schulen vermutlich nicht selten, da der Schulträger für die Ausstattung der jeweiligen Schule und die Betreuung des Verwaltungsnetzes zuständig ist. So wird oftmals der Schulträger festlegen, wo die Verwaltung der Schülerdaten stattfindet, ohne sich dabei bewusst zu sein, dass die Schule weiterhin in vollem Umfang für die Einhaltung der Bestimmungen über den Datenschutz verantwortlich bleibt. Konkret bedeutet das u. a., dass die Rechte von Betroffenen, z. B. auf Auskunft, gegenüber der Schule geltend zu machen sind. Der Auftrag an den Auftragnehmer (d. h. ggf. auch an den Schulträger, bei einem städtischen Gymnasium also an die Stadt selbst) muss überdies schriftlich erteilt werden, wobei mindestens die in § 7 Absatz 2 Satz 4 LDSG genannten Punkte geregelt sein müssen, zum Beispiel die notwendigen technischen und organisatorischen Maßnahmen nach § 9 LDSG. Die Schule muss sich zudem beim Auftragnehmer von der Einhaltung dieser Maßnahmen überzeugen, also zum Beispiel die Gewährleistung der Zutrittskontrolle oder die Prozesse der Datensicherung konkret überprüfen.

Dies war der betroffenen Schule durchaus bekannt. Die Ausgestaltung des mit dem Auftragnehmer abzuschließenden Vertrages gestaltete sich jedoch schwierig. Dies galt gleichermaßen für den Schulträger, für den die genannte Rollenverteilung ungewohnt war. Deshalb habe ich dem Kultusministerium vorgeschlagen, einen **Mustervertrag für eine Datenverarbeitung im Auftrag** für die Schulen zu entwickeln. Dies wurde vom Kultusministerium erfreulicherweise aufgegriffen und mittlerweile auch umgesetzt. Der Mustervertrag soll unter Berücksichtigung der an den von uns betreuten Schulen gewonnenen Erfahrungen kontinuierlich weiterentwickelt werden.

8.2.5 Umgang mit Fehlzeiten

Bei der Erfassung von Abwesenheitszeiten werden zwangsläufig personenbezogene Daten der Schülerinnen und Schüler von den Lehrkräften erhoben und gespeichert. Häufig handelt es sich dabei um besonders sensible Krankheitsdaten - ein Grund, im Rahmen der Zusammenarbeit mit den Schulen den dabei ablaufenden Prozess genauer unter die Lupe zu nehmen.

Ist ein Schüler aus zwingenden Gründen (z. B. Krankheit) am Schulbesuch verhindert, ist dies der Schule unter Angabe des Grundes und der voraussichtlichen Dauer der Verhinderung unverzüglich mitzuteilen (§ 2 Absatz 1 der Schulbesuchsverordnung - SchulBesV BW). In diesem Zusammenhang stellt sich immer wieder die Frage, wel-

che Personen Kenntnis von dieser Entschuldigung nehmen dürfen. Nach Auffassung der Kultusverwaltung müssen nur Klassenlehrer und Fachlehrer, bei berufschulpflichtigen Schülern auch der Ausbildungsbetrieb wissen, dass und weshalb ein Schüler (entschuldigt) fehlt, um darauf ggf. mit pädagogischen Mitteln reagieren zu können. Bereits daraus ergibt sich, dass auch nur diese Personen die Mitteilungen über das Fehlen einsehen dürfen, keinesfalls jedoch Lehrer, die den abwesenden Schüler nicht unterrichten, oder gar Mitschüler. Dies bedeutet aber auch, dass die Schule für eine sichere Aufbewahrung der Entschuldigungen sorgen muss.

Für datenschutzrechtlich problematisch halte ich es, wenn Schulen verlangen, die Entschuldigung per unverschlüsselter E-Mail zu übermitteln. Immerhin bieten solche ungeschützten Übertragungswege keinen hinreichenden Schutz vor unberechtigten Zugriffen Dritter. Überdies kann der Absenderangabe in einer E-Mail nicht immer vertraut werden, so dass sich hinter der Absenderadresse einer entsprechenden E-Mail nicht unbedingt tatsächlich auch ein Elternteil oder derjenige verbergen muss, dem die Erziehung oder Pflege eines Kindes anvertraut ist. Bekanntermaßen ist dies bei Entschuldigungen in Papierform auch nicht immer garantiert.

Schulen haben außerdem festzulegen, wann Entschuldigungen zu löschen sind. Die Aufbewahrungsdauer hat sich daran zu orientieren, wie lange die Schule die Entschuldigungen benötigt. Sollten z. B. Fehlzeiten einen Einfluss bei der Notenbildung haben (vgl. § 8 Absatz 4 und 5 der Notenbildungsverordnung), so wäre die Speicherung der Entschuldigung bis zur Bestandskraft des Zeugnisses erforderlich.

8.2.6 Datenweitergabe bei Umzug

Ein weiteres datenschutzrechtlich relevantes Thema ist die Weitergabe personenbezogener Daten an eine andere Schule, z. B. nach dem Umzug eines Schülers. Generell stellt sich aber, nicht nur an der von uns betreuten Grundschule, die Frage, welche Daten unter welchen Umständen datenschutzrechtlich weitergegeben werden dürfen.

Nach § 115 Absatz 3 des Schulgesetzes für Baden-Württemberg (SchG) darf die aufnehmende Schule die zu Verwaltungszwecken notwendigen Daten bei der abgebenden Schule erheben. Notwendige Daten sind beispielsweise Name, Vorname, Anschrift, Geburtsdatum, Schulabschluss (Qualifikation, Ergebnis, Noten maßgeblicher Fächer) oder Klassenstufe und Abgabeschulart.

Weitere Daten dürfen gem. § 16 LDSG nur übermittelt werden, wenn diese für die Erfüllung des Erziehungs- und Bildungsauftrags der neuen Schule erforderlich sind. Dies kann z. B. bei der Mitteilung über einen Schulausschluss nach § 90 SchG der Fall sein. Weitere personenbezogene Schülerdaten, die für die Aufgabenerfüllung der neuen Schule nicht erforderlich sind, dürfen nur mit Einwilligung der Erziehungsberechtigten (vgl. § 4 Absatz 1 Nummer 2 LDSG) weitergegeben werden.

Wechselt der Schüler nach der Grundschulzeit zu einer weiterführenden Schule, dürfen die Grundschulempfehlung für die weiterführende Schule und das Zeugnis nicht mehr von der Grundschule an die weiterführende Schule übermittelt werden. Grund hierfür ist der Wegfall der verbindlichen Grundschulempfehlung im Jahr 2011.

Die datenschutzrechtliche Beratung von Schulen und die Begleitung neuer Verfahren wird weiterhin ein Schwerpunkt meiner Tätigkeit sein. Die vom Kultusministerium im Jahr 2011 an meine Dienststelle abgeordnete Lehrkraft war ein wertvolles Bindeglied zwischen meiner Dienststelle, dem Ministerium und dem schulischen Alltag. Es ist zu hoffen, dass auch diese Form der Zusammenarbeit künftig fortgesetzt wird.

8.2.7 Soziale Netzwerke im Schulbetrieb

Die Nutzung von Sozialen Netzwerken wie Facebook, Google+, Studi VZ, aber auch Twitter ist heutzutage unter Schülerinnen und Schülern weit verbreitet. Eine Handreichung des Kultusministeriums stellt nun klar, dass eine dienstliche Kommunikation über Soziale Netzwerke nicht erlaubt ist.

Immer wieder haben sich besorgte Eltern darüber beschwert, dass an Schulen in Baden-Württemberg das Soziale Netzwerk Facebook, z. B. zur Vergabe und Durchführung von Hausaufgaben, zur Mitteilung und Verabredung von Terminen und für andere Zwecke eingesetzt werde. Dabei soll es sich weniger um private Absprachen von Lehrern mit Schülerinnen und Schülern untereinander, sondern um „offizielle“ Vorgaben der jeweiligen Lehrer gehandelt haben, die Facebook quasi als Kommunikationskanal zwischen sich und den Schülern empfahlen. Auf diese Weise seien auch Schülerinnen und Schüler veranlasst worden, sich auf Facebook anzumelden, die dort noch nicht registriert waren. Kein Wunder, dass manche der betroffenen Eltern sich hiergegen wehrten.

Das geschilderte Vorgehen der Lehrer ist aus datenschutzrechtlicher Sicht bedenklich. Derzeit erkenne ich nicht, dass der Einsatz Sozialer Medien, insbesondere Facebook, zur Aufgabenerfüllung der staatlichen Schulen erforderlich ist und damit den gesetzlichen Anforderungen des Landesdatenschutzgesetzes entspricht. Private Diensteanbieter dürfen im Rahmen der Aufgabenerfüllung nur unter den engen Voraussetzungen des Landesdatenschutzgesetzes für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten einbezogen werden. Eine enge (schulische) Zweckbegrenzung lässt sich hinsichtlich der mit Facebook übermittelten Daten ohnehin nicht verwirklichen, da das amerikanische Unternehmen die erhobenen Daten zur kommerziellen Verwertung von Nutzerprofilen verwendet. Dieser Zweck widerspricht den Vorgaben des Landesdatenschutzgesetzes hinsichtlich der öffentlichen Stellen in Baden-Württemberg. Es käme ja (hoffentlich) auch keine Schule auf die Idee, die Daten ihrer Schüler an die Werbebranche zu verkaufen. Nichts anderes würde im Grunde aber passieren, wenn eine Schule das vermeintlich kostenlose Soziale Netzwerk Facebook offiziell einsetzen würde. Abgesehen davon können die Lehrer, wenn Facebook zur Kommunikation mit den Schülern genutzt wird, praktisch nicht ihrer pädagogischen Verantwortung gerecht werden, schon weil sie dort kaum regulierend eingreifen können und die Einträge nur schwer zu löschen sind.

Zwar kann der Dienstherr die Nutzung des Sozialen Netzwerks Facebook durch Lehrpersonal zu privaten Zwecken kaum unterbinden. Sofern das Lehrpersonal aber Facebook (auch) für schulische und damit dienstliche Aufgaben einsetzt, ist aus meiner Sicht ein Einschreiten geboten, zumal den Schulen in Baden-Württemberg mit der Lernplattform Moodle eine datenschutzgerechte Alternative zur Verfügung steht. Diese Lernplattform, für die auch vielfältige Fortbildungen angeboten werden, bietet ein virtuelles Klassenzimmer, in welchem sich die Schüler mit dem Lehrer in einem geschützten Bereich austauschen können.

Das Kultusministerium hat dies genauso gesehen und die Verarbeitung von personenbezogenen Daten im Rahmen der schulischen Arbeit auf Sozialen Netzwerken von Anbietern im Sommer 2013 untersagt, soweit deren Server außerhalb des europäischen Wirtschaftsraumes betrieben werden, es sich um US-amerikanische Unternehmen handelt oder ein Zugriff von außerhalb des Europäischen Wirtschaftsraumes (EWR) möglich ist. Weiterhin möglich ist die Verwendung von Facebook zu „Demonstrationszwecken“, wenn also das Thema „Soziale Netzwerke“ im Unterricht behandelt wird. Die vom Kultusministerium verbreitete **Handreichung** verbietet ebenfalls den Einsatz von sog. Social Plugins wie des Like-it Buttons von Facebook auf den Internetseiten von Schulen, was ich ebenfalls nachdrücklich begrüße. Eine Überprüfung von Schul-Homepages hinsichtlich der Verwendung des Like-it Buttons durch meine Dienststelle hat inzwischen ergeben, dass nur wenige Schulen diesen einsetzen. Nachdem ich die Schulen angeschrieben hatte, entfernten alle Schulen den Like-it Button. Weitere Details zu dieser Untersuchung sind in Kapitel 11.2.3 zu finden.

Die Handreichung des Kultusministeriums hat umgehend eine breite fachliche und politische Debatte ausgelöst. Zwar gab es einige kritische Stimmen aus politischen Nachwuchsverbänden, die hier Technikmuffel am Werke sahen. Die zustimmenden Kommentare überwogen jedoch bei weitem; erfreulich und bemerkenswert war vor allem die Unterstützung durch Landeseltern- und Landesschülerrat sowie durch Lehrerverbände. Inzwischen haben andere Länder mit ähnlichen Vorgaben für den Schulbereich nachgezogen.

Zu meinem Bedauern hat das Kultusministerium die Verwendung von Fanpages durch Schulen nicht untersagt. Immerhin wurde klargestellt, dass weder personenbezogene Daten noch Bilder von Schülern oder anderen Personen auf Fanpages dargestellt werden dürfen und die Kommunikation der Schulen mit Schülern über diese Fanpages unzulässig ist. So gesehen können und dürfen Fanpages lediglich als Zugang zu den eigenen Internetseiten der jeweiligen Schule verwendet werden.

Mit der Handreichung des Kultusministeriums wurde die längst überfällige datenschutzrechtliche Handlungssicherheit für die Schulen geschaffen.

8.2.8 Einführung einer landeseinheitlichen Bildungsnummer

Nach längerer Pause unternimmt das Kultusministerium wieder einen Anlauf, um die Daten aller Schüler zentral zu speichern und um u. a. daraus Bildungsgangstatistiken abzuleiten.

Es scheint eine „never ending story“ zu sein. Bereits mein Vorgänger hatte sich mit dem Vorhaben der sog. **Schülerindividualdatei** mehrfach auseinandersetzen müssen; zur Vermeidung von Wiederholungen verweise ich auf den Beitrag „Die multifunktionale Schülerindividualdatei: ein Projekt mit vielen Fragezeichen“ im 25. Tätigkeitsbericht (LT-Drs. 13/3800), auf den Beitrag „Zum weiteren rechtlichen Schicksal der Schülerindividualdatei“ im 26. Tätigkeitsbericht (LT-Drs. 13/4910) sowie auf den Beitrag „Das sog. Nationale Bildungsregister“ im 27. Tätigkeitsbericht (LT-Drs. 14/650). Nun unternimmt das Kultusministerium wieder einen Anlauf, um die Daten aller Schüler im Land zentral zu speichern, auch um daraus Bildungsgangstatistiken abzuleiten. Diesmal nennt sich dieses Verfahren „Amtliche Schuldaten Baden-Württemberg“ (ASD-BW), wie wir von Vertretern des Kultusministeriums vor kurzem erfahren haben. Damit einhergehen wird vermutlich eine Änderung der Verordnung des Kultusministeriums über die Datenverarbeitung für statistische Erhebungen und schulübergreifende Verwaltungszwecke an Schulen (SchulStatDVV). Nach der bisherigen Planung sollen alle Schulen verpflichtet werden, ihre Schülerdaten zentral, im Rahmen einer Datenverarbeitung im Auftrag, in einer operativen Datenbank, voraussichtlich beim Informatikzentrum der Landesverwaltung Baden-Württemberg (IZLBW), abzulegen. Dies soll einerseits schulübergreifenden Verwaltungszwecken wie Schulwechsel, Schulkooperationen und zur Feststellung von Mehrfachbewerbungen, andererseits statistischen Zwecken dienen. Die Rechtsgrundlage hierfür findet sich in § 115 des Schulgesetzes. Zur eindeutigen Identifikation eines Schülers plant das Kultusministerium aber auch die Vergabe einer landeseinheitlichen und eindeutigen **Bildungsnummer**. Diese Bildungsnummer soll dem Schüler, z. B. bei einem Schulwechsel, mitgeteilt werden, damit der Schüler seine Nummer der neuen Schule mitteilen und diese die Schülerdaten von der alten Schule übernehmen kann. Dadurch möchte das Kultusministerium auch erreichen, dass Mehrfachbewerbungen, wie sie z. B. nach Ende der Grundschulzeit bei einer Bewerbung für weiterführende Schulen vorkommen können, erkannt werden und dass nicht ein Schüler an mehreren Schulen eingeplant wird.

Datenschutzrechtlich wird darauf zu achten sein, dass eine Schule nur die für ihre eigenen Aufgaben nötigen Daten bekommt. Derzeit sehe ich nicht, dass dafür eine landeseinheitliche und permanent zugeteilte Bildungsnummer erforderlich ist. An die Erforderlichkeit einer zentralen Datenspeicherung unter Verwendung einer einheitlichen Bildungsnummer ist im Hinblick auf die damit verbundene Missbrauchsgefahr und das Risiko von Datenverknüpfungen ein strenger Maßstab anzulegen. Eine für das gesamte Schulleben, also über alle Schularten hinweg vergebene einheitliche Bildungsnummer, die vielfältige Auswertungen

erlauben würde, wäre daher datenschutzrechtlich bedenklich. Der nächste Schritt wäre dann vermutlich eine länderübergreifende, also bundesweite Bildungsnummer, denn Schulwechsel gibt es natürlich auch über Ländergrenzen hinweg. Eine Umfrage bei den Kolleginnen und Kollegen in anderen Ländern hat übrigens ergeben, dass dort nur vereinzelt vergleichbare Überlegungen angestellt werden.

Neben der operativen Datenbank plant das Kultusministerium ein **Data-Warehouse**, in welchem die Daten aus der operativen Datenbank für statistische Zwecke längerfristig gespeichert werden sollen. In den Datensätzen des Data-Warehouses sollen die Daten zwar in pseudonymisierter Form vorliegen, trotzdem besteht das Risiko, dass z. B. bei einem ungewöhnlichen Bildungsverlauf eines Schülers ein Personenbezug hergestellt werden kann. Damit wäre auch dieses Data-Warehouse den Regelungen des Landesdatenschutzgesetzes unterworfen. Sollte das Projekt wirklich erforderlich sein, dann sollte dafür gesorgt werden, dass sich die Datenerhebung für statistische Zwecke nur auf das für die Steuerung der Schulen notwendige Maß (z. B. für Zwecke der Bildungsplanung) beschränkt. Weiterhin müssen Rückschlüsse aus den Datensätzen des Data-Warehouses auf die Daten der operativen Datenbank technisch und organisatorisch verhindert werden. Daher sollte dieses Data-Warehouse personell, organisatorisch, räumlich und verfahrensmäßig getrennt vom Verwaltungsvollzug betrieben und das Statistikgeheimnis gewahrt werden. Darum halte ich einen Betrieb des Data-Warehouses durch das Statistische Landesamt ohne Zugriff durch das Kultusministerium für sinnvoller, um eine Trennung zwischen Verwaltung und Statistik zu gewährleisten.

An eine landeseinheitliche Bildungsnummer ist datenschutzrechtlich im Hinblick auf ihre Erforderlichkeit ein strenger Maßstab anzulegen.

8.2.9 Lehreraus- und -fortbildung

Verschiedene Einrichtungen aus dem Geschäftsbereich des Kultusministeriums bieten mittlerweile Fortbildungen für Lehrkräfte zum Thema Datenschutz an. Auch in der Lehrerausbildung findet der Datenschutz zunehmend Beachtung. Meine Dienststelle beteiligt sich regelmäßig daran.

Das Kultusministerium hat in Zusammenarbeit mit der Landesakademie für Fortbildung und Personalentwicklung an Schulen, mit den Regierungspräsidien und mit Mitarbeitern meiner Dienststelle eine **Konzeption für zentrale und regionale Fortbildungsmaßnahmen zu den Themen "Datenschutz und Urheberrecht in der Schulpraxis"** erarbeitet. Dazu wurden umfangreiche zielgruppenspezifische Fortbildungsmodule zu datenschutzrechtlichen Themen an Schulen entwickelt und Materialien auf dem Lehrerfortbildungsserver (siehe *http://lehrerfortbildung-bw.de/sueb/recht/index.htm*) bereitgestellt. Ferner wurde eine umfangreiche Stoffsammlung für den Themenbereich "Datenschutz an Schulen" mit zahlreichen Umsetzungsbeispielen entworfen.

Für folgende Zielgruppen wurden Fortbildungsangebote und die entsprechenden Fortbildungsmaterialien entwickelt:

- neu ernannte Schulleiterinnen und Schulleiter sowie Schulleiterinnen und Schulleiter, die diese Funktion schon länger ausüben,
- behördliche (schulische) Datenschutzbeauftragte,
- Multimediaberaterinnen und -berater als schulinterne Multiplikatoren und Ansprechpartner für das Kollegium,
- Netzwerkberaterinnen und -berater, die das Unterrichtsnetz der Schule betreuen,
- Moodle-Administratorinnen und -Administratoren, die die schulische Moodle-Installation (Lernplattform) betreuen,
- Fachberaterinnen und Fachberater, die in der Fortbildung und in der Schulaufsicht tätig sind, sowie
- Lehrkräfte.

Die **Landesakademie für Fortbildung und Personalentwicklung an Schulen** hat - teilweise unter Mitwirkung von Mitarbeitern meiner Dienststelle - die Fortbildungskonzepte erprobt, Konzeptionen und Materialien überarbeitet und im Anschluss in zahlreichen Veranstaltungen Multiplikatoren (in der Regel Lehrkräfte) für alle genannten

Fortbildungsmaßnahmen geschult. Die Fortbildungsveranstaltungen werden auf regionaler Ebene unter Regie des jeweiligen Regierungspräsidiums durch Tandems von Juristen und Lehrkräften mit vertieften IT-Kenntnissen durchgeführt. Alle Multiplikatoren setzen die beschriebenen Maßnahmen auf der Ebene der Regierungspräsidien regional um.

Den behördlichen Datenschutzbeauftragten wird in zweitägigen Seminaren ein tiefergehendes Wissen vermittelt. Für die Schulleiterinnen und Schulleiter und die sonstigen Personengruppen finden eintägige Veranstaltungen statt. An der Entwicklung der Fortbildungskonzeption war meine Dienststelle aktiv beteiligt.

Das **Regierungspräsidium Stuttgart** hat darüber hinaus bereits in den Staatlichen Schulämtern "Inhouse-Veranstaltungen" zum Thema Datenschutz an Schulen veranstaltet, teilweise unter Mitwirkung meiner Mitarbeiter. Außerdem hat ein Mitarbeiter meiner Dienststelle in Zusammenarbeit mit dem Kultusministerium Schulnetzberater der Kreismedienzentren geschult.

Als ausgesprochen sinnvoll hat sich auch die Mitwirkung meiner Dienststelle am „Medienpädagogischen Kolloquium“ der Pädagogischen Hochschule Ludwigsburg erwiesen. Mit einem Gastbeitrag zum Thema informationelle Selbstbestimmung wurde das Ziel verfolgt, die angehenden Lehrer für Datenschutzfragen zu sensibilisieren.

Der datenschutzkonforme Umgang mit personenbezogenen Daten an Schulen setzt gut ausgebildetes Personal voraus. Der vom Kultusministerium eingeschlagene Weg, behördliche Datenschutzbeauftragte zu qualifizieren und Schulleitungen, Lehrerinnen und Lehrern Fortbildungen und Schulungen zum Thema Datenschutz anzubieten, muss weiterbeschritten werden.

8.3 Datenschutz als Unterrichtsthema

Es reicht nicht aus, dass der Datenschutz in der Schulverwaltung beachtet wird. Wichtiger ist es, dass er auch Thema im Unterricht wird.

8.3.1 Datenschutz macht Schule

Durch das Internet haben die heutigen Schüler viele Möglichkeiten, die frühere Schülergenerationen nicht hatten. Dies birgt jedoch neue Gefahren bzw. verstärkt bereits vorhandene Risiken. Dies gilt nicht nur für die Akteure selbst, sondern auch für viele Mitbetroffene, die davon nichts erfahren. Wenn nun z. B. sehr einfach personenbezogene Daten anderer über Soziale Netzwerke verbreitet werden können, beispielsweise Bilder von Freunden und Verwandten, so kann auch deren Grundrecht auf informationelle Selbstbestimmung betroffen sein. Auch früher schon vorhandene Probleme des Schulalltags wie Hänseleien oder gar Mobbing werden durch die neuen technischen Möglichkeiten verstärkt. Das Internet erweist sich - wie in der Computerkriminalität generell (vgl. Jahresbericht des Landeskriminalamtes 2012 zur Cyberkriminalität) - auch insoweit nur als modernes Mittel zu einem bekannten Zweck. In Bezug auf den Datenschutz sehe ich als Gefahren u. a., dass

- personenbezogene Daten (z. B. Namen und Bilder) von Dritten (z. B. von Freunden o.ä.) ohne Einwilligung verbreitet werden (evtl. auch unwahre Dinge, wie z. B. beim Mobbing),
- eigene personenbezogene Daten unbedarft oder unfreiwillig weitergegeben werden (z. B. bei Online-Spielen o.ä.),
- Datensammlungen und Verknüpfungen durch Dienstleister zu detaillierten personenbezogenen Profilen führen können und
- diese Daten im Internet aller Erfahrung nach nicht mehr zu löschen sind.

Neben datenschutzrechtlichen Gefahren können z. B. aber auch Urheberrechtsverletzungen, Internetbetrug oder das Eindringen in fremde Systeme (Phishing, Schadprogramme etc.) drohen. So können z. B. durch Schadprogramme personenbezogene Daten gesammelt und für Straftaten verwendet werden.

Aus allem folgt, dass Datenschutz und Medienkompetenz zunehmend wichtige Themen (nicht nur) für Jugendliche sein müssen. Dabei geht es neben den rechtlichen Belangen auch um ethische und moralische Orientierungen, nicht zuletzt

wegen den Auswirkungen auf unsere Gesellschaft. Um sich selbst eine angemessene Meinung bilden zu können, sind zunächst Kenntnisse über die Funktionsweise und die Rahmenbedingungen des Internets erforderlich. Jugendliche sollten daher zum Beispiel:

- den Aufbau des Internets verstehen,
- die Funktion eines Cookies erklären können,
- Datenbanken als schnell durchsuchbare Quelle von Informationen kennen,
- Zählpixel und Like-It-Button als Möglichkeit verstehen, um zentrale Datensammlungen anzulegen,
- Möglichkeiten und Grenzen der Verschlüsselung nachvollziehen können und
- die technischen Gefahren bei der Verwendung des Internets oder von mobilen Geräten kennen (Viren, Spam usw.).

Dazu gehört natürlich auch, dass die Jugendlichen konkret lernen, wie und wo sie z. B. die Privatsphäreneinstellungen vornehmen können und welche Bedeutung diese haben. Allerdings wandelt sich die Technik so rasch, dass Anpassungen der Lerninhalte unumgänglich sein werden.

Weiterhin sind aber auch Kenntnisse über die Grundrechte, welche den Jugendlichen und ihren Mitmenschen zustehen, zu vermitteln.

Im Anschluss könnten mit den Jugendlichen Werte und Haltungen in einem kritischen Diskurs entwickelt werden, um z. B. folgende Fragen zu klären:

- Warum soll ich meine Privatsphäre bzw. die des Anderen schützen?
- Wo ziehe ich für mich persönlich die Grenze zwischen privat und öffentlich?
- Welche Folgen haben Cyber-Mobbing und Stalking?
- Welche gesellschaftlichen Auswirkungen haben das Internet oder die Sozialen Netzwerke auf unser Privat- oder Arbeitsleben?

Diese Ausführungen sollen exemplarisch andeuten, was nach meinen Vorstellungen in Zukunft im Unterricht an den Schulen vermittelt werden müsste.

Das **Bundesinnenministerium** setzt sich mittlerweile, nicht zuletzt auf Anregung der Konferenz der Datenschutzbeauftragten, dafür ein, den Datenschutz als Bildungsaufgabe in der Europäischen Datenschutz-Grundverordnung zu verankern, weil „ein Bewusstsein der Bürgerinnen und Bürger für die mit der Nutzung der Informationstechnologie verbundenen Gefahren“ unverzichtbar sei. Auch die **Kultusministerkonferenz** hat anerkannt, dass der Datenschutz verstärkt als Thema in den Unterricht einfließen muss. In der am 8. März 2012 von der Kultusministerkonferenz verabschiedeten Empfehlung „Medienbildung in der Schule“ (vgl. http://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf) bildet der Datenschutz (zusammen mit dem Urheberrecht) eines der insgesamt acht Handlungsfelder (siehe dort Kapitel 3.6). Die Empfehlung soll - so die Verfasser - dazu beitragen, Medienbildung als Pflichtaufgabe schulischer Bildung nachhaltig zu verankern. Denn Medienkompetenz gelte in nahezu allen Bereichen allgemeiner und beruflicher Bildung inzwischen als unverzichtbare Schlüsselqualifikation, die für die Entwicklung der eigenen Persönlichkeit, aber auch für die selbstbestimmte aktive und politische Teilhabe an gesellschaftlichen Prozessen von großer Bedeutung sei.

Datenschutz muss als Teil der Medienkompetenz in Zukunft verstärkt in den Bildungsplänen verankert werden.

8.3.2 Medienkompetenz macht Bildung

Beim Medienkongress des Landesmedienzentrums hat meine Dienststelle die Gelegenheit erhalten, Vorschläge für die Berücksichtigung des Datenschutzes als Unterrichtsthema zu unterbreiten.

Erfreut war ich, als das Landesmedienzentrum Baden-Württemberg (LMZ) meine Dienststelle einlud, beim **Kongress „Medienkompetenz macht Bildung“** im Oktober 2012 im Forum „Datenschutz: Von der Rechtswissenschaft in die Schule“ mitzuwirken. Da seit 2011 ein Lehrer, der

besondere IT-Kompetenzen aufweist und zudem als Fachberater am Regierungspräsidium Stuttgart tätig ist, zu meiner Dienststelle abgeordnet ist, lag es nahe, ihn mit der Aufgabe zu betrauen, um dadurch datenschutzrechtliche und pädagogische Belange gleichermaßen einzubringen. Dabei kam und kommt es auch bei anderen Anlässen dieser Art nicht nur darauf an zu verdeutlichen, dass Datenschutzkompetenz auch aus pädagogischer Sicht ein wichtiger Teil der Medienkompetenz ist. Fast wichtiger noch als derartige theoretische Überlegungen sind für die Schulen praktische Ratschläge, wie das trockene Thema Datenschutz ganz konkret im Unterricht behandelt werden kann. Deshalb hat mein Mitarbeiter beim Kongress an Beispielen aufgezeigt, wie einzelne Unterrichtstunden oder auch Unterrichtsprojekte zum Datenschutz gestaltet werden könnten.

Für eine praxisnahe Vermittlung des Themas Datenschutz im Unterricht sind geeignete Darstellungsformen und Lerninhalte zu entwickeln. Meine Dienststelle wird die Kultusverwaltung dabei weiter unterstützen.

8.3.3 Die Bildungsplanreform 2015 und der Datenschutz

Durch die Mitarbeit meiner Dienststelle im Beirat zur Bildungsplanreform 2015 besteht die Chance, den Datenschutz auch in den Bildungsplänen zu verankern.

Zum Schuljahr 2015/2016 will das Kultusministerium in Baden-Württemberg die Bildungspläne weiterentwickeln. Da mir das Unterrichtsthema Datenschutz wichtig ist, habe ich mich darüber gefreut, dass einer meiner Mitarbeiter in den **Beirat zur Bildungsplanreform 2015** berufen wurde. Aufgabe dieses Gremiums, in dem Vertreterinnen und Vertreter aus Wissenschaft, Wirtschaft, Gesellschaft und Politik mitwirken, ist es, die Weiterentwicklung des Bildungsplans kritisch und konstruktiv zu begleiten und den vielfältigen Sachverstand seiner Mitglieder einzubringen. Allerdings besteht der Beirat aus über 40 Mitgliedern, die ganz unterschiedliche Fachbereiche und damit sehr heterogene Interessen vertreten.

Die Medienbildung ist eines der fünf Leitprinzipien des neuen Bildungsplans, was dem Datenschutz als wichtigem Teil der Medienbildung entgegen kommt. Leider soll die Medienbildung aber kein eigenes Schulfach sein, sondern fächerübergreifend vermittelt werden. Ich habe die Sorge, dass die Medienbildung aus unterschiedlichen Gründen im Schulalltag unter den Tisch fallen könnte. Ein eigenständiges Fach „Medienkompetenz“ würde hingegen die Gewähr dafür bieten, dass diese Schlüsselkompentenz angemessen berücksichtigt wird.

Als Grundlage für die Medienbildung dient dem Kultusministerium das Mediencurriculum des Landesmedienzentrums. Dieses hat dankenswerterweise meiner Dienststelle die Gelegenheit eröffnet, das Mediencurriculum um einige datenschutzrechtliche Aspekte zu ergänzen. Wie jedoch das Mediencurriculum endgültig in den einzelnen Fächern abgebildet wird, muss sich erst noch zeigen.

Ein Bildungsplan mit datenschutzrechtlichen Inhalten ist zwar notwendig, aber noch nicht hinreichend, um die informationelle Selbstbestimmung im realen Unterricht als Thema nachhaltig zu verankern. Nach der Festlegung des Bildungsplans muss deshalb auch die entsprechende Fortbildung der Lehrkräfte verstärkt werden. Dazu sollten die Lerninhalte exemplarisch vor allem in praktischen Unterrichtssequenzen vorgestellt werden.

Wichtig wäre es zudem, dass datenschutzrechtliche Fragestellungen integrale Bestandteile von Zwischen- und Abschlussprüfungen sowie der regulären Evaluation und Qualitätssicherung des Unterrichts werden, um eine größere Verbindlichkeit und eine stärkere Berücksichtigung in der Aus- und Fortbildung zu erzielen.

Ich werde die Arbeit am Bildungsplan 2015 weiter konstruktiv begleiten. Ein eigenständiges Fach „Medienkompetenz“ halte ich für wünschenswert. Zumindest sollte der Datenschutz als Teil der Medienbildung verbindlich als Prüfungsstoff berücksichtigt werden.

9. Datenschutz in der Arbeitswelt

9.1 Die Feststellung der Alkoholisierung von Beschäftigten am Arbeitsplatz

Der Umgang mit Alkohol am Arbeitsplatz durch Unternehmen wirft neben arbeitsrechtlichen und arbeitsmedizinischen auch datenschutzrechtliche Fragen auf. Dem berechtigten Interesse eines Unternehmens, Verstöße gegen ein Alkoholverbot am Arbeitsplatz beweiskräftig feststellen zu können, stehen das allgemeine Persönlichkeitsrecht und das Recht der Arbeitnehmer auf körperliche Unversehrtheit gegenüber.

Ein Unternehmen, das kein absolutes Alkoholverbot für seine Beschäftigten während der Arbeitszeit eingeführt hatte, wollte in Fällen von wiederholt festgestelltem Alkoholmissbrauch am Arbeitsplatz individuelle Alkoholverbote mit den betroffenen Arbeitnehmern vereinbaren. Es legte uns eine entsprechende Formulierung mit der Bitte um Stellungnahme vor. Diese enthielt neben der Verpflichtung des Mitarbeiters, künftig auf jeglichen Konsum von Alkohol am Arbeitsplatz zu verzichten und die Arbeit nicht unter Einfluss von Restalkohol aufzunehmen, auch eine Verpflichtung des Arbeitnehmers, bei Anzeichen von unerlaubtem Alkoholkonsum am Arbeitsplatz (z. B. Atemalkohol) einen Alkoholtest mittels „Alkomat“ beim Werkschutz durchführen zu lassen.

Während ich gegen die vertragliche Vereinbarung individueller Alkoholverbote mit Arbeitnehmern, die durch Alkoholmissbrauch am Arbeitsplatz gegen ihre arbeitsrechtlichen Verpflichtungen verstoßen habe, - zumindest wenn dem eine einschlägige Abmahnung vorausgeht - keine grundlegenden Bedenken hatte, erschien die Vereinbarung über die Durchführung von Alkoholtests problematisch. In der arbeitsgerichtlichen Rechtsprechung ist anerkannt, dass ein Arbeitnehmer wegen des verfassungsmäßig garantierten Grundrechts auf körperliche Integrität weder zu einer Untersuchung seines Blutalkoholwertes noch zur Mitwirkung an einer Atemalkoholanalyse gezwungen werden kann. Ein derartiger Eingriff in das Persönlichkeitsrecht und in die körperliche Integrität eines Arbeitnehmers ist nicht ohne seine Einwilligung möglich. Der Abschluss einer unbefristeten, bindenden und damit nicht widerrufbaren zivilrechtlichen Vereinbarung über die Mitwirkung an einer Atemalkoholanalyse kann die Freiwilligkeit der Einwilligung des Mitarbeiters zu dem Zeitpunkt, an dem die Untersuchung tatsächlich stattfinden soll, in Frage stellen. Statt eine vollstreckbare Mitwirkungspflicht des Arbeitsnehmers an einem Atemalkoholtest zu vereinbaren, sollte der Arbeitgeber den Arbeitnehmer immer dann, wenn ihm Anhaltspunkte für einen Alkoholmissbrauch am Arbeitsplatz bekannt werden, auf die Möglichkeit hinweisen, durch die freiwillige Mitwirkung an objektiven Tests (z .B. mittels „Alkomat“ oder einer von einem Arzt entnommenen Blutprobe) den Verdacht einer Alkoholisierung auszuräumen. Einer vertraglichen Verpflichtung des Mitarbeiters bedarf es dazu nicht.

Arbeitnehmer können wegen ihres verfassungsmäßig garantierten Grundrechts auf körperliche Integrität vom Arbeitgeber weder zu einer Untersuchung ihres Blutalkoholwertes noch zur Mitwirkung an einer Atemalkoholanalyse gezwungen werden.

9.2 Die Einholung von Auskünften über Arbeitnehmer und Bewerber durch Arbeitgeber bei anderen Arbeitgebern (sog. Arbeitgeberauskunft)

In der Praxis bestehen manchmal Unsicherheiten darüber, ob, unter welchen Voraussetzungen und in welchem Umfang ein Arbeitgeber Auskünfte bei anderen Arbeitgebern über deren (frühere) Beschäftigte einholen und das angefragte Unternehmen solche Auskünfte erteilen darf.

Ein freiberuflich tätiger IT-Berater wollte von uns wissen, ob die Praxis von Personalberatungsfirmen, die ihn an potentielle Arbeitgeber vermitteln sollten, rechtmäßig ist, zunächst die Kontaktdaten ehemaliger Kollegen und Vorgesetzter, die Auskunft über ihn geben könnten, zu erheben (Name, Firma, Position, Telefonnummer, E-Mail-Adresse). Um das Ergebnis vorwegzunehmen: Hiergegen bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken.

Vielfach sind Arbeitgeber daran interessiert, über Zeugnisse und schriftliche Referenzen hinaus Informationen über neu einzustellende Arbeitnehmer einzuholen. Dies gilt insbesondere dann, wenn es sich um leitende Angestellte oder solche in besonderer Vertrauensstellung handelt. Wege, an die gewünschten Informationen heranzukommen, gibt es viele, von denen auch Gebrauch gemacht wird, wie Umfragen ergeben haben, nicht zuletzt mit Hilfe des Internets und einschlägiger Suchmaschinen (vgl. z. B. Umfrage im Auftrag des Branchenverbandes BITKOM vom Oktober 2011). Das ist datenschutzrechtlich jedoch u. U. heikel (vgl. auch 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 26).

Als Informationsmittel etabliert ist dagegen neben dem Zeugnis die **Auskunft des ehemaligen Arbeitgebers**. Diese wird zumeist mündlich erteilt. In der datenschutzrechtlichen Literatur ist anerkannt, dass ein (früherer) Arbeitgeber im Allgemeinen Auskünfte nur mit Zustimmung des betroffenen Arbeitnehmers erteilen darf und Angaben, die keinen Bezug zur fachlichen Befähigung oder zum Verhalten des Arbeitnehmers aufweisen, generell unzulässig sind. An der Erhebung von Kontaktdaten früherer Arbeitgeber bei einem Bewerber besteht daher grundsätzlich ein berechtigtes Interesse des Arbeitgebers. Es handelt sich insoweit - ungeachtet einer fehlenden Rechtspflicht sowohl des Bewerbers als auch der benannten Referenzperson zur Auskunftserteilung - um Informationen, die zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich sein können. Für das Verhältnis von freiberuflich Tätigen zu Personalberatungsfirmen, die für Arbeitgeber freie Mitarbeiter suchen, gelten diese Grundsätze entsprechend. Auch insoweit kann die Erhebung der für eine Kontaktaufnahme erforderlichen personenbezogenen Daten eines als Referenzperson benannten Dritten durch den Arbeitgeber gem. § 28 Absatz 1 Nummer 2 und Absatz 2 Nummer 2a BDSG zulässig sein. In der Benennung der Referenzperson durch den Arbeitnehmer ist zugleich dessen Zustimmung in die Einholung von Auskünften durch den Arbeitgeber bzw. durch die Personalberatungsfirma zu sehen. Ohne eine entsprechende vertragliche Vereinbarung besteht allerdings keine rechtliche Verpflichtung von Bewerbern zur Benennung von Referenzpersonen.

Ein Arbeitgeber darf bei einem anderen Arbeitgeber Auskünfte über einen Arbeitnehmer grundsätzlich nur mit Zustimmung des Betroffenen einholen. Angaben, die keinen Bezug zur fachlichen Befähigung oder zum Verhalten während des Arbeitsverhältnisses aufweisen, sind dabei generell unzulässig. In der Benennung eines früheren Vorgesetzten oder Kollegen als Referenzperson durch den Betroffenen kann eine konkludente Zustimmung in die Einholung entsprechender Auskünfte liegen.

9.3 Datenschutzrechtliche Fragen bei Personalakten

Die Führung von Personalakten wirft immer wieder datenschutzrechtliche Fragen auf. So wird das Prinzip der Richtigkeit bei der Personalaktenführung häufig missachtet.

Ein Dienstherr hatte einen Beamten aufgefordert, Unterlagen zur Berechnung des Urlaubsanspruchs vorzulegen. Diese Unterlagen wurden in die **Personalakten** des Beamten aufgenommen. Die Aufnahme dieser Schriftstücke in die Personalakte erfolgte unstreitig zu Recht. Der Beamte beschwerte sich bei meiner Dienststelle jedoch u. a. darüber, dass eine notwendige **Anhörung** gem. § 87 Absatz 4 des Landesbeamtengesetzes (LBG) unterblieben sei. Der Dienstherr konnte seinerseits nicht darlegen, dass, zu welchem genauen Zeitpunkt und in welcher Form eine Anhörung stattgefunden hat. Generell ist in diesem Zusammenhang darauf hinzuweisen, dass der Beamte nach § 87 Absatz 4 LBG über Beschwerden, Behauptungen tatsächlicher Art und Bewertungen, die für ihn ungünstig sind oder ihm nachteilig werden können, vor deren Aufnahme in die Personalakte gehört werden muss. Eine besondere Form ist hierbei nicht vorgeschrieben. Es empfiehlt sich jedoch, zu Beweiszwecken zumindest einen Vermerk über die Anhörung des Beamten in die Personalakte aufzunehmen.

In dieser Angelegenheit war auch zu klären, was **zulässiger Personalakteninhalt** ist. Zur Personalakte gehören nach § 50 Satz 2 des Beamtenstatusgesetzes alle Unterlagen, die den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Zu diesen Vorgängen gehören - neben Personalunterlagen und dienstlichen Beurteilungen - nicht nur diejenigen, die den Inhalt des Dienstverhältnisses insgesamt oder einzelne sich daraus ergebende Rechte und Pflichten bestimmen oder verändern, sondern auch die Unterlagen, die die Art und Weise erhellen, in der die jeweilige Entscheidung vorbereitet worden ist, oder die Aufschluss über Gesichtspunkte und Erwägungen geben, die für die einzelne, das Dienstverhältnis berührende Maßnahme oder dafür, dass sie unterblieben ist, maßgebend waren. Auch Unterlagen zur Urlaubsberechnung sind nach § 86 Absatz 6 Satz 1 sowie § 88 Absatz 1 Satz 3 LBG Teil der Personalakte.

Vor der Aufnahme in die Personalakte muss der Beamte über Beschwerden, Behauptungen und Bewertungen, die für ihn ungünstig sind oder nachteilig werden können, gehört werden.

Nicht in die Personalakte gehören Vorgänge, die sich auf mehrere Beamte beziehen oder die allein die persönlichkeitsrechtlich geschützte Privatsphäre des Beamten berühren. Hierzu gehören insbesondere Vorgänge über die politische und weltanschauliche Überzeugung und über die Mitgliedschaft in Gewerkschaften und Berufsverbänden. Vermerke und sonstige Aufzeichnungen, die lediglich führungsunterstützenden Charakter haben und die ihrer Natur nach nur vorübergehend gelten (z. B. Zielvereinbarungen) sowie Beschwerden, die sich ausschließlich gegen die sachliche Entscheidung eines Beamten richten, sind nur zu den Sachakten zu nehmen.

In weiteren vergleichbaren Fällen im Bereich des Arbeitnehmerdatenschutzes waren von meiner Dienststelle ebenfalls Anfragen zur Aufnahme von Beschwerden oder Behauptungen tatsächlicher Art, die für den Betroffenen ungünstig sind oder nachteilig werden können, zu bearbeiten. Für die nach dem Tarifvertrag der Länder (TV-L) Beschäftigten ist die Anhörung vor der Aufnahme negativer Vorgänge in die Personalakte in § 3 Absatz 6 TV-L geregelt und folgt für Arbeitnehmer aus dem Grundsatz der allgemeinen Fürsorgepflicht des Arbeitgebers in Verbindung mit § 83 des Betriebsverfassungsgesetzes.

10. Datenschutz in der Wirtschaft

10.1 Kündigung des betrieblichen Datenschutzbeauftragten im Insolvenzverfahren?

Im Berichtszeitraum beschwerte sich der bisherige Datenschutzbeauftragte einer insolventen Ladenkette darüber, dass ihm durch die Insolvenzverwalter gekündigt, er von seiner Tätigkeit mit sofortiger Wirkung freigestellt und gleichzeitig von seiner Funktion als betrieblicher Datenschutzbeauftragter entbunden worden sei. Ein neuer Datenschutzbeauftragter sei als sein Nachfolger bestellt worden.

Es war erklärter Wille des Gesetzgebers, im Rahmen der 2. BDSG-Novelle im Jahre 2009 die Rechtsstellung des betrieblichen Datenschutzbeauftragten zu verbessern (siehe BT-Drs. 16/12011, S. 30), indem er einen besonderen Schutz des betrieblichen Beauftragten gegen Widerruf und Kündigung einführte (§ 4f Absatz 3 Sätze 4, 5 BDSG) und den **Kündigungsschutz** sogar mit einer nachwirkenden Geltung (§ 4f Absatz 3 Satz 6 BDSG) versah.

Bereits der Widerruf der Bestellung ist nach § 4f Absatz 3 Satz 4 BDSG an hohe Hürden geknüpft - in den Kommentaren wird vom „Ausnahmecharakter“ des Widerrufs gesprochen (vgl. Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage, Rdnr. 182 zu § 4f) -, um die Unabhängigkeit des Beauftragten sicherzustellen: Nach § 4f Absatz 3 Satz 4 BDSG kann die Bestellung zum Beauftragten für den Datenschutz in entsprechender Anwendung von § 626 BGB, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Als wichtige Gründe kommen insbesondere solche in Betracht, die mit der Funktion und Tätigkeit des Datenschutzbeauftragten zusammenhängen und eine weitere Ausübung dieser Tätigkeit unmöglich machen oder sie zumindest erheblich gefährden. Beispielsweise ein Geheimnisverrat, fehlendes Fachwissen oder eine dauerhafte Verletzung der Kontrollpflichten als Datenschutzbeauftragter können wichtige Gründe für den Widerruf der Bestellung eines internen Beauftragten für den Datenschutz sein. Im vorliegenden Fall wurden solche Vorwürfe nicht erhoben.

Noch höhere Hürden hat der Gesetzgeber beim Thema Kündigung gesetzt: Nach § 4f Absatz 3 Satz 5 BDSG ist die ordentliche Kündigung eines (internen) betrieblichen Datenschutzbeauftragten, der nach § 4 Absatz 1 BDSG gesetzlich verpflichtend zu bestellen ist - schlicht unzulässig, es besteht also in diesem Falle ein Kündigungsverbot. Selbst nach dem Ende (auch) der Tätigkeit als betrieblicher Beauftragter für den Datenschutz ist eine ordentliche Kündigung erst ein Jahr nach der Abberufung zulässig, es sei denn, dass Gründe für eine außerordentliche Kündigung vorliegen, § 4f Absatz 3 Satz 6 BDSG.

Die Kündigung eines betrieblichen Beauftragten für den Datenschutz ist nur dann zulässig, wenn Tatsachen für eine außerordentliche Kündigung i.S.v. § 626 BGB vorliegen. § 626 Absatz 1 BGB setzt für den Ausspruch einer fristlosen Kündigung eines Dienstverhältnisses einen wichtigen Grund, nämlich das Vorliegen von Tatsachen, aufgrund derer dem Kündigenden unter Berücksichtigung der Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Dienstverhältnisses bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Dienstverhältnisses nicht zumutbar ist, voraus. Darüber hinaus kann die Kündigung nach § 626 Absatz 2 BGB nur binnen zwei Wochen erfolgen, nachdem der Kündigende von den für die Kündigung maßgebenden Tatsachen Kenntnis erlangt hat.

Bei entsprechender Anwendung dieser Vorschrift kann demnach der Widerruf der Bestellung zum Datenschutzbeauftragten - abgesehen von dem hier nicht vorliegenden Verlangen der Aufsichtsbehörde - aus wichtigem Grund nur dann erklärt werden, wenn Tatsachen vorliegen, aufgrund derer dem Widerrufenden unter Berücksichtigung der Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung der Tätigkeit der jeweiligen Person als Datenschutzbeauftragter unzumutbar ist, und die dem Widerrufenden innerhalb der letzten zwei Wochen bekannt geworden sind (so zutreffend das Landesarbeitsgericht Berlin-Brandenburg,

Urteil vom 28. Mai 2009 - Az. 5 Sa 425/09, 5 Sa 434/09, 5 Sa 425/09, 5 Sa 434/09 - <juris>).

Nach § 626 Absatz 1 BGB kommen als wichtige Kündigungsgründe in erster Linie Gründe im Verhalten des Gekündigten und nur ausnahmsweise betriebsbedingte Gründe in Betracht. Dies gilt auch für die Ausübung des Widerrufsrechts der Bestellung des Datenschutzbeauftragten durch den Arbeitgeber. Vorliegend wurden solche Tatsachen nicht vorgebracht. Demnach können betriebsbedingte Gründe für einen Widerruf der Bestellung unter Berücksichtigung des besonderen Charakters von § 4f Absatz 3 Satz 4 BDSG als Schutzvorschrift für die unabhängige Tätigkeit des Datenschutzbeauftragten nur aufgrund ganz besonderer Ausnahmesituationen in Betracht kommen. Könnte sich der Arbeitgeber unter Berufung auf unternehmerische Entscheidungen ohne weiteres auf betriebsbedingte Gründe für einen Widerruf der Bestellung des Datenschutzbeauftragten berufen, könnte der mit den gesetzlichen Vorschriften beabsichtigte besondere Schutz der Tätigkeit des Datenschutzbeauftragten sonst zu leicht umgangen werden (Landesarbeitsgericht Berlin-Brandenburg, a.a.O.).

Dies macht zudem deutlich, dass das Gesetz streng zwischen dem Rechtsverhältnis als Beauftragter für den Datenschutz und dem zugrundeliegenden Arbeitsverhältnis (Grundverhältnis) unterscheidet, wobei das schuldrechtliche Grundverhältnis zur Durchführung der Aufgaben als Datenschutzbeauftragter im Rahmen des jeweiligen Arbeitsverhältnisses unlösbar mit seiner Bestellung nach dem BDSG verknüpft ist (vgl. Urteil des Bundesarbeitsgerichts vom 13. März 2007 - Az. 9 AZR 612/05 -, EzA § 4 f BDSG Nr. 1).

Widerruf und Kündigung sind also getrennt voneinander vorzunehmen und zu prüfen. Erforderlich ist stets der Widerruf der Bestellung als betrieblicher Datenschutzbeauftragter (soweit diese nicht zeitlich befristet ist oder eine einvernehmliche Rücknahme erfolgt), da sonst der nachwirkende Kündigungsschutz des § 4f Absatz 3 Satz 6 BDSG keinen Sinn machen würde (vgl. auch Gola/Schomerus, Kommentar zum BDSG, Rn. 40a zu § 4f).

Damit dürfen gerade nicht arbeitsrechtliche Überlegungen im Vordergrund stehen. Anders als beim Kündigungsschutz geht es also nicht um einen Arbeitsplatzschutz des Beschäftigten (und Datenschutzbeauftragten), sondern um die Wirksamkeit des Datenschutzes (so Simitis. a.a.O.). Diese Einordnung führte nach meiner Auffassung auch dazu, dass kein Raum für Umdeutungen oder Auslegungen der Kündigung nach arbeitsrechtlichen Gesichtspunkten besteht, da der Anknüpfungspunkt beim Datenschutz liegt.

Zu klären blieb die Frage, wie sich dieser datenschutzrechtliche Widerrufs- und Kündigungsschutz auf den Fall einer Insolvenz des Unternehmens auswirkt. Selbstverständlich kann es keinen dauerhaften Kündigungsschutz für den Beauftragten geben, wenn das beschäftigende Unternehmen insolvent geht und am Ende des Verfahrens u. U. liquidiert wird. Hier greifen ähnliche Überlegungen wie etwa bei der Fusion zweier Unternehmen[31].

Auch dafür können die Regelungen direkt dem BDSG entnommen werden: Da das insolvente Unternehmen gem. § 4 Absatz 1 BDSG zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, erlischt diese Pflicht erst dann, wenn - nach Abschluss des Insolvenzverfahrens - in dem Unternehmen (samt Tochterfirmen) keine Verarbeitung von personenbezogenen Daten mehr stattfindet oder im Rahmen der Abwicklung des Unternehmens die Mitarbeiterzahl i.S.v. § 4f Absatz 1 BDSG entsprechend unter die gesetzliche Grenze sinkt. Ist das Unternehmen sodann nicht mehr verpflichtet, einen Beauftragten für den Datenschutz zu bestellen, gilt gem. § 4f Absatz 3 Satz 5 BDSG auch der Kündigungsschutz nicht mehr. Eine betriebsbedingte Kündigung ist dann zulässig, wobei die Bestellung zum Datenschutzbeauftragten unabhängig vom Arbeitsverhältnis erlischt, wenn die Voraussetzungen des § 4f Absatz 1 Satz 1 BDSG nicht mehr vorliegen.

[31] Siehe hierzu z. B. das Urteil des Bundesarbeitsgerichts zur Fusion zweier Krankenkassen (BAG, Urteil vom 29. September 2010 – 10 AZR 588/09 –, BAGE 135, 327 - 333).

Allein die Eröffnung eines Insolvenzverfahrens stellt keinen wichtigen Grund i.S.d. § 626 BGB dar und kann folglich den Widerruf der Bestellung und die Kündigung eines Beauftragten für den Datenschutz i. S. v. § 4f Absatz 3 Satz 5 BDSG nicht begründen.

10.2 Datenschutzkonformes „Double-Opt-in“ bei Werbung per E-Mail

Das Oberlandesgericht München hat in einem Urteil am 27. September 2012 (Az. 29 U 1682/12[32]) entschieden, dass bereits der Versand einer Bestätigungsmail, mit der die Echtheit einer E-Mail-Adresse im Rahmen eines „Double-Opt-in-Verfahrens“ geprüft werden soll, mangels nachgewiesener Einwilligung des Adressaten unzulässige Werbung und damit einen Eingriff in den eingerichteten und ausgeübten Gewerbetrieb (die Klägerin war eine Steuerberatungskanzlei) darstellt. Diese Entscheidung hat im Bereich der Werbung zu großer Unsicherheit geführt.

Nach § 7 Absatz 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG) ist eine geschäftliche Handlung - insbesondere Werbung -, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, unzulässig. Liegt kein gesetzlicher Ausnahmetatbestand i. S. v. § 7 Absatz 3 UWG vor, ist die Nutzung der E-Mail-Adresse für Werbezwecke allein bei Vorliegen einer Einwilligung des Beworbenen zulässig.

In welcher Form die Einwilligung einzuholen ist, ist gesetzlich nicht geregelt. In den letzten Jahren hat sich hierbei das sog**. „Double-Opt-in-Verfahren“** durchgesetzt. Dieses Verfahren besteht aus drei Schritten:

- Eintragung:
  Insbesondere zur Abonnierung eines E-Mail-Newsletters trägt sich der künftige Empfänger mit seiner E-Mail-Adresse (manchmal auch zusätzlich mit seinem Namen) in die entsprechende Maske auf der Internetseite eines Unternehmens ein und klickt den Button „Anmelden“ (1. Opt-in). In der Regel findet sich dort auch der Hinweis, dass mit dem Klicken des Buttons „Anmelden“ oder „Eintragen“ in die Zusendung des Newsletters, also von Werbung, eingewilligt wird.

- Bestätigungsmail:
  Anschließend wird von diesem Unternehmen (in der Regel automatisiert) eine E-Mail an die eingetragene E-Mail-Adresse geschickt, die sog. „Bestätigungsmail“, in der der Empfänger aufgefordert wird, den in dieser Mail enthaltenen Aktivierungslink anzuklicken, um so endgültig in den Newsletter-Verteiler eingetragen zu werden. In der Regel ist in dieser „Bestätigungsmail“ auch zu lesen, dass diese gelöscht werden könne, wenn die Anmeldung zum Newsletter nicht durch den Inhaber der E-Mail-Adresse erfolgt sei.

- Betätigen des Aktivierungslinks:
  Erst mit dem Anklicken dieses Aktivierungslinks (2. Opt-in) erfolgt die Eintragung in den Verteiler des Newsletters. Wird die Bestätigungsmail nicht beachtet (also der Aktivierungslink nicht angeklickt), wird der Newsletter nicht abonniert.

Nach der Rechtsprechung des Bundesgerichtshofs (BGH) stellen alle auf Absatzförderung gerichteten Handlungen bzw. Äußerungen eines Unternehmens Werbung i. S. des § 7 Absatz 2 Nr. 3 UWG dar (Urteil vom 17. Juli 2008 - Az. I ZR 197/05 - FC Troschenreuth, Tz. 14 ff.). Der BGH geht für dieses Begriffsverständnis vom allgemeinen Sprachgebrauch und der Definition des Begriffs der Werbung in Artikel 2 Nr. 1 der Richtlinie 2006/114/EG über irreführende und vergleichende Werbung aus. Danach ist Werbung jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen zu fördern.

Nach diesen Grundsätzen fällt nach Ansicht des Oberlandesgerichts München auch eine E-Mail, mit der zur Bestätigung einer Bestellung im

[32] Das Urteil im Internet: http://www.gesetze-bayern.de/jportal/portal/page/bsbayprod.psml?doc.id=KORE416292012&st=ent&showdoccase=1&paramfromHL=true

„Double-Opt-in-Verfahren“ aufgefordert wird, als Werbung unter das Verbot des § 7 Absatz 2 Nr. 3 UWG. Dabei sei es nicht erforderlich, dass die Bestätigungs-E-Mail selbst eine Werbebotschaft enthält.

Diese Einschätzung ist indes abzulehnen, weil sie sach- und praxisfremd ist und dazu führen würde, dass zum Beispiel eine Newsletter-Anmeldung nicht mehr rechtssicher - oder nur noch mit aufwendiger Briefpost - möglich ist. Die Entwicklung des „Double-Opt-in-Verfahrens“ hatte gerade das Ziel, ein für den modernen, oft onlinegestützten Rechtsverkehr brauchbares Prozedere zu entwickeln, das sowohl für den Werbenden als auch für den Beworbenen ein Stück mehr Rechtssicherheit bringt. Die Überprüfung der Übereinstimmung des Eintragenden mit dem Inhaber der E-Mail-Adresse, der die Bestätigungs-E-Mail erhält, ist ja gerade das Anliegen dieses Verfahrens. Wenn man nun bereits diese Bestätigungs-E-Mail als Werbung ansieht, würde das „Double-Opt-in-Verfahren“ in sich zusammenfallen, da die Bestätigungs-E-Mail bereits die volle Haftung des Werbenden auslöst.

Entscheidend ist, dass das „Double-Opt-in-Verfahren“ von den werbenden Unternehmen richtig angewandt wird und die rechtlichen Voraussetzungen strikt eingehalten werden. So muss die Internetseite, auf der die Eintragung z. B. für die Abonnierung eines E-Mail-Newsletters stattfindet, die Möglichkeit der ausdrücklichen und informierten Einwilligung zur E-Mail-Werbung - etwa durch das Anklicken einer Checkbox - enthalten. Checkboxen, die bereits ein voreingetragenes Häkchen enthalten, sind unzulässig. Auch versteckte Hinweise in Allgemeinen Geschäftsbedingungen genügen nicht. Der Beworbene muss zudem konkret wissen, in welche Werbung er einwilligt. Außerdem dürfen die Hinweise nicht fehlen, dass und wo bzw. wie diese Einwilligung jederzeit widerrufen werden kann.

Das Unternehmen selbst muss diese Eintragung, die die datenschutz- und wettbewerbsrechtliche Einwilligung darstellt, protokollieren und jederzeit vorlegen können. Die Protokollierung sollte die Eintragung selbst betreffen sowie den Zeitpunkt der Eintragung.

Da die Bestätigungs-E-Mail noch die Aktivierung des darin enthaltenen Links verlangt, muss diese Bestätigungs-E-Mail selbst noch werbefrei sein und sich inhaltlich auf den Hinweis hinsichtlich der Aktivierung des Links zur endgültigen Aufnahme in z. B. einen Unternehmens-Newsletter beschränken. Ein vollständiges Impressum darf ebenfalls nicht fehlen.

Wichtig ist später auch, dass die nachfolgende E-Mail-Werbung immer die Möglichkeit des Widerrufs, also etwa der Abmeldung vom Newsletter, enthalten muss.

Sowohl die Bestätigungs-E-Mail als auch die Aktivierung des Bestätigungs-Links sollten genau protokolliert werden. Nur dann kann das werbende Unternehmen seinen Darlegungs- und Beweispflichten nachkommen, wenn es einmal zum Streitfall kommt. Eine 100-prozentige Sicherheit kann allerdings auch dieses Verfahren nicht bieten: Der Bundesgerichtshof hat am 10. Februar 2011 (Az. I ZR 164/09[33]; im Anschluss an BGH, Urteil vom 11. März 2004, Az. I ZR 81/01, E-Mail-Werbung I) festgestellt, dass die Werbezusendung auch dann wettbewerbswidrig ist, wenn die E-Mail-Adresse zwar im „Double-Opt-in-Verfahren“ erlangt wurde, der Verbraucher aber darlegen kann, dass die per E-Mail übermittelte Bestätigung nicht von ihm stammte.

Das „Double-Opt-in-Verfahren“ hat sich als praxistaugliche und effiziente Methode für ein mit dem Datenschutzrecht und dem Wettbewerbsrecht im Einklang stehendes E-Mail-Marketing durchgesetzt. Bei Beachtung insbesondere der datenschutzrechtlichen Vorgaben sollte dieses Verfahren auch in Zukunft Bestand haben.

[33] Im Internet ist das Urteil hier zu finden: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=57082&linked=urt&Blank=1&file=dokument.pdf

10.3 Rechtliche Anforderungen an eine gesetzeskonforme Datenschutzerklärung für Internetseiten

Auch wenn die verantwortlichen Stellen in der gesetzlichen Pflicht stehen, ihre Datenverarbeitung möglichst transparent zu gestalten, kommt die aktive Information der Betroffenen noch allzu oft zu kurz; sehr deutlich wird das etwa bei Online-Datenschutzerklärungen. Gelegentlich gefährdet eine fehlerhafte Unterrichtung sogar die Zulässigkeit der Datenverarbeitung. Zudem hat das Oberlandesgericht Hamburg im Juli 2013 entschieden, dass mangelhafte Datenschutzerklärungen auch wettbewerbsrechtliche Unterlassungsansprüche begründen können. Ausgehend von diesen Erfahrungen und Aussichten haben Mitarbeiter meiner Dienststelle eine Handreichung erarbeitet, die sich in erster Linie an Internetauftritte privater Anbieter richtet und Ausführungen zu rechtlichen Anforderungen, aber auch ausführliche Erläuterungen und Empfehlungen enthält; sie soll demnächst auf meiner Internetseite veröffentlicht werden.

Die folgenden Ausführungen enthalten größtenteils keine sog. materiellen Anforderungen an die Zulässigkeit oder den Einsatz einzelner Verfahren. Sie konzentrieren sich auf die Anforderung an die Transparenz der „ohnehin“ stattfindenden Datenverarbeitung.

§ 13 des Telemediengesetzes (TMG) - Pflichten des Diensteanbieters
(1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31)[34] in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

§ 4 des Bundesdatenschutzgesetzes (BDSG) - Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über
1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten.

§ 93 des Telekommunikationsgesetzes (TKG) - Informationspflichten
(1) Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind die Teilnehmer auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Nutzer sind vom Diensteanbieter durch allgemein zugängliche Informationen über die Erhebung und Verwendung personenbezogener Daten zu unterrichten. Das Auskunftsrecht nach dem Bundesdatenschutzgesetz bleibt davon unberührt.

Ist in jedem Internetauftritt eine **Datenschutzerklärung** erforderlich? - Praktisch ja, und nicht nur auf Internetseiten. Die Unterrichtungspflicht besteht für jedes Telemedium (Internetseiten, aber z. B. auch Apps), bei dessen Nutzung personenbezogene Daten der Nutzer erhoben oder verwendet werden, und zwar unabhängig davon, ob es für geschäftliche oder für private Zwecke eingerichtet wurde. Beispielsweise muss auch auf „privaten“ Fotogalerien oder persönlichen Blogs eine Datenschutzerklärung vorhanden sein. Ausnahmen sind nur vereinzelt vorgesehen, etwa für reine Rundfunkangebote (z. B. Webcasting, Live-Streams).

Die Unterrichtungspflicht für ein Telemedium ergibt sich zunächst aus § 13 Absatz 1 TMG. Daneben bestehen jedoch in jedem Fall die allgemeine Unterrichtungspflicht nach § 4 Absatz 3 BDSG sowie in vielen Fällen auch fachgesetzliche Unterrichtungspflichten, z. B. nach § 93 Absatz 1 TKG.

[34] Gemeint ist der Europäische Wirtschaftsraum (EWR).

In den allermeisten Fällen findet ein datenschutzrechtlich relevanter Umgang aller Beteiligten mit personenbezogenen Daten statt, z. B. in Form von Reichweitenanalyse, Cookies oder der Protokollierung von IP-Adressen. Bereits die in jedem Fall nötige Erhebung (aus dem sog. Request des Nutzer-PCs) und Nutzung (für die sog. Response) der IP-Adresse fällt darunter.

Leider zeigt meine Erfahrung, dass der Umfang oder gar das vollständige Fehlen einer Datenschutzerklärung noch allzu oft nichts mit dem Umfang der Datenverarbeitung zu tun hat und regelmäßig zu (verständlicher!) Unsicherheit bei den Nutzern und in der Folge zu Beschwerden bei der Datenschutzaufsicht führt. Daher empfehle ich bereits aus Gründen der Transparenz, in jedem Fall eine Datenschutzerklärung anzubieten, ggf. mit der Information, dass außer der Erhebung und Nutzung der IP-Adresse im Request-Response-Zyklus kein Umgang mit personenbezogenen Daten stattfindet.

Die Pflicht zur Unterrichtung nach § 13 Absatz 1 TMG trifft den Diensteanbieter nach § 2 Satz 1 Nummer 1 TMG, d. h. „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“. Ausgenommen sind nach § 11 Absatz 1 TMG Dienste, deren Bereitstellung „im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt“, z. B. ein rein dienstliches Intranet oder eine E-Learning-Plattform. Zudem sind nach § 11 Absatz 3 TMG „Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen“ von der Unterrichtungspflicht nach TMG (aber nicht nach anderen Gesetzen wie dem BDSG oder insbesondere dem TKG) ausgenommen. Hierunter fallen typischerweise Access-Providing und E-Mail-Dienste.

Die Pflicht zur Unterrichtung nach § 4 Absatz 3 BDSG über den Umgang mit grundsätzlich allen weiteren personenbezogenen Daten trifft die jeweilige verantwortliche Stelle nach § 3 Absatz 7 BDSG, die nämlich „personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“. Auszunehmen sind hier zwar nach § 1 Absatz 2 Nummer 3 BDSG nicht-öffentliche Stellen (d. h. in der Regel Privatpersonen), die personenbezogene Daten ausschließlich für persönliche oder familiäre Tätigkeiten erheben oder verwenden. Der Schritt in die Weltöffentlichkeit des Internets führt aber auch Betreiber von „privaten“ Internetseiten aus diesem engen Ausnahmebereich heraus in die allgemeine datenschutzrechtliche Unterrichtungspflicht. Nur wenn Internetseiten lediglich einem engen und einzeln bekannten privaten (in der Regel: familiären) Personenkreis zugänglich sind, beispielsweise passwortgesichert, kann im Einzelfall solch eine Ausnahme denkbar sein.

Die **Unterrichtungspflicht** erstreckt sich nicht auf die **Internetseiten dritter Anbieter**, auch wenn entsprechende Links angeboten werden. Ein Hinweis in der Datenschutzerklärung, dass das eigene Internetangebot bei der Betätigung von externen Links verlassen wird und daher die Datenschutzerklärung dann nicht mehr gilt, wäre jedoch wünschenswert, ebenso wie die besondere Kennzeichnung jedes externen Links.

Davon streng zu trennen sind **fremde Dienste**, die in das eigene Internetangebot eingebunden werden wie z. B. Google Maps, Youtube oder Yahoo! Search. Da durch das Einbinden solcher fremden Inhalte zwangsläufig die IP-Adresse und oft auch noch mehr personenbezogene Daten an den Drittanbieter übertragen werden, findet zumindest eine Übermittlung statt, über die nach § 13 Absatz 1 TMG unterrichtet werden muss. Da die Übermittlung in der Regel schon beim Aufruf der entsprechenden Unterseite beginnt, kann es hilfreich sein, wenn der Nutzer im Rahmen der Datenschutzerklärung möglichst genau darüber unterrichtet wird, auf welchen Unterseiten oder Subdomains welche Dienste eingebunden sind, so dass anstelle des gesamten Internetangebots nur diese Seiten umgangen zu werden brauchen, soweit der Nutzer das wünscht.

Eine mangelhafte Unterrichtung ist nicht einfach ein unterlassener Service, sondern ein manifest rechtswidriger Zustand. Ist eine Unterrichtung in der Formulierung der **Bußgeldvorschrift** § 16

Absatz 2 Nummer 2 TMG „nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig“ erteilt worden, kommt alleine dafür eine Geldbuße von bis zu 50.000 € in Betracht, auch wenn daraus kein Schaden entstanden ist. Da die Vorschrift auch Fahrlässigkeit erfasst, ist Unachtsamkeit keine Entschuldigung.

Werden mangelhafte Teile der Datenschutzerklärung für eine Einwilligung herangezogen (siehe weiter unten), ist die Einwilligung ggf. unwirksam und die Datenverarbeitung, die auf dieser Einwilligung beruht, in der Regel rechtswidrig. Daraus könnten sich neben Bußgeldern (z. B. aufgrund von § 43 Absatz 2 Nummer 1 BDSG) insbesondere auch Ansprüche der betroffenen Personen auf **Schadensersatz** nach § 7 BDSG ergeben.

Neben Bußgeldern zur Ahndung kommen meist auch **Maßnahmen nach § 38 Absatz 5 BDSG** in Betracht, mit denen die Aufsichtsbehörde Korrekturen von datenschutzrechtlichen Missständen anordnet oder im äußersten Fall ein Verfahren ganz untersagt.

Schließlich hat das OLG Hamburg der Datenschutzerklärung mit Urteil vom 27. Juni 2013[35] auch eine wettbewerbsrechtliche Dimension zuerkannt: § 13 TMG sei eine das Marktverhalten regelnde Norm und schütze Interessen sowohl der Mitbewerber als offenbar auch der Verbraucher, so dass ein Verstoß dagegen eine unlautere geschäftliche Handlung i. S. d. § 4 UWG sei, gegen den ggf. ein wettbewerbsrechtlicher Unterlassungsanspruch bestehen könne. Auf diesem Weg würde insbesondere Mitbewerbern und Verbraucherschutzorganisationen über die Paragraphenkette §§ 3, 4 Nummer 11, 8 UWG i. V. mit § 13 Absatz 1 TMG die Möglichkeit erwachsen, mit Abmahnungen gegen mangelhafte Datenschutzerklärungen bzw. einzelne Datenverarbeitungsverfahren vorzugehen. Allerdings ist das Kammergericht (KG) Berlin in einem anderen Zusammenhang zum gegenteiligen Schluss gekommen[36].

[35] Urteil „Wettbewerbsverstoß wegen fehlender Datenschutzhinweise“, Aktenzeichen 3 U 26/12
[36] Urteil „Gefällt-mir-Button“ vom 29. April 2011, Aktenzeichen 5 W 88/11

10.3.1 Verpflichtende Bestandteile

In § 13 Absatz 1 TMG wird ausdrücklich verlangt, den Nutzer „zu Beginn des Nutzungsvorgangs … in allgemein verständlicher Form zu unterrichten“ und die Unterrichtung „für den Nutzer jederzeit abrufbar“ zu halten.

Da bereits beim ersten Aufrufen jeder Internetseite personenbezogene Daten übertragen werden, kann kein allzu langer uninformierter Aufenthalt in Kauf genommen werden. Nachdem das Angebot aufgerufen wurde, muss die Datenschutzerklärung mit einem Schritt („Klick“) erreichbar sein („zu Beginn des Nutzungsvorgangs“). Da ein Nutzungsvorgang oft nicht auf der Startseite, sondern - z. B. über eine Suchmaschine - auf einer Unterseite beginnt, muss auch auf jeder Unterseite ein Link direkt zur Datenschutzerklärung angeboten werden (datenschutzrechtliche 1-Klick-Regel).

Für den 1-Klick-Link ist zudem eine typische, aussagekräftige Schaltfläche nötig, z. B. „Datenschutz“, „Datenschutzerklärung“ oder „Datenschutzprinzipien“. Englische Begriffe wie „Privacy Policy“ sollten unterbleiben oder zumindest nur zusammen mit einer deutschen Fassung verwendet werden („Datenschutz / Privacy Policy“). Eine Zusammenlegung auf einer Unterseite mit dem Impressum, den AGBs o. Ä. ist nur akzeptabel, wenn dies aus der Linkbezeichnung bereits hervorgeht. In diesen Fällen gilt die 1-Klick-Regel selbstverständlich auch für die Auffindbarkeit der zusammengelegten Texte.

Eine Zusammenfassung des Textes der Datenschutzerklärung mit dem Text des Impressums, der AGBs o. Ä. ist nur akzeptabel, wenn die Datenschutzerklärung inhaltlich und optisch sauber davon abgegrenzt wird. Keinesfalls ist die Datenschutzerklärung Bestandteil der AGBs, da sie keine Willenserklärung ist, die einer vertraglichen Vereinbarung bedürfte. Eine undifferenzierte Vermischung (z. B. die Datenschutzerklärung als Unterpunkt der AGBs) ist daher nicht akzeptabel.

Die Datenschutzerklärung als allgemeine und umfassende Unterrichtung muss zudem von datenschutzrechtlichen oder anderen Einwilligungstex-

ten (z. B. in die Zusendung von Werbung) sauber getrennt werden, auch begrifflich.[37]

Die folgende Aufzählung einzelner **Pflichtbestandteile** dürfte für die gängigen Konstellationen und Datenverarbeitungen ausreichen. Dennoch könnten einzelne Regelungen, insbesondere aus Fachgesetzen, weitere Unterrichtungen nötig machen. Die in der Praxis noch oft zu beobachtende Methode, schlicht den Gesetzeswortlaut zu wiederholen oder auf „die gesetzlichen Bestimmungen“ zu verweisen, ist in den meisten Fällen nicht genug aussagekräftig.

- **Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten**
  Das schließt insbesondere das Löschkonzept (auch und gerade für Cookies) und sämtliche Übermittlungen an Dritte (auch über eingebettete Dienste) ein. Sämtliche Zwecke der Datenverarbeitung müssen angegeben werden. Soweit nicht offensichtlich, müssen insbesondere die Zwecke der einzelnen Pflichtfelder angegeben werden. In der Regel wird es für die gebotene Konkretheit nötig sein, die Rechtsgrundlagen gleich mit anzugeben (z. B. „postalische Werbung an unsere Kunden nach § 28 Absatz 3 Satz 2 Nummer 1 BDSG“, „automatisierte Entscheidung nach § 6a Absatz 2 BDSG über die Zahlungsarten, die wir Ihnen für eine Bestellung in unserem Online-Shop anbieten“).
- **Unterrichtung über Verarbeitung der Daten außerhalb des Europäischen Wirtschaftsraums (EWR)**
  Hier müssen zumindest die betroffenen Datenarten und nach Möglichkeit die jeweiligen Staaten genau benannt werden (z. B. Übermittlung „von zur Rechnungserstellung benötigten Kundendaten an ein Dienstleistungsrechenzentrum in der Schweiz“).
- **Einsatz von Cookies, Web-Bugs u. v. m.**
  Das gilt zumindest, soweit es sich nicht um rein technische Objekte handelt, bei denen ein Personenbezug (auch über die IP-Adresse) sowohl im Moment der Nutzung als auch in der Zukunft ausgeschlossen ist. Dass die Aufzählung von einer Erläuterung der datenschutzrelevanten Eigenschaften der einzelnen Objekte begleitet werden muss, versteht sich von selbst.
- **Hinweis auf das Widerrufsrecht bezüglich elektronisch erklärter Einwilligungen**
  Soweit die Möglichkeit zu Einwilligungen in elektronischer Form angeboten wird, muss nach § 13 Absatz 3 TMG bzw. nach § 28 Absatz 3a BDSG ausdrücklich auf das jederzeitige Widerrufsrecht hingewiesen werden.
- **Information über mögliche anonyme oder pseudonyme Nutzungsmöglichkeiten**
  Auch hier muss die Information nach § 13 Absatz 6 TMG von einer entsprechenden Anleitung begleitet werden. Dies gilt insbesondere für die Deaktivierung datenschutzrelevanter Cookies u. Ä., soweit das möglich ist.
- **Hinweis auf die Widerspruchsmöglichkeit gegen das Erstellen von Nutzungsprofilen**
  Das ist eine Spezialregelung nach § 15 Absatz 3 TMG. Die Verwendung solcher (pseudonymer) Nutzungsprofile erkennt der Nutzer teilweise daran, dass die Werbung auf den von ihm besuchten Seiten im Lauf der Zeit immer besser zu seinen Interessen zu passen scheint.
- **Identität und Erreichbarkeit der beteiligten verantwortlichen Stellen nach BDSG**
  Da diese Angaben dem Betroffenen ggf. als Ausgangspunkt für die Verfolgung seiner Rechte dienen sollen, ist die vollständige, ladungsfähige Anschrift nötig.
- **Erreichbarkeit des betrieblichen Datenschutzbeauftragten**
  Nach § 4f Absatz 5 BDSG können sich Betroffene jederzeit - soweit eine Bestellpflicht besteht - an den betrieblichen Datenschutzbeauftragten wenden, dem in diesem Zusammenhang (auch) eine unabhängige Kontroll- und ggf. Vermittlungsfunktion zukommt. Der Zugang zu diesem fundamentalen Recht darf nicht durch allzu hohe Hürden erschwert werden.

[37] Umgekehrt kann bei der Einholung von datenschutzrechtlichen Einwilligungen jeweils Bezug auf eine Stelle in der Datenschutzerklärung genommen werden, solange die Konkretheit der Einwilligung und die Verständlichkeit nicht darunter leiden. Unter anderem ist dafür in der Regel eine satzgenaue Verlinkung nötig.

In der Regel unverzichtbar sind Unterrichtungen über Analysewerkzeuge wie Google Analytics oder Piwik, aber auch über „ungefilterte“ Social Plugins. Hier liegen die datenschutzrechtlichen Probleme zumeist eher bei den Fragen zu den rechtlichen Anforderungen an den eigentlichen Einsatz. Oben Gesagtes zu Erwähnung, Erläuterung und ggf. Anleitung zur Deaktivierung durch den Nutzer gilt selbstverständlich auch hier.

10.3.2 Freiwillige, aber ratsame Bestandteile

Eine „Datenschutzerklärung“ in ihrer gängigsten Form als kompakte Darstellung der datenschutzrechtlich relevanten Vorgänge ist nach dem Wortlaut der Gesetze zwar nicht zwingend vorgeschrieben, aber sehr sinnvoll. Sind die Informationen verstreut, wird der Nutzer kaum feststellen können, ab wann er umfassend informiert wurde. Unbedingt ratsam ist daher eine Bündelung der gesetzlichen Unterrichtungspflichten in einer allumfassenden Datenschutzerklärung, auch wenn dadurch einzelne Unterrichtungen, etwa über das jederzeitige Widerrufsrecht (§ 13 Absatz 3 TMG) oder über das Recht zum Werbe- und Weitergabewiderspruch (§ 28 Absatz 4 Satz 2 BDSG), mehrfach vorkommen, sowohl im Text der Datenschutzerklärung als auch an den Stellen, an denen die Einwilligungen eingeholt werden bzw. die Unterrichtungen erfolgen und mit dem Setzen eines „Häkchens“ durch den Nutzer protokolliert werden sollen.

Die folgenden **Empfehlungen** zu weiteren Angaben entstammen der täglichen datenschutzrechtlichen Beratungspraxis aufgrund von Anfragen und Beschwerden Betroffener. Da nicht jede Information für jedes Angebot sinnvoll ist und ein Zuviel an Information schlimmstenfalls das Gegenteil bewirkt, soll die folgende Zusammenstellung nur Anregungen für eigene Überlegungen bieten.

- **Abgrenzung des von der Datenschutzerklärung erfassten Bereichs**
  Wünschenswert wären ausdrückliche Informationen über Hoster und weitere beteiligte Provider, externe Links, Anbieter eingebetteter Dienste u. Ä., auch über die einfache Angabe von Übermittlungen und Empfängern hinaus.
- **Hinweise auf Datenschutzrechte der betroffenen Person, soweit diese Hinweise nicht gesetzlich vorgeschrieben sind**
  Hierunter fallen etwa die allgemeinen Rechte auf
  - Widerruf von Einwilligungen,
  - Auskunft nach § 34 BDSG und ggf. nach § 6a Absatz 3 BDSG u. Ä., soweit Hinweise darauf nicht verpflichtend vorgeschrieben sind, und
  - Berichtigung nach § 35 Absatz 1 BDSG.

  Wenn im Einzelnen besondere Anforderungen an die Identifikation der betroffenen Person gestellt werden (z. B. wenn es erforderlich ist, dass die vollständige Anschrift oder das Geburtsdatum angegeben wird), ist neben der Kontaktseite die Datenschutzerklärung dafür der Ort der Wahl. Hinsichtlich der Werbe- und Weitergabewidersprüche bietet sich ggf. auch eine kurze Erläuterung des Sperrlistenverfahrens an.
- **Information über das Einsichtsrecht in das (eigene) Jedermannverzeichnis nach § 4g Absatz 2 Satz 2 BDSG**
  Die Verpflichtung zum Führen eines sog. Jedermannverzeichnisses und der anlasslosen Einsichtgewährung trägt dem Grundsatz der Öffentlichkeit der Datenverarbeitung Rechnung. Da sich keine Betriebs-, Geschäfts- oder sonstigen Geheimnisse, aber einige nützliche Informationen in diesem Verzeichnis finden, spricht aus datenschutzrechtlicher Sicht zudem wenig dagegen und viel dafür, das Verzeichnis selbst zum Herunterladen einzustellen.
- **Informationen über und Erläuterung von Sicherungsmaßnahmen**
  Denkbar sind z. B. verschlüsselte Übermittlung, Nutzung von https oder eine Möglichkeit zur verschlüsselten Kontaktaufnahme.
- **Angabe der zuständigen Datenschutzaufsichtsbehörde(n)**
  Der Hinweis auf die zuständige Datenschutzaufsichtsbehörde ist sinnvoll, weil sich die örtliche Zuständigkeit der Datenschutzaufsicht im Unterschied zu den Verbraucherschutzeinrichtungen nicht am Betroffenen, sondern am Sitz der verantwortlichen Stelle orientiert.

- **Ggf. einige Hinweise an Minderjährige bzw. Eltern**
  Der Hinweis, dass personenbezogene Daten über die IP-Adresse soweit möglich (auch) dem Anschlussinhaber zugerechnet werden, kann nie schaden. Zudem können bei Minderjährigen besondere rechtliche Voraussetzungen für eine wirksame datenschutzrechtliche Einwilligung bestehen (so muss die Tragweite der Einsichtsfähigkeit im jeweiligen Alter angepasst sein) oder auch freiwillige schützende Kriterien vom Diensteanbieter aufgestellt werden.

Auch wenn die rechtlichen Vorgaben nicht einfach sind, führt kein Weg an einer ernsthaften Beschäftigung der Verantwortlichen mit dem Thema „Datenschutzerklärung“ vorbei - nicht nur, weil ein Verstoß unangenehm und teuer werden kann, sondern vor allem, weil Transparenz eine tragende Säule für die wirksame Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung ist. Den bestehenden Lücken gilt es zwar im Einzelfall mit datenschutzaufsichtsrechtlichen Verfahren oder Bußgeldern entgegenzutreten. Genauso wichtig sind aber passende Informationsmaterialien und ggf. Beratungen.

10.4 Nicht alles ist Spam: Datenschutzkonforme elektronische Werbung aufgrund des Privilegs nach § 7 Absatz 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG)

Viele Beschwerden im Bereich der Werbung drehen sich um Werbe-E-Mails. Für deren rechts- und datenschutzkonformen Einsatz existiert eine eigentlich hinreichende Vorgabe in Gestalt von § 7 UWG. In der Praxis bereitet deren Anwendung allerdings durchaus noch Probleme.

Eine typische Beschwerde ging Mitte 2012 ein: Der Betroffene hatte ein Produkt eines Verlags in dessen Downloadshop erworben. Einige Zeit später erhielt er eine Werbe-E-Mail von diesem Verlag, auf die er - wie er erklärte - mit einer Widerspruchs-E-Mail an die für diesen Zweck angegebene Adresse reagierte. Da er vom Verlag keine Antwort erhielt, wandte er sich an meine Dienststelle.

Für die datenschutzrechtliche Bewertung von **Werbung per elektronischer Post** (E-Mail, SMS, MMS) ist - neben den allgemeinen Vorschriften - speziell § 7 Absatz 3 UWG heranzuziehen. § 7 UWG verfolgt sowohl wettbewerbsrechtliche (beispielsweise verbraucherschützende) als auch datenschutzrechtliche Ziele. Mit dem Datenschutz gemein hat er die für das Wettbewerbsrecht ansonsten eher untypische Wirkung eines Verbots mit Erlaubnisvorbehalt für die in Absatz 2 Nummern 2 und 3 aufgeführten Kommunikationswege (Telefonanruf, automatische Anrufmaschine, Telefax, elektronische Post). In Bezug auf elektronische Post liest sich das wie folgt:

§ 7 UWG - Unzumutbare Belästigungen
(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. …
(2) Eine unzumutbare Belästigung ist stets anzunehmen
...
3. bei Werbung unter Verwendung einer automatischen Anrufmaschine, eines Faxgerätes oder elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt
…
(3) Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn
1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
3. der Kunde der Verwendung nicht widersprochen hat und
4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Grundsätzlich ist also Werbung per elektronischer Post nur mit vorheriger ausdrücklicher Einwilligung des Betroffenen zulässig.

Das **Privileg für elektronische Werbung ohne Einwilligung des Betroffenen** greift nur, wenn alle vier in § 7 Absatz 3 aufgezählten Voraussetzungen eingehalten werden (sog. kumulativer Ausnahmetatbestand). Ansonsten würde die uneingewilligte Werbe-E-Mail eine unzumutbare Belästigung darstellen, gegen deren Wiederholung der belästigte Verbraucher mit Hilfe einer Verbraucherschutzorganisation vorgehen könnte. In datenschutzrechtlicher Hinsicht ist dann eine unbefugte Nutzung erfolgt (nämlich die Nutzung der gespeicherten E-Mail-Adresse für die wettbewerbswidrige Zusendung sowie der weiteren personenbezogenen Daten, die in die Gestaltung und den Inhalt der Werbe-E-Mail eingeflossen sind); allerdings ist diese unbefugte Nutzung nicht bußgeldbewehrt, solange die betroffene Person nicht selbst zuvor einen Werbewiderspruch nach § 28 Absatz 4 BDSG eingelegt hat.

Die Prüfung der Werbe-E-Mail anhand des Anforderungskatalogs des § 7 Absatz 3 UWG ergab im Einzelnen Folgendes:

- **Angabe im Zusammenhang mit einem vorausgegangenen Verkauf (§ 7 Absatz 3 Nummer 1 UWG):**
  Das Privileg beschränkt sich auf Bestandskunden, wobei es sich nicht unbedingt um einen Online-Verkauf handeln muss. Im Fall des Verlags wurde vom Betroffenen online ein Rechtschreibkorrekturprogramm aus dem Downloadshop erstanden, nachdem er dort ein Kundenkonto angelegt hatte. Die E-Mail-Adresse war beim Anlegen des Kontos abgefragt worden. In der Folge bestand ein Zusammenhang mit jedem Kauf, der über dieses Kundenkonto erfolgte.

- **Eigenwerbung für ähnliche Angebote (§ 7 Absatz 3 Nummer 2 UWG):**
  Die Frage, was man sich denn unter dieser „Ähnlichkeit“ von eigenen Waren oder Dienstleistungen vorzustellen habe, war für die Zulässigkeit der hier behandelten Werbe-E-Mail entscheidend. Nach einer Auslegung durch das OLG Jena[38] liegt eine solche Ähnlichkeit vor, wenn alle beworbenen Produkte dem gleichen typischen Verwendungszweck oder Bedarf wie die bereits gekauften Produkte dienen oder wenn sie ihnen als Zubehör zugerechnet werden können. Nach Ansicht des KG Berlin[39] reicht zudem eine lediglich teilweise Überschneidung der Verwendungszwecke nicht aus: Jemand, der ein Geduldsspiel kauft, braucht noch kein Interesse an Silvesterpartyartikeln zu haben, auch wenn durchaus eine Schnittmenge der Verwendungszwecke existieren mag (z. B. Geschenke für einen Party-Gastgeber).
  Im Fall des Verlags hatte der Kunde ein Rechtschreibkorrekturprogramm gekauft und daraufhin Werbung für ein elektronisches Bewerbungspaket (bestehend aus einer Vorlagensammlung, einem Ratgeber für Vorstellungsgespräche u. Ä.) erhalten. Dass sich das gekaufte Produkt auch zum „beworbenen“ Zweck sinnvoll verwenden ließe, war mir hier zu wenig, da aus dem Kauf eines sehr alltäglichen Produkts auf einen vergleichsweise spezialisierten Bedarf hätte geschlossen werden müssen. In der Folge war das der ausschlaggebende Grund, aus dem ich die fragliche Werbe-E-Mail als unzulässig bewertete.

- **Kein Widerspruch (§ 7 Absatz 3 Nummer 3 UWG):**
  Das ist inhaltlich die simpelste, erfahrungsgemäß aber dennoch eine konfliktträchtige Anforderung, da der Widerspruch in aller Regel elektronisch erfolgt und für den Betroffenen der Nachweis nicht immer einfach ist, dass der Widerspruch zugegangen ist. Auch der Verlag trug vor, nie einen Widerspruch vom Betroffenen erhalten zu haben. Da der Betroffenen aber nach dem Zeitpunkt des (strittigen) Widerspruchs ohnehin keine entsprechende Werbung mehr erhalten hatte, kam es hierauf nicht mehr an.

- **Belehrungspflicht (§ 7 Absatz 3 Nummer 4 UWG):**
  „Bei Erhebung … klar und deutlich“ bedeutet, dass der Hinweis nicht im Kleingedruckten un-

[38] Urteil vom 21. April 2010, 2 U 88/10

[39] Beschluss vom 18. März 2011, 5 W 59/11

tergehen oder anderswie am Adressaten vorbeigeschmuggelt werden darf. „Bei jeder Verwendung klar und deutlich“ fordert die Wiederholung dieser Belehrung bei jeder werblichen Ansprache. Im Fall des Verlags war am Inhalt und an der Präsentation der Belehrungen lediglich auszusetzen, dass durch die Formulierung „Sie hatten sich für den Empfang von Informationen unseres Downloadshops registriert“ dem Betroffenen gerade die falsche Rechtslage vermittelt wurde, was dann auch prompt zur Beschwerde geführt hatte.

Da mir der Verlag im Rahmen des datenschutzrechtlichen Verfahrens versicherte, inzwischen nicht mehr vom Privileg nach § 7 Absatz 3 UWG Gebrauch zu machen, konnte ich es in diesem Fall bei dem Hinweis darauf belassen, dass den Anforderungen an die Ähnlichkeit der beworbenen Produkte und an die Information über die Rechtslage genauer hätte nachgekommen werden müssen. Sanktionen kamen nicht in Betracht.

Eine gewissenhafte Einhaltung der gesetzlichen Anforderungen eröffnet Unternehmen das heutzutage bedeutende Feld der elektronischen Werbung. Dabei hat der Gesetzgeber durchaus mit Absicht vorgesehen, dass ein privilegiert werbendes Unternehmen im Gegenzug strenge Informationspflichten beachten und eine niederschwellige Widerspruchslösung bereithalten muss. Der infolge der kumulativen Voraussetzungen sehr enge Erlaubnistatbestand spiegelt wider, dass es sich bei dem Verzicht auf eine Einwilligung um die Ausnahme von der Regel handelt. Entsprechend streng werde ich die Inanspruchnahme des Privilegs für elektronische Werbung prüfen.

10.5 Datenschutz und digitales Wasserzeichen bei erworbenen und heruntergeladenen Musikdateien

Das Telekommunikations- oder Fernmeldegeheimnis bietet in seiner zeitgemäßen Ausprägung als Anonymität im Internet nicht nur dem unbedarften User, sondern leider auch illegalen Machenschaften den gewünschten Schutz, etwa wenn es um die unbefugte Weitergabe urheberrechtlich geschützter Werke wie Software oder Hörspiele geht. Die Rechtsverfolgung durch die Rechteinhaber mit Hilfe von IP-Adressen wurde im Jahr 2008 durch eine Novelle des Urheberrechtsgesetzes entscheidend erleichtert. Eine neuere Methode, die sich stattdessen eines dateigebundenen digitalen Wasserzeichens bedient, warf nun erneut datenschutzrechtliche Fragen auf.

Beim **Standard-Verfahren** werden Internet-Tauschbörsen nach urheberrechtlich geschützten Werken abgesucht. Wenn die hierfür genutzte Software das gesuchte Werk in der Tauschbörse findet, beginnt sie das betreffende Werk herunterzuladen. Dabei werden neben dem Hash-Wert des geschützten Werks noch Datum und Uhrzeit des Herunterladevorgangs sowie die zu diesem Zeitpunkt zugeteilte dynamische IP-Adresse des Anbieters, die Größe der Datei und die Netzwerkadresse des Software-Clients erhoben und gespeichert. Für die Zuordnung der IP-Adresse wird von einem Internet-Zugangsanbieter eine Auskunft über sog. Verkehrsdaten benötigt, die aufgrund des Verfassungsrangs des Fernmeldegeheimnisses strengen Regelungen nach dem Telekommunikationsgesetz unterworfen ist. Bis zur Änderung des Gesetzes über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, UrhG) im Jahr 2008 war die nötige Auskunft nur auf dem Weg der Strafanzeige bei der Staatsanwaltschaft zu erhalten.Weitere Einzelheiten sind dem vierten Tätigkeitsbericht des Innenministeriums aus dem Jahr 2007 zu entnehmen (Kapitel 12.1 „Identifizierung möglicher Urheberrechteverletzer in Internet-Tauschbörsen“, S. 218 ff).

Digitale Wasserzeichen dagegen werden direkt mit der einzelnen Datei verbunden. Technisch wird das bei einem Hörspiel oder bei Musik durch minimale Veränderungen der Aufzeichnungen auf der „Tonspur“ der Audiodatei verwirklicht, die für das Ohr des Konsumenten nicht hörbar sind, mit einer entsprechenden Software aber aufgelöst und dechiffriert werden können. Beim Download des Hörspiels aus dem Onlineshop des Verlags wird so jeder Kopie eine individuelle Information (in zusätzlich verschlüsselter Form) aufgeprägt, die fortan mit dieser Datei verbunden ist und auch bei einer Weitergabe oder Vervielfältigung dieser

Datei bestehen bleibt. Die Anbringung und die Verwaltung der Wasserzeichen übernahm als verantwortliche Stelle in einem von mir untersuchten Fall der Verlag, der auch den Onlineshop betrieb. Das Wasserzeichen ist verlagsintern dem Kunden zugeordnet, der die Datei aus dem Shop heruntergeladen hat. Für Dritte ist es der Konstruktion nach ein Pseudonym. Um Urheberrechtsverletzungen verfolgen zu können, werden Dateien zu geschützten Werken, die in Tauschbörsen angeboten werden, daraufhin untersucht, ob sie ein solches „Wasserzeichen" des Verlags tragen. Ist das der Fall, kann verlagsintern der Ersterwerber ermittelt werden, aus dessen „Händen" die Datei stammt. Telekommunikationsdaten werden für die Herstellung des ersten Personenbezugs daher nicht benötigt.

Ein erster wesentlicher Unterschied zwischen beiden Verfahren besteht darin, dass die Datei bis zu ihrer Veröffentlichung möglicherweise von Konsument zu Konsument weitergegeben wurde und folglich zwei ganz verschiedene Personen an entgegengesetzten Enden dieser Kette ins Visier der Verfolger geraten können, auch wenn derselbe Zweck verfolgt wurde.

Ein berechtigtes Interesse des Rechteinhabers an der Nutzung und daher auch an der Erhebung der fraglichen Identifikationsdaten steht bei keinem der Verfahren in Frage, da ihm zum einen ein Schadensersatzanspruch zustehen könnte, zum anderen die Verfolgung der Straftat nur auf seinen Antrag hin geschehen würde.

10.5.1 Verfolgung über die IP-Adresse am Ende der Kette

In der im Jahr 2004 zu beurteilenden Konstellation war das Ergebnis gewissermaßen unentschieden: Weder die schutzwürdigen Interessen der Betroffenen noch die urheberrechtlichen Interessen der Verletzten überwogen in überzeugendem Maß.

Die damals angekündigte Änderung des Urheberrechtsgesetzes trat am 1. September 2008 in Kraft und löste das Dilemma zugunsten der Erhebung ohne Mitwirkung des Betroffenen. Der neue § 101 Absatz 9 UrhG sieht seitdem die gesetzliche Möglichkeit vor, den Personenbezug von IP-Adressen mit Hilfe einer Auskunft durch den Internet-Zugangsanbieter herzustellen. Einzige Voraussetzung für diesen Eingriff in das Fernmeldegeheimnis ist eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten, für die lediglich ein Antrag des Verletzten erforderlich ist; insofern werden die Verkehrsdaten sogar ohne (vorherige) Kenntnis des Betroffenen erhoben.

Ob die vorgeschaltete richterliche Prüfung in dieser Fallkonstellation auch in der praktischen Umsetzung in jedem Fall ausreichenden Grundrechtsschutz gewährt oder ob gerade im typischen Rahmen von Massenverfahren (landläufig bekannt als „Abmahnwellen") die eingehende Prüfung des Einzelfalls leiden könnte, wie die schleswig-holsteinische Datenschutzaufsichtsbehörde in einer etwas anderen Konstellation annahm[40], kann nur die weitere Erfahrung zeigen.

10.5.2 Verfolgung über das digitale Wasserzeichen am Anfang der Kette

Was ist hier nun anders? Erhoben werden zunächst im Wesentlichen zwei völlig andere Daten, nämlich

- die Angabe, wer die angebotene Datei beim Verlag erworben hat (oder, mit anderer Stoßrichtung: die Datei welches Käufers angeboten wird), außerdem
- die Vermutung, dass der Ersterwerber gegen § 16, 17 oder 19a UrhG verstoßen und damit insbesondere eine Straftat nach § 106 UrhG begangen hat sowie möglicherweise zu Schadensersatz herangezogen werden kann.[41]

[40] Pressemitteilung „Abmahnwelle zeigt: IP-Adressen-Schutz ist wichtig - ULD gibt Tipps und warnt vor Trittbrettfahrern" des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 16. Dezember 2013

[41] Die Vermutung selbst mag auf den ersten Blick keine Einzel*angabe* i. S. der Definition von § 3 Absatz 1 BDSG sein. Allerdings werden aufgrund dieser Vermutung in aller Regel weitere, „unpersönliche" Angaben mit dem Betroffenen verbunden, denen das sog. Zweckelement gemein ist, dass sie der Ermittlung des Sachverhalts zulasten oder zugunsten des Betroffenen dienen oder dienen könnten.

Nicht erhoben werden (zumindest vom Konzept her) Drittdaten sowie insbesondere keine Telekommunikationsdaten, weder desjenigen, der die Datei anbietet, noch des hier vom Wasserzeichen Betroffenen.

Wiederum entsteht ein Dilemma daraus, dass die Daten zwar aufgrund berechtigten Interesses, aber nicht beim Betroffenen erhoben werden und keine Rechtsvorschrift die heimliche Erhebung vorsieht.

Die Änderung des Urheberrechtsgesetzes hilft hier nicht weiter. Im Gegenteil könnte sie die Erforderlichkeit dieses Werkzeugs nun erst recht in Frage stellen, da dem Verletzten ja der Zugriff auf die Verletzenden grundsätzlich offensteht, indem er vom Ende der Kette her jeden Beteiligten auf Auskunft über die (direkte) Herkunft der Datei in Anspruch nehmen und sich so Glied um Glied zum mutmaßlichen Erstverletzer vorarbeiten kann, der die Datei bei ihm bzw. beim Verlag zunächst rechtmäßig erworben hatte. Das ist ein vom Gesetz gebahnter Weg. Andererseits ändert sich durch die „Abkürzung“ für den Betroffenen und seine Daten im Ergebnis nichts, da auch sämtliche Daten entlang der Kette einschließlich seiner eigenen ohne seine Mitwirkung erhoben werden.

Die Unkenntnis des Betroffenen beschränkt sich auf den konkreten Zusammenhang sowie den Zeitpunkt und ggf. den Ort der Erhebung, sofern er bereits beim Kauf umfassend über das digitale Wasserzeichen einschließlich der Zwecke und der Anwendung unterrichtet wird, was sowohl aufgrund der allgemeinen Unterrichtungspflichten nach § 4 Absatz 3 BDSG als auch zur Milderung des eventuellen Eingriffs unbedingt nötig ist. Meiner diesbezüglichen Forderung kam der Verlag schon deshalb nach, weil er sich von einem entsprechenden Hinweis vor dem Kauf auch eine präventive Wirkung versprechen konnte.

In den hochrangigen Schutzbereich des Fernmeldegeheimnisses wird nicht eingegriffen; insbesondere wird auch die Hürde der richterlichen Anordnung nicht umgangen. Die Erhebung der Verkehrsdaten ist nämlich nicht Zweck des gesetzlich eingeräumten Vorgehens, sondern nur Mittel zum Zweck einer vornehmlich außerhalb des Telekommunikationsbereichs angesiedelten Rechtsverfolgung.

Insgesamt ist der anvisierte Eingriff selbst in datenschutzrechtlicher Hinsicht daher als milder zu werten als die Inanspruchnahme von Telekommunikationsdaten. Da nach bisheriger Rechtsprechung[42] die Erschöpfung der Verbreitungsrechte beim Download urheberrechtlich geschützter Werke i. S. von § 17 Absatz 2 UrhG gerade nicht eintritt, dürfte auch ein hinreichender Verdacht gegen den Ersterwerber als Erstverletzer begründet sein.

Zu bedenken ist allerdings, dass die Datei in jedem Fall (pseudonyme) Daten des Erstverletzers ggf. auch unabhängig von seinem Verschulden in die Welt hinausträgt. Im äußersten Fall könnten von Dritten aus einer großen Zahl entsprechender Dateien neue pseudonyme Profile erstellt werden, mit deren Hilfe auch ein brauchbarer Personenbezug nicht mehr völlig ausgeschlossen werden kann.

Ob unter diesen Gesichtspunkten eine Interessenlage vorliegt, die die Datenerhebung ohne Mitwirkung des Betroffenen i. S. von § 4 Absatz 2 Satz 2 Nummer 2 Buchstabe a Alternative 2 BDSG im Rahmen des Geschäftszweck erfordert und die schutzwürdigen Interessen des Betroffenen in der Abwägung unterliegen lässt, sollte vorsichtshalber in jedem Einzelfall vorab konkret geprüft werden. Nach Angaben des Verlags war ein entsprechender Nachforschungsauftrag bisher allerdings noch von keinem Rechteinhaber erteilt worden. Das Verfahren an sich zu untersagen scheint mir jedenfalls noch nicht angezeigt zu sein.

Wesentliche Voraussetzung für diese vorsichtig bejahende Einschätzung ist allerdings, dass beim Download urheberrechtlich geschützter Werke keine Erschöpfung der entsprechenden Verwertungsrechte eintritt und daher insbesondere auch gegen den Ersterwerber der Datei bereits infolge der Entdeckung der Datei in einer Tauschbörse ausreichender Verdacht eines Rechtsbruchs besteht.

[42] z. B. OLG Stuttgart, Urteil „Hörbuch-AGB“ vom 3. November 2011, Aktenzeichen 2 U 49/11

Sofern sich daher in Zukunft die Rechtsprechung des Europäischen Gerichtshofs[43] hinsichtlich des Weiterverkaufs gebrauchter Softwarelizenzen - wonach sich grundsätzlich auch Verwertungsrechte an nichtkörperlichen, online erworbenen Kopien erschöpfen können - auch auf die Rechtslage bei Hörspieldateien auswirken sollte, müsste in der Folge auch diese datenschutzrechtliche Einschätzung sicherlich nochmals überdacht werden.

Die Rechtsverfolgung im Internet wirft nach wie vor grundsätzliche Fragen auf. Zwar wurde 2008 durch die einfachgesetzliche Einschränkung eines Grundrechts die Position der Rechteinhaber gestärkt. Doch führt der vom Gesetzgeber gebahnte Weg noch immer mit Hilfe hoheitlichen Eingreifens durch eine geschützte Sphäre. Auch wenn noch viele Fragen offen sind, sollte neuen Lösungsansätzen jedenfalls Raum und die nötige juristische Aufmerksamkeit gewährt werden.

10.6 Geldwäscheprävention und Beschäftigtendatenschutz

Die grundsätzliche Erforderlichkeit von Maßnahmen zur Geldwäscheprävention ist - auch soweit sie den Beschäftigtendatenschutz berührt - unbestritten. Es bedarf hierfür jedoch klarer Regelungen, um eine unverhältnismäßige Mitarbeiterkontrolle auszuschließen.

Die vom Gesetzgeber geforderten **Datenverarbeitungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung** machen auch vor Beschäftigtendaten nicht halt. Dies verdeutlicht z. B. die zum 1. März 2012 in Kraft getretene Änderung des § 9 Absatz 2 Nr. 4 des Geldwäschegesetzes (GwG) über die „internen Sicherungsmaßnahmen“. Bis dahin hatten die verantwortlichen Stellen lediglich sicherzustellen, dass die mit der Durchführung von Transaktionen und mit der Anbahnung und Begründung von Geschäftsbeziehungen befassten Beschäftigten über die Methoden der Geldwäsche und der Terrorismusfinanzierung sowie über die Pflichten nach dem GwG unterrichtet werden.

Die Änderung des § 9 Absatz 2 Nr. 4 GwG hat die Rechtslage jedoch deutlich verschärft. Zu den von den verpflichteten Stellen zu treffenden internen **Sicherungsmaßnahmen** gehören nunmehr auch geeignete risikoorientierte Maßnahmen zur Prüfung der Zuverlässigkeit der Beschäftigten. Unklar bleibt allerdings, wie diese Prüfung zu erfolgen hat. In Anbetracht des rechtsstaatlichen Verhältnismäßigkeitsgrundsatzes ist eine regelmäßige Einholung von Führungszeugnissen und Bonitätsabfragen zu allen Mitarbeitern - unabhängig vom konkreten Einsatzgebiet des jeweiligen Beschäftigten - jedenfalls rechtswidrig. Nach der Begründung des Gesetzentwurfs (BT-Drs. 17/6804, S. 34) haben die verpflichteten Arbeitgeber bei der Kontrolle der Zuverlässigkeit der Beschäftigten auch im laufenden Arbeitsverhältnis hinsichtlich der Kontrolldichte und der einzusetzenden Kontrollinstrumente einen risikoangemessenen **Beurteilungsspielraum**. Dessen praktische Anwendung sei gegenüber den für die Kontrolle der geldwäscherechtlichen Vorschriften zuständigen Behörden im Einzelfall plausibel darzulegen.

Für Unternehmen, die einerseits ihren pflichtgemäßen Beitrag zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung leisten und andererseits unverhältnismäßige und damit unzulässige Datenerhebungen vermeiden wollen, wäre eine klarere Regelung wünschenswert, um ein höheres Maß an Rechtssicherheit zu schaffen. Insoweit wäre daher eine Klarstellung seitens des Gesetzgebers zu begrüßen.

Meine Dienststelle wird auch in Zukunft die Gesetzgebung im Bereich des Geldwäschepräventionsrechts kritisch beobachten.

[43] Urteil „UsedSoft“ vom 3. Juli 2012, Rechtssache C-128/11

10.7 Der übereifrige Hausverwalter

Immer wieder erhalte ich Beschwerden von erbosten Wohnungseigentümern, deren Hausverwaltung unaufgefordert an alle Eigentümer der Wohnanlage Listen verschickt, auf denen Hausgeldabrechnungen sowie Strom- und Gasverbrauchsdaten zu jedem einzelnen Eigentümer aufgeführt sind, so dass jeder Hausbewohner feststellen kann, was der Nachbar verbraucht und zu zahlen hat. Das Unbehagen der Eigentümer ist nur zu gerechtfertigt.

Die Hausverwaltung dürfte solche personenbezogenen **Abrechnungsdaten** an alle Wohnungseigentümer **ohne Einwilligung der Betroffenen** nur versenden, wenn dies für die Erfüllung der Pflichten aus dem Verwaltervertrag erforderlich wäre und kein Grund zu der Annahme bestünde, dass ein entgegenstehendes schutzwürdiges Interesse des betroffenen Miteigentümers überwiegt. Es fehlt jedoch bereits an der Erforderlichkeit der Versendung, da der Verwalter hierzu grundsätzlich nicht verpflichtet ist. Zwar hat er den Wohnungseigentümern **Einsicht in die Abrechnungsunterlagen** zu gewähren. Zur Erfüllung dieser Pflicht genügt es aber bereits, wenn diese Unterlagen den Einsichtsberechtigten auf Verlangen offengelegt werden. Die Offenlegung hat somit nur zu erfolgen, wenn der Einsichtsberechtigte gegenüber dem Verwalter erklärt hat, dass er Einsicht in die Abrechnungsunterlagen wünsche. Hinzu kommt, dass das Einsichtsrecht grundsätzlich beim Verwalter auszuüben ist. Der einzelne Miteigentümer kann aus den Unterlagen des Verwalters Fotokopien fertigen, hat aber keinen Anspruch gegen den Verwalter auf Übersendung solcher Kopien. Denkbar ist auch eine elektronische Einsichtnahme in die Abrechnungsunterlagen bei sicherer Authentifizierung des die Einsicht begehrenden Eigentümers.

Gegen eine Pflicht der Hausverwaltung zur unaufgeforderten **Übersendung** der genannten Listen spricht auch, dass die Kenntnis der Einzelabrechnungen für die Beschlussfassung über die Jahresabrechnung in der Eigentümerversammlung nicht notwendig ist. Jeder Miteigentümer kann bereits aus der ihn betreffenden Einzelabrechnung ersehen, nach welcher Methode der Verwalter die Einzelabrechungen, auf denen die Gesamtjahresabrechnung beruht, erstellt hat. Für die Kontrolle, ob die anderen Einzelabrechungen konsequent nach derselben Methode erstellt worden sind, kann der einzelne Miteigentümer auf sein Einsichtsrecht beim Verwalter verwiesen werden. Dies ist jedenfalls dann ausreichend, wenn der Verwalter die Miteigentümer auf die Möglichkeit der Einsichtnahme hingewiesen hat.

Schließlich ist die Übersendung auch nicht erforderlich, um der Wohnungseigentümergemeinschaft die Geltendmachung ihrer Zahlungsansprüche gegen säumige Eigentümer zu ermöglichen. Denn für eine effektive Durchsetzung der Gemeinschaftsansprüche reicht es aus, wenn der Verwalter den Wohnungseigentümern zunächst die Anzahl der säumigen Mitglieder und die Höhe der von ihnen geschuldeten Beträge in anonymisierter Form mitteilt. Die Wohnungseigentümergemeinschaft kann dann durch Beschluss entscheiden, dass der Verwalter die Namen der Schuldner offenlegen soll, wenn dies beispielsweise notwendig ist, um die Erfolgaussichten einer gerichtlichen Geltendmachung abzuschätzen. Ein berechtigtes Interesse an der unaufgeforderten Übersendung der Hausgeldtabelle oder der Einzelabrechungen ist daher auch unter diesem Aspekt zu verneinen.

Hingegen kommt ein schutzwürdiges Interesse des betroffenen Eigentümers am Ausschluss der Übermittlung jedenfalls dann in Betracht, wenn er der Ansicht ist, dass die offenen Hausgeldforderungen ganz oder teilweise unberechtigt sind. Zudem erlauben die Angaben zum Strom- und Gasverbrauch zumindest in begrenztem Umfang Rückschlüsse auf seine persönliche Lebensgestaltung. Für die Schutzwürdigkeit seines Interesses spricht auch, dass in der Regel eine Vielzahl von Miteigentümern keine Einsicht in die Abrechnungsunterlagen wünscht und die Geltendmachung offener Hausgeldforderungen dem Hausverwalter überlässt.

Die unaufgeforderte Übersendung personenbezogener Abrechnungsdaten an alle Eigentümer einer Wohnungseigentümergemeinschaft ist datenschutzrechtlich unzulässig.

10.8 Die verweigerte Selbstauskunft

Der Auskunftsanspruch des Betroffenen dient der Durchsetzung seines Grundrechts auf informationelle Selbstbestimmung. Seine Erfüllung ist daher von essentieller Bedeutung für einen effektiven Datenschutz.

Vereinzelt kommt es vor, dass ein Versicherungskunde den Eindruck gewinnt, Informationen zu seinen Versicherungsverträgen seien durch einen Versicherungsmitarbeiter gegen seinen Willen an seinen Bekanntenkreis gelangt. Ein hiervon Betroffener bat daraufhin die Versicherung um **Selbstauskunft** nach § 34 BDSG darüber, an wen seine personenbezogenen Daten weitergegeben worden seien. Erstaunen mischte sich mit Ärger, als die Versicherung die Selbstauskunft mit dem Hinweis auf entgegenstehende Geschäftsgeheimnisse und auf ihre arbeitsrechtliche Fürsorgepflicht verweigerte. Die Selbstauskunft könne nicht erteilt werden, weil im Fall der Rechtswidrigkeit einer Datenweitergabe der offenherzige (ehemalige) Mitarbeiter mit Schadensersatzforderungen seitens des betroffenen Kunden rechnen müsse.

Eine Verweigerung der Selbstauskunft aus den vorgenannten Gründen kommt hier jedoch nicht in Betracht. Zwar kann die verantwortliche Stelle die Auskunft über die Empfänger der bei ihr gespeicherten personenbezogenen Daten verweigern, soweit das Interesse an der Wahrung ihres Geschäftsgeheimnisses gegenüber dem Interesse des Betroffenen überwiegt. Das Vorliegen eines solchen Geheimnisses kann aber nicht damit begründet werden, dass das Unternehmen aufgrund der arbeitsrechtlichen Fürsorgepflicht gegenüber seinem ehemaligen Mitarbeiter verpflichtet sei, diesen vor zivil- oder strafrechtlichen Sanktionen zu bewahren. Zudem ist die Information über einen begangenen Datenschutzverstoß nicht als Geschäftsgeheimnis anzusehen.

Selbst wenn die Erteilung der Selbstauskunft ein **Geschäftsgeheimnis** des Unternehmens berühren würde, dürfte das Interesse an dessen Wahrung nicht das Interesse an der Auskunftserteilung überwiegen. Zweck des Selbstauskunftsanspruchs ist es gerade, die Geltendmachung weiterer Rechte des Betroffenen, wie beispielsweise auch Schadensersatzansprüche wegen Verletzung des informationellen Selbstbestimmungsrechts, zu ermöglichen. Dies spricht in der Regel für ein Überwiegen des Auskunftsanspruchs. Das muss erst recht gelten, wenn das entgegenstehende Interesse der verantwortlichen Stelle allein darauf gerichtet ist, die Geltendmachung solcher Ansprüche gegen sich selbst und ihre Mitarbeiter zu verhindern.

Unternehmen sollten die datenschutzrechtlichen Auskunftsansprüche ihrer Kunden auch dann erfüllen, wenn diese die Selbstauskunft in einem Rechtsstreit wegen fehlerhafter Datenweitergabe gegen sie verwenden könnten.

10.9 Datenübermittlungen an Auskunfteien bei Anfragen nach Kreditkonditionen

Damit Bankkunden auf der Suche nach dem günstigsten Kredit nicht am Ende die Dummen sind, müssen Banken bei Kreditkonditionenanfragen große Sorgfalt im Umgang mit Auskunfteien üben.

Kreditinstitute dürfen an Auskunfteien nicht nur unter den Voraussetzungen des § 28a Absatz 1 BDSG personenbezogene Daten ihrer Kunden übermitteln. Dies gilt zum einen für Angaben zu nicht oder zu spät beglichenen Forderungen gegen ihre Kunden (sog. Negativdaten), wobei die Voraussetzungen nach § 28a Absatz 1 BDSG einzuhalten sind. Zum anderen dürfen Kreditinstitute nach § 28a Absatz 2 BDSG auch Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung bestimmter Arten von Bankgeschäften an Auskunfteien (sog. Positivdaten) weitergeben. Ein pünktlich und regelmäßig zurückgezahlter Kredit kann dabei als Anzeichen für eine hohe Zahlungsfähigkeit und Zahlungswilligkeit gewertet werden. Darüber hinaus lässt sich anhand der Positivdaten feststellen, ob das Gesamt-

volumen der vom Kunden aufgenommenen Kredite ihn finanziell zu überfordern droht, so dass eine weitere Kreditvergabe mit einem erhöhten finanziellen Ausfallrisiko verbunden wäre.

Dieser Eindruck kann jedoch fälschlicherweise entstehen, wenn bereits jede Anfrage eines Betroffenen nach den Konditionen, zu denen ihm ein Kredit gewährt werden kann, an Auskunfteien gemeldet und dort als Antrag auf Einräumung eines Kredits gewertet wird. Dies kann insbesondere dann geschehen, wenn die Bank zur Ermittlung der **Kreditkonditionen** eine Bonitätsprüfung bei einer Auskunftei durchführt und dabei als Grund für die Abfrage angibt, dass der Abschluss eines Kreditvertrags bevorstehe. Der Kunde, der als kritischer Verbraucher das für ihn günstigste Kreditangebot ermitteln will, wird zu diesem Zweck bei einer Vielzahl von Banken nach den für ihn geltenden Kreditkonditionen anfragen. Finden diese Anfragen Eingang in den Auskunfteidatenbestand, so besteht die Gefahr, dass diese zum Betroffenen aufgrund seines vermeintlich enormen Kreditbedürfnisses nur noch schlechte Bonitätsauskünfte erteilt.

Der Gesetzgeber hat diese Gefahr erkannt. § 28a Absatz 2 Satz 4 BDSG bestimmt daher:

> Kreditinstitute dürfen einer Auskunftei nur dann melden, dass der Betroffene nach Kreditkonditionen gefragt hat, wenn die Auskunftei diese Anfrage nicht in ihre Bonitätsauskunft gegenüber Dritten einbezieht.

Eine Erhebung meiner Dienststelle bei zwei Bankenverbänden und sechs Kreditinstituten im Land ergab, dass die Banken dieser Anforderung des Datenschutzrechts genügen. In der Mehrzahl der Fälle ermitteln die Kreditinstitute die einschlägigen Kreditkonditionen, indem sie die hierfür erforderlichen Daten direkt beim Betroffenen erfragen, ohne auf Bonitätsdaten von Auskunfteien zurückzugreifen. Einige Banken holen mit Einverständnis des Kunden eine Bonitätsauskunft bei der Schufa ein. Dabei geben sie gegenüber dieser an, dass dies nur zur Ermittlung von Kreditkonditionen erfolgt. Aufgrund des zwischen den Banken und der Schufa geschlossenen Vertrags darf diese Information nicht in den Auskunftsdatenbestand der Auskunftei übernommen werden. Die Angabe, dass der Kunde eine Kreditkonditionenanfrage gestellt hat, erfolgt daher nicht „zur zukünftigen Übermittlung“ durch die Auskunftei im Rahmen von Bonitätsauskünften an Dritte.

Meine Dienststelle wird auch künftig darauf achten, dass die Kreditinstitute bei der Zusammenarbeit mit Auskunfteien die Vorgaben des Datenschutzrechts beachten.

10.10 Bei Anruf Bonitätsbeichte

Dass Wirtschaftsauskunfteien personenbezogene Bonitätsdaten sammeln, ist im Grundsatz zu akzeptieren. Der Sammeleifer geht aber zu weit, wenn die Betroffenen am Telefon zu ihrer Bonität ausgefragt werden.

Ein Bürger unseres Landes fühlte sich empfindlich gestört, als eine Auskunftei bei ihm anrief, um ihn nach seiner Bonität zu befragen. Da in frei zugänglichen Informationsquellen, wie z. B. öffentlichen Registern, ihrer Ansicht nach keine aussagekräftigen Daten vorhanden waren, wandte sie sich nunmehr direkt an ihn. Die Telefonnummer hatte sie der Homepage des betroffenen Bürgers entnommen.

Der **Anruf der Auskunftei** beim Bürger war rechtswidrig. Zwar ist eine Auskunftei berechtigt, im Rahmen der Gesetze die Daten zu erheben, die sie zur Beauskunftung ihrer Kunden benötigt. Weiterhin trifft es zu, dass personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind. Dies berechtigt die Auskunftei in der Regel aber nicht dazu, den Betroffenen anzurufen. Denn in der telefonischen Kontaktaufnahme zum Betroffenen liegt eine Nutzung von personenbezogenen Daten, nämlich seiner Telefonnummer, zum Zweck der Datenerhebung. Auch eine solche Nutzung ist ohne Einwilligung des Betroffenen nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet. Das Bundesdatenschutzgesetz erlaubt die Nutzung personenbezogener Daten für

eigene Geschäftszwecke, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und das entgegenstehende schutzwürdige Interesse des Betroffenen nicht überwiegt.

Die Erforderlichkeit der telefonischen Kontaktaufnahme zur Sammlung von Bonitätsdaten darf schon deshalb bezweifelt werden, weil der Auskunftei hierfür auch der Postweg zur Verfügung steht. Jedenfalls überwiegt aber das schutzwürdige Gegeninteresse des Betroffenen, denn der Anruf stellt eine unzumutbare Belästigung i. S. des Gesetzes gegen den unlauteren Wettbewerb dar. Eine Belästigung ist schon deshalb anzunehmen, weil der Anrufer dem Adressaten sein Anliegen mit dem Anruf derart aufdrängt, dass der Angerufene sich gegen seinen Willen damit befassen muss.

Zur Beantwortung der Frage, ob die mit dem Telefonanruf verbundene Belästigung unzumutbar ist, bedarf es einer Abwägung zwischen den Interessen der Auskunftei und denen des betroffenen Adressaten. Zulasten der Auskunftei ist zu berücksichtigen, dass ihr mit den amtlichen Schuldnerverzeichnissen und den amtlichen Insolvenzbekanntmachungen sowie aus Meldungen unbeglichener Forderungen genug andere Quellen für Bonitätsdaten des Betroffenen zur Verfügung stehen, auch wenn diese im konkreten Fall nicht ergiebig sein mochten. Zugunsten des Betroffenen ist darüber hinaus die Gefahr einer Summierung von Belästigungen zu berücksichtigen, falls andere Auskunfteien ebenfalls bei ihm Bonitätsdaten telefonisch abfragen.

Der Betroffene willigt auch nicht dadurch stillschweigend in die Kontaktaufnahme ein, dass er seine gewerbliche Telefonnummer auf der Homepage seines eigenen Unternehmens bekannt gegeben hat. Es ist anerkannt, dass die bloße Bekanntgabe der Telefonnummer in Telefonbüchern, auf Visitenkarten oder in Briefköpfen nicht Ausdruck der Bereitschaft ist, mit jedem Kontakt aufnehmen zu wollen. Dies gilt daher auch bei Angabe der Telefonnummer auf der eigenen Homepage.

Auskunfteien dürfen die Betroffenen nicht mit unerwünschten Telefonanrufen behelligen.

10.11 Auskunft unter Vorbehalt

Wirtschaftsauskunfteien verfolgen den Geschäftszweck, Anfragen von Unternehmen zur Bonität potentieller Geschäftspartner zu beantworten, damit diese beurteilen können, inwieweit ein Geschäft für sie mit finanziellen Risiken verbunden ist. Doch können die Auskunfteien der Wirtschaft nur behilflich sein, wenn ihre Auskünfte der Wahrheit entsprechen. Unzutreffende Informationen sind nicht nur geeignet, die Persönlichkeit des Betroffenen zu schädigen, sie würden auch dazu führen, dass der anfragenden Stelle möglicherweise ein lukratives Geschäft entgeht, wenn der Geschäftspartner zu Unrecht von der Auskunftei als kreditunwürdig eingeschätzt wird.

Angesichts der zahlreichen Einmeldungen von sog. Bonitätsnegativmerkmalen bei den Auskunfteien erwartet die Rechtsprechung nicht von diesen, dass sie stets jede Speicherung auf ihre inhaltliche **Richtigkeit** überprüfen. Die Verantwortung für die Korrektheit der Einmeldung liege bei der Stelle, die die Auskunftei vom abträglichen Zahlungsverhalten eines Schuldners informiert. Auf dieses Privileg können sich die Auskunfteien aber dann nicht berufen, wenn sie selbst mehr oder weniger willkürlich Anfragen mit Angaben beantworten, die nahezu zwingend den Betroffenen in Misskredit bringen. So wurde die Bonitätsanfrage eines Unternehmens zu einer bestimmten Person mit der Auskunft beantwortet, zu dieser würden keine **Bonitätsnegativmerkmale** vorliegen, wohl aber zu einer Person mit ähnlichen Personalien. Der Betroffene, auf den sich die Anfrage bezog, erhielt daraufhin weder einen Kredit noch einen Handyvertrag. Eine solche unüberlegte Auskunft genügt, um einen Menschen zumindest teilweise von der Teilnahme am Geschäftsverkehr auszuschließen.

Die betroffene Auskunftei wollte ihr Vorgehen damit rechtfertigen, dass es immer wieder vorkomme, dass Betrüger sich ähnlicher Identitäten bedienen würden, um Leistungen zu erschleichen. Dass die Auskunfteien daran mitwirken wollen,

solches zu verhindern, ist datenschutzrechtlich nicht zu kritisieren. Doch dann muss von ihnen - wie gesagt, sowohl im Interesse des Betroffenen wie auch zu Gunsten des anfragenden Unternehmens - erwartet werden, dass sie in ausreichendem Maße prüfen, ob auch der „abweichende“ Datensatz sich auf die angefragte Person bezieht. Die gegenteilige Vorgehensweise ist rechtswidrig (vgl. OLG Hamburg, Beschl. v. 23. Januar 1987 - 11 W 96/86 -) und wurde von den Aufsichtsbehörden (AG Auskunfteien des Düsseldorfer Kreises) als nicht akzeptabel abgelehnt.

10.12 Das Register nach §§ 38 Absatz 2, 4d, 4e BDSG - wer muss was an die Aufsichtsbehörde melden?

Häufig wird die Frage an mich herangetragen, was seitens nicht-öffentlicher Stellen in das bei der Aufsichtsbehörde geführte Register nach § 38 Absatz 2 BDSG gemeldet werden müsse.

Nach § 4d BDSG müssen nicht-öffentliche Stellen Verfahren automatisierter Datenverarbeitung vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde (für alle Unternehmen und Vereine ist dies in Baden-Württemberg meine Dienststelle) melden. Die Aufsichtsbehörde führt gem. § 38 Absatz 2 BDSG ein Register dieser Meldungen (sog. „**Verfahrensregister**“; eine strukturierte Sammlung der eingehenden Meldedokumente), das, bis auf die gemeldeten Datensicherungsmaßnahmen und die gemeldeten zugriffsberechtigten Personen, von jedermann voraussetzungsfrei eingesehen werden kann.

Diese Meldepflicht entfällt immer dann, wenn

- die verantwortliche Stelle einen (betrieblichen) Beauftragten für den Datenschutz bestellt hat (§ 4d Absatz 2 BDSG) *oder*

- die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (§ 4d Absatz 3 BDSG).

Im Regelfall besteht daher keine Meldepflicht.

Der Meldepflicht unterliegen Verfahren automatisierter Verarbeitung von personenbezogenen Daten nach § 4d Abs. 4 BDSG aber grundsätzlich immer dann (also unabhängig von den beiden eben genannten Ausnahmen), wenn diese Daten geschäftsmäßig

- zum Zweck der Übermittlung (§ 29 BDSG, z. B. Auskunfteien, Adresshändler) oder
- zum Zweck der anonymisierten Übermittlung (§ 30 BDSG) oder
- zum Zweck der Markt- oder Meinungsforschung (§ 30a BDSG)

gespeichert werden.

Die Meldung selbst stellt keinen Antrag auf Überprüfung der Datenverarbeitungsverfahren durch die Aufsichtsbehörde dar. Eine solche Vorabkontrolle ist nur in besonders sensiblen und risikobehafteten Fällen der Datenverarbeitung nach § 4d Absatz 5 BDSG erforderlich. Für diese Kontrolle ist nicht die Aufsichtsbehörde, sondern der betriebliche Datenschutzbeauftragte zuständig, § 4d Absatz 6 BDSG. Ein Unternehmen ist gem. § 4f Absatz 1 Satz 6 BDSG stets zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet, wenn die Datenverarbeitung einer Vorabkontrolle bedarf.

Was sind die Inhalte der Meldepflicht?

Die Inhalte dieser Meldung richten sich nach § 4e BDSG. Zur strukturierten Erfassung bietet meine Dienststelle Vorlagen zum Herunterladen auf ihrer Internetseite an (http://www.baden-wuerttemberg.datenschutz.de/orientierungshilfen-merkblatter/ <Sonstiges>). Erfasst werden Angaben zur Identifizierung der verantwortlichen Stelle (§ 4e Satz 1 Nummern 1 bis 3 BDSG), die Beschreibungen der einzelnen Datenverarbeitungs-

verfahren (IT-Prozesse; § 4e Satz 1 Nummern 4 bis 8 BDSG) sowie als nicht-öffentlicher Teil die Angaben zu technischen und organisatorischen Maßnahmen (§ 4e Satz 1 Nummer 9 BDSG).

§ 4e Satz 2 BDSG stellt sicher, dass jede Änderung der gemeldeten Angaben unaufgefordert der Aufsichtsbehörde zu melden ist, um das Register aktuell zu halten. Ein Verstoß gegen die Meldepflicht ist nach § 43 Absatz 1 Satz 1 Nummer 1 BDSG bußgeldbewehrt.

Was ist der Unterschied zwischen der Meldepflicht, der Verfahrensübersicht und dem sog. Verfahrensverzeichnis?

Auch wenn die Meldepflicht nach § 4d Absätze 2, 3 BDSG entfällt, muss jedes Unternehmen zumindest eine (interne) Verfahrensübersicht erstellen (Transparenz nach innen). Dies ergibt sich aus § 4g Absatz 2 Satz 1 BDSG: *„Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen.“* Diese Verfahrensübersicht ist sozusagen die Arbeitsgrundlage für den betrieblichen Datenschutzbeauftragten. Der betriebliche Datenschutzbeauftragte muss die Inhalte des § 4e Satz 1 Nr. 1 bis 8 BDSG dieser Verfahrensübersicht (also alles aus der Verfahrensübersicht bis auf den Bereich Daten-Sicherheitsmanagement) auf Antrag für jedermann zugänglich machen, § 4g Absatz 2 Satz 2 BDSG. Dieses öffentlich zugängliche Papier wiederum nennt man Verfahrensverzeichnis (Transparenz nach außen) oder auch „Jedermannverzeichnis“. Teilweise veröffentlichen Unternehmen dieses Verzeichnis auf ihrer Internetseite, was Auskünfte erleichtern kann.

Wenn es keinen betrieblichen Datenschutzbeauftragten gibt, muss nach § 4g Absatz 2a BDSG der Leiter der nicht-öffentlichen Stelle (z. B. der Geschäftsführer des Unternehmens, der Firmenchef) dafür sorgen, dass in ein solches Verfahrensverzeichnis Einblick genommen werden kann.

11. Technik und Medien

11.1 Videoüberwachung

11.1.1 Einleitung

Der Abschnitt Videoüberwachung ist - leider - zu einem festen Bestandteil meines Tätigkeitsberichts geworden. Wir bewegen uns offenkundig auf eine flächendeckende Überwachungsinfrastruktur zu. Videoüberwachungskameras gehören zu unserem Alltag: in der S-Bahn, im Kaufhaus, im Parkhaus, im Restaurant, an Tankstellen oder in Wohnanlagen, mitunter auch in der Fußgängerzone oder auf bestimmten öffentlichen Plätzen. Gerade im Hinblick auf die fortschreitende Technik (Erhöhung der Speicherkapazitäten, Digitalisierung, Zoomfunktion, Gesichtserkennung oder intelligente Bildinterpretation) kann der Einsatz von Videotechnik im öffentlichen Raum einen latenten Überwachungsdruck auslösen, zu Misstrauen und Unsicherheit führen und die Unbefangenheit menschlichen Verhaltens beeinträchtigen. Die Videoüberwachung ist inzwischen zu einer „Jedermann-Technik" geworden, die sich vergleichsweise kostengünstig installieren und einfach betreiben lässt, so dass auch Privatpersonen immer häufiger Kameras einsetzen. Es muss auch nicht mehr der Computer eingeschaltet werden, um die Bilder zu betrachten; häufig reicht schon der Blick auf das Smartphone, auf das die Aufnahmen drahtlos übertragen werden. Die Zahl der Anfragen und Beschwerden, die meine Dienststelle erreichen, steigt stetig an.

Angesichts des Umfangs unzulässiger **Videoüberwachung** muss man von einem **Kampf der Aufsichtsbehörden gegen Windmühlen** sprechen. Diese haben den Kampf jedoch aufgenommen und sich aufgrund der zunehmenden Bedeutung des Themas sowie der Breite der auftretenden Fragen in der Prüfpraxis zu einer Ad-hoc-Arbeitgemeinschaft „Videoüberwachung" zusammengeschlossen, die sich im Januar und im November 2013 unter der Federführung meiner Dienststelle in Stuttgart getroffen hat. Ihr Ziel ist, den Erfahrungs- und Meinungsaustausch unter den Aufsichtsbehörden zu fördern und Leitlinien für eine einheitliche Rechtsauslegung zu erarbeiten. Die Arbeitsgruppe beschäftigt sich mit zahlreichen Auslegungsfragen und Fallkonstellationen, von der Beurteilung von Videoüberwachung in Schwimmbädern über Wildkameras oder dem Einsatz von sog. Dashcams in privaten Fahrzeugen bis hin zur Diskussion neuer Entwicklungen wie Google Glass. Darüber hinaus soll eine gemeinsame Orientierungshilfe der Aufsichtsbehörden des Bundes und der Länder für den zulässigen Einsatz von Videotechnik erarbeitet werden.

11.1.2 Videoüberwachung in und an Taxis

Im Berichtszeitraum musste ich mich gemeinsam mit meinen Kollegen in den anderen Ländern mit dem Thema Videoüberwachung in und an Taxis beschäftigen. Hintergrund waren Gespräche mit verschiedenen Taxiverbänden, die unter der Federführung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen stattfanden.

Das Anliegen vieler Taxiunternehmen ist es, ihre Fahrzeuge sowohl mit Innen- als auch mit Außenkameras auszustatten. Von der **Innenkamera** verspricht man sich, Überfälle auf Taxifahrer und Taxifahrerinnen zu verhindern oder zumindest besser aufzuklären. Die **Außenkamera** soll dazu dienen, Geschehensabläufe besser rekonstruieren sowie kritische Verkehrssituationen und Unfälle nachvollziehen und auswerten zu können. Diese Bildaufnahmen sollen insbesondere bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen im Zusammenhang mit anderen Unfallbeteiligten als Nachweis herangezogen werden.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich bewerten beide Kameratypen als datenschutzrechtlich kritisch. Der Düsseldorfer Kreis hat sich in seinem Beschluss vom 26./27. Februar 2013 (s. Anhang 24) zu der Erforderlichkeit einer Videoüberwachung durch Taxiunternehmen wie folgt geäußert:

Eine anlasslose Videoüberwachung des Fahrzeuginnenraums, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das

gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste, ist die Videoaufzeichnung vielmehr auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken. Darüber hinaus sind alternative und weniger einschneidende Schutzmaßnahmen, wie anlassbezogene Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals vorab zu prüfen. Ferner gilt es eine unverzügliche Löschung der Aufnahmen in der Regel nach 24, spätestens nach 48 Stunden, einen deutlich sichtbaren Hinweis auf die Videoüberwachung an den Fahrgasttüren sowie die notwendigen technisch-organisatorischen Maßnahmen für die Sicherung der Daten zu gewährleisten.

Hinsichtlich der Außenkamera haben die Aufsichtsbehörden festgehalten, dass diese datenschutzrechtlich unzulässig ist. Für den Einsatz einer Kamera, mit der gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können, bestehe keine Rechtsgrundlage. Das informationelle Selbstbestimmungsrecht umfasse das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dieses Interesse überwiege das Aufklärungsinteresse des Taxiunternehmens. Durch eine solche Kamera würde außerdem das schutzwürdige Interesse des Taxifahrers selbst verletzt, keiner permanenten Überwachung und Analysemöglichkeit seines Fahrverhaltens ausgesetzt zu sein.

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

11.1.3 Videoüberwachung in Arztpraxen

Meine Dienststelle erreichen immer wieder Anfragen und Beschwerden zu dem Thema Videoüberwachung in Arztpraxen. Die Bandbreite der überwachten Bereiche reicht vom Eingang über die Anmeldung bis hin zum Wartezimmer.

Nach Maßgabe des § 6b BDSG ist eine **Videoüberwachung** durch private Unternehmen nur zulässig, soweit sie zur **Wahrnehmung des Hausrechts** oder zur **Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke** erforderlich ist und keine Anhaltspunkte bestehen, dass **schutzwürdige Interessen** der Betroffenen überwiegen.

Die Überwachung von Eingangsbereichen zu Praxisräumen zur Verhinderung und Aufklärung von Einbrüchen kann aus diesem Grund allenfalls außerhalb der Sprechzeiten zulässig sein. Während der Sprechzeiten habe ich dagegen die Zulässigkeit von Videoüberwachungsmaßnahmen regelmäßig verneint, da aufgrund des Publikumsverkehrs und der Anwesenheit von Personal in den Praxisräumlichkeiten solche Vorkommnisse nach der Lebenserfahrung zu dieser Zeit nicht stattfinden. Eine Videoüberwachung für diesen Zweck ist daher während der Öffnungszeiten nicht erforderlich. Ferner überwiegt zu diesen Zeiten das Recht des Einzelnen, das Gebäude zu betreten, ohne dass dies mittels Videotechnik dokumentiert wird.

In einem für die **Überwachung von Arztpraxen** typischen Fall wurde als Begründung für die Überwachung des **Anmeldebereichs** vorgetragen, dass dieser nicht durchgängig besetzt sei. Durch eine Übertragung des Überwachungsbildes auf zwei Monitore in andere Arbeitsräume ohne Patientenverkehr, könne der Mitarbeiter erkennen, dass sich jemand anmelden möchte. Außerdem sei es zum Diebstahl der im Rezeptionsbereich befindlichen Kaffeekasse gekommen.

Ich habe den Betreiber gebeten, die Videokamera abzubauen, weil sie weder erforderlich noch verhältnismäßig war. Eine Videoüberwachung ist erforderlich, wenn es kein in die Rechte der Betroffenen weniger einschneidendes Mittel gibt, um den angestrebten Zweck zu erreichen. Dem Umstand, dass die Rezeption nicht regelmäßig besetzt ist, kann beispielsweise dadurch Rechnung getragen werden, dass die Praxisräume nur derjenige betreten kann, der zuvor eine Klingel betätigt hat. Alternativ wäre vorstellbar, dass die Praxismitarbeiter, auch wenn sie sich nicht im Anmeldebereich befinden, durch akustische oder optische Signale auf das Betreten der Praxis aufmerksam gemacht werden. Dies stellt ohne Zweifel das mildere Mittel gegenüber einer Videobeobachtung dar. Aber auch hinsichtlich der Verhinderung und Aufklärung des Diebstahls der Kaffeekasse war das schutzwürdige Interesse der betroffenen Patienten höher zu gewichten. Der Einsatz von Videoüberwachungskameras stellt nach der Rechtsprechung des Bundesverfassungsgerichts einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht dar. Das Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu können, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Hierzu gehört auch der unbeobachtete Arztbesuch. Bei der Videoüberwachung einer Arztpraxis fällt erschwerend ins Gewicht, dass ein Filmen von Patienten eine Erhebung von Gesundheitsdaten darstellt. Hierbei handelt es sich um besondere Arten personenbezogener Daten i. S. des § 3 Absatz 9 BDSG, die einem besonderen Schutz unterworfen sind und deren Verarbeitung sehr sensibel ist. Dies war im Rahmen der Interessenabwägung zu berücksichtigen. Bei einer Videoüberwachung darf außerdem die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Interesses an der Überwachung stehen. Das Interesse an der künftigen Verhinderung des Diebstahls der Kaffeekasse mit einem überschaubaren Bargeldinhalt stand außer Verhältnis zu dem erheblichen Eingriff in das Persönlichkeitsrecht der Patienten, zumal eine große Zahl von Personen unter einen Generalverdacht gestellt wurde. Ich habe dem Praxisinhaber geraten, die Kaffeekasse regelmäßig zu leeren, um den Schaden - bei einem möglichen Diebstahl - so gering wie möglich zu halten. Schließlich war in dem zu entscheidenden Fall die Videoüberwachung auch unter dem Gesichtspunkt des Beschäftigtendatenschutzes bedenklich, da der Rezeptionsarbeitsplatz vollumfänglich von der Kamera erfasst wurde, ohne dass dies erforderlich war.

In einem anderen Fall erkundigte sich ein Arzt, ob er sein **Wartezimmer**, welches nicht einsehbar sei, videoüberwachen dürfe. Nicht klar geworden ist mir, zu welchem Zweck er dies beabsichtigte. Auch hier dürfte aus den o. g. Gründen das informationelle Selbstbestimmungsrecht der Patienten überwiegen. Die wartenden Patienten würden einem ständigen Überwachungsdruck ausgesetzt und könnten sich der Überwachung kaum entziehen, ohne diese durch ein konkretes Fehlverhalten veranlasst zu haben.

Videoüberwachung in Arztpraxen ist ein sensibles Thema. Insbesondere aufgrund der Tatsache, dass das Filmen von Patienten eine Erhebung von Gesundheitsdaten darstellt, ist besondere Vorsicht geboten. Inhaber von Arztpraxen sollten sich daher mit den Voraussetzungen einer Videoüberwachung gründlich auseinandersetzen.

11.1.4 Zulässigkeit von Wildkameras

Heutzutage kann man offenbar nicht einmal mehr unbeobachtet im Wald spazieren gehen. Im Berichtszeitraum häuften sich die Anfragen zur Zulässigkeit von sog. Wildkameras.

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) und die Verarbeitung und Nutzung der durch eine solche Videoüberwachung erhobenen Daten ist nur unter den Voraussetzungen des § 6b BDSG zulässig. Bei Waldgebieten handelt es sich um einen öffentlich zugänglichen Raum i. S. dieser Vorschrift, da gem. § 37 des Landeswaldgesetzes (LWaldG) jedem das Betreten des Waldes zum Zwecke der Erholung gestattet ist. **Wildkameras** sind daher als **Videoüberwachungsanlagen** zu qualifizieren.

Eine Videoüberwachung kann nach § 6b Absatz 1 BDSG beispielsweise zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig sein. Voraussetzung ist allerdings, dass sie erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dem Persönlichkeitsrecht des Betroffenen, z. B. eines Spaziergängers oder Wanderers, der von der Kamera aufgezeichnet wird, ist in diesem Zusammenhang ein hoher Stellenwert einzuräumen. Zweifelhaft ist bereits, ob der Einsatz hoch auflösender Kameras, die es auch erlauben, u. U. Personen zu identifizieren, für jagdliche Beobachtungszwecke erforderlich ist. Gerade der Wald ist ein Bereich, welcher der Erholung der Menschen dient und in dem man sich unbeobachtet bewegen können sollte. **Wildkameras sind daher in der Regel unzulässig**, weil die berechtigten Interessen der Waldbesucher überwiegen.

Der Einsatz von Wildkameras ist denkbar, wenn ein Bereich erfasst wird, der von Personen nicht betreten werden darf, bspw. eine jagdliche Einrichtung nach § 37 Abs. 4 Nr. 6 LWaldG i. V. m. § 16 des Landesjagdgesetzes. Hervorzuheben ist in diesem Zusammenhang, dass es sich bei einer Kirrung nicht um eine solche jagdliche Einrichtung handelt, d. h. ein allgemeines Betretungsverbot besteht hier nicht. Eine datenschutzrechtliche Zulässigkeit kann in begründeten Einzelfällen außerdem angenommen werden, wenn Personen nicht identifizierbar sind, z. B. weil die Auflösung der Kamera sehr gering ist oder lediglich der Bodenbereich aufgenommen wird, so dass allenfalls die Beine erfasst werden.

Der Wald ist ein Bereich, welcher der Erholung der Menschen dient und deshalb von Überwachungseinrichtungen frei bleiben sollte.

11.1.5 Videoüberwachung an Schulen nach § 20a LDSG

Während des Berichtszeitraums war ich mit Videoüberwachung an Schulen mehrfach in Form von Anfragen von Kommunen und Schulen, aber auch Beschwerden, beschäftigt. Die Thematik war bereits Gegenstand meines 29. Tätigkeitsberichts (LT-Drs. 14/5500, S. 29 ff.). Zwischenzeitlich hat sich jedoch durch die Einführung der speziellen Rechtsgrundlage des § 20a LDSG (vgl. hierzu 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 18) die Rechtslage geändert, so dass ich das Thema erneut aufgreifen möchte.

Gem. § 20a LDSG kann eine Videobeobachtung im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts zum Schutz von Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen aufhalten oder zum Schutz von Kulturgütern, öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden und sonstigen baulichen Anlagen öffentlicher Stellen zulässig sein. Der Schutz von Schulen wird in der Gesetzesbegründung (LT-Drs. 14/7313, S.13) ausdrücklich als zulässiger Zweck angeführt.

Videoüberwachungstechnik darf jedoch nur unter strikter Beachtung des Erforderlichkeits- und Verhältnismäßigkeitsgrundsatzes eingesetzt werden. Voraussetzung ist, dass Tatsachen die Annahme rechtfertigen, dass das zu schützende Rechtsgut oder Objekt gefährdet ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Eine **Überwachung einer Schule** während der Unterrichtszeiten dürfte in der Regel unzulässig sein. Eine Videoüberwachung während des laufenden Schulbetriebs stellt regelmäßig einen schwerwiegenden Eingriff in das Persönlichkeitsrecht der Schülerinnen, Schüler und Lehrkräfte dar, die sich der Überwachung nicht entziehen können, da sie zum Besuch der Schule und zum Aufenthalt auf dem Schulgelände verpflichtet sind. Im Übrigen können die persönlichen Aufsichtspflichten der Lehrkräfte nicht durch optisch-elektronische Systeme ergänzt oder ersetzt werden.

Mir ist oftmals entgegen gehalten worden, dass die Videoüberwachung zum Zwecke der Alamierung bei bzw. der Verhinderung von Amokläufen erforderlich sei. Hier stellt sich unter Verhältnismäßigkeitsgesichtspunkten die Frage, was der Einsatz von Videotechnik zusätzlich zu milderen Mitteln, wie funkgestützter Alarm oder Ähnlichem,

zu leisten im Stande ist, was diesen gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung der Schüler und Lehrer rechtfertigen würde. Zumindest zur Verhinderung von Amokläufen dürfte das Mittel der Videoüberwachung ungeeignet sein, da die bloße Präsenz von Kameras einen zu einer solchen Gewalttat entschlossenen Täter von seinem Vorhaben kaum abbringen wird.

Eine **Videoüberwachung während des laufenden Schulbetriebs** kann nur in besonderen Ausnahmefällen und in sehr eingeschränktem Umfang zulässig sein. Denkbar ist beispielsweise die Überwachung schlecht einsehbarer Fahrradständer, wenn es in der Vergangenheit bereits wiederholt zu Diebstählen und erheblichen Beschädigungen gekommen ist. Sofern keine weniger einschneidenden Maßnahmen in Betracht kommen und den betroffenen Schülern die Möglichkeit eingeräumt wird, einen unbeobachteten Bereich zum Abstellen ihres Fahrrads zu benutzen, kann eine Videoüberwachung u. U. zulässig sein.

Außerhalb der Unterrichtszeiten ist eine punktuelle Videoüberwachung denkbar, jedoch muss es in der Vergangenheit bereits zu entsprechenden Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung gekommen sein oder es müssen beweiskräftige Tatsachen dafür vorliegen, dass solche in Zukunft begangen werden sollen. Dass eine Schule erfahrungsgemäß häufig Gegenstand von Vandalismus ist, genügt nicht. Darüber hinaus muss vorrangig geprüft werden, ob es alternativ zu einer Videoüberwachung keine weniger belastenden und ebenfalls wirksamen Schutzmaßnahmen gibt, etwa die Einzäunung des Geländes und seine Sicherung durch das Abschließen aller Tore, der Einsatz von Bewegungsmeldern mit Scheinwerfern, Alarmanlagen etc. Hinsichtlich der Verhinderung von Graffiti und Schmierereien kommt u. U. ein Auftragen von speziellen farbabweisenden oder abwaschbaren Folien oder Farben o.Ä. in Betracht. Ergibt die Prüfung, dass andere Maßnahmen nicht ausreichen, muss weiter bedacht werden, wie sichergestellt wird, dass Personen, die sich nachmittags oder abends zulässigerweise in dem Schulgebäude oder auf dem Schulgelände aufhalten, z. B. Teilnehmer und Besucher einer Schulveranstaltung oder Mitglieder von Sportvereinen, welche die Sporteinrichtungen nutzen, nicht in ihrem Persönlichkeitsrecht beeinträchtigt werden. Ferner ist zu prüfen, wie eine Überwachung in örtlicher und zeitlicher Hinsicht eingeschränkt werden kann. Sind die Vorkommnisse in der Vergangenheit vor allem nachts aufgetreten, erscheint eine auf die Nachtstunden beschränkte Überwachung ausreichend.

Vor dem erstmaligen Einsatz von Videoüberwachungstechnik hat eine **schriftliche Freigabe durch die verantwortliche Stelle** zu erfolgen. In der schriftlichen Freigabe müssen gem. § 20a Absatz 6 LDSG der Zweck der Videoüberwachung angegeben, weitere wesentliche Festlegungen für das Verfahren getroffen und das Ergebnis der Zulässigkeitsprüfung im Einzelnen dargelegt werden.

Eine Videoüberwachung an Schulen ist nur unter engen Voraussetzungen möglich und bedarf einer sehr sorgfältigen Vorbereitung. Im Ergebnis kommt es für die Zulässigkeit entscheidend auf die konkreten Umstände des Einzelfalles an.

11.2 Soziale Netzwerke

11.2.1 Facebook und der Datenschutz

Das Wachstum sozialer Netzwerke, vor allem des US-amerikanischen Anbieters Facebook, geht auch in Deutschland nahezu ungebrochen weiter. Der Datenschutz hat auf der nationalen Ebene einen schweren Stand. Weder ist eine freiwillige Selbstregulierung noch eine hinreichende Anwendbarkeit des deutschen Datenschutzrechts sichergestellt.

Soziale Netzwerke verbreiten sich im Alltag zusehends; im Jahre 2012 wurden sie von 47 Prozent der 14- bis 64-jährigen Personen in Deutschland genutzt. 51 Prozent in der Altersgruppe der 14- bis 19-Jährigen stimmten sogar der Aussage „Ich kann mir ein Leben ohne soziale Netzwerke nicht mehr vorstellen“ zu. Dies geht aus der Studie der Allensbacher Computer- und Technik-Analyse 2012 hervor. Nach eigenen Angaben des Unternehmens vom 16. September 2013 nutzen

mittlerweile über 25 Millionen Menschen in Deutschland **Facebook** mindestens einmal im Monat. 19 Millionen Menschen in Deutschland nutzen Facebook täglich.

Den größten Zuspruch erfahren außereuropäische soziale Netzwerke wie Facebook, Instagram oder Whatsapp. Junge Menschen nutzen Whatsapp mehr als eine Stunde und Facebook 44 Minuten täglich. Dies ergab eine Umfrage unter 2.500 Studenten im Alter von 18 bis 25 Jahren, wie das Magazin Focus im September 2013 berichtete. Datenschutzfreundlichere deutsche soziale Netzwerke schrumpfen dagegen stark. Nach Medienberichten sank die Zahl der monatlichen Seitenaufrufe zwischen 2011 und 2012 bei StudiVZ, SchülerVZ und FreundeVZ auf nur noch 77 Millionen. Die Zahl der monatlichen Seitenaufrufe von Werkenntwen habe sich in einem Jahr halbiert, im Dezember 2012 waren es nur noch 76 Millionen. SchülerVZ stellte den Betrieb im Frühjahr 2013 sogar ganz ein.

Der regen Verwendung sozialer Netzwerke zum Trotz scheint es vielen Nutzern an dem Bewusstsein zu mangeln, dass soziale Netzwerke keine abgeschottete „virtuelle“ Welt sind, sondern quasi nur die Spitze des Eisbergs bilden, deren eigentliches Ziel die umfassende kommerzielle Ausbeutung der Nutzerdaten nach allen Regeln des **Data Mining** ist. Mittlerweile ist manchen bewusst geworden, dass ihr Online-Verhalten Konsequenzen im „realen“ Leben nach sich ziehen und die freie Verfügbarkeit ihrer preisgegebenen personenbezogenen Daten auch die Begehrlichkeiten bzw. Gegenreaktionen Dritter wecken kann. Das beschäftigt zum Beispiel die arbeitsgerichtliche Rechtsprechung zusehends: So können **negative Äußerungen von Arbeitnehmern in sozialen Netzwerken gegenüber einem Arbeitgeber** die Kündigung nach sich ziehen. Auch die Betätigung eines Like-Buttons, mit der jemand seine Unterstützung der negativen Äußerung eines Anderen über den Arbeitgeber signalisiert, kann zu einer Abmahnung führen. Die Polizeibehörden verwenden mittlerweile Facebookprofile zur Identifizierung von Personen auf „Blitzerfotos“. Die Auskunftei Schufa wollte in Zusammenarbeit mit dem Hasso-Plattner-Institut der Universität Potsdam aus Nutzerdaten bei Facebook, Twitter und XING Erkenntnisse über die Kreditwürdigkeit der Nutzer gewinnen und nahm erst nach öffentlichen Protesten davon Abstand. Besonders fortschrittlich wollte die sächsische Landesregierung sein und für viel Geld eine Software kaufen, die politische Meinungsbekundungen der Bürger bei Facebook und in Blogs erfassen sollte; auch hier sorgten öffentliche Proteste für ein vorläufiges Ende des Vorhabens.

Die grundsätzliche datenschutzrechtliche Beurteilung von sozialen Netzwerken, die bereits im 30. Tätigkeitsbericht beschrieben wurde, hat sich nicht geändert. Das Grundrecht auf informationelle Selbstbestimmung wird auch weiterhin von den Betreibern der meisten sozialen Netzwerke missachtet. Die Problematik der informierten Einwilligung besteht ebenso fort wie die Erstellung von nicht anonymisierten Nutzerprofilen. Insoweit verweise ich auf meine damaligen Ausführungen (vgl. LT-Drs. 15/955, S. 46 ff.).

Der Düsseldorfer Kreis hatte am 8. Dezember 2011 in einem Beschluss (vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, Anhang 43) die Rechtslage und die sich daraus ergebenden Anforderungen dargelegt, die das deutsche Datenschutzrecht an die Betreiber von sozialen Netzwerken, an die Betreiber von Fanpages und Anbieter deutscher Websites, die Social Plug-ins auf ihren Webseiten einbinden, stellt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veröffentlichte am 13. März 2013 die **Orientierungshilfe „Soziale Netzwerke“**, die die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen soll. Die Konferenz wies in diesem Zusammenhang darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzniveaus für soziale Netzwerke fortentwickelt werden muss, „insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht.“ Auch der europäische und der nationale Gesetzgeber wurden ausdrücklich aufgefordert, einen ausreichenden Datenschutzstandard zu sichern. Die

Orientierungshilfe kann von meiner Internetseite heruntergeladen werden, http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/03/OH-Soziale-Netzwerke-2013-03.pdf#.

Die Aufforderung an die Gesetzgeber, in sozialen Netzwerken ein datenschutzfreundliches Niveau auf normativem Wege zu gewährleisten, erhält durch das Scheitern der freiwilligen Selbstregulierung sozialer Netzwerke weiteres Gewicht (siehe hierzu Kapitel 1.4.5). Seit über zwei Jahren liegt außerdem ein **Gesetzentwurf des Bundesrats zur Änderung des Telemediengesetzes** (BR-Drs. 156/11) auf Eis, mit dem insbesondere die Informationspflichten der Dienstanbieter verstärkt werden sollten. Dieser Gesetzentwurf sollte rasch reaktiviert werden, falls es nicht bald zu einer entsprechenden Regelung auf europäischer Ebene komm.

Durch die gesteigerte Aufmerksamkeit der Nutzer beim Umgang mit Cookies und den verschiedenen Möglichkeiten, diese zu löschen oder zu blockieren, suchen soziale Netzwerke nach neuen Wegen, um das Nutzungsverhalten auch ohne die Verwendung von leicht zu löschenden Cookies zu „tracken“, also aufzeichnen und auswerten zu können. Facebook bietet beispielsweise derzeit mit dem sog. Optimized CPM (Optimierter Tausend-Kontakt-Preis) eine neue Tracking-Methode an. Bei dieser Tracking-Methode setzt Facebook auf die Bequemlichkeit seiner Nutzer, die sich häufig nach Besuch des sozialen Netzwerks nicht abmelden. Dadurch ermöglichen sie Facebook, mit Hilfe der Facebook-ID, eine Nummer, die jeder Nutzer von Facebook bei der Registrierung zugewiesen bekommt, ihr Verhalten auch auf anderen Seiten und sogar über unterschiedliche Browser und Endgeräte hinweg zu erfassen. Dazu müssen die Werbekunden von Facebook lediglich einen Code auf ihren Webseiten einbetten. Melden sich die Nutzer bei Facebook nicht ab, kann Facebook dann feststellen, ob ein Nutzer die vom Werbekunden gewünschte Aktion durchgeführt hat, beispielsweise eine Registrierung oder einen Kauf.

Das Löschen seines Benutzerprofils bei einem sozialen Netzwerk oder auch einzelner Beiträge kann nach wie vor ein schwieriges Unterfangen sein. Nach einer Marktanalyse des Verbraucherzentrale Bundesverbandes e.V., veröffentlicht im Mai 2013, bieten nur acht von 19 untersuchten Plattformen Löschmöglichkeiten in den Kontoeinstellungen oder Profilinformationen an. Bei sieben Plattformen benötigen die Verbraucher die „Hilfe“-Funktion, um herauszufinden, wie sie ihr Profil löschen können, vier Onlineangeboten bieten das Löschen eines Nutzerprofils gar nicht an. Auf drei Seiten wurde das Nutzerkonto nicht gelöscht, sondern lediglich deaktiviert, so dass es auch zwei Jahre nach der vermeintlichen Löschung ohne großen Aufwand wiederhergestellt werden konnte.

Seitdem ein österreichischer Student die Herausgabe zumindest eines Teils seiner von Facebook gespeicherten Daten erreichte, ist außerdem bekannt, dass bei Facebook gelöschte Daten lediglich deaktiviert und weiter auf den Servern von Facebook gespeichert werden.

Einen Erfolg für den Datenschutz in Deutschland war die Zusage von Facebook gegenüber dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, die **biometrische Gesichtserkennung** in Europa nicht mehr zu verwenden. Der Hamburger Kollege hat sich davon überzeugt, dass Facebook die bisher erfassten biometrischen Daten gelöscht hat.

Im Jahr 2013 sorgte auch das neue Produkt **Facebook Home** für Schlagzeilen und für kritische Anmerkungen aus Datenschutzsicht. Facebook Home ist eine App, mit deren Hilfe der Nutzer auf seinem Smartphone neue Bilder, Nachrichten und andere Inhalte angezeigt bekommt, die Freunde geteilt oder markiert haben, und Nachrichten mit Freunden über Facebook und SMS austauschen kann. Die App nistet sich tief im Betriebssystem des Smartphones ein und bekommt dabei eine nahezu hundertprozentige Kontrolle über alle installierten Anwendungen. Sie zeichnet nach eigener Aussage von Facebook auch auf, welche Apps auf dem sog. Home Launcher installiert sind. Jegliche Benutzung des Services wird für 90 Tage identifizierbar gespeichert. Deshalb rate ich von der Nutzung von Facebook Home ab.

Eine weitere neue Funktion, die Facebook zwar bisher nur in den USA eingeführt hat, die aber

über eine simple Umstellung der Sprache von Deutsch auf Englisch auch in Deutschland schon genutzt werden kann, ist der Graph Search. Graph Search ist eine Art soziale Suche für die Nutzer von Facebook, die das soziale Netzwerk zu einer schier unerschöpflichen sozialen Datenbank für alle Nutzer macht. Graph Search zeigt alle Beiträge von allen Nutzern an, die diese jemals bei Facebook getätigt haben, wenn diese den Beitrag nicht für die öffentliche Sichtbarkeit eingeschränkt haben. Er ermöglicht Themensuchen wie beispielsweise „Männer, die Prostituierte mögen“ ebenso wie die Suche über einen bestimmten Nutzer. Letzteres wird durch eine Änderung der Privatsphäreeinstellungen von Facebook möglich, nach der jeder Nutzer über die Suchfunktion des Netzwerks gefunden werden kann. Dabei zeigt der Graph Search auch Bilder, Posts, Kommentare über einen Nutzer an, die er nicht selbst, sondern Freunde von ihm getätigt haben.

Facebook, der Weltmarktführer im Bereich der sozialen Netzwerke, ist im Berichtszeitraum aber auch Gegenstand verschiedenster, teilweise widersprüchlicher **Rechtsprechung** geworden.

Anfang März 2013 gab das Landgericht Berlin (LG Berlin) einer Klage des Verbraucherzentrale Bundesverbandes e.V. statt und stellte in einem Urteil (Az. 16 O 551/10) fest, dass die Funktion „Freunde finden“ in der von Facebook verwendeten Form nicht mit dem BDSG zu vereinbaren ist. Nach Ansicht des LG Berlin entsprachen weder die zu dem damaligen Zeitpunkt verwendete Einwilligung im Rahmen der Registrierung noch die Erläuterungen der Funktion „Freunde finden“ den Anforderungen an eine informierte Einwilligung gem. § 4a BDSG. Gleichzeitig entschied es, dass nach Artikel 3 Absatz 1 Satz 1 der Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I) aufgrund einer ausdrücklichen Vereinbarung zwischen Facebook und den deutschen Nutzern deutsches Recht anwendbar ist.

Das Oberverwaltungsgericht Schleswig-Holstein (OVG Schleswig-Holstein) hat im Gegensatz zum LG Berlin im April 2013 in zwei unanfechtbaren Beschlüssen (Az. 4 MB 10/13 und 11/13) festgestellt, dass kein deutsches, sondern irisches Datenschutzrecht auf die Verarbeitung der Facebook-Nutzerdaten anwendbar ist, da die Datenverarbeitung nach Ansicht des OVG bei der irischen Niederlassung von Facebook stattfindet. Den Beschlüssen des OVG Schleswig-Holstein lag eine Klage von Facebook gegen eine Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) vom Dezember 2012 zu Grunde. Das ULD hatte als Reaktion auf die Klarnamenpflicht bei Facebook mit Verweis auf § 13 Absatz 6 Satz 1 TMG eine Anordnung gegen Facebook USA und Facebook Irland mit dem Inhalt erlassen, die Nutzung unter einem Pseudonym zu ermöglichen und aus diesem Grunde gesperrte Konten wieder zu entsperren. Das OVG Schleswig-Holstein gab der Klage von Facebook statt, Facebook kann daher auch weiterhin eine Klarnamenpflicht von seinen Nutzern fordern und Konten, die unter einem Pseudonym verwendet werden, sperren.

Der Ansicht des OVG Schleswig-Holstein, dass die Datenverarbeitung bei der irischen Niederlassung von Facebook stattfinde, widerspricht allerdings die Erfahrung, die ein Reutlinger Strafrichter Anfang 2012 bei dem Versuch machte, einen Facebookaccount zu beschlagnahmen, weil er sich davon Erkenntnisse bezüglich der Verabredung einer Straftat zwischen den Tatbeteiligten versprach. Das Rechtshilfeersuchen an die irischen Behörden scheiterte daran, dass Facebook die Daten des in Deutschland lebenden Angeklagten in den USA gespeichert hatte.

Zuletzt hat das Schleswig-Holsteinische Verwaltungsgericht in drei Verfahren festgestellt, dass die Betreiber von sog. Fanpages bei Facebook nicht für Datenschutzverstöße von Facebook verantwortlich seien (Urt. v. 9. Oktober 2013, Az. 8 A 218/11, 8 A 14/12, 8 A 37/12). Das Gericht ließ dabei offen, ob die vom ULD gerügten datenschutzrechtlichen Verstöße erfolgt waren, entscheidend sei vielmehr, dass nur Facebook einen Zugriff auf die Daten der Nutzer habe und die Fanseitenbetreiber keine Mitverantwortung an etwaigen Datenschutzverstößen durch das Unternehmen treffe, weil sie weder tatsächlich noch rechtlich auf die Datenverarbeitung durch Facebook Einfluss nehmen könnten. Ich halte die Ent-

scheidung für wenig überzeugend, denn sie blendet die Verantwortung des Fanpagebetreibers dafür aus, dass er selbst eine Fanseite eingerichtet und damit überhaupt erst die datenschutzrechtlich problematische Datenverarbeitung durch Facebook ermöglicht hat. Mein Kieler Kollege hat deswegen auch Rechtsmittel eingelegt. Die Entscheidung hat allerdings erneut die Notwendigkeit einer europäischen Datenschutzreform mit einem hohen Datenschutzniveau deutlich gemacht.

11.2.2 Mitwirkung an Vorgaben für die Landesverwaltung

Das Interesse der Landesverwaltung, über soziale Netzwerke in direkten Kontakt mit dem Bürger zu treten und dessen Interesse an der Arbeit der Landesverwaltung zu wecken, ist weiterhin ungebrochen.

Diesem Interesse steht die datenschutzrechtliche Problematik beim Umgang mit sozialen Netzwerken gegenüber, die ich weitgehend bereits im 30. Tätigkeitsbericht geschildert habe. Die Informationspolitik z. B. von Facebook über seinen Datenumgang ist weder für die Aufsichtsbehörden noch für die Nutzer transparent gestaltet. Dadurch können die Prozesse noch immer nicht abschließend datenschutzrechtlich bewertet werden.

Ich bin weiterhin der Ansicht, dass die Rechtmäßigkeit des Datenumgangs von Facebook an deutschem Recht zu messen ist und Betreiber von Webseiten mit Social Plug-ins und von Facebook-Fanpages datenschutzrechtlich verantwortliche Stellen sind. Insoweit überzeugt die Argumentation der Entscheidungen des Oberverwaltungsgerichts Schleswig-Holstein und des Schleswig-Holsteinischen Verwaltungsgerichts (siehe dazu 11.2.1) nicht. Daher halte ich auch weiterhin an der Ansicht fest, dass § 15 Absatz 3 des Telemediengesetzes (TMG) für die Beurteilung der datenschutzrechtlichen Zulässigkeit aufgrund der Erstellung von Nutzungsprofilen durch Facebook maßgeblich ist.

Unabhängig von der Frage des anwendbaren nationalen Rechts auf die Tätigkeit von Facebook sind öffentliche Stellen an deutsches Recht gebunden. Sie sollten zudem eine **Vorbildfunktion** einnehmen und den Bürger keinesfalls mit seinen Daten dafür zahlen lassen, dass er mit der öffentlichen Stelle in Kontakt treten möchte. Ich empfehle daher allen öffentlichen Stellen in Baden-Württemberg,

- auf die Verwendung von Social Plug-ins wie den sog. Facebook-Like-Button auf ihren Seiten generell zu verzichten, weil hierdurch selbst von nicht bei Facebook registrierten Nutzern personenbezogene Daten zum Zwecke der Profilbildung durch den Betreiber des sozialen Netzwerks gewonnen werden können;
- stattdessen allenfalls den sog. Zwei-Klick-Button zu verwenden, der es ermöglicht, dass Daten nur nach Information des Nutzers und mit dessen aktivem Zutun an den Betreiber des sozialen Netzwerks Facebook übermittelt werden. Eine entsprechende Lösung wurde beispielsweise für das Landesportal Baden-Württemberg gewählt.

Die Einrichtung und Nutzung einer sog. **Fanpage** bei Facebook (oder einem vergleichbaren sozialen Netzwerk) durch öffentliche Stellen in Baden-Württemberg ist derzeit insbesondere aufgrund des Verstoßes gegen § 15 Absatz 3 TMG datenschutzkonform nicht möglich. Falls eine öffentliche Stelle trotz der datenschutzrechtlichen Bedenken eine Fanpage einrichten will, sollte diese Seite lediglich Informationen enthalten und vorzugsweise auf das eigene Informationsangebot der Stelle im Internet verlinken. Auf Kommunikationsmöglichkeiten für Besucher der Fanseite - etwa auf der Pinnwand oder über Kommentierungsfunktionen - ist dementsprechend zu verzichten.

Diese Position habe ich 2013 bei mehreren Veranstaltern gegenüber Vertretern der Landesverwaltung vorgetragen, z. B. bei einer Sitzung des Arbeitskreises der IT-Referenten, bei den Pressereferenten sowie bei den Organisationsreferenten der Ministerien und des Rechnungshofes.

Derzeit begleite ich zudem eine interministerielle Arbeitsgruppe, die sich die Erarbeitung eines Leitfadens zur Nutzung sozialer Netzwerke zum Ziel gesetzt hat. Ich hoffe, dass dabei dem Datenschutz ebenso Rechnung getragen wird wie dem

Interesse der Ministerien, in direkten Kontakt mit den Bürgern und Bürgerinnen des Landes zu treten.

11.2.3 Die Verwendung des Facebook-Like-Buttons durch öffentliche Stellen in Baden-Württemberg

Die Betreiber von Internetseiten eröffnen durch die Einbindung von **Social-Plug-ins** Facebook, Twitter oder Google die Möglichkeit, an verschiedene Daten der Besucher der Webseite zu gelangen, selbst wenn die Besucher zu diesem Zeitpunkt nicht bei dem entsprechenden Dienst angemeldet waren oder überhaupt nicht registriert sind. Zu diesen Daten können beispielsweise die IP-Adresse des Rechners, die URL-Adresse der aufgerufenen Webseite und der Zeitpunkt des Webseitenaufrufs gehören. Dazu muss der Betreiber auf seiner Webseite den sogenannten iFrame einbinden. Der iFrame ist eine extra Seite innerhalb der Webseite des Betreibers, die sich bei Aufruf der Webseite in diese automatisch eingebettet. Der Quellcode des iFrames stammt vom sozialen Netzwerk und kann vom Betreiber einer Webseite ohne weiteren Aufwand eingebunden werden. Bereits bei Aufruf der Webseite sendet der Browser dann an Facebook die URL der Webseite als Referer und ggf. einen bereits von Facebook früher gesetzten Cookie (datr-Cookie). Der datr-Cookie wird bei einem Aufruf der Webseite von Facebook auf dem Computer des Nutzers abgelegt, auch wenn dieser nicht bei Facebook registriert ist, weist eine Speicherfrist von zwei Jahren auf und enthält eine eindeutige (Wieder-)Erkennungs-ID. Wenn der Nutzer gerade bei Facebook angemeldet ist, enthält der Cookie seine Facebook-Sitzungs-ID. Die aufgerufene Webseite kann damit dem Facebook-Mitglied konkret zugeordnet werden. Hat ein Nicht-Facebook-Mitglied schon einmal die Webseite von Facebook aufgerufen, wird der datr-Cookie ebenso an Facebook gesendet. Mit diesen Informationen kann Facebook ein Profil des Nutzers erstellen. Meldet sich ein Nutzer bei Facebook an oder registriert er sich innerhalb von zwei Jahren, kann Facebook diese Daten dann auch einer im Grundsatz bestimmbaren Person zuordnen. Wenn ein Nicht-Facebook-Mitglied noch nie die Facebook-Webseite aufgerufen hat oder regelmäßig seine Cookies löscht, erhält Facebook lediglich dessen IP-Adresse. Nach eigenen Angaben von Facebook wird die IP-Adresse für Aufrufe aus Deutschland durch eine generische ersetzt und so anonymisiert, wenn der Nutzer nicht den Like-Button betätigt. Betätigt ein Nutzer den Like-Button, erhält Facebook, unabhängig davon, ob der Nutzer bei Facebook angemeldet ist oder nicht, noch zusätzlich Informationen über Datum, Zeit, URL und Browsertyp des Nutzers. Nach eigenen Angaben löscht Facebook diese Informationen nach 90 Tagen.

Ähnliche Social Plug-ins werden auch von Twitter oder Google verwendet. Damit könnten soziale Netzwerke Daten des Nutzers erheben, ohne dass dieser dazu seine Einwilligung erklärt hat. Da die Daten bereits beim Laden einer Webseite erhoben werden, wird dem Nutzer darüber hinaus die Möglichkeit genommen, sich über die diese Datenerhebung zu informieren und eine informierte Einwilligung gem. § 12 Absatz 1 i. V. m. § 13 Absatz 1 Telemediengesetz (TMG) oder einen Widerspruch nach § 15 Absatz 3 TMG zu erklären. Aus diesem Grunde dulde ich derzeit lediglich die Verwendung von Social Plug-Ins unter der Bedingung, dass der Webseitenbetreiber den sog**. Zwei-Klick-Button** verwendet. Nur mit dieser Lösung ist gewährleistet, dass Daten nur nach Information des Nutzers und mit dessen aktivem Zutun übermittelt werden.

Aus diesem Grunde habe ich im Sommer angekündigt, die Internetauftritte von Behörden und anderen öffentlichen Stellen des Landes Baden-Württemberg überprüfen lassen. Meine Mitarbeiter haben insgesamt 4.394 Internetseiten mit einem speziellen **Prüfprogramm** untersucht. In nur 47 Fällen konnten sie direkt auf der Webseite des Betreibers eingebundene Like-Buttons finden. Das ist eine erfreulich geringe Quote von rd. 1,1 %. Ich habe die Betreiber der problematischen Internetauftritte gebeten, künftig generell auf die Verwendung des Like-Buttons zu verzichten. Aufgrund meiner Intervention haben sie mittlerweile ganz auf die Einbindung des Like-Buttons verzichtet oder den Like-Button durch die Zwei-Klick-Lösung ersetzt.

11.3 Neue Vorgaben zur Datenträgervernichtung - die neue DIN 66399

Als bei der New Yorker Thanksgiving-Parade im November 2012 Papierschnipsel aus vertraulichen Dokumenten der Polizei als Konfetti auf die feiernde Menge herabregneten, sorgte diese Datenpanne weltweit für Schlagzeilen. Lesbare Informationen über Autokennzeichen, Sozialversicherungsnummern, ja selbst über verdeckt ermittelnde Polizeibeamte lagen auf der Straße. Die nur unzureichend grob geschredderten Akten stammten von der Polizei eines angrenzenden Landkreises.

Auch in Deutschland tauchen immer wieder bei Altpapiersammlungen, in Altpapiercontainern und im Hausmüll ungeschredderte Akten auf. Vielfach misslingt auch die Löschung elektronischer Daten oder vermeintlich gelöschte Daten auf ausgesonderten Computern werden wieder zum Leben erweckt. Mobile Endgeräte und Datenträger verschärfen die Problematik heute erheblich. Unternehmen sollten daher regelmäßig die eigene Datenträgervernichtung kritisch überprüfen, zumal mit der **DIN 66399** bereits seit 1. Oktober 2012 ein neuer Handlungsmaßstab zur Verfügung steht.

Jeder, der selbst oder im Auftrag vertrauliche, personenbezogene und/oder sensible Daten verarbeitet, hat eine **datenschutzgerechte und sichere Vernichtung und Entsorgung der Datenträger** sicherzustellen. Dabei sind Datenträger so zu vernichten, dass die Reproduktion der auf ihnen enthaltenen Daten entweder unmöglich ist oder weitgehend erschwert wird. Verstöße gegen diese Pflichten können eine Ordnungswidrigkeit nach dem Bundesdatenschutzgesetz (BDSG) darstellen und ein empfindliches Bußgeld zur Folge haben. Daneben sollte auch der Schutz von Geschäftsgeheimnissen und die Einhaltung von Compliance-Regeln Anlass zur Sorgfalt sein. Der Normenausschuss Informationstechnik und Anwendungen (NIA) des Deutschen Instituts für Normung (DIN) hat im Herbst 2012 eine neue Norm für die Vernichtung von Datenträgern vorgestellt. Sie spezifiziert die technischen und organisatorischen Maßnahmen, die von den verantwortlichen Stellen zu ergreifen sind. Die Änderungen gegenüber der - sehr maschinenorientierten - Vorläufernorm DIN 32757-1 von 1987 sind umfangreich. So beinhaltet die DIN 66399 nun drei Schutzklassen, sieben statt bisher fünf Sicherheitsstufen sowie zusätzlich Materialklassifikationen. Gegenüber der alten Norm hat die DIN 66399 erheblich an Umfang gewonnen. Sie besteht nun aus drei Teilen: „Grundlagen und Begriffe“, „Anforderungen an Maschinen zur Vernichtung von Datenträgern“ und „Technische und organisatorische Anforderungen an die Prozesse der Datenträgervernichtung“. Während die beiden ersten Teile die alte Norm vor allem in Bezug auf die Vernichtung elektronischer Datenträger zeitgerecht fortentwickeln, sind die Anforderungen an die Prozesse der Datenträgervernichtung im dritten Teil neu.

11.3.1 Grundlagen und Begriffe (DIN 66399-1)

Bereits der erste Teil macht die Unterschiede zur Vorläufernorm deutlich, was den Überblick erleichtert. Schwerpunkte sind die **Ermittlung des Schutzbedarfs**, der daraus abgeleiteten **Schutzklasse** und der entsprechenden **Sicherheitsstufe**. Die Sicherheitsstufen wurden überarbeitet und erweitert. Die höchste Sicherheitsstufe 7 verlangt, dass eine Reproduktion nach dem derzeitigen Stand von Wissenschaft und Technik unmöglich sein muss. Die niedrigste Sicherheitsstufe 1 hingegen erlaubt die Wiederherstellung der Daten ohne besondere Hilfsmittel und Fachkenntnisse, erfordert jedoch einen erheblichen Zeitaufwand. Das Zusammenfügen der einzelnen, noch lesbaren Papierschnipsel im eingangs genannten Beispiel dürfte wohl in diese Kategorie fallen. Diese Form der *Risikoanalyse* - bei der die Aspekte Wirtschaftlichkeit und Angemessenheit durchaus eine Rolle spielen können - dürfte den Sicherheitsbeauftragten der Unternehmen vertraut sein. Anhand des Schutzbedarfs (normal für interne Daten; hoch für vertrauliche Daten; sehr hoch für besonders vertrauliche und geheime Daten), deren Schutzklasse und der im zweiten Teil beschriebenen sieben Sicherheitsstufen sollte aber auch der unerfahrene Anwender in der Lage sein, die für seine Datenträger erforderliche Sicherheitsstufe zu ermitteln. Die differenzierte Einordnung bedingt allerdings einen gewissen Aufwand. Wer nur geringe Mengen von Datenträgern zu vernichten hat und die Datenträgervernichtung eher „nebenbei“

erledigen muss, sollte sich - z. B. wenn es um für die Vernichtung von Papier geht - auf die „sichere Seite“ begeben und ein Gerät erwerben, das (mindestens) die Sicherheitsstufe 3 oder 4 realisiert.

11.3.2 Anforderungen an Maschinen zur Vernichtung von Datenträgern (DIN 66399-2)

Im zweiten Teil der neuen Norm findet der Anwender die ihm von Abschnitt 5 der DIN 32757-1 bekannten Angaben zu Materialteilchengrößen und Sicherheitsstufen. Wegen der Erweiterung um zwei Sicherheitsstufen sind die Definitionen aber teilweise neu gefasst worden. Die Norm spezifiziert jetzt auch die Datenträgervernichtung bei elektronischen Datenträgern. Die dargestellte Prüfung von Maschinen auf Normkonformität dürfte eher für die Maschinenhersteller interessant sein.

Aufgrund der Ermittlung des Schutzbedarfs im ersten Teil definiert die Norm im zweiten Teil drei Schutzklassen, sechs Materialklassifizierungen und sieben Sicherheitsstufen. In der Materialklassifizierung werden die Grenzwerte der Materialteilchenflächen spezifiziert. Den Anwendern, deren Maschinen die Sicherheitsstufe der DIN 32757-1 nur knapp erfüllen, dürfte sich eine Prüfung an Hand der neuen Klassifizierung empfehlen. Die Norm benennt aber auch Faktoren, die zu einer Erhöhung der Sicherheitsstufe führen können, ohne dass die Materialteilchenflächen die Anforderungen der jeweiligen Sicherheitsstufe erfüllen. So erfüllen Papierschnipsel der Sicherheitsstufe 2 (Materialteilchenfläche kleiner/gleich 800 mm² oder Streifenbreite kleiner/gleich 6 mm) die nächsthöhere Sicherheitsstufe 3 dann, wenn sie vermischt oder gepresst werden, weil die Reproduktion hierdurch erschwert wird.

11.3.3 Prozess der Datenträgervernichtung (DIN SPEC 66399-3)

Der dritte Teil ist keine offizielle DIN-Norm, sondern eine Spezifikation des zuständigen DIN-Ausschusses, also eher eine Vornorm. Die neuen Handlungsanweisungen spiegeln aber Erfahrungen wider, die auch bei der Empfehlung der richtigen technisch-organisatorischen Maßnahmen durch die Datenschutzaufsicht eine wichtige Rolle spielen. Insofern ist es kein Fehler, die innerbetrieblichen Prozesse, aber auch die vertragliche Gestaltung der Datenträgervernichtung durch externe Dienstleister (Datenverarbeitung im Auftrag) an den beschriebenen Verfahrensschritten auszurichten, zumal die Norm für alle am Vernichtungsprozess Beteiligten gelten soll. Drei Prozessvarianten werden zur Auswahl gestellt: 1. Die verantwortliche Stelle vernichtet die Datenträger selbst. 2. Die Datenträger werden von einem Dienstleister vor Ort vernichtet. 3. Die Datenträger werden von einem Dienstleister abgeholt und extern vernichtet. Diesen Varianten werden die Prozesse und Faktoren Personal, Organisation (bei der verantwortlichen Stelle und beim Dienstleister), Sammlung, Lagerung, Transport, Vernichtung und Kontrolle zugeordnet, die an Hand von Tabellen im Hinblick auf die erforderliche Schutzklasse zu prüfen sind.

11.3.4 Löschen personenbezogener Daten auf Datenträgern

Die DIN 66399 ordnet personenbezogene Daten (z. B. Adressdaten) bereits in die Schutzklasse 1 ein. Die Datenträger, auf denen die personenbezogenen Daten gespeichert sind, bedürfen nach der Klassifizierung gemäß DIN 66399 jedoch mindestens einer Vernichtung nach Sicherheitsstufe 3.

Gesundheitsdaten sind besondere Arten personenbezogener Daten nach § 33 Absatz 1 des Landesdatenschutzgesetzes (LDSG) bzw. § 3 Absatz 9 BDSG, unterfallen der höchsten Schutzklasse 3 und damit mindestens einer Vernichtung nach Sicherheitsstufe 4.

Ein Beispiel: Meist bewegt sich Schriftgut (Material: Papier) in den Bereichen

- Sicherheitsstufe 3:
  Sensible und vertrauliche Daten sowie personenbezogene Daten, die einem erhöhten Schutzbedarf unterliegen.
- Sicherheitsstufe 4:
  Besonders sensible und vertrauliche Daten sowie personenbezogenen Daten, die einem erhöhten Schutzbedarf unterliegen.

- Sicherheitsstufe 5:
  Geheim zu haltende Informationen mit existenzieller Wichtigkeit für eine Person, ein Unternehmen oder eine Einrichtung.

Ich empfehle zur datenschutzgerechten Vernichtung des anfallenden Schriftguts mit Informationsdarstellung in Originalgröße auf Papier mit personenbezogenen Daten als Inhalt gemäß DIN 66399 das Schreddern mit mindestens Sicherheitsstufe P-4, bei geheimzuhaltenden Informationen mit mindestens Sicherheitsstufe P-5.

Die Informationsdarstellung und Datenträgerart (Materialklassifikation) sind zu berücksichtigen. So ist bei Halbleiterspeichern aufgrund der geringen Bauteilgröße unbedingt darauf zu achten, dass nicht nur das Medium (z. B. USB-Stick), sondern auch der Speicherchip selbst tatsächlich (mehrfach) zerteilt wird.

Beim **Löschen von sensiblen oder vertraulichen Daten** auf magnetischen Datenträgern ist zu gewährleisten, dass die Daten sicher, d. h. vollständig und unumkehrbar, gelöscht werden. Einfache Löschbefehle des jeweiligen Betriebssystems oder auch das Formatieren des Datenträgers reichen hierzu in der Regel nicht aus, denn dabei werden nur die Indexeinträge modifiziert. Die Daten selbst bleiben auf dem Datenträger erhalten und können mit frei verfügbaren Softwarewerkzeugen leicht wiederhergestellt werden. Daten, die sicher gelöscht werden sollen, müssen durch **physikalische Maßnahmen** (mechanische oder thermische Zerstörung, magnetische Durchflutung des Datenträgers) oder durch mehrmaliges Überschreiben unkenntlich gemacht werden. Das Löschverfahren, die Ergebnisse sowie das Datum sind zu dokumentieren, damit die verantwortliche Stelle nachweisen kann, ihrer Verantwortung beim Umgang mit dem Datenträger nachgekommen zu sein.

Ist die Möglichkeit gegeben, die Datenträger jederzeit direkt vor Ort durch den jeweils Verantwortlichen der Daten zu vernichten, so erhöht dies wesentlich die Sicherheit und ist anderen Verfahren vorzuziehen.

Fallen Daten unterschiedlicher Sicherheitsstufen an, wird eine Trennung in die verschiedenen Sicherheitsstufen empfohlen. Ist dies nicht möglich, so muss eine Vernichtung grundsätzlich und einheitlich gemäß der höheren Sicherheitsstufe erfolgen, um das Risiko einer unzureichenden Vernichtung zu minimieren.

Der verantwortlichen Stelle obliegt die Prüfung und Anpassung ihres Entsorgungskonzepts zur datenschutzgerechten Vernichtung von Datenträgern unter Berücksichtigung der DIN 66399, die Festlegung des Schutzbedarfs und die Zuordnung der erforderlichen Schutzklassen und Sicherheitsstufen sowie die Prüfung und Anpassung der Bestandsverträge zur Datenträgerentsorgung an die neue DIN 66399.

Die DIN 66399 führt die DIN 32757-1 konsequent fort. Die meisten Anwender dürften auf der sicheren Seite sein, wenn sie für die Vernichtung von Datenträgern Schredder der geforderten Sicherheitsstufe verwenden und das Vorgehen an den Handlungsempfehlungen der Norm ausrichten. Professionelle Datenträgervernichter verfügen zudem über eingespielte und weitgehend sichere Prozessabläufe. Meldepflichtige Vorfälle sind in den letzten Jahren hier nur vereinzelt bekannt geworden. Die neue Norm berücksichtigt erfreulicherweise auch aktuelle technische Entwicklungen. Bei Datenpannen dürfte daher eine Entschuldigung durch die Berufung auf Unkenntnis künftig schwerfallen.

11.4 Cloud-Lösungen für Verwaltung und Wirtschaft

11.4.1 Cloud Computing - zum Stand der Diskussion

Seit der Behandlung des Themas im 30. Tätigkeitsbericht (LT-Drs. 15/955, S 44 f.) haben sich verschiedene Projekte fortentwickelt, so dass datenschutzrechtliche Anforderungen an das Cloud Computing weiter konkretisiert werden können. So verkündete etwa im öffentlichen Bereich im Frühjahr 2013 eine Gemeinde aus dem Heckengäu,

sie werde in Zusammenarbeit mit einem großen IT-Konzern kommunale Verwaltungsverfahren in die Cloud eben jenes Konzerns auslagern. Ich habe die Gemeinde gebeten, mir eine rechtliche und technische Darstellung des Unterfangens zukommen zu lassen. Im privaten Bereich werden vielfach Beratungswünsche an mich herangetragen, wie es mit der datenschutzrechtlichen Zulässigkeit spezifischer Dienste bestellt sei. Zwar können die nachfolgenden Darstellungen eine gewisse Orientierung bieten, aber eine einzelfallbezogene Beratung nicht ersetzen, für die meine Mitarbeiter und ich im Rahmen unserer Kapazitäten zur Verfügung stehen.

Die in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011 (vgl. 30. Tätigkeitsbericht, LT-Drs. 19/955, Anhang 22) und mit der **Orientierungshilfe „Cloud computing“**[44] beleuchteten datenschutzrechtliche Inhalte sind nun mit Leben zu füllen; dabei wird konkret zu klären sein, wie die allgemeinen Anforderungen nach offenen, transparenten und detaillierten Informationen der Cloud Computing Anbieter zu technischen, organisatorischen und rechtlichen Rahmenbedingungen der angebotenen Dienstleistungen umgesetzt werden können. Wie müssen die geforderten transparenten, detaillierten, eindeutigen und vertraglich verbindlichen Regelungen der Cloud gestützten Datenverarbeitung in einem Vertrag formuliert werden? Wie soll insbesondere festgehalten werden, an welchem Ort die Daten verarbeitet werden, obwohl das Geschäftsmodell des Cloud Computing aus Gründen der optimalen Kapazitätsauslastung im Grunde „nomadisierende“ Datenbestände voraussetzt? Um EU-weit eine einheitliche Behandlung zu gewährleisten, hat sich die Artikel-29-Gruppe zum Ziel gesetzt, einen Verhaltenskodex für Cloud Computing Anbieter („Cloud Data Processor Code of Conduct“) zu erstellen. In den Erörterungsprozess über zu treffende Maßnahmen ist auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) eingetreten. Dessen Ausarbeitung „Sicherheitsempfehlungen für Cloud Computing Anbieter“ benennt Anforderungen an die Informationssicherheit, die Cloud Computing Anbieter nach Auffassung des Bundesamts erfüllen sollten. Aus den genannten Darstellungen kristallisiert sich der folgende, vorläufige, datenschutzrechtliche Anforderungskatalog heraus:

- **Systeme und Management**
  Der Cloud Computing Anbieter sollte in der Lage sein, geeignete technische und organisatorische Maßnahmen umzusetzen (Rechenzentrum-Sicherheit, Server-Sicherheit, Netzwerk-Sicherheit, Cloud-Dienst-Sicherheit, Datensicherheit, Kryptographie). Er muss geeignete Systeme zur Authentisierung, Autorisierung und zum Zugriffsschutz implementieren und deren korrekte Arbeitsweise durch Überwachungssysteme sicherstellen. Hierfür sollte er ein organisatorisches und technisches Managementsystem installieren.
- **Sicherheitsmanagement**
  Die Systeme sollten in ein umfassendes Sicherheitsmanagement eingebunden sein.
- **Privacy by design**
  Die Soft- und Hardwaresysteme des Anbieters sollten dem Prinzip des “privacy by design“ folgen. Das heißt, dass schon beim rechtlichen und technischen Entwurf der Cloud-Dienste datenschutzrechtliche Aspekte berücksichtigt werden sollen. Nur dann ist gewährleistet, dass bei der Inbetriebnahme den datenschutzrechtlichen Vorgaben entsprochen werden kann und sich keine Lücken bei der Verarbeitung hinsichtlich der Vertraulichkeit, Integrität und Authentizität der personenbezogenen Daten auftun.
- **Personal**
  Das Personal des Anbieters und ggf. der Unterauftragnehmer sollte datenschutzrechtlich verpflichtet werden. Die Eignung der Mitarbeiter sollte geprüft werden. Bei Beendigung der Tätigkeit sollten die ausscheidenden Mitarbeiter auf ihre Pflichten hingewiesen werden.
- **Kontrollmöglichkeit**
  Der Anbieter sollte es den Anwendern ermöglichen zu prüfen, ob die zugesagten Eigenschaften des Cloud-Dienstes eingehalten werden. Die technischen Komponenten sollten so beschaffen sein, dass die Anwender die Möglichkeit haben zu kontrollieren, ob die

[44] *http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Orientierungshilfe_Cloud-Computing_AK_Technik_AK_Medien_.pdf*

personenbezogenen Daten datenschutzrechtlich zulässig verarbeitet werden. Das heißt, dass den Anwendern über eine Schnittstelle eröffnet werden sollte, lesend auf die für diese Beurteilung erforderlichen Systeminformationen zugreifen zu können.

- **Protokollierung, Überwachung und Ereignismanagement**
  Die Systemaktivitäten und Eingriffe in die Systeme von Seiten der Systemverwaltung sollten protokolliert werden. Der Anbieter sollte in der Lage sein, die Funktionsfähigkeit seiner Cloud-Dienste zu überwachen und bei Eintreten von Angriffen auf die Systeme zeitnah geeignete Gegenmaßnahmen zu ergreifen.
- **Malware und Backup**
  Der Anbieter muss die Systeme gegen Schadsoftware schützen. Er muss für eine konsistente Sicherung der personenbezogenen Daten sorgen.
- **Notfallmanagement**
  Der Anbieter sollte ein Notfallmanagement installieren, das Maßnahmen beschreibt, die im Notfall zu ergreifen sind. Im Notfall sollten Ausweichmöglichkeiten (Auslegung von redundanter Soft- und Hardware, geographische Lokation) bestehen. Mit den Anwendern abgestimmte Prozeduren für den Wiederanlauf sollten beschrieben werden.
- **Portabilität und Interoperabilität**
  Wenn Cloud-Dienste bei mehreren Anbietern genutzt werden, sollte sichergestellt sein, dass die Dienste, sofern erforderlich, zusammenarbeiten. Es könnten Gründe bestehen, dass Dienste zu einem anderen Anbieter migriert werden müssen. Deshalb sollte der Portabilität der Dienste Beachtung geschenkt werden.
- **Nachhaltigkeit**
  Der Anbieter sollte gewährleisten, dass technische Änderungen an einem Cloud-Dienst zu keiner Verringerung der Vertraulichkeit, Integrität und Authentizität der personenbezogenen Daten führen.
- **Verantwortlichkeit der Anwender**
  Der Anbieter sollte die Verantwortlichkeiten der Anwender bzw. von Personal der Anwender ausdrücklich benennen und auf die Folgen bei Nichtbeachtung hinweisen.
- **Weisungsgebundenheit**
  Der Anbieter darf personenbezogene Daten nur auf Weisung des Kunden verarbeiten. Diese Anforderung spiegelt die Anforderung in den einschlägigen Vorschriften zur Verarbeitung personenbezogener Daten im Auftrag wider.
- **Rechtskonformität der Anwender**
  Cloud Computing Anwender, die personenbezogene Daten verarbeiten, unterliegen regelmäßig der Kontrolle einer Aufsichtsbehörde. Der Cloud Computing Anbieter sollte die Anwender bei der Erfüllung ihrer rechtlichen Verpflichtungen gegenüber der Aufsichtsbehörde unterstützen.
- **Datenübermittlung**
  Der Anbieter sollte sich verpflichten, dass personenbezogene Daten nicht in Länder übermittelt werden, für die nicht die gleiche Datenschutzgesetzgebung wie für den Anwender anzuwenden ist, es sei denn, dass die für den Anwender maßgebliche Datenschutzgesetzgebung die Übermittlung erlaubt.
- **Rechte der Betroffenen**
  Wenn Cloud-Anwender personenbezogene Daten mit einem Cloud Dienst verarbeiten, sollte gewährleistet sein, dass die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung gewahrt werden. Der Cloud-Computing-Anbieter sollte den Anwender in der Erfüllung dieser Rechte unterstützen.
- **Rechte Dritter**
  Der Cloud-Computing-Anbieter sollte den Anwender bei der Erfüllung direkter oder indirekter Rechte Dritter unterstützten.
- **Kooperation mit Aufsichtsbehörden**
  Der Anbieter sollte mit allen Datenschutzaufsichtsbehörden, die gesetzliche Aufgaben im Zusammenhang mit dem angebotenen Cloud-Dienst erfüllen, zusammen arbeiten.
- **Unterauftragsverhältnisse**
  Wenn ein Anbieter Dritte mit der Wahrnehmung von Aufgaben betraut, die den Cloud-Dienst realisieren oder dazu beitragen, sollten dem Anwender die Verarbeitungen, die der Unterauftragnehmer vornimmt, offen gelegt und erklärt werden, welche personenbezogenen Daten an den Unterauftragnehmer über-

mittelt werden. Die Unterauftragnehmer sollten vom Anbieter benannt werden.

- **Maßnahmen nach Vertragsende**
  Der Anbieter sollte darstellen, welche Prozesse er nach Vertragsbeendigung durchführt. Insbesondere sollte die Löschung personenbezogener Daten beim Anbieter geregelt werden.
- **Sicherheitsüberprüfung und -nachweise**
  Der Anbieter sollte die Sicherheit seiner Systeme von unabhängigen Stellen überprüfen lassen.
- **Eignung**
  Der Anbieter sollte seine organisatorische und fachliche Eignung nachweisen.

Schwierigkeiten bereitet die Gewichtung der Anforderungen in konkreten Anwendungsfällen, weshalb aus der Reihenfolge keine implizite Gewichtung abgeleitet werden sollte.

Die vielfältigen Probleme der rechtlichen und technischen Gestaltung des Cloud Computing hat auch das Bundesministerium für Wirtschaft erkannt und mit dem Technologieprogramm „Trusted Cloud“ die Entwicklung sicherer und rechtskonformer Cloud-Lösungen gefördert. Eine Reihe von Projekten wurde auf Kiel gelegt, deren Ergebnisse aus datenschutzrechtlicher Sicht hoffentlich geeignet sind, das notwendige Vertrauen der Anwender zu schaffen und mehr als Worthülsen in Hochglanzprospekten zu bieten.

Aus datenschutzrechtlicher Sicht wird beim Cloud Computing häufig der einfache Umstand übersehen, dass es sich regelmäßig um eine **Datenverarbeitung im Auftrag** handelt. Cloud Computing Anwender in der EU müssen deshalb prüfen, ob es bei der beabsichtigten Verarbeitung zu einer Übermittlung von personenbezogenen Daten in ein Drittland kommt und ob dieses Land ein angemessenes Datenschutzniveau hat. Gegebenenfalls ist der *Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates* einschlägig. Wenn es zur Übermittlung kommt, ist mit dem Cloud Computing Anbieter ein Vertrag abzuschließen, der die genannten Standardvertragsklauseln oder juristisch gleichwertige Formulierungen enthält. Wenn der Vertrag von einem Cloud Computing Anbieter vorgegeben wird, muss der Anwender prüfen, ob der Vertragstext die Anforderungen der Standardvertragklauseln erfüllt. Die im Einzelfall aufwendige Prüfung wurde in der „opinion 05/2013 on Cloud Computing“ der Artikel-29-Gruppe unter Nummer 3.5 ausführlich dargestellt. Ich will deshalb hier nur kurz aufzeigen, wo ich inhaltlich Abweichungen der Vertragsklauseln der Anbieter von den Standardvertragsklauseln festgestellt habe:

- Der Cloud Computing Anbieter muss die Möglichkeit der **Prüfung (Audit) vor Ort durch den Anwender** oder von ihm Beauftragte eröffnen. Der für den Anwender zuständigen Datenschutzaufsichtsbehörde muss ein Prüfrecht eingeräumt werden.
- **Einschränkungen** dahingehend, dass Abmachungen nur gelten, sofern es dem Anbieter (von dritter Seite) nicht verboten wird, sie zu erfüllen, sind unzulässig.
- Der Anbieter muss eine genaue **Frist** nennen, nach der er bei Vertragsende alle Daten in Speichern, Zwischenspeichern und Sicherungskopien löscht.
- Wenn der Anbieter **Unterauftragsnehmer** einschaltet, muss dieser Umstand unter Nennung des Unterauftragnehmers dem Anwender vorab mitgeteilt werden.
- Optimal wäre es, wenn sich der Anwender vom Anbieter bestätigen lassen kann, dass dieser die **Daten nur an einem bestimmten Ort** verarbeitet.

Damit bei verbreiteten Cloud Computing Diensten nicht jeder Anwender eine Prüfung vornehmen muss, sollten deren Anbieter darauf achten, dass ihre Individualverträge mit den **Standardvertragsklauseln** übereinstimmen. Deshalb steht die Artikel-29-Gruppe mit führenden Cloud Computing Anbietern in Verbindung, um sie auf die Defizite ihrer Vertragswerke hinzuweisen und sie zu veranlassen, die datenschutzrechtlichen Formulierungen zu verbessern.

Die vielfältigen Aktivitäten zahlreicher Gremien und Einrichtungen im In- und Ausland und die Formulierung von Anforderungskatalogen können

nicht über die Probleme hinwegtäuschen, die bei der Verarbeitung personenbezogener Daten in Clouds weiterhin bestehen. Denn letzten Endes ist der in einem Drittstaat ansässige Cloud-Anbieter der Jurisdiktion seines Landes unterworfen. Das könnte bedeuten, dass beispielsweise nationale **Sicherheitsbehörden des Drittstaats** legal unbeschränkten Zugriff auf die Daten haben oder sich verschaffen können (vgl. 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 46). Das sollte jeder bedenken, der meint, personenbezogenen Daten, aus welchen profanen Erwägungen auch immer, aus den Händen geben zu müssen.

11.4.2 Kann Dropbox unbedenklich genutzt werden?

Dropbox ist einfach zu verwenden, beliebt - und sicher? Mit Dropbox können Dateien zwischen Rechnern oder Smartphones synchronisiert werden. Und weil dies auch offline geschehen kann, werden bei Dropbox die Nutzerdateien verschlüsselt gespeichert. Aber den (privaten) Schlüssel, für jeden Nutzer einen, hält Dropbox quasi in den eigenen Händen.

Die rechtliche Situation

Die Dropbox Inc., USA, bietet ihren Speicherdienst auch in Deutschland an und unterliegt damit den Normen des Bundesdatenschutzgesetzes (BDSG). Nach § 1 Absatz 5 Satz 2 BDSG findet das Gesetz Anwendung, wenn der Hauptgeschäftssitz außerhalb der Europäischen Union oder des Europäischen Wertschaftraums liegt und personenbezogene Daten im Inland erhoben, verarbeitet und genutzt werden.

Findet allerdings die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten statt, entfällt die Anwendung des Bundesdatenschutzgesetzes (§ 1 Absatz 2 Nummer 3 BDSG). Zur Verarbeitung zählen unter anderem die Speicherung, Übermittlung und Löschung (§ 3 Absatz 4 Satz 1 BDSG).

Der Webdienst, den die Dropbox Inc. anbietet, ist im Wesentlichen ein Speicher- und Synchronisationsdienst. Damit lässt sich das Betriebsmodell von Dropbox als Cloud Computing in Form des Infrastructure as a Service (IaaS) klassifizieren (siehe auch 30. Tätigkeitsbericht, LT-Drs. 15/955, S. 44 ff.). Als zentrales Speichersystem kommt der von der Amazon.com Inc., USA, angebotene Cloud-Speicher Amazon Simple Storage Service (S3) zum Zuge. Die eigentliche Datenspeicherung erfolgt also nicht bei der Dropbox Inc., sondern bei der Amazon.com Inc.

Die funktionelle Leistung von Dropbox liegt in der Synchronisation der Daten zwischen verschiedenen Rechnern mit Hilfe des Cloud-Speichers der Amazon.com.

Dropbox ist als **Cloud-Anbieter** einzustufen. Ein Cloud-Anbieter ist jede natürliche oder juristische Person, die Cloud-Dienste zur Verfügung stellt (siehe auch Orientierungshilfe - Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0, abzurufen unter http://www.baden-wuerttemberg.datenschutz.de/technik). Hierzu kann, wie im Falle von Dropbox, der Cloud-Anbieter auch Unter-Anbieter, wie Amazon.com, einbeziehen.

Ein **Cloud-Anwender** ist jede natürliche oder juristische Person, die von Betroffenen personenbezogene Daten erhebt, verarbeitet oder nutzt und hierfür Cloud-Dienste in Anspruch nimmt. Betroffene können beispielsweise die Mitarbeiter in einem Unternehmen sein, wenn für das Teammanagement Dropbox eingesetzt wird.

Da sowohl der Cloud-Anbieter Dropbox Inc. als auch der Unter-Anbieter Amzon.com Inc. in den USA ihre Verarbeitungen vornehmen, gelten die besonderen Anforderungen des Bundesdatenschutzgesetzes für eine Datenübermittlung in das außereuropäische Ausland. Als Nachweis dafür, dass die Datenübermittlungen von und zu Dropbox mit dem europäischen Datenschutzniveau in Einklang stehen, hat sich Dropbox nach eigenen Angaben zur Einhaltung der Safe-Habor-Grundsätze verpflichtet (https://www.dropbox.com/help/238/en). Allerdings bleibt ein hier ansässiger Cloud-Anwender nach deutschem Datenschutzrecht in der Verantwortung, im Rahmen eines Vertrages zur Auftragsdatenverarbeitung den Schutz des allgemeinen Per-

sönlichkeitsrechts von Betroffenen und der Ausübung der damit verbundenen Rechte zu gewährleisten. Vor dem Hintergrund von Ausspähskandalen wie PRISM dürfte es für Cloud-Anwender aber immer schwieriger werden, diese Verantwortung und die verbundenen Kontrollaufgaben effektiv wahrzunehmen.

Die technischen Aspekte

Bei der Übertragung vom Dropbox-Client, der beispielweise auf dem Arbeitsplatzrechner oder Smartphone installiert ist, und der anschließenden Ablage der Daten auf dem Speichersystem werden diese verschlüsselt. Dazu bedient sich Dropbox der Transportverschlüsselung Secure Sockets Layer (SSL) und der AES-256-Bit-Verschlüsselung für die gespeicherten Daten. Dropbox gibt sowohl das Verschlüsselungsverfahren als auch den Schlüssel (serverseitig) vor. Einen eigenen (privaten) Schlüssel verwenden zu können, anstelle des vorgegebenen, wird nach Angaben von Dropbox für die Zukunft in Erwägung gezogen (https://www.dropbox.com/help/28/en).

Will man dennoch Dropbox mit eigener Verschlüsselung nutzen, muss man auf Verschlüsselungsprodukte Dritter zurückgreifen. Für private Zwecke bieten sich beispielsweise Truecrypt oder Boxcryptor an. Oder man verzichtet gänzlich auf die Cloud-Dienste von Dropbox und setzt mit ownCloud seinen eigenen Cloud-Server auf.

Kleine und mittlere Unternehmen, die sich dennoch der Cloud-Dienste von Dropbox oder eines anderen Cloud-Anbieters mit Hauptgeschäftssitz außerhalb der Europäischen Union oder des Europäischen Wertschaftraum bedienen wollen, sollten auf jeden Fall ein Verschlüsselungsprodukt nach ihren Anforderungen einsetzen. Was hierbei alles zu beachten gilt, ist in der IT-Grundschutz-Maßnahme „Auswahl eines geeigneten kryptographischen Produktes“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgeführt (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02165.html).

Die Übermittlung und Speicherung personenbezogener Daten mittels der Dropbox-Dienste unterliegen deutschem Datenschutzrecht. Aufgrund des Geschäftssitzes der Dropbox, Inc. in den USA gelten die besonderen Bestimmungen für die Datenübermittlung in Drittstaaten. Auch wenn die Dropbox Inc. angibt, die Vorgaben des Safe Harbor Framework Abkommens einzuhalten, besteht infolge des US Patriot Act bzw. des Foreign Information Security Act (FISA) das Risiko, dass US-Sicherheitsbehörden jederzeit auf die bei Dropbox gespeicherten Daten zugreifen können. Daran ändert auch die Verschlüsselung der Daten durch Dropbox nichts, weil Dropbox den Schlüssel vorgibt.

Eine Verschlüsselung mit eigenem privatem Schlüssel ist daher sehr zu empfehlen. Die Auswahl des Verschlüsselungsalgorithmus und eines ihn unterstützenden kryptographischen Produkts sollte an den eigenen Anforderungen und dem erforderlichen Schutzbedarf ausgerichtet sein. Auf was dabei zu achten ist, kann beispielsweise den IT-Grundschutz-Katalogen des BSI entnommen werden.

Inhaltsverzeichnis des Anhangs

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2012/2013

Anhang 1	Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke
Anhang 2	Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln
Anhang 3	Ein hohes Datenschutzniveau für ganz Europa!
Anhang 4	Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz
Anhang 5	Patientenrechte müssen umfassend gestärkt werden
Anhang 6	Orientierungshilfe zum datenschutzgerechten Smart Metering
Anhang 7	Melderecht datenschutzkonform gestalten!
Anhang 8	Einführung von IPv6 Hinweise für Provider im Privatkundengeschäft und Hersteller
Anhang 9	Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben
Anhang 10	Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten
Anhang 11	Europäische Datenschutzreform konstruktiv und zügig voranbringen!
Anhang 12	Beschäftigtendatenschutz nicht abbauen, sondern stärken!
Anhang 13	Pseudonymisierung von Krebsregisterdaten verbessern
Anhang 14	Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten
Anhang 15	Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor
Anhang 16	Europa muss Datenschutz stärken
Anhang 17	Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen
Anhang 18	Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln
Anhang 19	Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!
Anhang 20	Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages
Anhang 21	Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

31. Tätigkeitsbericht 2012/2013 - Inhaltsverzeichnis des Anhangs

Beschlüsse des Düsseldorfer Kreises 2012/2013

Anhang 22 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft
Anhang 23 Near Field Communikation (NFC) bei Geldkarten
Anhang 24 Videoüberwachung in und an Taxis
Anhang 25 Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Anhang 1

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 02. Februar 2012**

**Schuldnerverzeichnis im Internet:
Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.
Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

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

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

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

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

31. Tätigkeitsbericht 2012/2013

Anhang 2

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

Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat.

Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden. Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

Anhang 3

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

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren. Der Entwurf einer Datenschutz-Grundverordnung enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen

und

- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten. Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

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

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

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis
- eine Anhebung der Altersgrenze,
- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

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

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

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

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

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung).

Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

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

Anhang 4

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

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

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

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

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

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

31. Tätigkeitsbericht 2012/2013

Anhang 5

Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 23. Mai 2012

“Patientenrechte müssen umfassend gestärkt werden”

Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!

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

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

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

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.
- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.
- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

Anhang 6

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 27. Juni 2012**

Orientierungshilfe zum datenschutzgerechten Smart Metering

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

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.
- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

31. Tätigkeitsbericht 2012/2013

Anhang 7

Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 22. August 2012

Melderecht datenschutzkonform gestalten!

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

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

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

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

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage. Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.
- Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.
- Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.
- Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.
- Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.

- Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.
- Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

31. Tätigkeitsbericht 2012/2013

Anhang 8

Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. November 2012

Einführung von IPv6
Hinweise für Provider im Privatkundengeschäft und Hersteller

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

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.
- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.
- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.
- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.
- Interface Identifier und Präfix sollten synchron gewechselt werden.
- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.
- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.
- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.
- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.
- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der

IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.

- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.
- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

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

31. Tätigkeitsbericht 2012/2013

Anhang 9

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. November 2012**

**Reform der Sicherheitsbehörden:
Der Datenschutz darf nicht auf der Strecke bleiben**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich "überzogene" Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und ggf. wieder hergestellt werden.
Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

Anhang 10

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. November 2012**

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

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

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

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

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

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

31. Tätigkeitsbericht 2012/2013

Anhang 11

Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 7./8. November 2012

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

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

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

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die sog. alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.
  Jede Verarbeitung scheinbar “belangloser” Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich “belanglose” Daten von einer Regelung auszunehmen.
  Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.
- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.
- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.
- Mit Blick auf die Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

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

Anhang 12

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 25. Januar 2013**

Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.
- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.
- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.
- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.
- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

31. Tätigkeitsbericht 2012/2013

Anhang 13

Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 13./14.03.2013

Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden sog. Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert.

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

Anhang 14

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 13./14.03.2013**

Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

31. Tätigkeitsbericht 2012/2013

Anhang 15

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 13./14.03.2013**

**Soziale Netzwerke brauchen Leitplanken –
Datenschutzbeauftragte legen Orientierungshilfe vor**

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

Anhang 16

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 13./14.03.2013**

Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.
- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.
- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.
- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.
- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.
- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.
- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.

- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.
- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.
- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

Anhang 17

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 05. September 2013**

**Keine umfassende und anlasslose Überwachung durch Nachrichtendienste!
Zeit für Konsequenzen**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u. a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.
- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.
- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prü-

fen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.

- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen. Dazu gehört, - zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann. - sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben. - die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.
- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.
- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

Anhang 18

**Entschließung der Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 01. Oktober 2013**

**Sichere elektronische Kommunikation gewährleisten -
Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln**

Die elektronische Datenübermittlung zwischen den Bürgern bzw. der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung “Sicherheit bei E Government durch Nutzung des Standards OSCI” Bund, Ländern und Kommunen empfohlen hat. Das sog. Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

31. Tätigkeitsbericht 2012/2013

Anhang 19

**Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 01. Oktober 2013**

**Forderungen für die neue Legislaturperiode:
Die Datenschutzgrundrechte stärken!**

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt – wie repräsentative Studien belegen – mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.
- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.
- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z. B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

Anhang 20

**Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 01. Oktober 2013**

**Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit
in der 18. Legislaturperiode des Deutschen Bundestages**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung “Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen” verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

31. Tätigkeitsbericht 2012/2013

Anhang 21

Entschließung der Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 01. Oktober 2013

Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von “gläsernen Patientinnen und Patienten oder Versicherten” weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.
- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.
- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

Anhang 22

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 17. Januar 2012)**

**Einwilligungs- und Schweigepflichtentbindungserklärung
in der Versicherungswirtschaft**

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten.

Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen.

Anhang 23

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 18./19. September 2012)

Near Field Communikation (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

Anhang 24

**Beschluss der Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 26./27. Februar 2013)**

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis,

sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

Anhang 25

**Beschluss der Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich
(Düsseldorfer Kreis am 11./12. September 2013)**

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z.B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

Stichwortverzeichnis

AES-256 167
Akkreditierung
  Sicherheitsbereiche 53
Aktivierungslink 131
akustische Wohnraumüberwachung 61
Alkohol am Arbeitsplatz 126
Amazon Simple Storage 166
Anklageschrift
  Anschrift von Zeugen 72
Anti-Counterfeiting Trade Agreement (ACTA) 24
Antiterrordatei 62
API-Daten 24
Arbeitgeberauskunft 126
ArchiSafe 23
ArchiSig 23
ärztliche Privatpatienten-Leistungen
  Abrechnung der Forderungen durch Verrechnungsstellen 108
ASD-BW 117, 121
ASV-BW 118
Auskunfteien 145
BEA 110
Behandlungsvertrag nach § 630a BGB 108
Beherbergungsbetrieb 79
Beschäftigtendatenschutz 29
Bestandsdatenauskunft 42
Bettensteuer 79
Big Data 15
Bildungsnummer, landeseinheitliche 121
Bildungsplanreform 2015, Beirat 125
BLIDS 90
Bluetooth
  Lokalisierung 90
  Reisezeitermittlung 90
Boxcryptor 167
Bundesamt für Verfassungsschutz 66
Bundeskriminalamt 47, 63
Bundesmeldegesetz 81
Bundesverfassungsschutzgesetz
  Amtshilfe 66
Bundeszentralamt für Steuern 74
Clearingstelle des Landesapothekerverbands Baden-Württemberg 109
Cloud Computing 162
  Orientierungshilfe 163
  Standardvertragsklauseln 165
Com Vor 47
Datenschutzbeauftragter, behördlicher 77
  Fortbildung 117
Datenschutzbeauftragter, betrieblicher
  außerordentliche Kündigung 129
  datenschutzrechtlicher Widerrufs- und Kündigungsschutz 130
  Grundverhältnis 130
  Kündigung 129
  Pflicht zur Bestellung 108
  Widerruf der Bestellung 129
Datenschutzerklärung 133
Datenträgervernichtung 160
De-Mail 22, 31
Deutschland-online 46, 57
digitales Wasserzeichen 140
DIN 66399 160
DNA-Identifizierungsmuster 48
Drohnen
  unbemannte Luftfahrtsysteme 50
  Videoüberwachung 50
Dropbox 166
ECHELON 10
E-Government-Gesetz des Bundes 30
eID-Funktion 22
Einwilligungs- und Schweigepflichtentbindungserklärung
  Gesundheitsdaten, Versicherungen 107
Einwilligungserklärung 49, 58

Elektronische Signatur 22
ELENA-Verfahren 110
ELStAM 74
ElsterOnlinePortal 74
E-Mail-Newsletter 131
E-Mail-Werbung 131, 138
erkennungsdienstliche Behandlung 47
Ermittlungsmaßnahmen 69
EU-Datenschutz-Grundverordnung 18
Europäische Ermittlungsanordnung 68
Facebook 120, 154, 158, 159
Fanpage 120, 157
Finanzamt
  Zentrale Informations- und Annahmestellen (ZIA) 75
Flugpassagierdaten 23
Foreign Account Tax Compliance Act (FATCA) 25
fortgeschrittene Signatur 23
Funktionsübertragung
  in Justizvollzugsanstalt 71
  Teilprivatisierung 71
Gaststättengesetz
  Gestattungen nach § 12 54
Geldwäscheprävention 143
Gemeinderatssitzungen
  Live-Stream 78
  Pilotprojekte 78
  Podcast 78
Geschäftsgeheimnis 145
Gesetz gegen den unlauteren Wettbewerb (UWG) 131
Gesetzentwurf des Bundesrats zur Änderung des Telemediengesetzes (Drucksache 156/11) 28, 156
Gesundheitsdaten 108
Gewerbeordnung
  § 34a - Bewachungsgewerbe 54
GFHQ 9
großer Lauschangriff 61
Handelsübereinkommen zur Bekämpfung von Produkt- und Markenpiraterie (ACTA) 24
Haushaltsstatistik 74
Hilfsmittelverordnung 109
Hochschule für Polizei 57
iFrame 159
Infektionsschutzgesetz
  Zuständigkeit des Polizeivollzugsdiensts 41
Informationsmodell Polizei (IMP) 46
INPOL-Verbund 46
Instagram 155
Interessenbekundungsverfahren 58
IP-Adresse
  Auskunft über den Inhaber 42
Jedermannverzeichnis 149
Jobcenter 111
Justizvollzugsanstalt
  Funktionsübertragung 71
  Teilprivatisierung 71
  Übertragung von Vollzugsaufgaben 71
Kennzeichenerfassung (Kfz) 44
Kindertageseinrichtungen
  Anspruch auf einen Platz 115
  Broschüre 115
Klarnamenpflicht 157
Kodex für soziale Netzwerke 34
Kommunalabgaben 79
Kommunale Veröffentlichungen 78
Kontaktpersonen 64
Kontoauszüge 112
Kontrollbefugnis bei Staatsanwaltschaften 69
Krankenhaus
  Babygalerie 104
  Datenverlust 100
Krebsfrüherkennungs- und registergesetz
  Landeskrebsregistergesetz 94
Krebsregister 96
Kreditinstitute 145

Kündigung des betrieblichen
Datenschutzbeauftragten im
Insolvenzverfahren 129
LABIS 47
Landesamt für Verfassungsschutz 62, 66
Amtsdatei 65
Landeskriminalamt 56, 57, 60
Online-Sicherheits-Portal 56
Landesverfassungsschutzgesetz 61
Auskunft 66
Lehreraus- und -fortbildung 122
Like-Button 155, 159
Luftverkehrsgesetz 51
Luftverkehrsordnung 51
MDK-Gutachten 113
Melderecht
Hotelmeldepflicht 82
Meldescheine 82
Mitwirkung Wohnungsgeber 82
Widerspruchsmöglichkeit 82
Melderegisterauskünfte 81
Mikrozensus 74
Mitarbeiterdatenbank (MADB) der Polizei 48
MMS-Werbung 138
Musikdateien 140
NADIS 65
Nationales Waffenregister 57
NSA 9
OMS 110
Online-Datenschutzerklärung 133
Optimized CPM 156
Orientierungshilfe
Krankenhausinformationssysteme
(OH KIS) 97
OWi 21 86
ownCloud 167
Patientenrechte 92
Patientenrechtegesetz 92
Personalakten 127
Personalausweis 111
personengebundene Hinweise 46
Pflegeeinrichtungen 106
Pflegestützpunkte 104
PNR-Daten 23
POLAS-BW 47
Polizeigesetz
Änderungen 40
Durchführungsverordnung 42, 60
polizeiliche Auskunftssysteme
Datenspeicherung 46
Protokollierung von Abrufen 46
Polizeilicher Informations- und
Analyseverbund (PIAV) 46
Polizeistrukturreform 42, 57, 58
Clearingkommission 59
Personalkommissionen 59
Personalvertretungen 59
Predictive Policing 18
Protokolldaten 63
Pseudonymisierung 96
qualifizierte elektronische Signatur 23
Quellen-Telekommunikationsüberwachung 69
Rechtsextremismus-Datei-Gesetz 64
Register nach § 38 Absatz 2 des
Bundesdatenschutzgesetzes 148
Registrierungsprogramm
für Reisende (RTP) 24
Richtlinie über die Europäische
Ermittlungsanordnung 68
Safe Harbor 12, 26
Schufa 146
Schulbesuchsverordnung 118
Schule
Entschuldigungen 118
Fehlzeiten 118
Unterrichtsthema Datenschutz 123
Zusammenarbeit mit meiner Dienststelle
117
Schulverwaltungsprogramm 117
Schulwechsel 119
Secure Sockets Layer (SSL) 167

Selbstauskunft 145
  Verweigerung 145
Signaturgesetz (SigG) 23
Signaturrichtlinie 22
SMS-Werbung 138
Social Plug-In 120, 158, 159
Sozialamt 113
Soziale Netzwerke 34, 120, 154
Spähaffäre 9
Standardvertragsklauseln 26
  beim Cloud Computing 165
Steuerschuldner 79
Stiftung Datenschutz 33
Strafverfolgung
  grenzüberschreitende 68
Telekommunikationsüberwachung 69
Terrorismusabwehr 62
Tracking 156
Trennungsgebot/Trennungsprinzip 62
Truecrypt 167
Trugspur 48
Twitter 155, 159
unbemannte Luftfahrtsysteme
  Drohnen 50
Unterrichtungspflichten 133
Urheberrecht 140
USA Patriot Act 13, 167
verdeckte Ermittlungsmaßnahmen 69
Verfahrensübersicht 149
Verfahrensverzeichnis 149
Verfahrensverzeichnis, Schulen 117
Verkehrsordnungswidrigkeiten 86
Veröffentlichung von Bildern 78
Verwertungsrechte 140
Videoüberwachung 150
  an Schulen 153
  in Arztpraxen 151
  in und an Taxis 150
  verdeckte 50
  Wildkameras 152
Vorabkontrolle der Datenverarbeitung 108
Vorratsdatenspeicherung 41
Waffenbehörden 56
Waffengesetz 55
Werbung 131
  Bestätigungsmail 131
  Double-Opt-in 131
  Einwilligung 131
Whatsapp 155
Wohnungseigentümergemeinschaft 144
XING 35, 155
Zensus 2011 74
Zeugenschutz
  Anklageschrift 72
Zuverlässigkeitsprüfung 51
  § 5 Waffengesetz 51
  Bewerber für den Polizeivollzugsdienst 52
  dienstlich genutzte Gebäude 52
  Mitarbeiter von Sicherheitsdiensten 53
  Personal von Abschleppbetrieben 53
  Tag der Deutschen Einheit 2013 51
  Waffenbesitzer 54
Zwei-Klick-Button 158, 159