Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014

25. Tätigkeitsbericht

Tätigkeitsbericht 2013-2014

25. Tätigkeitsbericht

Dieser Bericht wurde am 17. Juni 2015 dem Präsidenten des Deutschen Bundestages, Herrn Dr. Norbert Lammert, überreicht.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Andrea Voßhoff

Unterrichtung

durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht 2013 und 2014 der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - 25. Tätigkeitsbericht -

Inhaltsverzeichnis

Im Tätigkeitsbericht sind nur die Entschließungen abgedruckt, auf die in den Beiträgen unmittelbar Bezug genommen wird. Alle Entschließungen der Datenschutzkonferenzen und weitere Informationen finden Sie auf der Internetseite der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.datenschutz.bund.de

Einführung

Der vorliegenden Tätigkeitsbericht ist der 25. Bericht seit Bestehen der Behörde des/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Nun ist die Zahl 25 oftmals Anlass einer ausdrücklichen Würdigung. Bei besonderen Ereignissen, wie z. B. Betriebszugehörigkeiten oder Dienstjubiläen oder sonstigen besonderen Ereignissen gibt die Zahl immer Gelegenheit zu einem Rückblick aber auch Ausblick. Zu diesem Bericht auch? In Anbetracht der gewaltigen Herausforderungen für den Datenschutz in der digitalen Welt sollte vielleicht die schlichte Anzahl der Tätigkeitsberichte der BfDI nicht an so prominenter Stelle in den Vordergrund gerückt werden. Da die ersten 13 Tätigkeitsberichte zudem Jahresberichte waren und der Berichtszeitraum erst seit dem 14. Tätigkeitsbericht zweijährig erfolgt, ist auch die Anzahl nicht gleichzusetzen mit einem Jubiläum der Dienststelle oder dem BDSG an sich.

Anlass, es doch zu tun, liefert ein immer lohnenswerter Blick in den ersten Tätigkeitsbericht, der das Berichtsjahr 1978, dem ersten Jahr der Geltung des BDSG mit dem Aufbau der Behörde, beschreibt.

Darin stellt der erste Bundesbeauftragte für den Datenschutz, Hans Peter Bull, gleich einleitend zu dem Bericht fest (1. TB, Bundestagsdrucksache 8/2460, Ziffer 1.1, S. 4):

„Der Gedanke, den Rechtsschutz des einzelnen bei der Datenverarbeitung durch eine besondere staatliche Kontrollinstanz zu gewährleisten, wurde im Parlament geboren. Der Regierungsentwurf eines BDSG (BT-Drs. 7/1027) sah eine solche Einrichtung noch nicht vor.“

Es war also das damalige Parlament, das den Weg einer staatlichen Kontrollinstanz ebnete. Erwähnenswert ist diese damalige Feststellung in diesem 25. Tätigkeitsbericht, weil im Berichtszeitraum 2013/2014 der Deutsche Bundestag mit dem mittlerweile in Kraft getretenen Gesetz zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde (Bundestagsdrucksache 18/ 2848) die BfDI zum 1. Januar 2016 aus der Dienstaufsicht des BMI und der Rechtsaufsicht der Bundesregierung herauslöst und damit - entsprechend den Vorgaben des EuGH - die völlige Unabhängigkeit herstellt und künftig die BfDI neben der gerichtlichen Kontrolle nur noch der parlamentarischen Kontrolle unterworfen ist.

Damit wird die vorausschauende Idee des damaligen Parlaments zur Einrichtung der staatlichen Aufsicht nach 36 Jahren vollständig umgesetzt und ist im 25. Tätigkeitsbericht ein mehr als bedeutsamer Berichtspunkt. Neben der damaligen parlamentarischen Entscheidung zur Einrichtung einer staatlichen Datenschutzaufsicht ist deren künftige völlige Unabhängigkeit im schwierigen „Fahrwasser“ des Datenschutzes in der digitalen Welt ein weitreichendes politisches Signal für eine Stärkung der staatlichen Kontrollinstanz auf Bundesebene.

So sehr einerseits die künftige Architektur der staatlichen Kontrollinstanz als politisches Signal bedeutsam ist, so fundamental haben im Berichtszeitraum u. a. die Enthüllungen Snowdens sowie die weitere rasante technologische Entwicklung der Digitalisierung existenzielle Fragen des Datenschutzes weiter herausgefordert.

In seiner Rede zum Tag der Deutschen Einheit im Jahr 2013 hat der Bundespräsident in beeindruckender Weise einen Befund herausgearbeitet, der kaum treffender die existenziellen Grundfragen des Rechts auf informationelle Selbstbestimmung darstellen kann.

So heißt es in seiner Rede:

„Wohin dieser tiefgreifende technische Wandel führen wird, darüber haben wir einfachen „User“ bislang wenig nachgedacht. Erst die Berichte über die Datensammlung der Dienste befreundeter Länder haben uns mit einer Realität konfrontiert, die wir bis dahin für unvorstellbar hielten. Erst da wurde den meisten die Gefahr für die Privatsphäre bewusst.

Vor 30 Jahren, erinnern wir uns, wehrten sich Bundesbürger noch leidenschaftlich gegen die Volkszählung und setzten am Ende das Recht auf informationelle Selbstbestimmung durch. Dafür hat das Bundesverfassungsgericht gesorgt. Und heute? Heute tragen Menschen freiwillig und gedankenlos bei jedem Klick ins Netz Persönliches zu Markte. Viele der Jüngeren vertrauen sozialen Netzwerken sogar ihr ganzes Leben an. Ausgeliefertsein und Selbstauslieferung sind kaum voneinander zu trennen ... Historisch betrachtet sind Entwicklungssprünge nichts Neues. Im ersten Moment erleben wir sie allerdings ratlos, vielleicht auch ohnmächtig. Naturgemäß hinken dann Gesetze, Konventionen und gesellschaftliche Verabredungen der technischen Entwicklung hinterher. Wie noch bei jeder Innovation gilt es auch jetzt, die Ängste nicht übermächtig werden zu lassen, sondern als aufgeklärte und ermächtigte Bürger zu handeln. So sollte der Datenschutz für den Erhalt der Privatsphäre so wichtig werden wie der Umweltschutz für den Erhalt der Lebensgrundlagen. Wir wollen und sollen die Vorteile der digitalen Welt nutzen, uns gegen ihre Nachteile aber bestmöglich schützen."

In diesem Sinne haben der so treffend dargestellte Befund und die sich daraus ergebenden Fragestellungen die Arbeit meines Hauses im Bereich der Beratung und Kontrolle im Berichtszeitraum geprägt. Mehr als unbefriedigend sind bisher die Antworten der Politik auf den existenziell gefährdeten Datenschutz, die durch die Enthüllungen Snowdens aber auch durch die ökonomische Datennutzung im Zeitalter von Big Data mehr als dringlich geboten sind. Auch wenn die „Digitale Agenda" der Bundesregierung durchaus vielversprechende Aussagen enthält, sie bedürfen der umfassenden und konsequenten Umsetzung. Vorsichtig optimistisch stimmt mich zudem, dass die Arbeiten an der so dringend nötigen Harmonisierung des europäischen Datenschutzrechts im Jahr 2014 wieder Fahrt aufgenommen haben.

Sind Daten global, muss auch der Schutz international sein. Dabei gilt es, ein hohes Datenschutzniveau nicht kommerziellen Interessen zu opfern oder zu schleifen. Wenn es heißt, Daten seien der Rohstoff des 21. Jahrhunderts, dann halte ich dagegen, dass personenbezogene Daten grundrechtlich geschützt sind. Sie sind Ausdruck unseres Persönlichkeitsrechts, das für unser gesellschaftliches Zusammenleben existenziell ist und nach meinem Verständnis unser Menschenbild prägt. Dieses Verständnis sollte Grundlage politisches Handelns in allen Fragen eines modernen Datenschutzes sein.

Der in diesem Tätigkeitsbericht erfasste Zeitraum beinhaltet auch das Jahr 2013 und damit noch einen Zeitraum, der in die Verantwortung meines Amtsvorgängers, Peter Schaar, fällt. Ihm darf ich an dieser Stelle für seine hervorragende Arbeit danken. Am 19. Dezember 2013 hat mich der Deutsche Bundestag zur Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt und am 6. Januar 2014 habe ich das Amt übernommen.

Neu an der Aufstellung des Berichts ist die Zuordnung der Themenfelder teilweise entsprechend der Arbeitsaufteilung der Ausschüsse des Deutschen Bundestages. Diese Darstellung unterstreicht die Bedeutung des Datenschutzes als Querschnittsaufgabe. Fragestellungen des Datenschutzes insbesondere in der digitalen Welt berühren eine Vielzahl von Gesetzgebungsvorhaben sehr nachhaltig und intensiv.

Insbesondere auch aus diesem Grunde ist es u. a. notwendig und wäre wünschenswert, ähnlich wie die Stellungnahme des Normenkontrollrates künftig auch die Ressortstellungnahmen der BfDI zum Bestandteil eines jeden Gesetzentwurfes zu machen, der parlamentarisch beraten wird.

Mit der Vorlage dieses Berichts darf ich mich sehr herzlich bei den Mitarbeiterinnen und Mitarbeitern des Hauses bedanken, die überwiegend die im Bericht dargestellten Tätigkeiten und Kontrollen ausgeführt haben. Ihr hoher Einsatz und ihr nahezu unermüdliches Engagement im Interesse des Datenschutzes sind insbesondere in Anbetracht der defizitären Personalausstattung in besonderer Weise erwähnenswert.

Den Bürgerinnen und Bürger, die mit ihren Eingaben aus der „gelebten" Datenschutzpraxis immer wieder auf Missstände hinweisen, darf ich ebenfalls sehr herzlich für ihren Einsatz für den Datenschutz danken.

Ebenso gilt mein Dank den Abgeordneten des Deutschen Bundestages aller Fraktionen sowie allen Institutionen, die sich auf vielfältige Art und Weise für den Datenschutz einsetzen und meine Mitarbeiter und mich in der täglichen Arbeit unterstützen.

Andrea Voßhoff

Zusammenfassung aller Empfehlungen

Ich empfehle dem Gesetzgeber im Bereich der Kontrolle der Nachrichtendienste zur Vermeidung von Kontrolllücken eine klarstellende gesetzliche Regelung zur Ausgestaltung der Kontrollstruktur. Ebenso empfehle ich, die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013 und 9. Oktober 2014 zur Unzulässigkeit anlassloser Überwachungen und zur effektiven Kontrolle der Nachrichtendienste zu berücksichtigen (Nr. 2.1.1 und Anlage 6 und 11).

Ich appelliere an den Gesetzgeber, meinen Forderungen nach dringend notwendiger personeller Verstärkung meiner Behörde jetzt zügig und angemessen Rechnung zu tragen, insbesondere auch bei der beabsichtigten Ausgestaltung meines Hauses als oberste Bundesbehörde. Nur dann ist eine effiziente Aufsicht im Sinne der Vorgaben des Bundesverfassungsgerichts (Urteil vom 24.04.2013, Az. 1 BvR 1215/07) zu gewährleisten (Nr. 2.4; 5.2).

Ich rege an, der BfDI die Möglichkeit einzuräumen, ihren turnusmäßigen Tätigkeitsbericht auch im Plenum des Bundestages vorstellen zu dürfen. Damit wird die Bedeutung des Datenschutzes in der digitalen Welt in besonderer Weise seitens des Parlaments zum Ausdruck gebracht.

Ich rege zudem an, die Stellungnahmen der BfDI im Rahmen von Ressortabstimmungen - ähnlich, wie die Stellungnahmen des NKR - den Gesetzgebungsvorhaben der Bundesregierung bei Einbringung in die parlamentarische Beratung beizufügen.

Ich empfehle dem Gesetzgeber, Konzeption und Finanzierung der Stiftung Datenschutz neu zu überdenken. Die Koordinierung der wissenschaftliche Begleitung der gesellschaftlichen Veränderungen durch die Digitalisierung und deren fundamentale Auswirkungen auf das informationelle Selbstbestimmungsrecht des Einzelnen ist unumgänglich. Die Stiftung Datenschutz könnte hier einen zentralen Platz einnehmen (Nr. 2.5).

Ich empfehle der Bundesregierung, die Datenschutzbehörden bei der Umsetzung der Digitalen Agenda hin zu einer datenschutzgerechten digitalen Gesellschaft einzubinden (Nr. 18.1).

Ich empfehle dem Gesetzgeber, Eingriffsbefugnisse der Sicherheitsbehörden in regelmäßigen Abständen auf ihre Effektivität, Notwendigkeit und Verhältnismäßigkeit zu überprüfen (Nr. 5.13).

Ich empfehle dem Gesetzgeber, eine bereichsspezifische gesetzliche Regelung für die Aufzeichnung von beim BKA eingehenden Telefongesprächen zu schaffen (Nr. 5.13.7).

Ich empfehle dem Bundesministerium der Justiz und für Verbraucherschutz, die Schuldnerverzeichnisführungsverordnung (SchuFV) dahingehend zu ändern, dass namensgleichen, aber nicht im Schuldnerverzeichnis eingetragenen Betroffenen ein Recht zugesprochen wird, auf eine mögliche Verwechslung mit dem eingetragenen Schuldner hinzuweisen und entsprechende Warnhinweise in das Schuldnerverzeichnis aufnehmen zu lassen (Nr. 6.6.1).

Ich empfehle dem Bundesministerium der Justiz und für Verbraucherschutz, bei der Veröffentlichung von Insolvenzbekanntmachungen auf dem elektronischen, länderübergreifend eingerichteten Justizportal www.insolvenzbekanntmachung.de den fehlenden Kopierschutz, die Speicherfristen und die unbeschränkte Suche innerhalb der ersten zwei Wochen überprüfen zu lassen (Nr. 6.6.2).

Ich empfehle dem Gesetzgeber, die Auskunftsansprüche in der StPO übersichtlich zu regeln (Nr. 6.8).

Ich empfehle dem Gesetzgeber eine Verbesserung: Wenn eine Eintragung durch fehlende rechtzeitige Mitteilung der Staatsanwaltschaft zu spät aus dem ZStV gelöscht wird, erhalten diejenigen Stellen keine Berichtigungsmeldung, die in der Zeit zwischen dem gesetzeskonformen Löschtermin und der tatsächlichen Löschung Auskunft erhalten haben. Eine solche Mitteilung ist bislang gesetzlich nicht vorgeschrieben und das derzeitige Verfahren deshalb nicht zu bemängeln. Gleichwohl sollte eine solche Mitteilung im Gesetz geregelt werden (Nr. 6.9).

Ich empfehle dem Gesetzgeber, beim Kontenabrufverfahren Rechtslage und Praxis der Abrufersuchen in Einklang zu bringen und dadurch die Kontenabrufersuchen auf das Notwendige zu begrenzen (Nr. 7.2).

Ich empfehle dem Bundesministerium der Finanzen, Kunden von der Regelabfrage dann auszunehmen, wenn eine Nichtveranlagungsbescheinigung vorliegt oder über einen längeren Zeitraum keine Kapitalerträge angefallen sind (Nr. 7.6).

Ich empfehle dem Bundesministerium der Finanzen, nochmals öffentlichkeitswirksam über den veränderten Verwaltungsvollzug bei der Kraftfahrzeugsteuer und das Widerrufsrecht der Lastschrifteinzugsermächtigung zu informieren (Nr. 7.7).

Ich empfehle dem Bundesministerium der Finanzen, die „Dienstanweisung zum Kindergeld nach dem Einkommensteuergesetz“ überarbeiten zu lassen und dort datenschutzgerechte Regelungen zu Aktenaufbewahrungs- und Löschungsfristen aufzunehmen (Nr. 7.8).

Ich empfehle der Bundesregierung, für die Identifizierung von Kunden nach dem Geldwäschegesetz auf die Möglichkeiten einer Videoidentifizierung zu verzichten. Es ist weder die Wirksamkeit einer solchen Identifizierung geklärt, noch entspricht dies den Vorgaben des Personalausweisgesetzes. Außerdem ist nicht sichergestellt, dass die anfallenden personenbezogenen Daten datenschutzkonform verarbeitet werden (Nr. 7.11).

Ich empfehle dem Gesetzgeber, mir stärkere Sanktionsmöglichkeiten gegenüber Telekommunikations- und Postdienstunternehmen einzuräumen und die Zuständigkeit für Bußgeldverfahren bei Verstößen gegen das Bundesdatenschutzgesetz zu übertragen (Nr. 8.7).

Ich empfehle dem Gesetzgeber, den offensichtlich unbeabsichtigten Wertungswiderspruch im §109a TKG durch eine gesetzliche Klarstellung zu beseitigen Nach § 109a TKG ist die Meldepflicht aufgrund des eindeutigen Wortlauts gegenwärtig auf die Erbringer von Telekommunikationsdienstleistungen im Sinne des § 3 Nummer 6a) TKG beschränkt. Mitwirkende gemäß § 3 Nummer 6b) TKG sind hingegen nicht zu einer Meldung verpflichtet. Damit wäre ein Diebstahl aller Kundendaten, die ihren Vertrag bei einem Vertriebspartner eines Telekommunikationsunternehmens abgeschlossen haben, nicht meldepflichtig, während der Diebstahl derselben Daten bei dem Telekommunikationsunternehmen selbst unter die Vorschrift des § 109a TKG fallen würde. (Nr. 8.7.1).

Ich empfehle dem Gesetzgeber, die Einwilligungslösung vor Setzen eines Cookies durch eine normenklare Regelung im Telemediengesetz umzusetzen (Nr. 8.8.1).

Ich empfehle dem Gesetzgeber, eine Änderung des § 75 SGB X herbeizuführen, die sowohl die Interessen der Wissenschaft als auch die Rechte der betroffenen Bürgerinnen und Bürger angemessen berücksichtigt (Nr. 9.5).

Ich empfehle dem Gesetzgeber, eine klarstellende Änderung des § 200 Absatz 2 SGB VII auf den Weg zu bringen, damit eine Umgehung des Regelungsgehalts zum Nachteil der Versicherten künftig ausgeschlossen ist (Nr. 9.6).

Ich empfehle dem Bundesministerium der Verteidigung, eine technische Lösung zur Datenlöschung nach Ablauf der Archivierungsfristen entwickeln zu lassen (Nr. 11.1.2).

Ich empfehle dem Gesetzgeber, durch eine Ergänzung des § 91 Absatz 5a SGB V klarzustellen, dass, wenn der G-BA mir Gelegenheit zur Stellungnahme gibt, die aus seiner Sicht maßgeblichen Erwägungen zum Datenschutz beizufügen sind (Nr. 13.6).

1 Revision des europäischen Datenschutzrechts

1.1 Datenschutz-Grundverordnung vor dem Abschluss?

Seit Januar 2012 wird über den von der Europäischen Kommission vorgelegten Entwurf einer Datenschutz-Grundverordnung im Rat der Europäischen Union und im Europäischen Parlament verhandelt. Dieses Reformvorhaben habe ich in den vergangenen zwei Jahren intensiv begleitet. Im Berichtszeitraum sind die Arbeiten entscheidend vorangekommen, mit einer Verabschiedung dieser Verordnung im Jahr 2015 ist zu rechnen.

Die Europäische Kommission hatte sich im Jahr 2012 bei der Präsentation ihrer Vorschläge das ehrgeizige Ziel gesetzt, die Datenschutz-Grundverordnung (DSGVO) bis zur Neuwahl des Europäischen Parlaments im Mai 2014 zu verabschieden. Zwar wurde dieses Ziel verfehlt, die Arbeiten sind jedoch vor allem im Jahr 2014 so weit vorangekommen, dass eine Verabschiedung im Jahr 2015 wahrscheinlich ist.

Zum Inhalt des Kommissionsvorschlages, seiner Struktur und datenschutzrechtlichen Bewertung hatte ich bereits in meinem 24. Tätigkeitsbericht (Nr. 2.1.1) ausführlich Stellung genommen.

Konnte man zwischenzeitlich durchaus daran zweifeln, ob die europäische Datenschutzreform überhaupt zustande kommt, hat das Europäische Parlament das Reformvorhaben entscheidend voran gebracht: Die vom zuständigen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) bereits im Oktober 2013 beschlossene gemeinsame Position hat das Plenum des Parlaments im März 2014 bestätigt und damit die erste Lesung im Parlament abgeschlossen. Nahezu 4.000 Änderungsanträge hatte der LIBE-Ausschuss hierfür in einem Kraftakt bewertet und zu einem Kompromissvorschlag zusammengeführt. Auch inhaltlich kann sich diese Einigung sehen lassen. Datenschutzbehörden in Deutschland und Europa sowie Vertreter der Zivilgesellschaft haben die Vorschläge ganz überwiegend positiv bewertet. Sie enthalten auch aus meiner Sicht beachtliche Verbesserungen gegenüber dem Entwurf der Kommission, der seinerseits schon gute Ansätze enthielt.

Im Rat der Europäischen Union gestalteten sich die Verhandlungen im Vergleich dazu wesentlich mühsamer. Dies ist einerseits angesichts der unterschiedlichen Interessen von 28 Mitgliedstaaten verständlich. Andererseits haben jedoch auch große Mitgliedstaaten - darunter Deutschland - durch ihre Verhandlungsführung zunächst nicht zu einer zügigen Beratung beigetragen. Nach der Einigung im Parlament ist der Rat jedoch sichtbar bestrebt, in konstruktiven und zielorientierten Verhandlungen zügig zum Ziel zu kommen. Dies wurde im Laufe des Jahres 2014 auch von der Bundesregierung zunehmend unterstützt.

Der Rat der Innen- und Justizminister hat sich über verschiedene Kapitel und horizontale Fragen der DSGVO grundsätzlich geeinigt: Dazu zählen die grundsätzlichen Aspekte des Marktortprinzips (Art. 3 Abs. 2 DSGVO, vgl. Nr. 1.2.7), die Übermittlung personenbezogener Daten in Drittstaaten (Kapitel V der DSGVO, vgl. Nr. 1.2.6), die Pflichten des Verantwortlichen (Kapitel IV der DSGVO) und die Geltung der DSGVO für die Datenverarbeitung im öffentlichen Bereich (Teile der Art. 1, 6 und 21, vgl. Nr. 1.2.1) einschließlich spezifischer Öffnungsklauseln für das mitgliedstaatliche Recht (Kapitel IX der DSGVO). In weiteren Kapiteln konnten ebenfalls Fortschritte erzielt werden.

Trotz dieser beachtlichen Entwicklung wird es unter der lettischen Ratspräsidentschaft noch erheblicher Anstrengungen bedürfen, um das Ziel einer Einigung über die gesamte DSGVO im Juni 2015 erreichen zu können.

Ebenso wie meine Kolleginnen und Kollegen in den Ländern und den anderen Mitgliedstaaten der EU habe ich mich konstruktiv, aber auch kritisch in die datenschutzpolitische Debatte eingebracht, um in den Verhandlungen immer wieder den Blick auf die Grundrechte der Menschen in Europa zu lenken.

So hat sich die 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschließung „Europa muss den Datenschutz stärken“ (vgl. Anlage 3) und entsprechenden Erläuterungen (vgl. Anlage 4) zu verschiedenen grundsätzlichen Themen der Datenschutzreform geäußert. In einer weiteren Entschließung zur Struktur der künftigen Datenschutzaufsicht in Europa hat sich die 87. Konferenz für eine starke und bürgernahe Datenschutzaufsicht und eine effiziente Kooperation der Datenschutzbehörden ausgesprochen und verbindliche Kompetenzen für den zu schaffenden Europäischen Datenschutzausschuss gefordert (vgl. unten Nr. 1.2.5).

Auch die Artikel-29-Gruppe hat sich regelmäßig mit der DSGVO befasst. Neben Stellungnahmen zu den Beschlüssen des Rates der Innen- und Justizminister und zum so genannten risikobasierten Ansatz (vgl. Nr. 1.2.3) stand auch hier einmal mehr die künftige Struktur der Datenschutzaufsicht und die Kooperation der Datenschutzbehörden im Mittelpunkt (vgl. Nr. 1.2.5).

Im November 2014 habe ich gemeinsam mit dem Europäischen Datenschutzbeauftragten in Brüssel eine Veranstaltung zur Reform des Europäischen Datenschutzrechts organisiert. Diese bot eine hervorragende Gelegenheit, sich mit hochrangigen Entscheidungsträgern über die erzielten Fortschritte bei den Verhandlungen und die noch offenen Fragen intensiv auszutauschen.

Angesichts der globalen Dimension der Verarbeitung personenbezogener Daten und der damit verbundenen enormen Herausforderungen für den Datenschutz halte ich ein Gelingen der Reform des europäischen Datenschutzrechts im Interesse der Bürgerinnen und Bürger, aber auch von Wirtschaft und Verwaltung für dringend notwendig. Nur ein starkes europäisches Datenschutzrecht kann eine Antwort auf die Herausforderungen des Internets, von Big-Data-Technologien und Cloud Computing, von Profiling und letztlich der sensorischen und elektronischen Erfassung aller Lebensbereiche geben und so weltweite Wirkung entfalten.

Quelle: Greser & Lenz, rdv-online

1.2 Wichtige Einzelaspekte der Datenschutz-Grundverordnung

Die insgesamt positive Entwicklung setzt sich aus vielen Bausteinen zusammen, von denen die wichtigsten im Folgenden genauer betrachtet werden.

1.2.1 Die Datenschutz-Grundverordnung soll auch für die öffentliche Verwaltung gelten!

Die Frage, ob auch die öffentliche Verwaltung - soweit es sich nicht um Behörden im Bereich der Strafverfolgung handelt - in den Anwendungsbereich der Datenschutz-Grundverordnung einbezogen werden soll, scheint nunmehr positiv beantwortet zu sein.

Wie bereits in meinem 24. Tätigkeitsbericht unter Nr. 2.1.1 erläutert, hat die Europäische Kommission die Regelungsstruktur der Europäischen Datenschutzrichtlinie von 1995 aufgegriffen und den öffentlichen Bereich grundsätzlich mit in den Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) einbezogen. Auch das Europäische Parlament hat diesen Ansatz in seinem Beschluss vom März 2014 nicht in Frage gestellt.

Wie sich jedoch bei den Verhandlungen im Rat gezeigt hat, stehen einige Mitgliedstaaten dieser Einbeziehung kritisch gegenüber. Hier hat insbesondere Deutschland eine zentrale Rolle gespielt. Dies ist insofern verständlich, als Deutschland vor allem im öffentlichen Bereich über ein in Jahrzehnten gewachsenes ausdifferenziertes bereichsspezifisches Datenschutzrecht verfügt, das Bund und Länder weitgehend erhalten wollen.

Ich habe das Ziel immer unterstützt, das bereichsspezifische Datenschutzrecht in Deutschland möglichst zu erhalten, soweit es sich um notwendige Präzisierungen auf im Vergleich zur DSGVO gleichem oder höherem Datenschutzniveau handelt. Allerdings war ich gegen ein Herausnehmen des öffentlichen Bereichs aus der DSGVO, stattdessen habe ich mich dafür ausgesprochen, den öffentlichen Bereich in die DSGVO einzubeziehen und die notwendigen Spielräume innerhalb der DSGVO zu schaffen, um das Gelingen der Reform insgesamt nicht zu gefährden (vgl. 24. TB Nr. 2.1.1).

Ob ein Erhalt des bereichsspezifischen Datenschutzrechts angesichts einer europäischen Verordnung europarechtlich überhaupt möglich sei, war lange unklar. Anders als die geltende Richtlinie von 1995 ist eine Verordnung unmittelbar anwendbares europäisches Recht, das keiner Umsetzung in nationales Recht mehr bedarf und eine solche auch nicht zulässt. Die Kommission hatte in ihrem Entwurf bereits Spielräume für das mitgliedstaatliche Recht vorgesehen, um bestimmte Einzelheiten der Verarbeitung personenbezogener Daten im öffentlichen Bereich regeln zu können. Diesen Ansatz hat das Europäische Parlament in seinem Vorschlag vom März 2014 aufgegriffen und den Spielraum für die nationalen Gesetzgeber konkretisiert. Auch im Rat zeichnete sich ab, dass die grundsätzliche Einbeziehung des öffentlichen Bereichs in den Anwendungsbereich der Verordnung von einer großen Mehrheit der Mitgliedstaaten akzeptiert wird.

Um den Bedenken der Bundesregierung und der Länder Rechnung zu tragen, hat die italienische Ratspräsidentschaft ebenfalls den grundsätzlichen Ansatz von Kommission und Parlament weiterverfolgt und für Artikel 1 der DSGVO eine generelle Öffnungsklausel vorgeschlagen. Diese soll es den Mitgliedstaaten ermöglichen, bei der Datenverarbeitung im öffentlichen Interesse oder durch Behörden zur Erfüllung öffentlicher Aufgaben spezifische Regelungen beizubehalten oder neue zu erlassen. Bedenken gegen die europarechtliche Zulässigkeit einer solchen Öffnungsklausel konnten ausgeräumt werden. Das von mir unterstützte Petitum der Bundesregierung, die Mitgliedstaaten auch zu solchen Regelungen zu ermächtigen, mit denen ein über die DSGVO hinausgehendes Datenschutzniveau geschaffen wird, hat der Rat aber bedauerlicherweise nicht aufgegriffen.

Weiterhin sollen in Kapitel IX für besondere Situationen weiterhin spezielle Öffnungsklauseln geschaffen werden, angesichts der allgemeinen Öffnungsklausel allerdings nur noch für den Ausgleich zwischen Datenverarbeitung und Meinungsfreiheit (vgl. Nr. 1.2.2), für das Verhältnis zu Informationsfreiheitsgesetzen und zur Infor-

mationsweiterverwendung, für die Datenverarbeitung im Beschäftigtenverhältnis, für die Datenverarbeitung zu wissenschaftlichen, statistischen, historischen und archivischen Zwecken sowie für die Datenverarbeitung durch Kirchen und religiöse Vereinigungen.

Aus deutscher Sicht lag dabei zum einen ein besonderes Augenmerk bei der Verarbeitung personenbezogener Daten durch Archive im öffentlichen Interesse. Dabei ging es nicht nur darum, für das Bundes- und die Landesarchive verlässliche Rahmenbedingungen für ihre künftige Arbeit zu schaffen, sondern auch darum, den besonderen Bedürfnissen des Bundesbeauftragten für die Stasi-Unterlagen Rechnung zu tragen. Insbesondere war darauf zu achten, dass datenschutzrechtliche Verpflichtungen - wie etwa das Recht auf Vergessen - dem wichtigen öffentlichen Interesse an einer dauerhaften Aufbewahrung und Verfügbarkeit (zeit-)historisch bedeutsamer Dokumente nicht zuwider laufen. Dies kann durch die vom Rat vorgeschlagene Öffnungsklausel gewährleistet werden.

Zum anderen war ich mir mit der Bundesregierung darüber einig, dass bei der Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis ein hohes Datenschutzniveau gelten muss, das - zugunsten der Beschäftigten - möglichst auch über die Anforderungen der DSGVO hinausgehen kann. Dabei wurde offenbar, dass hierfür die allgemeine Öffnungsklausel für den öffentlichen Bereich nicht genügen würde, denn die Datenverarbeitung erfolgt im Beschäftigungsverhältnis sehr weitgehend auch durch Unternehmen oder andere private Institutionen. Deshalb schlug der Rat auch hierfür eine Öffnungsklausel vor, wonach die Mitgliedstaaten die Datenverarbeitung in diesem Kontext konkretisieren können. Mit ihrem weitergehenden Vorschlag, den Mitgliedstaaten auch die Regelung eines höheren Datenschutzniveaus zu ermöglichen, ist die Bundesregierung bedauerlicherweise nicht durchgedrungen.

Diesem hier skizzierten Gesamtansatz haben die Mitgliedstaaten im Rat der Innen- und Justizminister im Dezember 2014 grundsätzlich zugestimmt.

Aus meiner Sicht stellt die Einigung im Rat einen guten Kompromiss dar, auf dessen Grundlage der weitaus größte Teil des bereichsspezifischen Datenschutzrechts in Deutschland und anderen Mitgliedstaaten erhalten bleiben kann. Soweit im Einzelnen noch kritische Punkte bestehen, hoffe ich auf Verbesserungen im anstehenden Trilog zwischen Kommission, Parlament und Rat.

1.2.2 Datenschutz und Meinungsfreiheit - ein Gegensatz?

Kann eine höchstgerichtliche Entscheidung zur Stärkung des Datenschutzes gleichzeitig die Meinungs- und Informationsfreiheit schwächen? „Ja“ behaupten einige und fordern daher die Einführung eines Streitschlichtungsmechanismus, um die Grundrechte in ein angemessenes Verhältnis zu bringen.

Das Google-Suchmaschinen-Urteil (vgl. Nr. 2.3.2) hat Datenschützer applaudieren lassen. Auch mich freut es, dass der Europäische Gerichtshof (EuGH) mit dieser Entscheidung ein weiteres Mal den Datenschutz als wichtiges Grundrecht herausgestellt hat, das es gerade in der heute immer weiter vernetzten und digitalisierten Welt zu bewahren gilt. Diese weitreichende Stärkung des Schutzes personenbezogener Daten durch den EuGH hat allerdings auch kritische Stimmen hervorgerufen, die das Urteil als zu einseitig und als Gefährdung der Meinungs- und Informationsfreiheit sehen. Wenn einzelne Beiträge im Internet durch das Löschen der entsprechenden Verlinkung bei Suchmaschinenbetreibern nicht mehr auffindbar seien, könne dies die grundrechtlich geschützte Meinungs- und Informationsfreiheit massiv einschränken.

Ich teile diese Bedenken nicht: Zum einen verlangt der EuGH nicht, Beiträge und Veröffentlichungen nicht mehr über Suchmaschinen auffindbar zu machen. Das Auffinden soll nur bei einer bestimmten Kombination von Suchbegriffen, die zudem noch zwingend im konkreten Zusammenhang mit einer bestimmten Person stehen, erschwert sein. Ein Zeitungsartikel z. B. kann daher auch dann weiterhin über Suchmaschinenbetreiber ge-

funden werden, wenn die Suchparameter die konkrete Person, die die Löschung des Links beauftragt hat, nicht miteinbeziehen. Auch wenn dies das Auffinden einzelner Beiträge erschweren kann, werden diese nicht vollständig unterdrückt. Im Übrigen gibt es keinen Rechtsanspruch auf Auffindbarkeit von Beiträgen in einer Suchmaschine (vgl. im Einzelnen Nr. 2.3.2).

Außerdem muss - und das ist für mich entscheidend - jeder Entscheidung über eine Aufhebung der Verlinkung stets eine umfassende Abwägung sämtlicher betroffener Rechte vorangehen. Hierbei ist selbstverständlich neben dem Recht auf informationelle Selbstbestimmung des Antragstellers auch die Meinungs- und Informationsfreiheit Dritter zu berücksichtigen.

Wie das BMI aber offensichtlich befürchtet, könnten sich die Verfahrensbeteiligten nicht an diese Grundsätze halten. Daher fordert es einen sogenannten Streitschlichtungsmechanismus im Rahmen der DSGVO. Eine unabhängige, nicht staatliche Stelle soll für alle verbindlich überprüfen, ob im Rahmen eines Löschantrages auch die Interessen der Autoren der betroffenen Veröffentlichungen hinreichend berücksichtigt und die in Rede stehenden Grundrechte der Beteiligten in ein ausgewogenes Verhältnis gebracht worden sind. Eine entsprechende Bindung der Datenschutzaufsichtsbehörden wird es dabei selbstverständlich nicht geben, so dass diese unabhängig von einem solchen Streitschlichtungsverfahren angerufen werden und - wie vom EuGH vorgesehen - betroffene Antragsteller bei der Durchsetzung ihrer Rechte unterstützen können.

Auch wenn ich grundsätzlich keine Einwände gegen unabhängige Streitschlichtungsmechanismen habe, sehe ich keine Notwendigkeit für eine solche Regelung. Auch der Rat der Europäischen Union hat bereits auf das Urteil des EuGH reagiert und eine Änderung in die DSGVO eingefügt: Artikel 80, der bereits vorher die Abwägung der in Rede stehenden Grundrechte forderte, wurde dahingehend erweitert, dass neben der Meinungsfreiheit künftig auch die Informationsfreiheit mit dem Recht auf Datenschutz abgewogen und abgestimmt werden soll. Hierzu können die Mitgliedstaaten nun im nationalen Recht Ausnahmen von bestimmten Kapiteln der DSGVO vorsehen.

1.2.3 Der risikobasierte Ansatz

Seit Beginn der Beratungen über die Datenschutz-Grundverordnung wird intensiv darüber diskutiert, ob das bisherige Regelungsmodell im Datenschutz durch ein risikobasiertes Modell ersetzt oder zumindest flankiert werden soll.

Die Europäische Kommission folgt mit der DSGVO dem gleichen Regelungsmodell, das schon der Europäischen Datenschutzrichtlinie von 1995 und dem deutschen Datenschutzrecht zugrunde liegt: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur dann erlaubt, wenn der Betroffene eingewilligt hat oder eine Rechtsgrundlage die Verarbeitung erlaubt. Dieses Regelungsmodell hat sich bewährt, weil entweder der Betroffene selbst entscheiden kann, wie mit seinen Daten umgegangen wird, oder der Gesetzgeber sich darüber Gedanken machen muss, ob eine Datenverarbeitung im überwiegenden Gemeinwohlinteresse notwendig und verhältnismäßig ist.

Dieses Modell sichert die Autonomie des Einzelnen und macht die Verarbeitung personenbezogener Daten ein Stück weit vorhersehbar und transparent. Dies gilt auch gerade in Zeiten von Internet und Big-Data-Technologien: Je unübersichtlicher die Datenverarbeitung wird, umso wichtiger ist ein klarer und transparenter rechtlicher Rahmen.

Im Laufe der Diskussionen über die Reform des europäischen Datenschutzrechts wurde und wird dieses Modell von einzelnen Vertretern aus Wirtschaft, Politik und Wissenschaft immer wieder in Frage gestellt: Das grundsätzliche Verarbeitungsverbot sei innovationshemmend und beeinträchtige den Wettbewerb mit anderen Wirtschaftsregionen außerhalb Europas. Gerade kleinere und mittlere Unternehmen würden vor große Hürden ge-

stellt, während globale Internetunternehmen sich kaum an diese Vorgaben hielten. Als mögliche Lösung wird dabei ein so genannter risikobasierter Ansatz vorgeschlagen, wonach die Verarbeitung personenbezogener Daten - jedenfalls im Bereich der Wirtschaft – grundsätzlich erlaubt sein müsse und lediglich die besonders risikobehaftete Datenverarbeitung verboten oder einschränkend reguliert werden solle.

Einen risikobasierten Ansatz in dieser Form lehne ich ab und habe dies ebenso wie meine Kolleginnen und Kollegen in den Ländern und in der Artikel-29-Gruppe immer wieder deutlich gemacht. Schon in seinem Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht klargestellt, dass es im Zeitalter automatisierter Datenverarbeitung kein belangloses Datum mehr geben könne. Jede Information über einen Einzelnen kann - je nach Kontext oder Verknüpfung - gleichzeitig eine triviale oder aber auch eine äußerst sensible Aussage treffen. Dies ist schwer vorhersehbar und macht schon deshalb eine standardisierte Abschätzung des Risikos schwierig. Der Gesetzgeber könnte immer nur solche Risiken regulieren, die er auch kennt. Dies wäre aber mit dem grundrechtlichen Schutz des Einzelnen nicht vereinbar.

Ein so verstandener risikobasierter Ansatz würde den Schutz der Betroffenen grundsätzlich schwächen: Nach dem geltenden Recht muss in der Gesetzgebung wie in der Gesetzesanwendung jeder neue Eingriff in das Recht auf informationelle Selbstbestimmung gerechtfertigt werden, sowohl politisch als auch ganz praktisch bei jeder Verarbeitung. Dies legt die Begründungslast auf die Seite derjenigen, die die Daten verarbeiten wollen. Dreht man dieses Prinzip um, müssten die Betroffenen rechtfertigen, warum bestimmte Datenverarbeitungen riskant sind. Dies würde ihre Position deutlich schwächen.

Nach meiner Auffassung verhindert das aktuelle Konzept des Datenschutzrechts - dem auch die DSGVO folgt - auch nicht innovative Geschäftsmodelle. Innovationsfähig zu sein kann nicht bedeuten, dass jede technische Lösung und jedes Geschäftsmodell erlaubt ist und das Recht dem zu folgen hat. Technische Lösungen und neue Geschäftsmodelle müssen sich vielmehr in den bestehenden - sich durchaus auch weiterentwickelnden - rechtlichen Rahmen innovativ einpassen. Hier kann Europa aufgrund seines strengen grundrechtsbetonten Datenschutzrechts ein Vorreiter in der Entwicklung datenschutzfreundlicher und damit vertrauenswürdiger Geschäftsmodelle sein. Dies sollten die europäischen Unternehmen als Chance und Wettbewerbsvorteil begreifen.

Aus diesen Gründen haben sich Vorschläge, die rechtliche Zulässigkeit oder die Einräumung grundlegender Betroffenenrechte von den Risiken einer Datenverarbeitung abhängig zu machen, erfreulicherweise weder im Europäischen Parlament noch im Rat durchsetzen können.

Gleichwohl enthält die DSGVO durchaus Elemente eines risikobasierten Ansatzes. Dies gilt vor allem für die Gewährleistung des technischen und organisatorischen Datenschutzes. Auch das ist nichts Neues, sondern findet sich bereits im geltenden Datenschutzrecht. So müssen die verantwortlichen Stellen nach § 9 BDSG nur die Maßnahmen treffen, deren Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht. Die DSGVO baut auf diesem Modell auf und skaliert eine Reihe von Elementen des technischen und organisatorischen Datenschutzes anhand der für den Einzelnen bestehenden Risiken. Dies gilt sowohl für die im Einzelnen zu treffenden Maßnahmen, z. B. eine Verschlüsselung wie etwa auch für die Frage, wann eine Datenschutz-Folgenabschätzung durchzuführen oder die Aufsichtsbehörde zu konsultieren ist.

Einem solchen risikobasierten Ansatz folgt insbesondere das Kapitel IV der DSGVO, über das sich der Rat bereits grundsätzlich geeinigt hat (vgl. Nr. 1.1).

1.2.4 Stärkung der Pseudonymisierung

Am 24. Oktober 2014 hat die Bundesregierung eine deutsche Note an den Vorsitz des Rates der Europäischen Union übermittelt, die sich mit der Pseudonymisierung (in Abgrenzung von der Anonymisierung) personenbezogener Daten befasst (vgl. Nr. 2.2.3).

Ziel des Papiers ist eine höhere Verbreitung der Pseudonymisierung personenbezogener Daten, um den Schutz für die Betroffenen zu verbessern. Hierfür schlägt die Note vor, pseudonyme Datenverarbeitung zu privilegieren: bei pseudonymer Datenverarbeitung sollen die schutzwürdigen Interessen des Betroffenen gegenüber dem berechtigten Interesse der Verantwortlichen für die Datenverarbeitung niedriger zu bewerten sein als bei einer Verarbeitung ohne diese Schutzmaßnahme. Darüber hinaus soll das Recht für Nutzer sozialer Netzwerke verankert werden, einen Alias (Pseudonym) anstelle ihres echten Namens zu nutzen.

Diesen Vorschlag begrüße ich, zumal viele der Anregungen, die ich im Rahmen der Ressortabstimmung auf Fachebene eingebracht habe, aufgegriffen worden sind. Eine maßvolle Privilegierung pseudonymer Datenverarbeitung ist durchaus ein gangbarer Weg, um Anreize für diese und weitere Schutzmaßnahmen zu geben.

Allerdings wäre eine kürzere und prägnantere Definition des Begriffes der Pseudonymisierung wünschenswert gewesen. Der Vorschlag weist einige Redundanzen auf und orientiert sich zu wenig an bereits vorhandenen Begriffsbestimmungen.

Auch der Vorschlag, soziale Netzwerke nutzen zu können, ohne die eigene Identität preisgeben zu müssen, wird von mir grundsätzlich unterstützt. Lediglich die vorgeschlagene Ergänzung in Erwägungsgrund 24 der DSGVO, nach der die Ausübung dieses Rechtes den Maßnahmen der Strafverfolgung nicht entgegenstehen darf, erscheint bedenklich. Im besten Fall soll hiermit lediglich klargestellt werden, dass strafrechtliche und strafprozessuale Befugnisse unberührt bleiben. Im schlechtesten Fall könnte allerdings daraus auch gefolgert werden, es müsse in einer Art Vorratsdatenspeicherung eine Nutzungsdatenbank geschaffen werden, die durch Abgleich mit Daten von Internetzugangsprovidern eine umfangreiche Überwachung der Internetnutzung ermöglichen würde.

Positiv bewerte ich auch die klare Abgrenzung zwischen den Begriffen der Pseudonymisierung und Anonymisierung. Wie der Vorschlag unmissverständlich klarstellt, sind pseudonymisierte Daten in keiner Weise mit anonymisierten Daten gleichzusetzen, sondern sehr wohl personenbezogene Daten. Sie fallen damit in den Anwendungsbereich der geltenden und zukünftigen Rechtsvorschriften. Die Note räumt mit dem weitverbreiteten Missverständnis auf, bei der Pseudonymisierung von Daten gehe der Personenbezug verloren. Das Konzept der Pseudonymisierung stellt vielmehr eine reine Schutzmaßnahme dar.

Es bleibt abzuwarten, inwieweit diese Vorschläge aufgrund der weit fortgeschrittenen Verhandlungen im Rat der Europäischen Union berücksichtigt werden. Ich würde es mir wünschen!

1.2.5 Zukunft der Datenschutzaufsicht

Die Zunahme grenzüberschreitender Datenübertragungen im Zuge einer globalen Wirtschaft und des wachsenden Angebotes von Waren und Dienstleistungen über das Internet erfordert übersichtliche Verfahren für Unternehmen und - auch im Sinne der Bürgerfreundlichkeit - eine effektive Zusammenarbeit der Datenschutzbehörden innerhalb der EU.

Die Europäische Kommission hat deshalb im Entwurf der DSGVO das Prinzip einer „zentralen Anlaufstelle“ („One-Stop-Shop“) vorgeschlagen. Unternehmen, die über mehrere Niederlassungen innerhalb der EU verfügen, sollen sich an die Datenschutzbehörde des Mitgliedstaates wenden können, in dem sich ihre Hauptniederlassung befindet. Diese so genannte federführende Behörde soll EU-weit zuständig sein für alle aufsichtsbehördlichen Maßnahmen und Entscheidungen gegenüber dem betreffenden Unternehmen, wobei sie mit den auf nationaler Ebene zuständigen Aufsichtsbehörden zu kooperieren hat. Daneben schlug die Kommission einen Abstimmungsmechanismus für bestimmte Fälle vor, in denen mehrere Mitgliedstaaten von einem Verarbeitungsvorgang betroffen sind. Durch dieses so genannte Kohärenzverfahren soll eine einheitliche Datenschutzpraxis innerhalb der EU erreicht werden (vgl. 24. TB Nr. 2.1.1).

Das Thema „One-Stop-Shop“ wurde sowohl im Europäischen Parlament als auch im Rat intensiv diskutiert.

In seinem Beschluss vom März 2014 befürwortet das Parlament den von der Kommission vorgeschlagenen Ansatz einer „federführenden Datenschutzbehörde“, sprach sich aber zugleich für eine stärkere Rolle des Europäischen Datenschutzausschusses - dem Nachfolgegremium der jetzigen Artikel-29-Gruppe - aus. Dieser soll in Einzelfällen einen Beschluss fassen können, der für die zuständigen nationalen Aufsichtsbehörden verbindlich ist. Das Parlament wendet sich mit diesem Ansatz gegen die im Ursprungsentwurf der DSGVO vorgesehene Befugnis für die Kommission, Durchführungsrechtsakte „zur ordnungsgemäßen Anwendung der Verordnung“ in Fällen erlassen zu können, an denen mehrere Aufsichtsbehörden im Rahmen des Kohärenzverfahrens beteiligt sind (vgl. zum Begriff des Durchführungsrechtsaktes Nr. 3.1.1).

Auch auf Ratsebene wurde das Thema „One-Stop-Shop“ im Berichtszeitraum intensiv beraten. Ein erstes substanzielles Zwischenergebnis konnte die litauische Präsidentschaft auf dem Rat der Innen- und Justizminister im Oktober 2013 erreichen. Die Mitgliedstaaten stimmten der Grundidee eines „One-Stop-Shop“-Mechanismus zu, der eine einheitliche und unbürokratische Entscheidung der federführenden Behörde am Ort der EU-Hauptniederlassung des Verantwortlichen in „wichtigen grenzüberschreitenden Fällen“ ermöglichen soll.

Bei den Verhandlungen blieb allerdings die Frage offen, wie weit die Entscheidungsbefugnis der federführenden Behörde geht. Zudem konnte keine Einigung darüber erzielt werden, welche Kompetenzen der künftige Europäische Datenschutzausschuss haben soll, falls sich die an einem multilateralen Verfahren beteiligten Aufsichtsbehörden nicht auf eine einheitliche Vorgehensweise einigen. Nach Auffassung eines Teils der Mitgliedstaaten, einschließlich Deutschlands, soll der Ausschuss verbindliche Entscheidungen zur Anwendung der DSGVO treffen können. Andere Mitgliedstaaten plädieren für stärkere Entscheidungsbefugnisse der federführenden Behörde.

Im Mittelpunkt der Beratungen stand darüber hinaus die Frage, wie das Modell der zentralen Anlaufstelle mit größtmöglicher Bürgernähe ausgestaltet werden kann: Die Bürgerinnen und Bürger sollen sich mit ihren Fragen und Beschwerden immer an „ihre“ Datenschutzbehörde vor Ort wenden können und sollen sich nicht um Zuständigkeitsfragen oder Abstimmungsmechanismen kümmern müssen. Dies führte in den Ratsverhandlungen notwendigerweise zu der Frage, wie die unterschiedlichen Datenschutzbehörden am Sitz des Unternehmens und am Wohnort der Betroffenen zu einheitlichen Entscheidungen kommen können. Der Juristische Dienst des Rates schlug deshalb in einem Gutachten im Dezember 2013 vor, dem Europäischen Datenschutzausschuss in bestimmten Fällen verbindliche Entscheidungsbefugnisse zu übertragen, in denen aufsichtsbehördliche Maßnahmen allein durch lokale Behörden nicht ausreichten.

Daraufhin entwickelte die italienische Ratspräsidentschaft ein Modell, das die Kontrolle und Ahndung von Verstößen gegen die DSGVO sowie die Bearbeitung von Bürgerbeschwerden grundsätzlich bei den nationalen Behörden belässt, diese aber in grenzüberschreitenden Fällen dazu verpflichtet, mit der federführenden Aufsichtsbehörde am Ort der EU-Hauptniederlassung des Datenverarbeiters zusammenzuarbeiten. Zudem sollen nach diesem Ansatz nicht nur die nationalen Behörden, sondern konsequenterweise auch die nationalen Gerichte für Beschwerdeverfahren von Einzelpersonen zuständig bleiben. Der Europäische Datenschutzausschuss soll - ähnlich der Position des Europäischen Parlaments - die Rolle einer Streitschlichtungsinstanz einnehmen, die verbindlich entscheiden kann, falls sich die federführende Behörde und mitbetroffene nationale Behörden nicht auf eine gemeinsame Vorgehensweise einigen können.

An den Beratungen zum „One-Stop-Shop“ und der künftigen Rolle des Europäischen Datenschutzausschusses habe ich mich intensiv sowohl auf nationaler als auch auf europäischer Ebene beteiligt. So hat auf meine Initiative hin die Datenschutzkonferenz im März 2014 eine Entschließung zur Struktur der künftigen Datenschutzaufsicht in Europa angenommen (vgl. Anlage 7). Darin spricht sie sich für verbindliche Entscheidungsbefugnisse des Europäischen Datenschutzausschusses aus.

Auch die Artikel-29-Gruppe befasste sich im Berichtszeitraum wiederholt mit dem Thema „One-Stop-Shop“. Auf meine Initiative verfasste sie auf der Basis der Entschließung der Datenschutzkonferenz einen gemeinsamen Standpunkt, der vom Vorsitz der Artikel-29-Gruppe im April 2014 an die griechische Ratspräsidentschaft übersandt wurde. Darin spricht sie sich ebenfalls für eine stärkere Rolle des Europäischen Datenschutzausschusses aus, der „verbindliche Leitlinien oder sonstige Maßnahmen“ annehmen können soll. Wie bereits die deutschen Aufsichtsbehörden lehnte auch die Artikel-29-Gruppe EU-weite Compliance-Verfahren ab.

Das Thema „One-Stop-Shop“ hat auf EU-Ebene innerhalb der vergangenen zwei Jahre eine insgesamt positive Entwicklung genommen. Wesentlich bleibt aus meiner Sicht, dass die nationalen Datenschutzbehörden aus dem Gesetzgebungsprozess gestärkt hervorgehen und über neue Kooperations- und Entscheidungsverfahren verfügen, die ein einheitliches und effektives Handeln in grenzüberschreitenden und EU-weiten Fällen ermöglichen. Dabei müssen das Kooperationsverfahren und die Zusammenarbeit innerhalb des Europäischen Datenschutzausschusses praktikabel bleiben. Es dürfen keine unverhältnismäßigen bürokratischen Belastungen für Betroffene und Unternehmen, aber auch nicht für die Datenschutzbehörden selbst entstehen.

Für Deutschland ist die Umsetzung der mit dem Prinzip des „One-Stop-Shops“ verbundenen Kooperationsmechanismen aufgrund der föderalen Kompetenzverteilung eine besondere Herausforderung. Die bestehenden Strukturen mit insgesamt 18 deutschen Datenschutzbehörden mit je eigenen Zuständigkeitsbereichen müssen spätestens mit Verabschiedung der DSGVO im Sinne einer effizienten, gleichwohl bürgernahen Datenschutzaufsicht überprüft werden. Dabei werden auf mich und meine Dienststelle im Zusammenhang mit der im Vergleich zur Artikel-29-Gruppe wesentlich bedeutenderen Rolle des Europäischen Datenschutzausschusses umfangreiche neue Aufgaben zukommen.

1.2.6 Drittstaatenübermittlungen, Safe-Harbor, Auswirkungen der Snowden-Affäre

Grenzüberschreitende Daten- und Informationsflüsse sind alltäglich geworden in der globalisierten und vernetzten Welt. Die hierzu in der Datenschutz-Grundverordnung vorgesehenen Regelungen bauen auf dem System und den Grundsätzen der Europäischen Datenschutzrichtlinie von 1995 auf.

Die DSGVO erlaubt Datenübermittlungen aus der EU in Drittstaaten, wenn sie entweder auf Beschlüssen der Europäischen Kommission zur Angemessenheit des Datenschutzniveaus im Empfängerstaat, auf rechtsverbindlichen Garantien zum Schutz personenbezogener Daten wie verbindlichen unternehmensinternen Vorschriften (BCR) oder Standardvertragsklauseln basiert. Sofern derartige Garantien fehlen, sollen Übermittlungen nur im Ausnahmefall für bestimmte, in der Verordnung festgelegte Situationen erlaubt sein. So können Übermittlungen in Drittstaaten dann zulässig sein, wenn der Betroffenen hierin ausdrücklich eingewilligt hat, vertragliche Vereinbarungen mit dem Betroffenen oder seine lebenswichtigen Interessen diese erfordern. Die DSGVO enthält aber auch eher vage Ausnahmetatbestände wie „wichtige Gründe des öffentlichen Interesses“ oder die berechtigten Interessen des Verantwortlichen (vgl. unten).

Diese Regelungen für Datenübermittlungen aus der EU in Drittstaaten sind von der Europäischen Kommission im Entwurf der DSGVO beibehalten und sowohl vom Europäischen Parlament in seinem Beschluss vom März 2014 als auch vom Rat im Juni 2014 gebilligt worden. Damit kam es im Rat nach mehr als zweijähriger Verhandlungsdauer - zusammen mit der grundsätzlichen Befürwortung des sog. Marktortprinzips (vgl. Nr. 1.2.7) - erstmals zu einer politischen Einigung über einen Teil des Verordnungsentwurfs.

Änderungsbedarf sehen das Europäische Parlament und der Rat unter anderem noch bei der Rolle des Europäischen Datenschutzausschusses, der eine Stellungnahme zum Datenschutzniveau eines Drittstaats abgeben soll, bevor die Kommission einen Beschluss über die Angemessenheit des Datenschutzniveaus trifft. Ferner soll nach Auffassung des Parlaments die Gültigkeitsdauer von Angemessenheitsbeschlüssen, die bereits auf Basis der Europäischen Datenschutzrichtlinie von 1995 erlassen wurden, beschränkt sein auf einen Zeitraum von fünf Jahren nach Inkrafttreten der DSGVO. Darunter würde auch die „Safe-Harbor“-Entscheidung 2000/520/EG (vgl. auch

Nr. 4.7.1) der Europäischen Kommission fallen. Datenübermittlungen aus der EU in Drittstaaten auf der Grundlage geeigneter Garantien sollen künftig neben den „klassischen“ Instrumenten wie BCR und Standardverträgen zudem auf der Grundlage genehmigter Zertifizierungsmechanismen und - nach Ansicht des Rates - genehmigter Verhaltenskodizes sowie „rechtsverbindlicher Instrumente“ zwischen staatlichen Behörden zulässig sein.

Anders als Kommission und Rat hat sich das Europäische Parlament dagegen ausgesprochen, Drittstaatsübermittlungen, die nicht häufig oder massiv sind, auch auf Basis des berechtigten Interesses des für die Verarbeitung Verantwortlichen oder Auftragsdatenverarbeiters zu ermöglichen. Diese Position teile ich. Diese neue Ausnahme des „berechtigten Interesses“ darf künftig keinesfalls zur Regel für Drittstaatentransfers werden. Andernfalls würden die datenschutzrechtlich spezifischeren Instrumente wie Standardverträge und -vertragsklauseln, die Einwilligung oder vertragliche Grundlagen unterlaufen. Auch die Artikel-29-Gruppe hat in einer Stellungnahme vom September 2014 betont, dass Datenübermittlungen in Drittstaaten auf Basis des „berechtigten Interesses“ Ausnahmecharakter haben sollten (vgl. WP 222 vom 17.09.2014).

Die Debatte über den Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten wurde im Jahre 2013 insbesondere durch die Erkenntnisse über das „PRISM-Programm“ der National Security Agency (NSA) angefeuert (vgl. Nr. 2.1). Sie hat das Europäische Parlament dazu bewogen, die Aufnahme eines spezifischen Artikels in der DSGVO zu Datenübermittlungen an Behörden und Gerichte in Drittstaaten zu fordern. Der entsprechende Änderungsvorschlag des Parlaments zu Artikel 43a DSGVO stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt werden noch vollstreckbar sind, wenn dies nicht in internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der Datenschutzbehörden sowie sonstiger zuständiger Stellen der EU-Mitgliedstaaten.

Diese von mir im Grundsatz unterstützte Forderung wurde zuvor bereits von der Artikel-29-Gruppe in ihrer Stellungnahme zum Entwurf der DSGVO vom März 2012 (WP 191 vom 23.03.2012) erhoben und in einer weiteren Stellungnahme vom September 2014 (WP 222 vom 17.09.2014) wiederholt. Mit der Schaffung einer entsprechenden Regelung wird die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Zu meinem Bedauern ist der Rat einer entsprechenden Initiative der Bundesregierung im September 2013 zur Aufnahme einer ähnlichen Regelung (hier unter der Bezeichnung Artikel 42a) in Kapitel V der DSGVO nicht gefolgt. Die Frage, unter welchen Voraussetzungen staatliche Stellen aus Drittstaaten Zugriff auf personenbezogene Daten europäischer Bürgerinnen und Bürgern erlangen können, muss in den bevorstehenden Verhandlungen zwischen Kommission, Parlament und Rat erneut intensiv erörtert werden.

1.2.7 Internettauglichkeit, Big Data, Profiling

Die gelegentlich geäußerte Kritik an der Internettauglichkeit der Datenschutz-Grundverordnung teile ich nicht. Die Diskussion darüber darf nicht zur Absenkung der datenschutzrechtlichen Standards durch die Datenschutz-Grundverordnung führen. Das Bestreben der Bundesregierung, bereits die Bildung von Profilen zu reglementieren, unterstütze ich.

Neben der Harmonisierung bildet die Modernisierung ein erklärtes Ziel der Novellierung des europäischen Datenschutzrechts. Mit der DSGVO sollen die seit Inkrafttreten der Europäischen Datenschutzrichtlinie von 1995 unverändert gebliebenen Datenschutzprinzipien an das digitale Zeitalter und die Anforderungen des globalen Datenverkehrs angepasst werden.

Innerhalb der Bundesregierung wurde die Internettauglichkeit des Regelwerks bisweilen in Zweifel gezogen. Datenschutzrechtliche Herausforderungen, die aus dem Cloud Computing, sozialen Netzwerken, der Datenverarbeitung durch mobile Verarbeitungssysteme (so genannte Wearables), durch Big-Data-Auswertungen und umfassende Profilbildungen (Profiling) erwachsen, würden - so die Kritik - durch die DSGVO nur unzureichend erfasst. Bewährte Rechtsinstrumente wie die Einwilligung und die Transparenzvorschriften müssten einerseits in Frage gestellt werden. Andererseits bedürfe es zusätzlicher Schutzmechanismen, möglicherweise aber auch ganz neuer Ansätze.

Dieser Kritik kann ich mich nicht anschließen. Schon heute sind Phänomene wie das Cloud Computing oder Big Data datenschutzrechtlich beherrschbar und datenschutzkonform einsetzbar, wenn auch unter strengen datenschutzrechtlichen Vorgaben. So lässt sich Cloud Computing innerhalb der EU auf der Grundlage der Auftragsdatenverarbeitung, außerhalb der EU mit den Regelungen zum Drittstaatentransfer abbilden. Big-Data-Anwendungen können bei Beachtung der Grundsätze der Zweckbindung, der Erforderlichkeit und Datensparsamkeit, der Verhältnismäßigkeit, der Transparenz, des technologischen Datenschutzes und mit den Methoden der Pseudonymisierung und Anonymisierung auch ohne Einwilligung der Betroffenen rechtskonform ausgestaltet werden. Die bereits jetzt bestehenden zentralen Prinzipien des Datenschutzrechts wie die Autonomie des Einzelnen, die Transparenz, die Zweckbindung und das Prinzip von Relevanz und Erforderlichkeit können daher einen wirksamen Schutz gewährleisten und sichern die allseits erwünschte und auch notwendige Technikneutralität des Datenschutzrechts. Denn angesichts der Innovationsgeschwindigkeit wäre es kurzsichtig, jede technologische Neuerung separat im Datenschutzrecht regeln zu wollen. Die grundsätzlichen Prinzipien des Datenschutzes müssen daher auch für die internetbasierte Datenverarbeitung gelten.

Das Argument der mangelnden Internettauglichkeit wird bisweilen aber nicht wegen fehlender Schutzmechanismen des Datenschutzrechts, sondern - im Gegenteil - wegen der angeblich zu hohen datenschutzrechtlichen Hürden angeführt. Das europäische Datenschutzrecht sei ein Wettbewerbshindernis auf dem digitalen Markt, weil es heimischen Unternehmen untersage, was Unternehmen in Drittstaaten - namentlich führenden US-Konzernen - erlaubt sei. Auch diese Argumentation überzeugt mich gleich aus mehreren Gründen nicht. Zum einen werden wegen des in der DSGVO vorgesehenen Marktortprinzips, das auch Unternehmen aus Drittstaaten europäischem Datenschutzrecht unterwirft, wenn diese auf dem europäischen Markt Waren und Dienstleistungen anbieten, in Europa gleiche Wettbewerbsbedingungen bestehen. Zum anderen darf es nicht der Anspruch eines ambitionierten europäischen Datenschutzrechts sein, Big-Data-Auswertungen oder andere Datenverarbeitungen durch Absenkung der rechtlichen Anforderungen zu legitimieren, nur weil diese technisch möglich sind. Das Recht hat nicht der Technik zu folgen, sondern die Aufgabe, angemessene Rahmenbedingungen für technische Entwicklungen zu setzen. Daher lehne ich einen risikobasierten Ansatz ab, bei dem nur besonders risikobehaftete Datenverarbeitungen dem Regime des Datenschutzrechts unterworfen werden sollen (vgl. Nr. 1.2.3).

Dagegen teile ich die Auffassung der Bundesregierung, dass die Anforderungen an die Bildung von Profilen bislang nicht ausreichend in der DSGVO niedergelegt sind, auch wenn es sich angesichts der zahlreichen Einsatzszenarien von Nutzer-, Verhaltens-, Bewegungs- und sonstigen Persönlichkeitsprofilen sicherlich nicht um ein rein internetspezifisches Problem handelt. Eine Reglementierung darf sich insbesondere nicht allein auf die nachteiligen Folgen einer Entscheidung beschränken, die auf der Basis des Profilings getroffen wurde. Vielmehr muss früher, nämlich bereits bei der Profilbildung selbst angesetzt werden. Während der Vorschlag der Europäischen Kommission nur „auf Profiling basierende Maßnahmen“ erfasst, die weder rein automatisiert sein noch rechtliche Wirkungen oder maßgeblich Beeinträchtigungen entfalten dürfen, enthält der Vorschlag des Europäischen Parlaments bereits deutliche Verbesserungen. Allerdings soll das grundsätzliche Verbot des Profilings nach dem Willen des Parlaments nur gelten, wenn die Profilbildung „Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat“. Im Rat zeichnet sich bislang zu dieser Frage noch kein klares Bild ab. Daher unterstütze ich das Anliegen der Bundesregierung, die Profilbildung unabhängig davon zu regeln, unter welchen Anforderungen eine nachgelagerte Entscheidung auf der Basis dieser Profilbildung - etwa die Entscheidung gegen den Abschluss eines Vertrags - erfolgen darf.

1.3 Regelungen zum Datenschutz in den Bereichen Polizei und Justiz

Im Schatten der Datenschutz-Grundverordnung ist der Entwurf für eine Richtlinie zum Datenschutz in den Bereichen Polizei und Justiz weiterhin auf einem mühsamen Weg. Sie dürfte Mindeststandards setzen, doch darüber hinaus ist noch vieles offen.

Der Entwurf für eine neue Richtlinie im Bereich von Polizei und Justiz ist auf einem mühsamen Weg, so hieß es im letzten Tätigkeitsbericht (24. TB Nr. 2.1.2). Diese Einschätzung hat sich als zutreffend erwiesen. Es ist gar nicht so einfach, so scheint es, von einem Fortschritt während der vergangenen zwei Jahre zu berichten. Deutlich geworden ist vor allem, dass der Entwurf der Richtlinie ganz im Schatten der Verhandlungen über eine Datenschutz-Grundverordnung (DSGVO, vgl. Nr. 1.1) steht. Insbesondere die Skepsis der Ratspräsidentschaften und im Rat selbst hat dazu geführt, dass intensive Verhandlungen der schwierigen Rechtsfragen in den letzten drei Jahren kaum stattgefunden haben.

Nach meiner Auffassung sollte es gleichwohl eine neue Richtlinie geben, die ein hohes Datenschutzniveau für jegliche Datenverarbeitung im Bereich der Polizei- und Strafverfolgungsbehörden in Europa sicherstellen sollte. Gegenwärtig gibt es den dafür notwendigen rechtlichen Rahmen im EU-Recht nicht. Der Rahmenbeschluss 2008/977/JI, auf den die Kritiker des Richtlinienentwurfs immer wieder als geltenden Rechtsrahmen verweisen, regelt den Datenschutz nur in einem begrenzten Anwendungsbereich, nämlich nur dann, wenn personenbezogene Daten von Strafverfolgungsbehörden innerhalb Europas übermittelt werden. Dies halte ich für nicht hinreichend. Wer zu Recht und immer wieder gegenüber Drittstaaten die Forderung nach einem hohen Datenschutzniveau gerade im Sicherheitsbereich stellt, sollte dies auch umfassend im eigenen Verantwortungsbereich sicherstellen. Zu meiner Freude haben die Europäische Kommission und das Europäische Parlament immer wieder darauf hingewiesen, dass es sich bei der DSGVO und der Richtlinie um ein Paket handelt, mit dem ein hohes Maß an Datenschutz für jegliche Verarbeitung in Europa sichergestellt werden soll. Von dem wenigen, das über das Vorankommen des Richtlinienentwurfs (sowohl aus dem Parlament als auch aus dem Rat) berichtet werden kann, möchte ich herausstellen, dass sowohl nach Auffassung des Rates als auch des Parlaments die Richtlinie nur Mindeststandards setzen soll. Die Richtlinie würde das Datenschutzniveau in den Mitgliedstaaten also nicht „deckeln“. Sie ließe ihnen den notwendigen Spielraum, ein höheres Datenschutzniveau zu erhalten und zu schaffen.

Das Schicksal der Richtlinie ist weiterhin unsicher. Wie während des Berichtszeitraums deutlich geworden ist, werden noch große Fragen des Anwendungsbereichs kontrovers diskutiert und sind weiterhin umstritten. Der Weg zu einer Richtlinie wird weiterhin mühsam und steinig sein. Ihr Schicksal bleibt mit den Verhandlungen über die DSGVO verbunden.

2 Grundsatzangelegenheiten

2.1 Der NSA-Skandal

2.1.1 NSA-Skandal - denn sie wissen (nicht), was sie tun?

Die Aufdeckung des NSA-Skandals hat meine Tätigkeit seitdem nachhaltig bestimmt, aber noch zu keinen greifbaren Ergebnissen geführt. Dies lag auch an mangelnder Kooperation.

Wie Edward Snowden enthüllt hat, haben US-amerikanische und britische Nachrichtendienste anlasslos massenhaft Telekommunikationsverkehre (Telefonate, E-Mails, SMS, Internetnutzung etc.) überwacht, gespeichert und analysiert - in einem bis dato unvorstellbarem Ausmaß. Betroffen sind auch deutsche Kommunikationsteilnehmer und Internetnutzer - offensichtlich auch Politiker in höchsten Staatsämtern. Zur Aufklärung dieser Vorfälle hat der Deutsche Bundestag einstimmig einen Parlamentarischen Untersuchungsausschuss (PUA) eingesetzt, der seine Arbeit am 3. April 2014 aufgenommen hat. Der Untersuchungsauftrag erstreckt sich nicht nur auf die Aktivitäten der ausländischen Nachrichtendienste (AND - vgl. Bundestagsdrucksache 18/843 vom 18.03.2014). Untersucht wird auch, ob deutsche Sicherheitsbehörden an diesen Vorfällen beteiligt waren und ob nationale Gesetze bzw. Beschränkungen verletzt bzw. umgangen worden sind. Eine solche Umgehung könnte z. B. vorliegen, wenn deutsche Stellen von ausländischen Partnern Daten erhalten haben, die sie nach deutschem Recht nicht hätten erheben dürfen bzw. deutsche Nachrichtendienste für AND in Deutschland Daten erhoben haben, welche die AND nach deutschem Recht nicht hätten erheben dürfen (sog. „Ring"-Tausch - Bundestagsdrucksache 18/843, I. 7). Gegenstand der Untersuchungen ist auch die Ausgestaltung der Kontrolle der Nachrichtendienste sowie die Klärung der Frage, ob die Nachrichtendienste und deren Fachaufsichtsressorts ihre gegenüber den Kontrollorganen - d. h. auch mir gegenüber - bestehenden Informations- und Mitwirkungspflichten erfüllt haben (vgl. in Bezug auf die BfDI Bundestagsdrucksache 18/843, I. 12, I. 17, II. 5). Wie der PUA beschlossen hat, nehme ich - vertreten durch Mitarbeiter meines Hauses - an den Sitzungen teil. Eine derartige Einbeziehung ist ein Novum, das ich begrüße. Ich werde die Aufklärungen des PUA nach besten Kräften unterstützen.

Bereits unmittelbar nach Bekanntwerden der ersten Enthüllungen von Edward Snowden im Juni 2013 hatte ich die Nachrichtendienste des Bundes (BfV, BND und MAD), deren Fachaufsichtsressorts (Bundeskanzleramt, BMI, BMVg) sowie das AA und das BMJV um Aufklärung bzw. Informationen gebeten. Nach geltendem Recht sind diese Stellen verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen. Die von mir angeforderten Informationen waren u. a. erforderlich, um Kontrollen vor Ort durchführen bzw. vorbereiten zu können. Trotz wiederholter Aufforderungen hatten sich das BMI und das BfV mit dem Hinweis auf meine vermeintlich bestehende Unzuständigkeit geweigert, mir die angeforderten Informationen zu geben. Diese Weigerungen habe ich im September 2013 förmlich beanstandet und auch öffentlich als schwerwiegende Rechtsverstöße benannt. Auch das hat aber nicht dazu geführt, mir die entsprechenden Informationen zu gewähren. Weitergehende Sanktionsmöglichkeiten habe ich nicht.

Trotz dieser Hindernisse habe ich u. a. erste Vor-Ort-Kontrollen beim BfV und dem BND durchgeführt. Insbesondere die Untersuchungen beim BND sind sehr zeit- und arbeitsintensiv und werden voraussichtlich noch weitere Zeit in Anspruch nehmen. Aufgrund von Geheimhaltungsvorschriften darf ich an dieser Stelle keine detaillierten Ausführungen hierzu machen. Im Rahmen der mir gesetzlich zustehenden Möglichkeiten werde ich meine Untersuchungen und Kontrollergebnisse den zuständigen Stellen mitteilen. Abschließende Bewertungen werde ich erst nach Abschluss meiner Kontrolle vornehmen können.

Beginnend mit den ersten Enthüllungen von Edward Snowden hatte ich dem für die Kontrolle der Nachrichtendienste des Bundes zuständigen parlamentarischen Kontrollgremium (PKGr) und der G10-Kommission des Deutschen Bundestages Kooperationsangebote zur Aufklärung der Sachverhalte und zur Optimierung der Kon-

trollen unterbreitet. Wie in früheren Tätigkeitsberichten ausgeführt (vgl. 24. TB Nr. 7.7.1 ff.), bestehen gravierende Defizite im Hinblick auf die Kontrolle der Nachrichtendienste und die gesetzliche Ausgestaltung der Kontrollstruktur.

Zwischenzeitlich hat das Bundesministerium des Innern zugestanden, dass ich zur Erfüllung meiner gesetzlichen Aufgaben auch personenbezogene Daten einsehen und verwenden darf, die nach dem Artikel-10-Gesetz gewonnen worden sind. Dies ist ein wichtiger, aber keineswegs ausreichender Schritt zur Behebung dieser Defizite. Notwendig sind gesetzliche Regelungen bzw. Klarstellungen. Diese stehen immer noch aus. Ich bedauere sehr, dass der Gesetzgeber entsprechende Novellierungen, z. B. in dem aktuellen Gesetz, durch das meine Behörde ab dem 1. Januar 2016 eine oberste Bundesbehörde werden wird, nicht aufgenommen hat.

Ich empfehle dem Gesetzgeber, dieses Defizit schnellstmöglich zu beseitigen. Dieser Apell gilt auch und insbesondere für die Zuweisung ausreichender Personal- und Sachmittel zur Durchführung adäquater Kontrollen.

Hierauf habe ich u. a. bereits in meinem Bericht an den Deutschen Bundestag zu den „Abhöraktivitäten US-amerikanischer Nachrichtendienste in Deutschland“ (Bundestagsdrucksache 18/59 vom 15.11.2013) hingewiesen.

Mein Bericht an den Deutschen Bundestag enthält auch umfängliche Bewertungen zur rechtlichen Situation auf nationaler und internationaler Ebene, eine Darstellung bestehender Problemlagen sowie meine Schlussfolgerungen und Handlungsempfehlungen. Auf diesen öffentlichen Bericht habe ich auch in Ausschusssitzungen, Interviews, Vorträgen und Publikationen hingewiesen.

Ich möchte aber auch an dieser Stelle noch einmal betonen, dass das System der „Checks and Balances“ im Bereich der Nachrichtendienste in eine massive Schieflage geraten ist. So sind, insbesondere seit dem Jahr 2001, die Aufgaben und Befugnisse der Sicherheitsbehörden sowie deren Personal- und Sachmittel erheblich ausgebaut, die verbundübergreifende Zusammenarbeit von Polizeien und Nachrichtendiensten national und international intensiviert, zentrale Großdatenbanken errichtet und eine neue Sicherheitsstruktur geschaffen worden. Die neu errichteten nationalen Kooperationszentren der Sicherheitsbehörden des Bundes und der Länder (z. B. das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ)) verdeutlichen exemplarisch diese Entwicklung.

Auf Seiten der Kontrollorgane ist keine entsprechende Entwicklung erfolgt, d. h. auch insoweit bestehen gravierende gesetzgeberische Defizite, die im Interesse der Bürgerinnen und Bürger schnellstmöglich beseitigt werden müssen. In Folge dieser Entwicklung ist es mir angesichts der mir zur Verfügung stehenden geringfügigen Personal- und Sachmittel nicht mehr möglich, meine gesetzlich zugewiesenen Beratungs- und Kontrollaufgaben angemessen zu erfüllen. Damit ist es mir auch nicht mehr möglich, die vom Bundesverfassungsgericht in seinem Urteil zum Antiterrordateigesetz betonte Kompensationsfunktion meiner Kontrollen für die betroffenen Bürgerinnen und Bürger sachgerecht zu gewährleisten, d. h. an Stelle der Betroffenen zu überprüfen, ob ihre Rechte bei heimlichen Eingriffen der Sicherheitsbehörden gewahrt worden sind. Nach dem Urteil des Bundesverfassungsgerichts sind diese Prüfungen von herausragender Bedeutung, da die Betroffenen in aller Regel keine Kenntnis von diesen heimlichen Eingriffen haben bzw. erlangen können. Ich appelliere dringend an den Gesetzgeber, seiner Verantwortung gerecht zu werden und ein ausgewogenes Verhältnis von Sicherheit und Kontrolle herzustellen.

Für den Schutz der Grundrechte und das Vertrauen der Bevölkerung in effiziente, unabhängige Kontrollorgane – und damit für Wesenselemente des demokratischen Rechtsstaates – ist dies unerlässlich.

Ich empfehle dem Gesetzgeber, bei den notwendigen Maßnahmen auch die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013 und 9. Oktober 2014 zur Unzuläs-

sigkeit anlassloser Überwachungen und zur effektiven Kontrolle der Nachrichtendienste zu berücksichtigen (vgl. Anlage 6 und 11).

2.1.2 Der „NSA Skandal“ - aus technologischer Sicht

Die globale Überwachungs- und Spionageaffäre hat offenbart, was viele in der Vergangenheit für nicht möglich hielten: Die flächendeckende elektronische Erhebung, Speicherung und Auswertung der Telekommunikationsdaten und des Internets sind technisch machbar! Die bisher eingesetzten Sicherheitsmechanismen müssen hinterfragt und überarbeitet werden.

Das Ausnützen der technologischen Entwicklung (z. B. größere Speicherdichten, höhere Prozessorleistungen, effizientere Suchalgorithmen) und die insgesamt höhere globale Vernetzung macht vieles möglich, was in der Vergangenheit als utopisch galt. Darauf setzen die Überwachungssysteme, die der Öffentlichkeit im Zuge des NSA-Skandals bekannt wurden: u. a. PRISM, Boundless Informant, Tempora, XKeyscore und Mail Isolation Control and Tracking. Schaut man sich diese Verfahren an, stellt man erstens fest, dass praktisch kein IT-System mehr von Überwachung verschont ist. Zweitens ist festzuhalten, dass der Einsatz von sicheren Verschlüsselungsverfahren zwar nicht alles, aber doch vieles verhindert hätte.

Dass Netze nicht immer sicher sind, darauf habe ich bereits im 14. Tätigkeitsbericht (Nr. 30.5) hingewiesen. Ich habe schon damals vorgeschlagen, das auch von Fachleuten favorisierte „Zwiebelmodell“ zu verwenden, bei dem durch mehrere übereinanderliegende und einander verstärkende Sicherheitsmechanismen die Datensicherheit insgesamt gestärkt wird - was im Übrigen nach wie vor aktuell ist. Bereits 1992 habe ich den Einsatz von Verschlüsselung für besonders schützenswerte Daten gefordert (vgl. 14. TB Nr. 30.3). Die Reaktion darauf war kaum messbar, stattdessen verwies man auf die hohen Kosten und Akzeptanzprobleme bei Anwendern. Die Kryptokontroverse verschärfte diese Diskussion Ende der 90er Jahre (vgl. 17. TB Nr. 8.10.2 ff.). Leider nahm der Einsatz von Verschlüsselungsverfahren als sog. Datenschutzbasistechnologie trotz fallender Kosten für Systeme und Verfahren und besserer Bedienbarkeit kaum zu, wie ich in der Folgezeit bei Beratungen und Kontrollen feststellen musste. Ich nahm diese „Verschlüsselungsmüdigkeit“ zum Anlass, in meinen 18. Tätigkeitsbericht erneut auf das Problem hinzuweisen und den Einsatz anzumahnen (Nr. 8.5 ff.). Dabei wurden auch konkrete Verfahren, deren Sicherheit und Bedienbarkeit dargestellt. Die Reaktion auf meine Anregung war aber eher bescheiden und wiederholte gebetsmühlenartig die hohen Kosten für die Verfahren und die angebliche Benutzerunfreundlichkeit. Meine Forderungen zum Einsatz von Verschlüsselungsverfahren musste ich deshalb stets von neuem wiederholen, weil die Ergebnisse aus den Beratungs- und Kontrollbesuchen keine Besserung zeigten. Ich zitiere hier aus dem 21. Tätigkeitsbericht für die Jahre 2005 und 2006 (Nr. 4.4.2): „*Leider musste ich bei Beratungen und Kontrollen immer wieder feststellen, dass nur in wenigen Fällen entsprechende [Verschlüsselungs-]Verfahren eingesetzt werden.“* Den Hinweis habe ich im Berichtszeitraum 2007-2008 abermals aufgegriffen (vgl. 22. TB Nr. 8.2).

Wie die heutigen Erfahrungen aus dem NSA-Skandal und die chronologische Abfolge ergeben, hätte der frühzeitige Einsatz von Verschlüsselungsverfahren viele unberechtigte Informationsflüsse erschwert oder abgewehrt. Das BSI bietet beispielsweise ein Verschlüsselungsprogramm für Windows kostenlos an, das sowohl den E-Mail-Verkehr schützt als auch die Speicherung der Daten in Dateien (Gpg4win). Aber auch auf dem freien Markt gibt es Programme wie PGP, die bei geeigneter Wahl der Schlüssel hinreichende Sicherheit bieten. Nur einsetzen müssen es die Nutzer schon.

Eine weitere Folge des NSA-Skandals ist die Verunsicherung vieler Bürgerinnen und Bürger. Sie stellen z. B. Fragen zur Sicherheit ihrer Daten bei Behörden und Unternehmen, oder zu Schutzmaßnahmen aus technologischer Sicht. Bei Verfahren mit sensiblen personenbezogenen Daten, beispielsweise bei der Einführung der elektronischen Gesundheitskarte, fordere ich daher nachdrücklich den konsequenten Einsatz von Verschlüsselungsverfahren zur Sicherung der Daten. Ohne angemessene IT-Sicherheit werden das Vertrauen in die Verfahren geschwächt und diese deswegen ungenügend genutzt. Als Konsequenz aus dem NSA-Skandal müssen meine For-

derungen in Zukunft endlich umgesetzt und die Erfahrungen meiner Dienststelle ernstgenommen werden. Das Vertrauen der Bürgerinnen und Bürger in die IT-Systeme des Bundes - in die IT-Sicherheit insgesamt - muss wieder gestärkt werden.

2.2 Big Data

Das Verarbeiten immer größerer Datenmengen ist durch bessere Speichertechnologien in neue Dimensionen gerückt. Heutzutage stehen die nötigen Speicherkapazitäten und Rechenleistungen zur Verfügung, um sehr große, aus unterschiedlichsten Quellen stammende Datenbestände miteinander zu verknüpfen und auszuwerten. Für diese, als „Big Data" bezeichneten Datenmengen werden immer neue Einsatzfelder in unterschiedlichsten Bereichen gefunden.

2.2.1 Big Data – Chancen und Risiken

Es heißt, dass sich das weltweite Datenvolumen durch die Digitalisierung des Alltags und den Drang, soweit möglich alles zu erfassen, alle zwei Jahre verdoppelt. Immer neuere Verfahren und Technologien werden genutzt, um weitere Anwendungsfelder beim Rechnen über große Datenmengen zu erschließen. Sowohl die Wirtschaft, als auch staatliche Institutionen sehen große Chancen bei der Verwendung von „Big Data". Hierdurch entstehen aber auch Risiken für das informationelle Selbstbestimmungsrecht.

Die gängigste Erklärung von Big Data umschreibt den Begriff als das Rechnen mit und Analysieren von großen komplexen oder auch sich dynamisch verändernden Datenmengen. Die Daten können unstrukturiert oder bereits teilweise strukturiert vorliegen und aus Verknüpfungen vielfältiger Datenbeständen zusammengeführt sein. Die Weiterentwicklung der Speicher-Technologien, die stetige Erhöhung der Rechenleistung und die Optimierung von Verfahren und Algorithmen ermöglicht es, derart große Datenvolumina oftmals nahezu in Echtzeit auszuwerten.

Die Daten stammen dabei aus vielfältigen Bereichen, seien es etwa die Anfragen bei einer Suchmaschine, Verbindungs- und Kundendaten aus Mobilfunkunternehmen, Daten aus sozialen Netzen wie Facebook, aus Blogs oder E-Mails, oder Daten der Energieversorger über den Energieverbrauch. Dabei beschränkt sich die Zusammenführung der Daten nicht auf die jeweiligen Bereiche. Vielmehr werden Datenbestände unterschiedlichster Herkunft miteinander verknüpft, um auf diese Weise umfassendere und genauere Analysen durchführen zu können. Mittlerweile gibt es zahlreiche Anwendungsfälle für Big Data:

In der medizinischen Forschung und Früherkennung etwa wird mit Big Data versucht herauszufinden, welche Behandlungsmethoden für den Patienten am besten sind. Die Auswertung großer Datenmengen soll dabei helfen zu ermitteln, welches Medikament das bestmögliche ist und es wird angestrebt, eine auf jeden Patienten zugeschnittene individuelle Therapie zu entwickeln.

In den Rechenzentren fallen an vielen Stellen umfassende Logdaten an. Diese werden zusammengeführt und ausgewertet, um Erkenntnisse über Anomalien, wie etwa Angriffe oder unrechtmäßige Datenbankabfragen, Veränderungen von Systemen oder Manipulationen zu gewinnen.

Die Echtzeitanalyse von Anfragen bei Suchmaschinen ist ein Positivbeispiel für Big-Data-Anwendungen. So kann z. B. eine auffällig hohe Zahl von Suchanfragen von Menschen einer Region, welche ein Krankenhaus oder Grippemittel suchen, auf eine bevorstehende Grippewelle schließen lassen.

Die Energieversorger bekommen durch die Einführung von Smart-Meter (vgl. auch 24. TB Nr. 10.1) eine Flut von Daten, welche sie zur Auswertung und Steuerung der Energieverteilung nutzen können. Big-Data-Techno-

logien können hier helfen, das schwankende Stromangebot von Windrädern und Solaranlagen zu managen und den Kunden auf sie zugeschnittene Tarife anzubieten. Aber auch das Ausspähen der Kunden wird möglich, wenn z. B. Rückschlüsse auf Lebensgewohnheiten anhand des in kurzen Messintervallen festgestellten Energieverbrauchs möglich werden.

Big-Daten-Verfahren, die personenbezogene Daten verwenden, können häufig nicht rechtskonform durchgeführt werden. Sie geraten in Konflikt mit den grundlegenden Datenschutzprinzipien der Zweckbindung, der Erforderlichkeit, der Verhältnismäßigkeit, der Direkterhebung und der Transparenz. Eine Verarbeitung personenbezogener Daten kann bei Big Data rechtssicher nur mit informierter und freiwilliger Einwilligung der Betroffenen durchgeführt werden. Dies ist in aller Regel aber nicht praktikabel oder möglich. Anonymisierungsfahren sind bei Big-Data-Anwendungen daher von herausragender Bedeutung. Bei wachsenden Datenbeständen aus unterschiedlichsten Bereichen besteht aber auch bei der Verwendung von an sich anonymen Daten die Gefahr, dass sie durch ihre Zusammenführung möglicherweise doch wieder einer bestimmten Person zugeordnet werden können. Big-Data-Verfahren müssen daher so ausgestaltet werden, dass während des gesamten Verarbeitungsprozesses keine Personenbeziehbarkeit besteht oder entstehen kann. Es reicht nicht aus, dass allein die Datenbasis, die Grundlage der Auswertung ist, keinen Personenbezug aufweist, wenn sich während des Verarbeitungsprozesses durch die Zusammenführung unterschiedlicher, für sich genommen nicht personenbezogener Informationen in der Zusammenschau Rückschlüsse auf eine identifizierbare Person ergeben. Und schließlich kann, insbesondere bei der Verwendung hoch selektiver Analysekriterien oder sehr kleinen Bezugsgruppen, auch das Ergebnis einer Big-Data-Auswertung personenbeziehbar sein. Hierbei spielt auch eine Rolle, ob Dritte, denen die ausgewerteten Daten übermittelt werden, mit bei diesen vorhandenen Erkenntnismöglichkeiten einen Personenbezug herstellen können Als ein erstes kritisches Beispiel von Big Data wird hierbei gerne die in 2006 von AOL (USA) vorgenommene Veröffentlichung von Suchergebnissen der eigenen Suchmaschine genannt. Hierbei wurden die AOL-Benutzerkennungen bei den angezeigten Suchanfragen zwar anonymisiert und durch eine Zahl ersetzt, aber die Kombination der komplett ungefilterten Suchdaten erlaubte erhebliche und detaillierte persönliche Rückschlüsse, da viele Benutzer nach für sie persönlich interessanten Daten suchen wie z. B. dem eigene Namen, lokale Adressen, bekannten Firmen, der eigenen Webseite oder den Namen von Familienangehörigen und Freunden.

Des Weiteren besteht das allgemeine Problem der Anwendung anonymisierter Erkenntnisse auf eine Einzelperson. Auch wenn Big Data mit anonymisierten Daten arbeitet, weist die Anwendung der Erkenntnisse zu einer Einzelperson, auf die die gewonnenen Erkenntnisse zutreffen, Personenbezug auf. Hieraus folgt, dass ein Personenbezug auch dann vorliegt, wenn Erkenntnisse genutzt werden, um zu bestimmen oder zu beeinflussen, wie eine Person behandelt oder beurteilt wird. So ist es im E-Commerce beispielsweise gängige Praxis, dass die Bandbreite der einem Kunden angebotenen Zahlverfahren davon abhängt, wie hoch die Ausfallwahrscheinlichkeit bei der Zahlung ist. Die Berechnung dieses Ausfallrisikos basiert auf der anonymisierten Auswertung einer Vielzahl von vorangegangenen Zahlungsfällen. Die daraus gewonnenen Erkenntnisse werden in eine Relation zu den vom Betroffenen vorhandenen Daten gebracht, um daraus letztlich die Risiken zu errechnen. Dieses Scoring weist naturgemäß eine Unschärfe auf, da es keine Vorhersage über das tatsächliche Verhalten trifft, sondern lediglich Wahrscheinlichkeiten berechnet - mit für den Einzelnen u. U. gravierenden Folgen.

Die Bedeutung von Big Data wird künftig durch die Erschließung weiterer Anwendungsgebiete und neuer Datenbestände noch zunehmen. Hierin sehe ich zwar große Chancen u. a. für die Wirtschaft; jedoch muss bei Big-Data-Verfahren die Einhaltung des Datenschutzes frühzeitig berücksichtigt und immer wieder neu bewertet werden.

Insgesamt bedarf es eines rechtlichen Rahmens, der möglichst globale Geltung hat. Die europäische Datenschutz-Grundverordnung, die derzeit beraten wird, ist hierzu ein erster wichtiger Schritt, da sie nicht nur europaweit zu einem harmonisierten Datenschutzniveau führt. Sie wirkt durch das Marktortprinzip und durch die Übermittlungsregeln auch deutlich über den europäischen Markt hinaus.

Weiter sind in einem starken Maße technologische Ansätze erforderlich, um die aufgezeigten Gefahren nicht Realität werden zu lassen. So unterstützen etwa intelligente Mechanismen zur Anonymisierung oder zu einer „starken“ Pseudonymisierung die Möglichkeit, Big-Data-Technologien datenschutzgerecht einzusetzen. Daraus lässt sich im Übrigen auch ein enormes Innovationspotential für die europäische IT-Wirtschaft schöpfen.

Kasten zu Nr. 2.2.1

Datenschutz-Anforderungen an Big Data:

1. Allgemein ist eine „sichere“ Anonymisierung von personenbezogenen Daten in einer frühen Phase von Verarbeitungsprozessen notwendig, jedoch besteht bei Big Data die Gefahr, dass der Personenbezug später wieder hergestellt werden kann. Die datenschutzrechtlichen Anforderungen müssen daher immer im Blick gehalten werden, auch wenn die Daten vermeintlich anonym sind.

2. Bereits beim Design angewendete Datenschutzfolgenabschätzung könnte helfen, Systeme datenschutzfreundlicher zu gestalten.

3. Begrenzung von Datenverknüpfungen, Kürzung der Speicherungsdauer, Gewährung einer stärkeren Kontrolle für die Nutzer:
   Wird die Menge der verfügbaren Daten bereits im Erhebungsstadium reduziert, stehen diese „eingesparten“ Daten für eine spätere Big Data-Nutzung nicht mehr zur Verfügung.

4. Schaffung von Transparenz und Wahlfreiheit durch Einholung von Einwilligungen der Betroffenen.

5. Dokumentation der Verantwortlichkeiten (Woher stammen die Daten? Wer hat sie erhoben?).

6. Besondere Schutzvorkehrungen bei der (zweckentfremdenden) Nutzung besonders sensibler Daten.

2.2.2 Internet der Dinge – Internet of Things

Big Data ist allgegenwärtig, auch in diesem Tätigkeitsbericht. Durch die globalen Entwicklungen beim Internet of Things (IoT) erhalten Fragen zum Datenschutz weiteren Auftrieb.

Seit einigen Jahren werden in der Wirtschaft, besonders im Handel, Produkte mit Hilfe von RFID-Systemen (vgl. Nr. 8.6) automatisch erkannt. In der Logistik werden Warenflüsse darüber gesteuert oder bei der Produktion Systeme zur eindeutigen Identifizierung von Komponenten etwa beim Einbau in Fahrzeuge eingesetzt. Nach den Vorstellungen von Wirtschaft und Industrie soll das (Wieder-) Erkennen von Produkten oder Ersatzteilen aber künftig noch weiter gehen: Immer mehr Geräte sollen künftig mit dem Internet verbunden und so in der Lage sein, miteinander zu kommunizieren. Teilweise haben die Benutzer davon keine Kenntnis. Die Hersteller solcher Produkte versprechen, unser Leben durch diese Technik viel angenehmer und einfacher zu machen, z. B. im Gesundheitswesen oder in Fahrzeugen. Wegen der Aktualität hat sich auch die Internationale Datenschutzkonferenz im Jahr 2014 dem Thema gewidmet (vgl. Nr. 4.3 sowie Kasten zu Nr. 2.2.2).

Dabei sind die Datenquellen für Big Data und das Internet der Dinge bereits in vielen Produkten enthalten, wie die folgenden Beispiele zeigen.

Ein moderner Fernseher ist heute quasi ein PC mit großem Monitor, eine Spielekonsole ein vollwertiges Mediencenter im Kinderzimmer und ein Smartphone im Verbund mit einem Fitnessarmband eine Datenzentrale mit sehr persönlichen Informationen über deren Nutzer. Fraglich ist, ob man auch diesen neuen technischen Errungenschaften der Unterhaltungsindustrie noch ohne größere Bedenken nutzen kann?

Mit neuen Spielekonsolen wird der Datenschutz im Kinderzimmer zum Thema, denn die neuen Gerätegenerationen verfügen über Sensoren, Kameras und Techniken, um etwa Spieler und deren Bewegungen zu erkennen oder mittels Gesten oder gesprochener Schlüsselwörter auf Eingaben zu reagieren. Dabei können Nutzer kaum noch kontrollieren, was über sie gespeichert wird. Eine Konsole registriert ständig alle möglichen persönlichen Informationen über ihre Nutzer: Reaktionsgeschwindigkeiten, Lernfähigkeit oder emotionale Zustände. Diese können dann auf einem externen Server verarbeitet und möglicherweise sogar an Dritte weitergegeben werden. Ob sie jemals gelöscht werden, kann der Betroffene kaum beeinflussen.

Zum Aktivieren der Systeme genügt ggf. bereits ein gesprochenes Schlüsselwort. Nutzer befürchten deshalb, jegliches gesprochene Wort könnte evtl. gespeichert und ausgewertet, die Konsole also zur Wanze werden. Eine missbräuchliche Nutzung der Mikrofonüberwachung durch den Hersteller halte ich für übertrieben, ein Bedrohungspotential durch Angreifer aus dem Internet mittels Ausnutzung von Sicherheitslücken aber für möglich. Bei manchen Modellen erfolgt die Gesichtserkennung auf der Konsole selbst, es können Kameraauswertungen wie etwa Gefühlszustände von Personen oder die Anzahl der im Raum befindlichen Personen erkannt werden. Für Werbeindustrie und Marktforschung sind dies wertvolle Informationen. Letztlich muss man dem Hersteller vertrauen, dass nicht verdeckt Daten erhoben und die Datenschutzbestimmungen eingehalten werden.

Auch moderne TV-Geräte haben inzwischen Spionagepotential. Kamen Fernseher in den 1990er Jahren noch ohne eigene Intelligenz und Vernetzung daher, so wurden mit der „Internetisierung“ des Wohnzimmers alle möglichen Geräte wie Blu-Ray-Spieler, Festplatten-Receiver, Tablets, Spielekonsolen und Smart TVs über den WLAN-Router in das eigene Netz geholt. Das Internet ist vom klassischen PC hin zu allen möglichen Endgeräten gewandert.

Mittels der neuen intelligenten Receiver mit Festplattenspeicher oder smarten Fernseher können nicht nur alle möglichen Medienformate abgerufen, sondern z. B. auch vielfältige Zusatzinformationen über den Videotextnachfolger Hybrid broadcast broadband TV (HbbTV) angezeigt werden. Dabei werden die aufbereiteten Informationen der TV-Sender und deren Mediatheken über das Internet nachgeladen. Eigentlich eine prima Sache, allerdings wird der Fernseher so zur „Datenschleuder“, und Nutzer können durch den Rückkanal zum Abrufen über das Netz eventuell eindeutig identifiziert werden. Dies wird durch die mögliche Übermittlung einer eindeutigen Gerätekennung erleichtert. Solche Fernseher teilen evtl. Dritten mit, welchen Sender man gerade sieht. Diese Daten können Dritte dann ggf. mit weiteren Daten verknüpfen, wie etwa Nutzerprofilen weiterer eigener Internet-Dienste.

Ein weiterer Trend sind gegenwärtig Fitness-Armbänder, die Bewegungs- und Gesundheitsdaten wie z. B. den Puls und Schlafdaten erfassen und überwachen. Die gesammelten Daten werden hierbei mittels Smartphone oder PC abgerufen und oftmals in die Cloud der Hersteller hochgeladen. Die neuen Generationen von Mobiltelefonen verfügen heute ebenfalls über Sensoren, welche mittels spezieller Apps Daten über uns sammeln. Dank eingebauter Ortsbestimmung werden die Informationen dann mit den Geodaten verknüpft und erlauben die Erstellung sehr persönlicher Bewegungs- und Gesundheitsprofile. Das Handy wird hierbei zum Dreh- und Angelpunkt und damit quasi zur Datenzentrale. Dieser Trend wird sich mittels neuer Geräte wie etwa Smartwatches weiter fortsetzen. Auch Krankenkassen und Versicherungen haben hier eine Marktlücke entdeckt und testen bereits mit kostenlos an Versicherte abgegebenen Fitness-Armbänder die Erkennung von Krankheiten. Vor allem bei Gesundheitsdaten ist hierbei besondere Vorsicht geboten. Man sollte keine Daten, die Gesundheitsprofile und Rückschlüsse auf Krankheiten zulassen, an Dritte weitergeben. Denn wer weiß, ob einem in Zukunft aus diesen Daten nicht einmal Nachteile erwachsen (vgl. hierzu auch Nr. 13.1)?

Verschiedene Hersteller und Kreditinstitute sind heute dabei, das Bezahlen per NFC (Near Field Communication) mittels Mobiltelefon zu erproben oder einzuführen. Die elektronische Geldbörse könnte schon bald andere Bezahlmethoden ergänzen oder ganz ersetzen. Jedoch verfügen derzeit nur die neueren und teureren Geräte über den hierzu nötigen Chip zur Kommunikation. Bei allen hier beispielhaft vorgestellten Geräten der Unterhaltungselektronik besteht grundsätzlich die Gefahr, dass persönliche Profile erstellt werden und möglicherweise gegen Datenschutzrecht verstoßen wird. Daher müssen sich auch die unterschiedlichen Arbeitsgruppen des Düsseldorfer Kreises und der Datenschutzkonferenz immer wieder mit den neuesten Trends befassen. Was uns in Zukunft an neuen Technologien begegnet und ob sich alle diese neuen Gerätschaften und Techniken trotz Datenschutzbedenken durchsetzen, bleibt abzuwarten.

Kasten zu Nr. 2.2.2

Die 36. Internationalen Datenschutzkonferenz am 13. und 14. Oktober 2014 (vgl. oben Nr. 4.3) hat zum IoT eine Erklärung erarbeitet, in der die Selbstbestimmung als ein unveräußerliches Recht aller Menschen anerkannt wird (in Englisch abrufbar auf meiner Internetseite unter www.datenschutz.bund.de). IoT erhöht das Risiko, dass Unternehmen und Behörden entweder Persönliches über uns erfahren oder wir unser Verhalten entsprechend anpassen. Beides beeinträchtigt das informationelle Selbstbestimmungsrecht. Die Konferenz hat deshalb folgende Empfehlungen abgegeben:

- Die Bedeutung der durch IoT erfassten Daten wird hinsichtlich Menge, Qualität, Aktualität und Sensibilität weiter wachsen. Daher sollten diese Daten grundsätzlich als personenbezogene Daten angesehen werden.

- Geschäftsmodelle, die auf IoT-Daten beruhen, müssen ausreichend transparent sein und darlegen, welche Dienstleistungen auf welche Daten zugreifen.

- Die Bedeutung des Ubiquitous Computing (vgl. 23. TB Nr. 1.5) wird zunehmen, daher werden anonyme Nutzungsmöglichkeiten oder Verpflichtungen zur Datensparsamkeit (§ 3a BDSG) immer wichtiger.

- Die Privatsphäre der Verbraucher muss durch Konzepte wie Privacy by Design und Privacy by Default von Anfang an geschützt werden. Datenschutz und Sicherheit müssen als Wettbewerbsvorteil betrachtet werden.

- Das Internet der Dinge stellt auch eine beträchtliche Herausforderung für die IT-Sicherheit dar. Um die mit IoT verbundenen Risiken zu minimieren, ist Ende zu Ende Sicherheit nicht nur bei individueller Kommunikation (z. B. E-Mail), sondern auch bei der Kommunikation zwischen „Dingen“ erforderlich. Dadurch wird beispielsweise das Mitlesen durch unbeteiligte smarte Geräte verhindert.

- Die Datenschutzgesetze und die neue europäische Datenschutz Grundverordnung müssen den Anforderungen, die sich aus IoT Technologien ergeben, gerecht werden.

Zum Internet of Things hat auch eine Unterarbeitsgruppe der Technology Subgroup ein Papier veröffentlicht (vgl. Nr. 3.1.4). Außerdem hat die Internationale Datenschutzkonferenz noch eine weitere Entschließung zu Big Data angenommen (diese ist ebenfalls in Englisch abrufbar auf meiner Internetseite unter www.datenschutz.bund.de).

2.2.3 Anonymisierung und Pseudonymisierung - aber bitte wirksam!

Maßnahmen des Datenschutzes durch Technik sind ein zentrales Werkzeug, um personenbezogene Daten zu schützen und klassische Datenschutzziele zu wahren. Dabei müssen aber die Wirksamkeit dieser Maßnahmen sichergestellt und mögliche Restrisiken beachtet werden. Dies gilt auch für Anonymisierung und Pseudonymisierung personenbezogener Daten.

Im Zeitalter von riesigen Datenmengen (vgl. dazu Nr. 2.2) kommt dem Schutz personenbezogener Daten eine immer größere Bedeutung zu. Gerade allgemein zugängliche, sogenannte „offene" Daten, bieten der Allgemeinheit immense Vorteile - sei es zu Zwecken der Forschung oder aufgrund der Möglichkeit der kostenlosen Nutzung. Weisen Daten jedoch einen Personenbezug auf, ist ihre Weitergabe oder Veröffentlichung datenschutzrechtlich bedenklich.

Neben den technisch-organisatorischen Maßnahmen nach § 9 BDSG sind Anonymisierung und Pseudonymisierung personenbezogener Daten wirksame Maßnahmen zu deren Schutz. Beide Konzepte werden jedoch oft - unwissentlich oder bewusst - miteinander vermischt.

Abgrenzung zwischen Anonymisierung und Pseudonymisierung

Das BDSG definiert die Anonymisierung als die unumkehrbare Veränderung personenbezogener Daten derart, dass die Zuordnung zu einer Person komplett ausgeschlossen oder nur mit einem unverhältnismäßig großen Aufwand möglich ist (vgl. Kasten a zu Nr. 2.2.3). Diese Definition beschreibt sowohl den Begriff der absoluten Anonymisierung, als auch die sogenannte faktische Anonymisierung. Eine faktische Anonymisierung liegt vor, wenn die Zuordnung von Daten zu einer Person nur mit unverhältnismäßigem Aufwand möglich ist. Anonymisierte Daten fallen nicht in den Anwendungsbereich der nationalen und europäischen Datenschutzvorschriften.

Im Gegensatz dazu werden bei der Pseudonymisierung die Identifikationsmerkmale von Datensätzen durch Kennzeichen (Pseudonyme) ersetzt (vgl. Kasten a zu Nr. 2.2.3). Die Pseudonymisierung stellt eine sinnvolle Schutzmaßnahme dar, da eine Verknüpfung zwischen den ursprünglichen und den pseudonymisierten Daten zwar gewollt sein kann (beispielsweise zur Mitteilung von Forschungsergebnissen an Betroffene), aber nur unter restriktiven Bedingungen und einem eingeschränkten Personenkreis möglich sein darf. Pseudonymisierung ist jedoch keine Anonymisierung. Das Ergebnis einer Pseudonymisierung bleiben personenbezogene Daten, die in den Anwendungsbereich der nationalen und europäischen Datenschutzvorschriften fallen.

Wirksamkeit der Anonymisierung

Bereits 1997 haben die Datenschutzbeauftragten des Bundes und der Länder in ihrem Arbeitspapier „Datenschutzfreundliche Technologien" die Qualität von Anonymisierungstechniken thematisiert (17. TB Nr. 8.5). Dort heißt es: „ein Höchstmaß an Anonymität wird erreicht, wenn personenbezogene Daten gar nicht erst entstehen." Da dies nicht immer möglich ist, müssen zwingend Kriterien für die Wirksamkeit der Anonymisierung und die Vermeidung von Restrisiken definiert werden.

So sollten sich Anonymisierungsverfahren immer an etablierten Verfahren und Algorithmen nach dem Stand der Technik orientieren. Selbst entwickelte eigene Verfahren weisen oft erhebliche Mängel auf. Daten sind zu löschen, wenn der Zweck zur Speicherung nicht mehr gegeben ist - übrigens nicht nur in diesem Kontext. Verfahren zur Anonymisierung sollten bereits in der Entwicklungsphase berücksichtigt (Stichworte Privacy by Design und Privacy by Default, vgl. 23. TB Nr. 3.1) und frühzeitig umgesetzt werden.

Die Artikel-29-Gruppe hat in einem richtungsweisenden Arbeitspapier zu Anonymisierungstechniken (WP 216 vom 10.04.2014, vgl. Nr. 3.1.4) deren Robustheit auf Grundlage von drei Risiken untersucht:

- Herausgreifen: die Möglichkeit, in einem Datenbestand einige oder alle Datensätze zu isolieren, welche die Identifizierung einer Person ermöglichen;

- Verknüpfbarkeit: die Fähigkeit, mindestens zwei Datensätze, die dieselbe Person oder Personengruppe betreffen, zu verknüpfen;

- Inferenz: die Möglichkeit, den Wert eines Merkmals mit einer signifikanten Wahrscheinlichkeit aus den Werten einer Reihe anderer Merkmale abzuleiten.

Nur Lösungen, die Schutz vor allen drei Risiken bieten, sind nach Auffassung der Artikel-29-Gruppe geeignet, eine Re-Identifizierung auszuschließen (vgl. Kasten b zu Nr. 2.2.3).

Einsatz von Pseudonymisierung

Die Artikel-29-Gruppe hat in ihrem Arbeitspapier auch mit dem Missverständnis aufgeräumt, Pseudonymisierung sei eine Anonymisierungstechnik. Sie widerspricht damit den Aussagen einiger Interessensgruppen, die pseudonymisierte Daten als eine eigene Klasse von personenbezogenen Daten deklarieren möchten.
Die genannten drei Kriterien für eine wirksame Anonymisierung sind im Falle der Pseudonymisierung gerade nicht erfüllt.

Pseudonymisierung kann jedoch gerade dann sinnvoll sein, wenn eine Anonymisierung von Daten nicht in Betracht kommt. Für den wirksamen Einsatz gelten ähnliche Prinzipien wie für die Anonymisierung. Zusätzlich muss gewährleistet sein, dass eine Re-Identifikation nur unter strikten Vorgaben und von einem stark begrenzten Personenkreis erfolgen darf. Die Artikel-29-Gruppe hat dazu in ihrem Papier Schwachstellen und häufige Fehler benannt.

Pseudonymisierung und Anonymisierung im Rahmen der Revision des europäischen Datenschutzrechts

Im Rahmen der Verhandlungen zur Datenschutz-Grundverordnung (DSGVO) hat die Bundesregierung eine Note an den Ratsvorsitz übermittelt, die sich mit den Themen Pseudonymisierung und Anonymisierung befasst und die ich in wesentlichen Teilen begrüße (vgl. Nr. 1.2.4). Die Note schlägt eine Privilegierung von pseudonymer Datenverarbeitung unter bestimmten Voraussetzungen vor.

Kasten a zu Nr. 2.2.3

§ 3 BDSG - Weitere Begriffsbestimmungen

[…]

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

[…]

Kasten b zu Nr. 2.2.3

Beispiel:

Ein Bundesinstitut führt eine Datenbank über eine äußerst seltene Krankheit. Es findet eine Anonymisierung der Daten auf den Wohnort der Personen statt. Somit ist es zunächst nahezu ausgeschlossen, einzelne Personen zu identifizieren.

Im Laufe der Zeit werden jedoch die Daten zu den Personen in der Datenbank um weitere Inhalte ergänzt: Zunächst wird gespeichert, wann eine Person erkältet war, dann, ob und wann sie einen Unfall hatte, später werden weitere Krankheiten ergänzt, usw. Damit ist es in Einzelfällen möglich, eine Person zu identifizieren, insbesondere wenn diese in einem Ort mit nur wenigen Einwohnern wohnt.

Im vorliegenden Fall handelt sich daher *nicht* um eine Anonymisierung, da aufgrund der Ergänzung weiterer Daten (Risiko: Verknüpfbarkeit) eine Isolation einzelner Datensätze (Risiko: Herausgreifen) und folglich eine Re-Identifikation möglich ist.

2.3 Entscheidungen des Europäischen Gerichtshofs

Mit zwei Entscheidungen hat der Europäische Gerichtshof (EuGH) innerhalb nur eines Monats die Datenschutzwelt erfreut bzw. erschüttert - je nachdem, welche datenschutzrechtlichen Standpunkte man einnimmt. Während das Urteil zur Vorratsdatenspeicherung die Fachleute nicht überraschte, kam die Entscheidung zu den Pflichten der Suchmaschinenbetreiber schon fast einem Donnerhall gleich. Mit beiden Urteilen hat der Europäische Gerichtshof deutlich gemacht, welche hohe Bedeutung den datenschutzsichernden Grundrechten zukommt.

2.3.1 Das Aus für die Vorratsspeicherung von Daten?

Der EuGH hat die Richtlinie über die Vorratsdatenspeicherung für europarechtswidrig und sogar rückwirkend für unwirksam erklärt.

Regelmäßig war das Thema Vorratsdatenspeicherung Gegenstand der vorangegangenen Tätigkeitsberichte (vgl. zuletzt 24. TB Nr. 6.1 und Kasten zu Nr. 6.2). Nachdem das Bundesverfassungsgericht (Urteil vom 02.03.2010) bereits das Gesetz zur Umsetzung der entsprechenden Richtlinie für nichtig erklärt hatte, entschied nun auch der EuGH (Urteil vom 08.04.2014, Az. C-293/12 und C-594/12), dass die Grundrechtsverstöße in der europäischen Richtlinie zur Vorratsdatenspeicherung selbst zu deren Ungültigkeit führen. Der durch die Richtlinie bedingte schwerwiegende und unverhältnismäßige Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten stelle einen Verstoß gegen Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union dar. Das Gericht kritisierte insbesondere die unzureichenden Vorgaben und fehlenden Konkretisierungen in der Richtlinie. Gerade mit Blick auf die weitreichenden Auswirkungen und die Aussagekraft, die eine umfassende Überwachung des Telekommunikationsverhaltens sämtlicher EU-Bürgerinnen und -Bürger mit sich bringe, habe der europäische Gesetzgeber klarere und präzisere Regeln festlegen müssen. Nur so hätten die in der Richtlinie vorgegebenen Maßnahmen als noch verhältnismäßige Regelungen ausgestaltet werden können, deren Grundrechtseingriff sich auf das absolut Nötigste beschränke.

Vor allen Dingen kritisierten die Luxemburger Richter, dass die Richtlinie dem Ziel der Bekämpfung schwerer Kriminalität dienen solle, aber keinerlei Beschränkungen der erfassten Daten oder Personen vorsehe, die zur Erreichung dieses Zieles tatsächlich benötigt würden. Vielmehr rechtfertige sie eine pauschale Speicherung sämtlicher Kommunikationsvorgänge und damit sogar solcher, die dem besonderen rechtlichen Schutz von Berufsgeheimnisträgern unterlägen.

Die Richtlinie stelle zudem weder objektive Kriterien für eine notwendige Beschränkung der Zugangsberechtigten zu den Vorratsdaten auf, noch verlange sie eine Vorabkontrolle des Zugangs zu den Daten durch eine unabhängige Stelle oder ein Gericht.

Die vorgesehene Speicherfrist von 6 bis 24 Monaten, so der EuGH weiter, sei ohne Vorgabe konkreter Kriterien festgesetzt worden, die eine Beschränkung der Speicherdauer auf das absolut Notwendige vorsähen.

Die Richtlinie schreibe schließlich keine Speicherung der Daten innerhalb des Unionsgebietes vor, so dass die zwingend notwendige und in der Grundrechtecharta explizit geforderte unabhängige Datenschutzaufsicht nicht vollumfänglich gewährleistet sei.

Als Folge des Urteils besteht im europäischen Rechtsraum nun keine Rechtsgrundlage für die Vorratsdatenspeicherung mehr.

Viele Innen- und Sicherheitspolitiker sowie Vertreter von Strafverfolgungsbehörden betonen allerdings nach wie vor, wie wichtig die Vorratsdatenspeicherung für eine funktionierende Kriminalitätsbekämpfung sei und dass es daher eines neuen nationalen Gesetzes bedürfe. Eine Antwort auf die Frage, wie dieses die durch den EuGH aufgestellten Vorgaben erfüllen kann, stand bei Redaktionsschluss aber aus. Insbesondere die Frage der Beschränkung der Datenerfassung auf tatsächlich relevante Kommunikationsvorgänge, die den Grundsätzen einer umfassenden anlasslosen Vorratsdatenspeicherung entgegensteht, bleibt unbeantwortet.

Ob es auf europäischer Ebene eine neue Initiative für eine Richtlinie zur Vorratsdatenspeicherung geben wird, ist angesichts der Ankündigungen der Europäischen Kommission, zunächst eine umfassende Evaluierung des Urteils sowie eine darauf basierende Folgenauswertung unter Beteiligung sämtlicher Interessenvertreter durchführen zu wollen, offen.

Ob das Urteil des EuGH das Aus für die Vorratsspeicherung von Daten gewesen ist, wird sich erst in der Zukunft zeigen. Die durch das Gericht aufgezeigten Defizite haben allerdings mit aller Klarheit deutlich gemacht, dass eine Vorratsdatenspeicherung in der bisherigen Form aus Gründen des Grundrechtsschutzes nicht möglich ist.

2.3.2 Neue Pflichten für Suchmaschinenbetreiber

Der EuGH hat in seinem wegweisenden Urteil vom 13. Mai 2014 (C 131/12) die datenschutzrechtliche Verantwortlichkeit von Suchmaschinenbetreibern wie Google für die Veröffentlichung von Suchergebnissen anerkannt und den betroffenen Nutzern unter bestimmten Voraussetzungen ein Recht auf Löschung der Verknüpfungen, die zu der ursprünglichen Website führen, zugesprochen.

Mit diesem Urteilsspruch aus Luxemburg haben die Meisten wohl nicht gerechnet: Das Votum des EuGH weicht nicht nur in der entscheidenden Frage deutlich von dem Schlussantrag des Generalanwalts, dem die Richter in aller Regel zu folgen pflegen, ab. Auch die Artikel-29-Gruppe hatte bislang nahezu einmütig die Position vertreten, ein Suchmaschinenbetreiber sei nicht für die Verarbeitung von personenbezogenen Daten verantwortlich, die auf der Website eines Dritten veröffentlicht sind und zu denen er durch Angabe des Links lediglich den Weg weist. Die im Jahr 2008 in der Stellungnahme zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148 vom 04.04.2008) thematisierte Verantwortlichkeit von Suchmaschinenbetreibern für die veröffentlichten Suchergebnisse war von der Artikel-29-Gruppe damals nur deshalb offen formuliert worden, um die von einem Mitgliedstaat bereits erlassenen Regelungen zum Entfernen von Inhaltsdaten aus dem Suchindex einzubeziehen.

Das Google-Urteil des EuGH führt nun bei einer ganzen Reihe praktisch hoch relevanter Auslegungsfragen zu neuen Sichtweisen und Rechtssicherheit: Fast schon beiläufig erklärte der EuGH, dass Werberepräsentanzen, die der Verkaufsförderung von Werbeflächen der Suchmaschine dienen, als „Niederlassungen“ anzusehen sind, die die Anwendbarkeit europäischen Datenschutzrechts auf Anbieter aus Drittstaaten, z. B. US-Diensteanbieter wie Google, begründen. Denn nach der europäischen Datenschutzrichtlinie 95/46/EG gilt europäisches Recht auch für Unternehmen außerhalb der EU, wenn die Datenverarbeitung „im Rahmen der Tätigkeiten einer Niederlassung ausgeführt“ wird. Ein solcher Zusammenhang sei, so der EuGH, bereits dann gegeben, wenn die Niederlassung die Datenverarbeitung wirtschaftlich fördere.

Von noch größerer Bedeutung und Tragweite ist die Aussage des EuGH, Suchmaschinenbetreiber, die Daten mit Indexierprogrammen auslesen, speichern und organisieren, auf ihren Servern aufbewahren und anschließend an die Nutzer weitergeben bzw. diesen bereitstellen, verarbeiteten eigenständig personenbezogene Daten und seien daher hierfür datenschutzrechtlich verantwortlich.

Die sich daraus ergebende Verpflichtung von Suchmaschinenanbietern, unter bestimmten Voraussetzungen Links zu Internetseiten mit Informationen über betroffene Personen zu entfernen, wird zu Recht als deutliche Stärkung des Datenschutzes angesehen, teilweise aber auch als Gefahr für die Presse- und Meinungsfreiheit kritisiert. Das Gericht, so die Kritiker, habe zu einseitig die datenschutzrechtlichen Interessen der Betroffenen berücksichtigt und die Interessen der Allgemeinheit an der Nutzung von Suchmaschinen und der Betreiber der Internetseiten vernachlässigt, denen die Suchmaschinen den Zugang zu einem großen Personenkreis verschaffen und die in ihrer Meinungs- und Pressefreiheit beeinträchtigt werden könnten. Sollten sich Suchmaschinenbetreiber wie Google in Anbetracht der zu erwartenden Flut von Löschungsaufforderungen im Zweifel für das Löschen der Verlinkung entscheiden, werde schließlich die Funktionsfähigkeit von Suchmaschinen eingeschränkt und die Auffindbarkeit von Inhalten im Netz beeinträchtigt. Es ist daher durchaus treffend, vom „Recht auf nicht gefunden werden“ statt vom „Recht auf Löschung“ zu sprechen, da der EuGH nicht die Löschung der ursprünglichen Website verlangt, sondern nur des darauf weisenden Links.

Die Datenschutzbeauftragten des Bundes und der Länder haben das Urteil des EuGH in ihrer Entschließung vom 9. Oktober 2014 begrüßt und eine effiziente Umsetzung angemahnt (vgl. Nr. 1.2.2 und Anlage 10). Die Artikel-29-Gruppe hat insbesondere die Notwendigkeit einer einheitlichen europäischen Vorgehensweise betont und nach intensiven Beratungen zum Ende des Jahres 2014 Leitlinien zur Umsetzung des Urteils veröffentlicht. Diese enthalten neben einer zusammenfassenden Würdigung der Entscheidung und daraus folgenden Vorgaben für die praktische Umsetzung in einem zweiten Teil Bewertungskriterien, die ein einheitliches Vorgehen der Datenschutzbehörden bei Beschwerden betroffener Nutzer über von Suchmaschinenanbieter abgelehnte Löschanträge sicherstellen sollen.

Ein berechtigtes Löschbegehren von Betroffenen setzt voraus, dass die entsprechenden Inhalte als verlinktes Suchergebnis durch den Suchmaschinenanbieter auf eine Anfrage ausgegeben werden, die anhand des Namens des Betroffenen durchgeführt wurde. Ist dies der Fall, konzentriert sich die weitere Prüfung auf die Fragen, ob die Daten auf den verlinkten Websites korrekt, besonders schützenswert oder überholt sind, ob es sich um beleidigende Inhalte oder üble Nachrede handelt, ob die betroffene Person negative Folgen befürchten muss oder besonderen Gefährdungen ausgesetzt sein kann. Im Hinblick auf das Informationsinteresse der Internetnutzer ist auch zu berücksichtigen, ob der Betroffene eine Person des öffentlichen Lebens ist und es sich um Informationen handelt, die für journalistische Zwecke veröffentlicht wurden. Die Entscheidung trifft die Datenschutzbehörde anhand der Fakten und nach Abwägung der unterschiedlichen Interessen, wobei jedoch ein einzelner Faktor nie ausschlaggebend sein kann.

Der Kriterienkatalog ist als nicht abschließende Liste anzusehen, die im Zuge der zunehmenden Anwendungserfahrungen erweitert werden kann. Informationen zu bisher bearbeiteten Fällen lagen bis Redaktionsschluss noch nicht vor. Die Leitlinien können auf meiner Website unter www.datenschutz.bund.de abgerufen werden.

2.4 Unabhängige Datenschutzaufsicht - endlich auch im Bund

Der Deutsche Bundestag hat am 18. Dezember 2014 ein Gesetz verabschiedet, mit dem die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit eine eigenständige oberste Bundesbehörde werden soll, die nur noch parlamentarischer und gerichtlicher Kontrolle unterliegt.

Seit ihrer Gründung im Jahre 1978 ist der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) beim Bundesministerium des Innern (BMI) eingerichtet. Die BfDI ist nach dem Bundesdatenschutzgesetz zwar unabhängig, jedoch unterliegt sie der Rechtsaufsicht der Bundesregierung und der Dienstaufsicht des BMI. Die in ihrer Dienststelle tätigen Beamten und Tarifbeschäftigten sind solche des BMI. Dienstvorgesetzter und oberste Dienstbehörde ist der Bundesminister des Innern.

Dieser organisatorische Aufbau und die Rechtsstellung der BfDI entsprechen nicht den europarechtlichen Vorgaben, wie sie sich aus der Europäischen Datenschutzrichtlinie von 1995 ergeben. Danach müssen die Mitgliedstaaten Aufsichtsbehörden einrichten, die die ihnen zugewiesenen Aufgaben „in völliger Unabhängigkeit“ wahrzunehmen haben.

Wie der Begriff der „völligen Unabhängigkeit“ zu interpretieren ist, hat der Europäische Gerichtshof (EuGH) in drei Urteilen gegen Deutschland (2010), gegen Österreich (2012) und gegen Ungarn (2014) konkretisiert. Konnte sich die Bundesregierung nach dem Urteil gegen Deutschland noch formal darauf berufen, dieses beziehe sich nur auf die Datenschutzaufsicht im nicht-öffentlichen Bereich in den Ländern (vgl. 23. TB Nr. 2.1), ergab sich spätestens aus dem Urteil zur Unabhängigkeit der österreichischen Datenschutzkommission klar, dass auch meine Rechtsstellung nicht den europäischen Vorgaben genügt, da die seinerzeitige österreichische Situation der rechtlichen Ausgestaltung nach dem BDSG sehr ähnlich war (vgl. 24. TB Nr. 3.1).

Meinen langjährigen Forderungen entsprechend hat die Bundesregierung den gesetzgeberischen Handlungsbedarf endlich erkannt und im Sommer 2014 einen entsprechenden Gesetzentwurf vorgelegt. Nach Befassung des Bundesrates und einer öffentlichen Sachverständigenanhörung im Innenausschuss des Deutschen Bundestages hat der Entwurf schließlich am 18. Dezember 2014 dessen Plenum passiert. Das Inkrafttreten ist für den 1. Januar 2016 vorgesehen.

Mit dem Gesetz wird meine Dienststelle vollständig aus dem BMI herausgelöst. Die Rechtsaufsicht der Bundesregierung und die Dienstaufsicht des BMI werden gestrichen. Konsequenterweise wird so eine neue Behörde in der Form einer obersten Bundesbehörde gegründet. Ich unterliege nur noch einer politischen Kontrolle durch den Deutschen Bundestag. Zudem sind meine Entscheidungen selbstverständlich gerichtlich überprüfbar.

Mit dieser Konstruktion erfüllt Deutschland die unabdingbaren Mindestanforderungen, die das europäische Recht aufstellt. Ich hätte mir jedoch mehr gewünscht.

So hatte ich u. a. vorgeschlagen, im Gesetz eine Regelung aufzunehmen, in der die Möglichkeit einer Kooperation und des Personaltausches mit allen Ressorts der Bundesregierung und anderen obersten Bundesbehörden vorgesehen wird. Die BfDI wird mit Abstand die kleinste oberste Bundesbehörde sein und verfügt nicht über einen Geschäftsbereich, sodass es notwendig ist, qualifiziertes und erfahrenes Personal auch aus anderen Behörden gewinnen zu können. Deswegen wären Wechselmöglichkeiten von und zu anderen obersten Bundesbehörden wichtig. Zurzeit verhandele ich mit dem BMI über eine entsprechende Vereinbarung. Mit der von mir vorgeschlagenen Regelung hätte eine derartige Vereinbarung mit anderen obersten Bundesbehörden auf einer sicheren rechtlichen Grundlage erfolgen können.

Darüber hinaus hatte ich zur Rechtssicherheit für die künftige Struktur als oberste Bundesbehörde angeregt, im Gesetz klarstellend die Möglichkeit vorzusehen, Außenstellen einzurichten. Dies hätte der vergleichbaren Regelung in § 2 Absatz 1 BRHG entsprochen.

Eine Regelung, die meine Zeugenaussagen vor Gerichten und parlamentarischen Untersuchungsausschüssen zum Teil vom Einvernehmen der Bundesregierung abhängig machen und damit weiterhin einem Genehmigungsvorbehalt der Exekutive unterstellen sollte, ist nach kontroverser politischer Diskussion wieder fallen gelassen worden. Nahezu alle Experten in der öffentlichen Anhörung des Deutschen Bundestages am 1. Dezember 2014 haben sich ebenso wie ich selbst deutlich gegen diese Regelung ausgesprochen, da sie einen unangemessenen und europarechtlich problematischen Eingriff in meine Unabhängigkeit dargestellt hätte. Nunmehr ist klargestellt, dass ich in den Fällen, in denen der Kernbereich der exekutiven Eigenverantwortung der Bundesregierung betroffen sein könnte, lediglich verpflichtet bin, die Bundesregierung zu konsultieren.

Zudem bedarf es einer Stärkung meiner Durchsetzungs- und Sanktionsbefugnisse insbesondere im Bereich der datenschutzrechtlichen Kontrolle im Post- und Telekommunikationsbereich. Verstoßen Anbieter von Post- oder Telekommunikationsdienstleistungen gegen die datenschutzrechtlichen Bestimmungen des Post- oder Telekommunikationsgesetzes, kann ich dies bislang nur mit dem Instrument einer Beanstandung gegenüber der Bundesnetzagentur rügen. Darüber hinaus fehlt mir in diesem Bereich auch die Befugnis, Bußgelder bei Verstößen gegen das Bundesdatenschutzgesetz zu verhängen. Verstöße bleiben auf diese Weise nicht selten folgenlos (vgl. 24. TB Nr. 6.9 m. w. N.). Gegenüber allen anderen Bereichen der Privatwirtschaft haben meine zuständigen Kolleginnen und Kollegen in den Ländern hingegen wirksame Anordnungs- und Untersagungsbefugnisse und können ganz überwiegend auch Ordnungswidrigkeiten verfolgen und Bußgelder verhängen. Hier muss dringend ein Gleichklang hergestellt werden. Ich habe deshalb im Gesetzgebungsverfahren darauf gedrungen, sich dieser Frage in einem weiteren Gesetzgebungsverfahren möglichst zeitnah anzunehmen, damit endlich auch im Bereich von Post und Telekommunikation die europarechtlich gebotenen wirksamen Einwirkungsbefugnisse geschaffen werden.

Zur Unabhängigkeit der Datenschutzaufsicht gehört aber noch mehr als die bloße organisatorische Verselbständigung der Behörde. Diese erzielt nämlich nicht die erforderliche Wirkung, wenn sie nicht die Kapazitäten und Möglichkeiten hat, diese unabhängige Kontrolle auch sicherzustellen. Ich kann meine Aufgabe als Hüterin des Grundrechts auf Datenschutz nur dann in völlig unabhängiger Weise ausüben, wenn ich über die dafür notwendigen Ressourcen verfüge.

Folgerichtig betrachtet auch der Entwurf der zurzeit intensiv beratenen Europäischen Datenschutz-Grundverordnung die Ausstattung der Datenschutzbehörden mit den für ihre Arbeit notwendigen Ressourcen als ein Element der völligen Unabhängigkeit der Datenschutzkontrolle.

Diesen Anforderungen genügt das Gesetz nicht. Weder zieht es ausreichend Konsequenzen aus der organisatorischen Verselbständigung der BfDI, noch - und dies ist noch gravierender - nimmt es sich der bereits jetzt bestehenden erheblichen Defizite bei ihrer Ausstattung an. Insbesondere im Bereich der so wichtigen Kontrolle der Nachrichtendienste, aber nicht nur dort, fehlen mir seit Jahren die personellen Ressourcen, um die vom Bundesverfassungsgericht für zwingend notwendig gehaltene Kontrolldichte auch tatsächlich gewährleisten zu können (vgl. auch Nr. 5.2).

Es bleibt zu hoffen, dass sich das Parlament bei den Haushaltsberatungen zu einer funktionsfähigen Datenschutzkontrolle bekennt und damit auch den Grundrechtsschutz der Bürgerinnen und Bürger verbessert. Aufgrund der Wahl durch den Deutschen Bundestag, der engen Kooperation mit dem Parlament und der Loslösung von der Bundesregierung stehe ich als Kontrollinstanz dem Parlament künftig näher, als es derzeit noch der Fall ist. Deshalb hoffe ich, es gehört zum Selbstverständnis des Deutschen Bundestages, „seine“ Datenschutzbehörde mit der für ihre Funktionsfähigkeit notwendigen Ausstattung zu versehen.

2.5 Zukunft der Stiftung Datenschutz

Statt der Überführung der Stiftung Datenschutz in die Stiftung Warentest bedarf es ihrer grundlegenden konzeptionellen Neuausrichtung.

Seit ihrer Errichtung im Januar 2013 leidet die Stiftung Datenschutz an einer strukturellen Unterfinanzierung, die nur durch jährliche Zuschüsse aus dem Bundeshaushalt und Rückgriffe auf das eigentlich als Stammkapital vorgesehene Stiftungsvermögen ausgeglichen werden kann. Es besteht damit die Gefahr, dass die Stiftung ihre satzungsmäßigen Aufgaben, die Prüfung von Produkten und Dienstleistungen auf Datenschutzfreundlichkeit, die Stärkung von Bildung und Aufklärung im Bereich des (Selbst-)Datenschutzes und die Entwicklung eines Datenschutzauditverfahrens entweder gar nicht oder nicht mit der wünschenswerten Wirkungsbreite wahrnehmen kann.

Dennoch halte ich die im Koalitionsvertrag vorgesehene Integration der Stiftung Datenschutz in die Stiftung Warentest für verfehlt. Zweifelsohne haben beide Stiftungen Schnittmengen, wenn es um die Prüfung von Produkten und Dienstleistungen auf Datenschutzfreundlichkeit geht, insbesondere wenn dies in Form von Testvergleichen erfolgen soll. Wie allerdings die Satzung der Stiftung Datenschutz bereits vorsieht, sollen Produktprüfungen möglichst in Zusammenarbeit mit anderen auf diesem Gebiet tätigen Institutionen erfolgen. Deutlicher hätte ein Hinweis auf die Stiftung Warentest kaum erfolgen können. Angesichts bestehender Kooperationsmöglichkeiten, die der Stiftung Datenschutz auch die ungleich besseren Verbreitungskanäle der Stiftung Warentest erschließen, führt eine institutionelle Überführung in die Stiftung Warentest eigentlich nicht weiter.

Auch wenn konkrete Planungen bislang nicht bekannt sind, würden mit der Überführung allerdings nicht zwei ebenbürtige Partner gleichberechtigt zu einer „Stiftungsfamilie“ zusammengeführt, sondern die Stiftung Datenschutz bestenfalls als „Juniorpartner“ unter das Dach der Stiftung Warentest eingegliedert. Der Verlust der Eigenständigkeit wäre für die Stiftung ohne weitere Zuschüsse auch finanziell nicht einmal vorteilhaft, so dass statt des erhofften Bedeutungszuwachses am Ende ein leiser Abgesang auf die Stiftung Datenschutz stehen könnte. Jedenfalls deutet der bisherige Verzicht der Stiftung Warentest auf die Besetzung des Beiratspostens in der Stiftung Datenschutz nicht unbedingt auf ein echtes Interesse. Schließlich halte ich auch das mit der institutionellen Überführung einhergehende politische Signal, Datenschutz sei ein Unterfall, ein bloßes Anhängsel des Verbraucherschutzes, für irreführend und konzeptionell falsch (vgl. unten Nr. 6.1).

Natürlich schöpft ein schlichtes „Weiter so“ das Potenzial der Stiftung ersichtlich nicht aus, deren Idee ich - wie mein Amtsvorgänger (vgl. 23. TB Nr. 2.5, 24. TB Nr. 3.6) - unterstütze. Für eine unabhängige Stiftung Datenschutz müssen jedoch Konzeption und Finanzierung neu überdacht werden. Statt der geplanten Nähe zur Stiftung Warentest wäre auch eine deutlichere Abgrenzung von dieser unter Verzicht auf (wertende) Prüfungen von Produkten und Dienstleistungen diskussionswürdig. Die Stiftung Datenschutz wäre dann schon von ihrer Konzeption her keine Stiftung „Datentest“, die stets Gefahr läuft, in Konkurrenz zu der ungleich bekannteren Schwesterstiftung zu stehen. Andere Standbeine der Stiftung, namentlich die Forschung und Bildung im Bereich des Datenschutzes, könnten demgegenüber finanziell und personell deutlich aufgewertet werden. Eine zu einer umfassenden Wissens- und Bildungsinstitution ausgebaute Bundesstiftung würde damit jenseits der datenschutzrechtlichen Einzelfallberatung durch die Datenschutzbehörden einen ihr gebührenden zentralen Platz einnehmen können.

2.6 Beratung in Datenschutzfragen - die Datenschutzbeauftragten in Bund und Ländern leisten Interpretationshilfe

Eine wichtige gesetzliche Aufgabe der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ist die Beratung der Bürgerinnen und Bürger, des Parlaments und der Regierung sowie ganz unmittelbar der ihrer Kontrolle unterliegenden Stellen. Sie arbeitet dabei intensiv mit den Datenschutzaufsichtsbehörden in den Ländern zusammen.

Ungeachtet der unterschiedlichen sachlichen und örtlichen Zuständigkeiten der BfDI, der Landesbeauftragten für den Datenschutz und des Bayerischen Landesamts für Datenschutzaufsicht ergeben sich bei der datenschutzrechtlichen Beratung häufig die gleichen oder sehr ähnliche Problemstellungen. Dies gilt in hohem Maße für praktische Fragen des technischen und organisatorischen Datenschutzes. Aber auch im Bereich des Datenschutzrechts beschäftigen sich die Datenschutzbehörden in Bund und Ländern nicht selten mit den gleichen Themen, was angesichts des identischen grundrechtlichen Hintergrunds und der für Bund und Länder in gleicher Weise geltenden Europäischen Datenschutzrichtlinie naheliegt.

Ein wichtiges Mittel, den verantwortlichen Stellen bei übergreifenden Themen praktische Hilfestellung zu geben, sind Orientierungshilfen oder vergleichbare Veröffentlichungen. Diese Publikationen werden in aller Regel von einem oder mehreren der zahlreichen Arbeitskreise oder Arbeitsgruppen der Konferenz der Datenschutzbeauftragten oder des Düsseldorfer Kreises entworfen. Damit wird die fachliche Expertise der Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörden optimal gebündelt und die Arbeit effizient aufgeteilt. Nach Billigung durch die Datenschutzkonferenz oder den Düsseldorfer Kreis werden die Orientierungshilfen veröffentlicht und allen interessierten Stellen über das Internet oder in den meisten Fällen auch in Papierform verfügbar gemacht.

Orientierungshilfen und vergleichbare Publikationen beruhen in der Regel auf konkreten Kontroll- und Beratungserfahrungen der Datenschutzbehörden. Sie greifen wichtige Fragen der praktischen Gewährleistung von Datenschutz und Datensicherheit auf, geben konkrete Tipps und Hinweise zur datenschutzgerechten Gestaltung von Verfahren in Staat und Wirtschaft und dienen häufig auch der Öffentlichkeit als wichtiges Hilfsmittel bei der „Übersetzung“ der datenschutzrechtlichen Anforderungen. Die Mitarbeiterinnen und Mitarbeiter der BfDI beteiligen sich bei der großen Mehrzahl der gemeinsam herausgegebenen Publikationen als Autoren. Einmal erstellt, müssen die Veröffentlichungen - gerade im Bereich des technischen und organisatorischen Datenschutzes - auch regelmäßig aktualisiert und auf dem neuesten technischen Stand gehalten werden. Als ein Beispiel sei die im Berichtszeitraum aktualisierte Orientierungshilfe zum Cloud Computing (vgl. unten Nr. 8.5) genannt.

Orientierungshilfen und Handreichungen

Neben der gemeinsamen Veröffentlichung von Orientierungshilfen und anderen Fachveröffentlichungen gebe ich auch in meinem eigenen Zuständigkeitsbereich eine Reihe von Informationsmaterialien heraus, die zu einem großen Teil auch der Beratung der öffentlichen Stellen des Bundes sowie der Post- und Telekommunikationsanbieter dienen. Hier seien in erster Linie die BfDI-Infos 1 bis 5 erwähnt, die auf sehr großes Interesse beim Fachpublikum, aber auch bei den Bürgerinnen und Bürgern stoßen. Darüber hinaus veröffentliche ich auch eine Vielzahl von Arbeitshilfen, Faltblättern und anderen Informationsmaterialien. Im Berichtszeitraum habe ich u. a. eine Orientierungshilfe zum Verfahrensverzeichnis in der Bundesverwaltung herausgegeben, die den Bundesbehörden mehr Sicherheit bei der Führung dieses Verzeichnisses an die Hand geben soll.

Die Erstellung und Aktualisierung all dieser Arbeitshilfen ist für meine Mitarbeiterinnen und Mitarbeiter mit einem nicht geringen Aufwand verbunden. Dieser lohnt sich aber, da so der Aufwand für Beratungen im Einzelfall reduziert werden kann - angesichts meiner knappen Personalausstattung ein nicht zu unterschätzender Faktor.

Das Verfahrensverzeichnis - Handreichung der BfDI

Meine Handreichung zur Erstellung des Verfahrensverzeichnisses soll eine einheitliche Handhabung in der Bundesverwaltung gewährleisten und bestehende Unsicherheiten über Anwendungsbereich und Inhalt beseitigen.

Jedem, der sich einen schnellen Überblick über Art und Umfang der Datenverarbeitung in einer verantwortlichen Stelle verschaffen will, ist das Verfahrensverzeichnis eine wertvolle Hilfe. Auch „neuen“ behördlichen und betrieblichen Datenschutzbeauftragten bietet es eine Orientierungshilfe weit über die Einarbeitungszeit hinaus.

Wie alle Daten verarbeitenden Stellen haben öffentliche Stellen des Bundes eine Übersicht über die bei ihnen eingesetzten Verfahren automatisierter Verarbeitungen zu führen (§ 4g Abs. 2 Satz 1 i. V. m. §§ 4e, 18 Abs. 2 Satz 2 bis 4 BDSG). Erstellung und Inhalt eines solchen Verfahrensverzeichnisses bereiten in der Praxis erfahrungsgemäß Schwierigkeiten und waren mehrfach Gegenstand meines Erfahrungsaustauschs mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden (vgl. unten Nr. 22.2). Die Anregung für eine konkretisierende Hilfestellung habe ich gerne in Form einer Handreichung (vgl. Anlage 15) aufgegriffen.

Dabei war es mir wichtig deutlich zu machen, dass die Erstellung und Aktualisierung des Verfahrensverzeichnisses - anders als in der Praxis bisweilen gehandhabt - nicht die Aufgabe der behördlichen Datenschutzbeauftragten ist. Gesetzlicher Adressat der Verzeichnispflicht ist allein die verantwortliche Stelle, die zur Erstellung und Führung der Übersicht auf ihre mit den jeweiligen Datenverarbeitungsverfahren befassten Organisationseinheiten zurückgreifen kann und soll. Den behördlichen Datenschutzbeauftragten ist das Verfahrensverzeichnis lediglich „zur Verfügung zu stellen“ (§ 4g Abs. 2 Satz 1 BDSG), damit diese einen Überblick über Art, Umfang, Ablauf und Zweck der eingesetzten Datenverarbeitungsverfahren gewinnen können.

Schwierigkeiten bereitet bisweilen schon die Frage, was überhaupt in das Verfahrensverzeichnis aufzunehmen, was also unter einem „Verfahren automatisierter Verarbeitung“ zu verstehen ist. Hier hilft ein Blick auf Artikel 18 Absatz 1 der europäischen Datenschutzrichtlinie 95/46/EG, der u. a. in § 4e BDSG (Inhalt der Meldepflicht) umgesetzt wurde, auf den wiederum die Vorschriften zum Verfahrensverzeichnis Bezug nehmen. Danach ist ein Verfahren die Gesamtheit von Verarbeitungsvorgängen „zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen“. Aufzunehmen ist also nicht jeder einzelne Verarbeitungsschritt, sondern es sind am Verarbeitungszweck orientierte Zusammenfassungen verschiedener Arbeitsschritte vorzunehmen. Zu erfassen sind also etwa Personalverwaltungs-, Zugangskontroll- oder Zeiterfassungssysteme, nicht aber diesen zugrunde liegende einzelne Verarbeitungsschritte oder aus diesen resultierende elektronische Dokumente und (Text-)Dateien. Der Verarbeitungszweck des Verfahrens muss so aussagekräftig sein, dass externe Dritte anhand der Angaben unzweifelhaft erkennen können, um was für eine Art von Datenverarbeitung es sich handelt.

In der Praxis wird die Erstellung des Verfahrensverzeichnisses nicht selten als bürokratische Pflichtaufgabe angesehen, deren Mehrwert hinterfragt wird. Zwar scheint die Publizitätsfunktion - das Verfahrensverzeichnis ist jedermann auf Antrag verfügbar zu machen - in der Praxis ein Schattendasein zu führen. Gleichwohl schafft das Verfahrensverzeichnis Transparenz für die interessierte Öffentlichkeit. Jede Person kann hierdurch feststellen, ob und inwieweit sie von einer Datenverarbeitung betroffen ist oder sein kann und kann daran anknüpfend ihre Datenschutzrechte geltend machen. Seiner Transparenzfunktion nach außen und innen wird das Verfahrensverzeichnis aber nur gerecht, wenn es stets vollständig und auf aktuellem Stand ist. Das permanente „Nachhalten“ kostet sicherlich Zeit und Mühe. Jede verantwortliche Stelle muss sich jedoch vor Beginn der Datenverarbeitung Gedanken über die Zwecke, den betroffenen Personenkreis, Löschfristen und über Fragen der Datensicherheit machen. Dies dokumentieren zu müssen, trägt bei der verantwortlichen Stelle auch zur Bewusstseinsbildung über Umfang und Auswirkung des jeweils von ihr eingesetzten Verfahrens automatisierter Verarbeitung bei.

Eine vollständige Auflistung aller Orientierungshilfen und vergleichbarer Veröffentlichungen finden Sie auf meiner Internetseite unter www.datenschutz.bund.de.

3 Europäische und internationale Angelegenheiten

3.1 Artikel-29-Gruppe und ihre Unterarbeitsgruppen

Die sog. Artikel-29-Gruppe ist das zentrale Koordinierungsgremium für die datenschutzrechtliche Aufsicht in der Europäischen Union. Dieser Gruppe gehören sowohl Vertreter der nationalen Datenschutzaufsichtsbehörden der Mitgliedstaaten als auch der Europäische Datenschutzbeauftragte und - ohne Stimmrecht - das Datenschutz-Fachreferat der Europäischen Kommission an, das auch die Aufgabe des Sekretariats der Gruppe wahrnimmt. Die Artikel-29-Gruppe untergliedert sich in Unterarbeitsgruppen („Subgroups“) zu allgemeinen und fachspezifischen Datenschutzthemen. In zwei der Subgroups nehme ich die Funktion des Koordinators wahr: In der sich mit technologischen Fragen des Datenschutzes befassenden „Technology Subgroup“ (T S - vgl. Nr. 3.1.4) und der mit Datenschutzfragen im Sicherheits- und Strafverfolgungsbereich befassten Subgroup „Borders, Travel, Law Enforcement“ (BTLE - vgl. Nr. 3.1.5).

Wie in den Vorjahren hat sich die Artikel-29-Gruppe mit einer breiten Palette von Themen befasst, von der Auslegung der europäischen Datenschutzrichtlinie 95/46/EG über die Reform des europäischen Datenschutzrechts und die Bewertung neuer Technologien bis hin zur Befassung mit den Snowden-Veröffentlichungen und den Aktivitäten ausländischer und europäischer Geheimdienste.

Das breite Spektrum der Artikel-29-Gruppe spiegelt sich auch in den erarbeiteten Arbeitspapieren wider: In den Jahren 2013 und 2014 hat das Gremium 16 Dokumente als Stellungnahmen („Opinions“) verabschiedet und zahlreiche Empfehlungen („Recommendations“) und sonstige Arbeitspapiere zu aktuellen datenschutzrechtlichen Fragestellungen zur Entscheidung angenommen.

Eine Liste der im Berichtszeitraum von der Artikel-29-Gruppe angenommenen Stellungnahmen und Dokumente finden Sie auf meiner Internetseite unter www.datenschutz.bund.de.

3.1.1 Subgroup Future of Privacy

Diese Unterarbeitsgruppe hat im Berichtszeitraum u. a. Positionen zur Reform des EU-Datenschutzrechts und insbesondere zum Vorschlag der Europäischen Kommission für eine Datenschutz-Grundverordnung erarbeitet.

Die Aufgabe der Unterarbeitsgruppe Future of Privacy der Artikel-29-Gruppe besteht in der Befassung mit grundsätzlichen datenschutzrechtlichen und -politischen Fragestellungen auf EU-Ebene. In diesem Kontext erarbeitete sie ein Positionspapier zu den im Kommissionsentwurf für eine Datenschutz-Grundverordnung vorgesehenen Ermächtigungen der Europäischen Kommission, sog. Durchführungsrechtsakte (WP 200 vom 22.01.2013) zu erlassen. Mit Nachdruck spricht sich die Gruppe insbesondere gegen die Befugnis der Europäischen Kommission aus, Durchführungsrechtsakte „über die ordnungsgemäße Anwendung der Verordnung“ zu erlassen. Hierin sieht sie eine unzulässige Beeinträchtigung der Unabhängigkeit der Datenschutzbehörden bei der Auslegung und Anwendung des Datenschutzrechts (vgl. Nr. 1.2).

Die Unterarbeitsgruppe befasste sich zudem intensiv mit dem Thema „One-Stop-Shop“ (vgl. hierzu Nr. 1.2.5) und Kooperation der EU-Datenschutzbehörden in grenzüberschreitenden Fällen und sprach sich unter anderem für eine starke Rolle des EU-Datenschutzausschusses bei der Lösung grenzüberscheitender Datenschutzfälle aus.

Des Weiteren erarbeitete die Unterarbeitsgruppe ein Empfehlungsschreiben („Advice Paper“) zu wesentlichen Elementen einer Regelung der Profilbildung in der Datenschutz-Grundverordnung. Nach Auffassung der Arti-

kel-29-Gruppe sollten Profilbildungen, die die Interessen oder Rechte des Betroffenen erheblich beeinträchtigen, verstärkten Transparenz-, Informations- und Schutzerfordernissen unterliegen.

Eine weitere Stellungnahme für die Artikel-29-Gruppe betrifft das Thema „Risikobasierter Ansatz im Datenschutzrecht". Hierin werden die Grundrechtsqualität und die Geltung der Grundprinzipien des Datenschutzes betont, unabhängig davon, um welche Art und Intensität der Datenverarbeitung es sich handelt, wie zum Beispiel Datenerfassungen im Rahmen von Big-Data-Anwendungen.

Schließlich hat sich die Unterarbeitsgruppe mit der praktischen Umsetzung des Urteils des Europäischen Gerichtshofs vom 13. Mai 2014 in der Rechtssache C-131/12 Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González befasst (vgl. Nr. 2.3.2).

3.1.2 Subgroup Key Provisions

In der Unterarbeitsgruppe wurden im Berichtszeitraum Stellungnahmen der Artikel-29-Gruppe zum Zweckbindungsgrundsatz und zum Begriff des „berechtigten Interesses" im Sinne des Artikels 7 lit. f) der europäischen Datenschutzrichtlinie 95/46/EG erarbeitet.

Die Aufgabe der Unterarbeitsgruppe (Subgroup) Key Provisions besteht in der Auslegung von Kernvorschriften der europäischen Datenschutzrichtlinie 95/46/EG. In der Stellungnahme zur Zweckbindung (WP 203 vom 02.04.2013) erläutert die Artikel-29-Gruppe, unter welchen Bedingungen eine Weiterverarbeitung von Daten für einen anderen als den ursprünglichen Erhebungszweck zulässig ist. Die Stellungnahme formuliert konkrete Kriterien, anhand derer die Prüfung der Rechtmäßigkeit einer Weiterverarbeitung vorzunehmen ist. Die Artikel-29-Gruppe empfiehlt, die Kriterien für rechtmäßige Weiterverarbeitungen innerhalb des künftigen EU-Rechtsrahmens gesetzlich zu regeln.

In der Stellungnahme zum „berechtigten Interesse" (WP 217 vom 09.04.2014) erläutert die Artikel-29-Gruppe die Interessenabwägung nach Artikel 7 lit. f) der Richtlinie anhand praktischer Fallbeispiele. Die Gruppe betont, dass das „berechtigte Interesse" einen eigenständigen Verarbeitungsgrund bildet, der eine umfassende Abwägung der Interessen des Verantwortlichen und des Betroffenen im Einzelfall erfordert. Sie empfiehlt, Kernkriterien dieser Abwägung innerhalb des künftigen EU-Rechtsrahmens zu benennen.

3.1.3 Subgroup International Transfers

Die bestehenden Regelungswerke für den Datenverkehr aus der EU in Staaten ohne angemessenes Datenschutzniveau (Verbindliche Unternehmensregeln, Standardvertragsklauseln) sind durch die Subgroup „International Transfers" weiterentwickelt worden.

International agierende Unternehmen und Marktteilnehmer haben ein nachvollziehbares wirtschaftliches Interesse an einem globalen Datenaustausch über Landesgrenzen und Kontinente hinweg. Entsprechende Rechtsinstrumente müssen allerdings den Datenschutzbedürfnissen der betroffenen Menschen gerecht werden und die Daten der EU-Bürgerinnen und -Bürger angemessen absichern - in einer globalisierten Welt der Datenströme eine große Herausforderung. Eine wesentliche Aufgabe der Subgroup „International Transfers" ist es daher, praxisnahe Auslegungshilfen für die Rechtsinstrumente des internationalen Datenverkehrs bereitzustellen.

Die Subgroup hat im Berichtszeitraum hierzu mehrere Arbeitspapiere für die Artikel-29-Gruppe vorbereitet. Das Dokument „Erläuterndes Dokument über verbindliche Unternehmensregelungen für Auftragsdatenverarbeitung" (WP 204 vom 19.04.2013) enthält Erläuterungen für die „Verbindlichen Unternehmensregeln", die sog. Binding Corporate Rules (BCR, vgl. hierzu Kasten zu Nr. 3.1.3). Der von mir in diesem Zusammenhang im Jahr

2013 ausgerichtete Workshop zu Praxisfragen bei der Prüfung von BCR durch deutsche und europäische Datenschutzaufsichtsbehörden, an dem Vertreter aus 17 EU-Mitgliedstaaten teilgenommen haben, ist auf große Resonanz gestoßen.

Im 24. Tätigkeitsbericht (Nr. 2.4.1.2.) habe ich von den Bemühungen der Subgroup berichtet, gemeinsam mit Vertretern der APEC („Asia-Pacific-Economic Cooperation“) die beiden Regelungssysteme der BCR in der EU und der Cross-Border Privacy Rules (CBPR) zu harmonisieren und, wenn möglich, eine Interoperabilität zwischen BCR und CBPR herzustellen. Angesichts der im Verhandlungsverlauf immer deutlicher zu Tage getretenen strukturellen Unterschiede zwischen den beiden Systemen konnte dieses ambitionierte Ziel vorerst leider nicht erreicht werden. Gleichwohl wurde unter meiner Mitarbeit eine Stellungnahme (WP 212 vom 27.02.2014) erarbeitet, das es den in beiden Wirtschaftsräumen tätigen Unternehmen ermöglicht, den Aufwand für die Zertifizierung durch die zuständigen Behörden unter den jeweiligen Regelungsregimen zu reduzieren. Ich bin zuversichtlich, dass der begonnene Austausch den Grundstein für weitere Annäherungen und Harmonisierungsbemühungen zwischen APEC und EU bilden kann (vgl. auch Nr. 4.7.2).

Im Berichtszeitraum konnte zudem der Prozess zur Implementierung der BCR der Deutschen Telekom AG im Verfahren gegenseitiger Anerkennung unter meiner Federführung erfolgreich abgeschlossen werden. Durch das effiziente Verfahren der gegenseitigen Anerkennung (Mutual Recognition) werden die konzernweit und unabhängig vom Standort der Konzernteile geltenden BCR der Telekom AG nun von allen Datenschutzbehörden der Europäischen Union anerkannt. Ich bedanke mich insbesondere bei meinen Kollegen aus Polen und Österreich als Co-Berichterstatter für die gute Zusammenarbeit während des Anerkennungsverfahrens (vgl. unten Nr. 8.8.9).

Weiter wurde das Arbeitspapier (WP 214 vom 21.03.2014) von der Artikel-29-Gruppe verabschiedet, das sich mit komplexen datenschutzrechtlichen Fragen beim Einsatz von Auftragsdatenverarbeitern als Subunternehmer in Ländern ohne angemessenes Datenschutzniveau befasst. Das Regelungswerk der Standardvertragsklauseln soll in geeigneten Fällen um ein Verfahren für eine gegenseitige Anerkennung ähnlich dem Verfahren bei BCR ergänzt werden. Dies wird künftig zu einer spürbaren Entlastung der Unternehmen, aber auch der zu beteiligenden europäischen Datenschutzaufsichtsbehörden bei der Beurteilung der Standardvertragsklauseln führen.

Des Weiteren habe ich mich auch im Rahmen der Unterarbeitsgruppe in die Diskussion zwischen der Artikel-29-Gruppe und der Welt-Anti-Doping-Agentur (WADA) zu den drängenden Fragen des Schutzes der personenbezogenen Daten von Sportlerinnen und Sportlern eingebracht (vgl. Nr. 19.1).

Kasten zu Nr. 3.1.3

Binding Corporate Rules

Personenbezogene Daten dürfen nur dann in Staaten, die über kein angemessenes Schutzniveau im Sinne von Artikel 25 der Datenschutzrichtlinie 95/46/EG verfügen, übermittelt werden, wenn die eng gefassten Voraussetzungen von Artikel 26 Absatz 1 der Richtlinie erfüllt sind. Diese Einschränkungen werden den Datenübermittlungsbedürfnissen international tätiger Konzerne nicht immer gerecht.

Artikel 26 Absatz 2 der Datenschutzrichtlinie 95/46/EG erlaubt daher Datenübermittlungen in Drittstaaten auch dann, wenn ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten bestehen. Diese Garantien können u. a. auch durch verbindliche Unternehmensregelungen - sog. Binding Corporate Rules (BCR) geschaffen werden.

Diese verbindlichen Regelungen sorgen konzernintern für ein angemessenes Datenschutzniveau durch Aufstellung von Datenschutzprinzipien, deren Einhaltung geschult und überwacht wird, sowie durch interne wie externe Beschwerdemechanismen für die von der Datenverarbeitung betroffenen Personen.

BCR werden durch die zuständige Datenschutzaufsichtsbehörde mit dem Konzern abgestimmt und in einem effizienten Verfahren zur gegenseitigen Anerkennung (Mutual Recognition) mit zwei weiteren europäischen Datenschutzaufsichtsbehörden auf Übereinstimmung mit den rechtlichen Vorgaben überprüft. Nach Abschluss des Verfahrens gelten die BCR in allen 21 EU-Mitgliedstaaten, die am Mutual-Recognition-Verfahren teilnehmen, als anerkannte Basis für die Erlaubnis von Datenübermittlungen auf deren Grundlage.

3.1.4 Technology Subgroup - technologischer Datenschutz auch in Brüssel

Die Unterarbeitsgruppe „Technology" hat im Berichtszeitraum u. a. zu mobilen Anwendungen, zu Anonymisierungstechniken und zum Internet der Dinge Stellung genommen.

Die seit dem Jahr 2010 unter Leitung eines Mitarbeiters meiner Dienststelle tätige Unterarbeitsgruppe „Technology" beschäftigt sich mit den ebenso komplexen wie drängenden Herausforderungen des technologischen Datenschutzes.

Hierzu hat die Unterarbeitsgruppe u. a. folgende Arbeitspapiere verfasst:

Eine Stellungnahme zu mobilen Anwendungen („Apps") auf intelligenten Endgeräten (WP 202 vom 27.02.2013) analysiert den Rechtsrahmen für die Bereitstellung und Nutzung von Apps, insbesondere die Anforderungen an die Einwilligung zur Verarbeitung personenbezogener Daten und die Datenschutzgrundsätze der Zweckbindung und der Datenminimierung. Ein weiteres Kernelement des Papiers sind Empfehlungen an App-Entwickler, App-Stores sowie Hersteller von Betriebssystemen und Endgeräten, beispielsweise für die Umsetzung der technischen und organisatorischen Maßnahmen, um den Schutz personenbezogener Daten zu gewährleisten.

In ihrem Arbeitspapier zu Anonymisierungstechniken (WP 216 vom 10.04.2014) erläutert die Unterarbeitsgruppe die Anforderungen an die Anonymisierung personenbezogener Daten und benennt Kriterien für wirksame Anonymisierungsverfahren. Die Gruppe geht auf die Problematiken der Profilbildung und die Gefahren der Re-Identifizierung von Individuen in anonymisierten Datenbeständen ein. Die Stellungnahme stellt schließlich einmal mehr klar, dass Pseudonymisierung keine Anonymisierungstechnik ist (vgl. dazu Nr. 2.2.3).

Das Dokument zum „Internet der Dinge" (WP 223 vom 16.09.2014, vgl. Nr. 2.2.2) enthält erste Einschätzungen zu der omnipräsenten, oft unsichtbaren Vernetzung virtueller Komponenten und Dienste. Betroffene laufen Gefahr, hierdurch die Kontrolle über ihre Daten zu verlieren. Die Stellungnahme erläutert die Erfordernisse für eine rechtswirksame Einwilligung in eine Datenverarbeitung und spricht eine Reihe von Empfehlungen aus, die sich an die Verantwortlichen für Informationstechnik richten.

Schließlich hat die Unterarbeitsgruppe noch folgende Arbeitspapiere erarbeitet:

- Stellungnahme zu einer Vorlage der Europäischen Kommission für die Datenschutzfolgenabschätzung intelligenter Netze und Messsysteme (WP 205 vom 22.04.2013 und WP 209 vom 04.12.2013, vgl. 24. TB Nr. 10.1),

- Papier zur Einwilligung für die Verwendung von Cookies (WP 208 vom 02.10.2013),

- Stellungnahme zur Meldung von Verletzungen des Schutzes personenbezogener Daten (WP 213 vom 25.03.2014) und

- Bewertung der Anwendbarkeit der Richtlinie 2002/58/EG für das sogenannte Device Fingerprinting (WP 224 vom 25.11.2014), der Wiedererkennung eines Endgerätes anhand seines sogenannten Fingerabdrucks als Alternative zur Verwendung von Cookies.

Ein weiteres Schwerpunktthema war die Bewertung der neuen Google-Datenschutzerklärung (vgl. Nr. 8.9.2).

3.1.5 Aus der Arbeit der BTLE-Subgroup

BTLE steht für Borders, Travel and Law Enforcement. Die Arbeitsgruppe hat sich in den vergangenen zwei Jahren als eine wichtige Untergruppe der Artikel-29-Gruppe etabliert.

Im letzten Tätigkeitsbericht noch als der neue B(ee)TLE vorgestellt (24. TB Nr. 2.4.1.4), hat sich die von einem Mitarbeiter meiner Dienststelle gemeinsam mit einem niederländischen Kollegen koordinierte BTLE-Subgroup fest in der Artikel-29-Gruppe etabliert. Sie bereitet im Wesentlichen alle datenschutzrechtlichen Themen aus den Bereichen der Grenz- und Migrationskontrolle sowie der polizeilichen und justiziellen Zusammenarbeit in Strafsachen vor. Darüber hinaus befasst sich die Arbeitsgruppe mit dem Datenschutz im gesamten Reiseverkehr.

Einen Schwerpunkt bildeten in den vergangenen zwei Jahren die Folgen der Enthüllungen von Edward Snowden, zu denen eine Stellungnahme und ein darauf aufbauendes Arbeitsdokument erarbeitet worden sind (Stellungnahme 4/2014 vom 10.04.2014, WP 228 vom 05.12.2014). Weitere Arbeitsschwerpunkte waren das sogenannte Smart-Borders-Programm (vgl. unter Nr. 3.4), das Rahmenabkommen zwischen der EU und den USA (vgl. Nr. 3.5), die Folgen der EuGH-Entscheidungen zur Vorratsdatenspeicherung von Telekommunikationsdaten (vgl. Nr. 2.3.1), die Richtlinie über den Datenschutz im Bereich von Polizei und Justiz (vgl. Nr. 1.3) sowie die Übermittlungen von Fluggastdaten (vgl. Nr. 4.7.3) und Finanztransaktionsdaten an ausländische Sicherheitsbehörden. Aus der BTLE-Subgroup hat die Artikel-29-Gruppe auch die Datenschutzexperten entsandt, die für die Europäische Kommission an den sog. gemeinsamen Überprüfungen („Joint Reviews“) der PNR- und TFTP-Abkommen in den USA bzw. Australien teilgenommen haben, in zwei Fällen auch unter Beteiligung eines Mitarbeiters meiner Dienststelle.

3.1.6 E-Government-Subgroup

Die Unterarbeitsgruppe E-Government & Biometrics setzte im Berichtszeitraum ihre Arbeit als E-Government-Subgroup unter neuem Namen fort.

Die Unterarbeitsgruppe E-Government-Subgroup befasst sich grundsätzlich mit datenschutzrechtlichen Fragestellungen, die öffentliche Stellen als Datenverarbeiter betreffen.

Als wichtigste Punkte, mit denen sich die Unterarbeitsgruppe in den Jahren 2013 und 2014 befasst hat, können genannt werden:

- Entwurf der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (vgl. auch Nr. 8.3):

  In einem von der Unterarbeitsgruppe entworfenen Brief machte die Artikel-29-Gruppe die Kommission auf einige im Verordnungsentwurf enthaltene datenschutzrechtliche Probleme aufmerksam, z. B. auf die Frage, was eine „eineindeutige“ Identifizierung oder Identität ist („unambiguous identity“) und ob eine solche in jedem Fall benötigt wird. Die meisten der aufgezeigten Probleme wurden in der im September 2014 veröffentlichten Verordnung berücksichtigt. Für die Zukunft will die Artikel-29-Gruppe die Kommission bei der

Erarbeitung der Implementierungs- und Durchführungsrechtsakte aufgrund der Verordnung weiter unterstützen.

- Umfrage unter den Mitgliedern der Artikel-29-Gruppe zu den Anforderungen an Datensicherheit bei der elektronischen Kommunikation mit der öffentlichen Verwaltung, insbesondere auch bei der elektronischen Identifizierung:

  Trotz der geringen Resonanz in den Mitgliedstaaten konnte die Unterarbeitsgruppe als Ergebnis der von ihr durchgeführten Umfrage festhalten, dass die Voraussetzungen und Anforderungen in den Mitgliedstaaten sehr unterschiedlich sind. Weil sich die Unterarbeitsgruppe deswegen kaum auf gemeinsame Grundsätze würde einigen können, hat sie das Mandat nicht weiter verfolgt.

- Stellungnahme zum Entwurf zur Überarbeitung der PSI (public sector information)- bzw. Open-Data-Richtlinie aus dem Jahr 2003 (Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors; mittlerweile veröffentlicht im Amtsblatt vom 27.06.2013, L 175/1):

  Im Dezember 2011 hatte die Kommission den Entwurf zur Überarbeitung der o. g. Richtlinie veröffentlicht. Darin wird der Grundsatz aufgestellt, dass Informationen, die bei öffentlichen Stellen rechtmäßig vorhanden sind, sowohl für kommerzielle als auch für nicht kommerzielle Zwecke weiterverwendbar sind. Ausnahmen von diesem Grundsatz können u. a. aus Datenschutzgründen gemacht werden. Die hierzu im Juni 2013 veröffentlichte Stellungnahme (WP 207, Opinion 6/2013 vom 5. Juni 2013) empfiehlt u. a. „mit Nachdruck, dass von der öffentlichen Stelle eine gründliche Datenschutzfolgenabschätzung durchgeführt wird, bevor sie personenbezogene Daten zu Zwecken der Weiterverwendung bereitstellt“ (Kap. 4.2).

- Diskussion mit der Kommission über Datenschutzprüfungen bei EU-Forschungsprojekten und sog. ethical guidelines, insbesondere im Zusammenhang mit dem EU-Rahmenprogramm HORIZON 2020 für Forschung und Innovation.

3.2 International Working Group on Data Protection in Telecommunications

Die International Working Group on Data Protection in Telecommunications (IWGDPT) beschäftigt sich mit Themen im Bereich der Telekommunikation und seit Anfang der 1990er Jahre vor allem mit Fragen des Datenschutzes im Internet. Hierzu hat sie zahlreiche Arbeitspapiere und Empfehlungen erarbeitet und veröffentlicht, die weltweit Beachtung finden.

Die IWGDPT, auch bekannt als „Berlin Group“, wurde im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten im Jahr 1983 auf Initiative des Berliner Datenschutzbeauftragten gegründet, unter dessen Vorsitz sie nach wie vor arbeitet. Teilnehmer sind Datenschutzbehörden, aber auch Regierungsstellen, Vertreter internationaler Organisationen und Wissenschaftler aus aller Welt.

Im Berichtszeitraum hat sie folgende Papiere veröffentlicht, die auf meiner Internetseite unter www.datenschutz.bund.de verfügbar sind:

- Arbeitspapier zu Big Data und Datenschutz: Bedrohung der Grundsätze des Datenschutzes in Zeiten von Big-Data-Analysen (Skopje, 5./6. Mai 2014)

- Arbeitspapier zum Datenschutz bei Überwachung aus der Luft (Berlin, 2./3. September 2013)

- Arbeitspapier zum Recht auf vertrauliche Telekommunikation (Berlin, 2./3. September 2013)

- Arbeitspapier und Empfehlungen zu der Veröffentlichung personenbezogener Daten im Web, der Indexierung des Inhalts von Websites und dem Schutz der Privatsphäre (Prag, 15./16. April 2013)

- Arbeitspapier zu Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar (Prag, 15./16. April 2013)

Die IWGDPT tagt zwei Mal im Jahr, im Herbst in Berlin und im Frühjahr auf Einladung einer teilnehmenden Behörde/Stelle in deren Heimatland.

3.3 „Smart Borders" vor dem Intelligenztest

Die Zweifel am milliardenschweren Projekt namens „smart borders" bestehen weiter. Nun sollen eine Studie und ein Pilotprojekt weitere Aufklärung bringen. Ich halte Vorsicht für geboten.

Hinter dem Schlagwort „smart borders" steht ein umfangreiches Gesetzespaket. Dies sieht in erster Linie vor, die Ein- und Ausreise aller Nicht-EU-Bürger in das EU-Gebiet elektronisch zu erfassen. Darüber hinaus soll die Einreise für Drittstaatsangehörige erleichtert werden, wenn sie sich zuvor haben überprüfen und registrieren lassen. Ob dieses Vorhaben tatsächlich so intelligent ist, wie der Titel suggeriert, habe ich schon im letzten Tätigkeitsbericht erheblich in Zweifel gezogen (24. TB Nr. 2.5.3.4). Diese beziehen sich sowohl auf die praktische Durchführbarkeit als auch auf die rechtlichen Anforderungen der Erforderlichkeit und der Verhältnismäßigkeit des Kernstücks des Programms, der Einrichtung eines so genannten Einreise- und Ausreiseregisters („Entry-Exit-System"). Im Berichtszeitraum hat auch die Artikel-29-Gruppe das Vorhaben umfassend und grundlegend in einer Stellungnahme kritisiert (5/2013 vom 06.06.2013). Die Kritik der Artikel-29-Gruppe deckt sich im Wesentlichen mit meinen Kritikpunkten. Sie wurde auch dem Innenausschuss des Europäischen Parlaments in einer Anhörung vorgetragen.

Was hat sich seit der Vorlage des Gesetzespakets getan? Viele Abgeordnete des Europäischen Parlaments haben über die Parteigrenzen hinweg Zweifel an dem Vorhaben geäußert. Dabei ging es einerseits um datenschutzrechtliche Bedenken. Andererseits fragten sich viele Abgeordnete, wie sie es politisch verantworten könnten, in wirtschaftlichen Krisenzeiten ein milliardenschweres Konzept zu befürworten, dessen Nutzen auch ihnen unklar blieb. Im Ergebnis hat man sich darauf geeinigt, zunächst eine Studie und dann ein Pilotprojekt durchzuführen, bevor eine politische Entscheidung über „smart borders" getroffen werden soll. Dabei gebe ich zwei weitere Punkte zu bedenken: Zum einen handelt es sich um ganz erhebliche Investitionssummen und damit verbundene ökonomische Interessen, die auf dem Spiel stehen. Zum anderen legen die Regierungen der Mitgliedsstaaten, anders als die Europäische Kommission, besonderen Wert darauf, biometrische Daten zu erfassen und die neu zu schaffenden Datenbanken für die Polizeien (umfangreich) nutzbar zu machen. Diese Zuspitzung durch den Rat der Europäischen Union ruft starke Bedenken hervor, weil sie den Verdacht nährt, die Polizeien sollten routinemäßig und anlasslos weiteren Zugang zu Datenbanken erhalten, die rein administrativen Zwecken dienen. In diesem Sinne hat sich auch die Artikel-29-Gruppe kritisch in einem Schreiben an Rat, Kommission und Europäisches Parlament geäußert. Es bleibt abzuwarten, wie der beschriebene Prozess von Studie und Pilotprojekt das politische Verfahren beeinflussen wird.

3.4 Wieviel Schutz kann das „umbrella agreement" bringen?

Das geplante Abkommen zwischen der EU und den USA kann ein erster wichtiger Schritt zu einem erhöhten Datenschutzniveau im transatlantischen Datenverkehr zwischen Sicherheitsbehörden sein.

Die Kritik am Umgang von US-Sicherheitsbehörden mit den Daten von (EU-) Bürgerinnen und Bürgern ist schon seit vielen Jahren ein Dauerbrenner der datenschutzrechtlichen Diskussion. Man denke nur an die Abkommen mit den USA über die Übermittlung von Fluggastdaten (23. TB Nr. 13.9) und Finanztransaktionsdaten

(SWIFT bzw. TFTP - 23. TB Nr. 13.6) und die damit verbundenen Diskussionen über die verschiedenen Datenschutzkulturen in den USA und in Europa. Ich halte es für richtig, in einem neuen Rahmenabkommen zwischen den USA und der EU („umbrella agreement“) datenschutzrechtliche Standards festzulegen, die von den jeweiligen Sicherheitsbehörden bei der Übermittlung und Verarbeitung von Daten im transatlantischen Datenverkehr einzuhalten sind. Schon in meinem 23. Tätigkeitsbericht finden sich wesentliche Aussagen zu den Voraussetzungen, die vorliegen müssen, um das Abkommen zu einem Erfolg zu machen. Sie betreffen die Begrenzung überlanger Speicherfristen, unabhängige Datenschutzkontrollinstanzen und die gerichtliche Durchsetzbarkeit von Datenschutzrechten europäischer Bürgerinnen und Bürger (vgl. 23. TB Nr. 13.8). Nachdem die Verhandlungen über das Abkommen jahrelang sehr zäh verliefen, haben sie im letzten Jahr nach Aussagen der Europäischen Kommission deutlich Fahrt aufgenommen. Es wurde in Fachkreisen aufgehorcht, als die damaligen US-Justizminister Holder und die zuständige EU-Kommissarin Malmström im Juni 2014 verkündeten, die Verhandlungen seien weit vorangeschritten. Besondere Beachtung verdiente dabei die Äußerung des US-Justizministers, dass sich die US-Regierung dafür einsetzen werde, den Rechtsschutz von europäischen Bürgerinnen und Bürgern in den USA zu verbessern. Dies ist in der Tat ein zentraler Punkt. Denn ohne mehr Rechtsschutz und Rechtssicherheit halte ich die Frage nach dem Sinn des Abkommens für berechtigt. Ich begrüße es, dass auch die Europäische Kommission und der Rat diesem Punkt höchste Priorität einräumen. Gleichzeitig zeigt die gewählte Formulierung des US-Justizministers auch Grenzen auf: Sie lässt offen, wofür genau die US-Regierung sich einsetzen will, und sie macht deutlich, dass sie die notwendigen Standards nicht ohne den Kongress schaffen kann. Zugleich halte ich es für wichtig, die Erwartungen an ein solches Abkommen nicht zu überhöhen. Seine Grenzen findet es in seinem Anwendungsbereich, der nur Daten erfasst, die übermittelt werden. Nicht erfasst würden somit sonstige Daten, die die US-Sicherheitsbehörden unabhängig von einer Übermittlung aus der EU in den USA verarbeiten. Meine Einschätzung im 23. Tätigkeitsbericht, dass es nach schwierigen und langwierigen Verhandlungen aussehe, hat sich bestätigt. Noch steht ein erfolgreicher Abschluss aus. Das Abkommen wäre zwar nur ein erster Schritt, aber doch ein wichtiger, wenn die Standards angemessen hoch sind und verbindliche und einklagbare Rechte festgeschrieben werden.

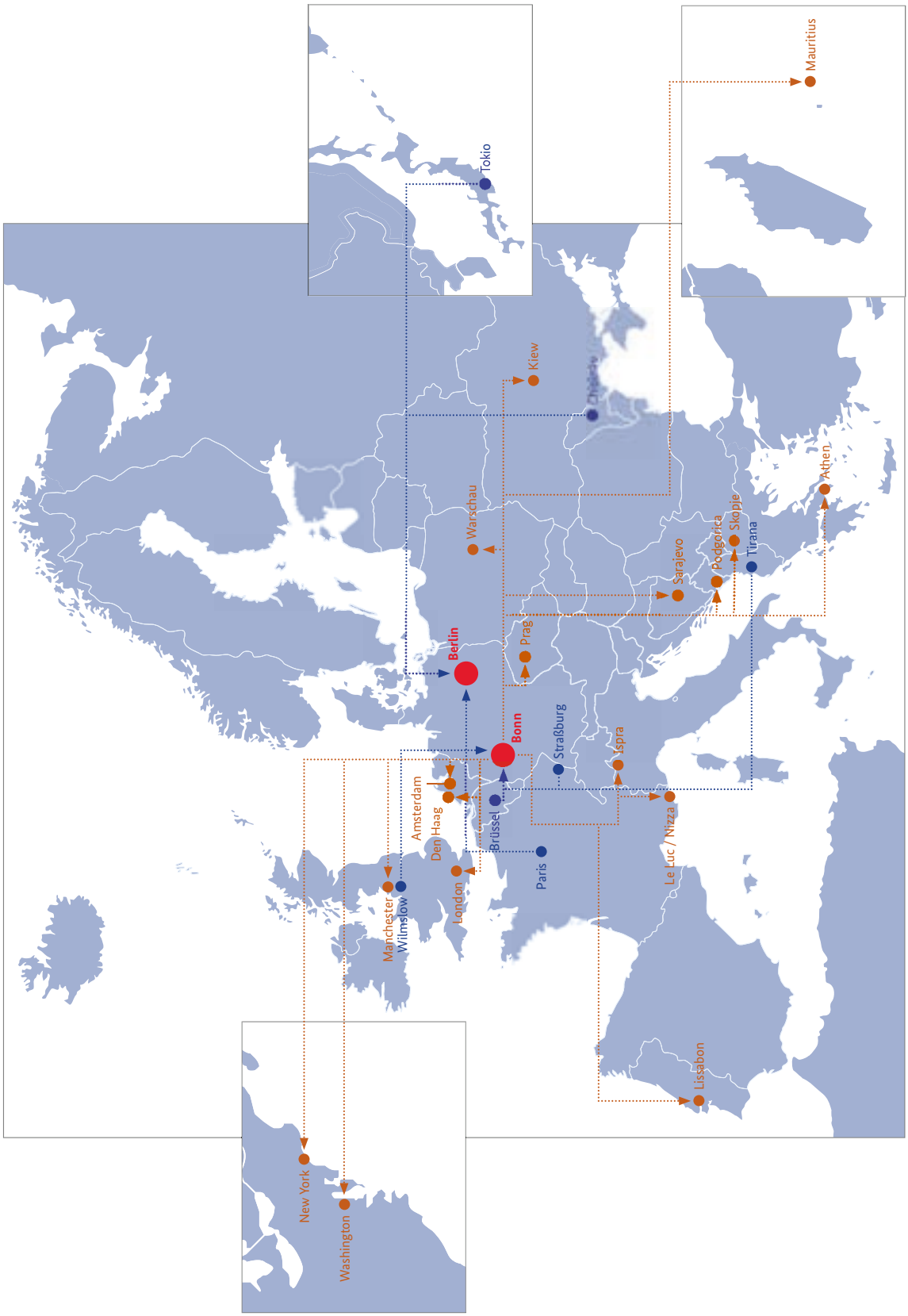
A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit
- Arbeitskreis Europa

Europäische Datenschutzkonferenz
Artikel-29-Datenschutzgruppe mit
- Subgroup Financial Matters,
- Subgroup Biometrics & eGovernment,
- Health Data Subgroup,
- BTLE Subgroup,
- Technology Subgroup,
- Future of Privacy Subgroup,
- Key Provisions Subgroup,
- Subgroup International Transfers,
- WADA-Subgroup

Case Handling Workshop
Internationale Datenschutzkonferenz mit
- International Working Group Enforcement Coordination,
- International Working Group on Data Protection in Telecommunications (IWGDPT bzw. „Berlin Group“)

Zusammenarbeit mit internationalen und europäischen Datenschutzbehörden



4 Auswärtiger Ausschuss / Ausschuss für Angelegenheiten der Europäischen Union / Ausschuss für Menschenrechte und humanitäre Hilfe

4.1 Datenschutz international - Artikel 17 IPBPR

Der fortschreitenden Globalisierung der Datenströme kann nicht allein mit nationalen oder europarechtlichen Initiativen begegnet werden. Deswegen habe ich mich für die Stärkung des Rechts auf Privatsphäre auch auf völkerrechtlicher Ebene eingesetzt.

Die im Jahr 2013 durch Edward Snowden aufgedeckten geheimdienstlichen Überwachungsaktivitäten und die rasante Vervielfältigung der weltweit verfügbaren Daten machen deutlich, dass nationale oder regionale Ansätze zum Schutz dieser Daten in ihrer Wirkung begrenzt sind.

Daher habe ich die Ankündigungen im Acht-Punkte-Programm der Bundesregierung begrüßt, sich zum besseren Schutz der Privatsphäre auf internationaler Ebene für ein Zusatzprotokoll zu Artikel 17 des Internationalen Paktes über Bürgerliche und Politische Rechte der Vereinten Nationen (IPBPR) einsetzen zu wollen.

Bedauerlicherweise fand die Initiative der Bundesregierung für die Einberufung einer IPBPR-Vertragsstaatenkonferenz nur wenige Unterstützer. Seitens der Bundesregierung (AA) wurde ich zudem auf die Gefahr hingewiesen, dass Initiativen zur Verbesserung des Datenschutzes auf UN-Ebene verwässert werden könnten, was im Ergebnis zu einer Schwächung führen würde.

Weitaus erfolgreicher war die deutsch-brasilianische Initiative für eine Resolution (A/C.3/68/L.45) der Generalversammlung der Vereinten Nationen, die den Schutz der Privatsphäre betont und u. a. die Hohe Kommissarin der Vereinten Nationen für Menschenrechte beauftragt, einen Bericht über den Schutz der Privatsphäre im Kontext der Überwachungsmaßnahmen vorzulegen (vgl. Nr. 4.3). Die Hochkommissarin verweist in dem im Juni 2014 vorgelegten Bericht (A/HRC/27/37.) auf die bestehenden völkerrechtlichen Regelungen wie Artikel 17 IPBPR, stellt aber einen Mangel an Umsetzung der Vorgaben in nationale Regelungen sowie eine unzureichende Aufsicht fest. Sie empfiehlt den Staaten eine Prüfung ihrer nationalen Regelungen auf Übereinstimmung mit dem internationalen Menschrecht und regt einen Dialog aller betroffenen Interessenvertreter an.

Die 36. Internationale Datenschutzkonferenz, die vom 13. bis 16. Oktober 2014 in Mauritius stattfand, hat dieses Angebot für einen multilateralen Dialog zu Fragen des Datenschutzes im Lichte der modernen Kommunikationstechnologie mit einer von mir unterstützten Entschließung aufgegriffen (in Englisch abrufbar auf meiner Website www.datenschutz.bund.de und unter www.privacyconference2014.org). Bereits die 35. Internationale Datenschutzkonferenz hatte sich im September 2013 in Warschau für ein Zusatzprotokoll zu Artikel 17 IPBPR ausgesprochen, dessen Grundlage die von der Internationalen Datenschutzkonferenz im Jahr 2009 verabschiedeten internationalen Standards zum Schutz von personenbezogenen Daten und der Privatsphäre (Erklärung von Madrid) sein soll (vgl. Nr. 4.3, abrufbar über meinen Internetauftritt unter www.datenschutz.bund.de).

Es ist ein gutes Signal, dass die Bundesregierung ihre Bemühungen für einen besseren Schutz der Privatsphäre auf internationaler Ebene fortsetzt. Beleg hierfür ist die Resolution A/C.3/69/L.26, die Ende 2014 erneut zusammen mit Brasilien in die Generalversammlung eingebracht wurde und auf der Website der Vereinten Nationen www.un.org. abrufbar ist.

Der Vorstoß der deutsch-brasilianischen Initiative, einen Sonderberichterstatter für die Debatte um das Recht auf Privatheit im digitalen Zeitalter einzusetzen, findet meine volle Unterstützung.

4.2 Europäische Datenschutzkonferenz

Die jährliche Frühjahrskonferenz („Spring Conference") der europäischen Datenschutzbeauftragten befasste sich in den Jahren 2013 und 2014 vor allem mit der Zukunft des Datenschutzes in Europa.

Die europäische Datenschutzkonferenz, an der Datenschutzbehörden aus Europa sowie Vertreter der Europäischen Kommission, des Europarats und der OECD teilnehmen, findet traditionell in den Monaten April oder Mai eines Jahres statt und wird daher auch „Frühjahrskonferenz" genannt - im Gegensatz zur regelmäßig im Herbst stattfindenden Internationalen Datenschutzkonferenz (vgl. oben Nr. 4.3). Das Forum dient dem Gedanken- und Erfahrungsaustausch aller europäischen Datenschutzbeauftragten und ist daher weiter gefasst als die Datenschutzgremien der Europäischen Union; es schließt insbesondere die Datenschutzbeauftragten aus den Ländern Südosteuropas mit ein.

Zur Frühjahrskonferenz des Jahres 2013 hatte die portugiesische Datenschutzbehörde vom 16. bis 17. Mai nach Lissabon eingeladen. Die Konferenz diskutierte die Zukunft des Datenschutzes in Europa und verabschiedete hierzu eine Entschließung. Darin betonen die europäischen Datenschutzbeauftragten, die derzeit parallel stattfindenden Datenschutz-Revisionen - einerseits die Reform des Datenschutzrechtsrahmens der EU und andererseits die Modernisierung der Datenschutzkonvention des Europarates - müssten im Gleichklang erfolgen, um spätere Wertungswidersprüche zu vermeiden. Zudem befasste sich die Konferenz in weiteren Entschließungen mit der Sicherstellung eines angemessenen Datenschutzes bei Europol sowie mit der aus Sicht der Konferenz unerlässlichen Gewährleistung des Datenschutzes in einer transatlantischen Freihandelszone (TTIP vgl. Nr. 8.7).

Am 5. Juni 2014 luden der Europarat und die französische Datenschutzbehörde (CNIL) gemeinsam zur Frühjahrskonferenz nach Straßburg ein. Zentrales Thema war die Verbesserung der europaweiten Zusammenarbeit der Datenschutzaufsichtsbehörden, insbesondere im Hinblick auf multinationale oder global tätige Unternehmen. Die Konferenz hat zu diesem Zweck eine Arbeitsgruppe eingesetzt, die bis zur nächsten Frühjahrskonferenz Vorschläge ausarbeiten soll. Ich unterstütze deren Tätigkeit, weil ich die Zusammenarbeit der Aufsichtsbehörden, um die jeweiligen Aufgaben effektiv wahrnehmen zu können, als essentiell erachte (vgl. Nr. 4.4). Darüber hinaus hat die Konferenz der europäischen Datenschutzbeauftragten eine Entschließung zur Modernisierung der Datenschutzkonvention des Europarates beschlossen, in der die Mitgliedstaaten des Europarates u. a. aufgefordert werden, an einem hohen Datenschutzniveau auch dann festzuhalten, wenn andere Staaten von außerhalb des Europarates der Konvention beizutreten beabsichtigen.

Die Entschließungstexte der Frühjahrskonferenzen 2013 und 2014 sind auf meiner Internetseite abrufbar unter www.datenschutz.bund.de.

Die nächste Frühjahrskonferenz wird auf Einladung der britischen Datenschutzbehörde im Mai 2015 in Manchester stattfinden.

4.3 Internationale Konferenz der Datenschutzbeauftragten

Die Internationale Datenschutzkonferenz befasste sich mit wichtigen Zukunftsthemen und nahm Initiativen zur Verbesserung der globalen Zusammenarbeit an.

Nach zwei Veranstaltungen in Lateinamerika in den Jahren 2011 (Mexiko) und 2012 (Uruguay) kehrte die Internationale Datenschutzkonferenz nach Europa zurück. Die 35. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre wurde auf Einladung des polnischen Datenschutzbeauftragten vom 23. bis 26. September 2013 in Warschau ausgerichtet. Unter dem Titel „A Privacy Compass in a Turbulent World" machte es sich die Konferenz zur Aufgabe, den Nutzern und allen betroffenen Menschen Orientierung zu geben in einer unübersichtlichen Welt immer neuer und datenintensivere Anwendungen und Dienstleistungen.

Im Rahmen ihrer „closed session“, die den Datenschutzbeauftragten selbst und ihren Vertretern vorbehalten ist, beschäftigte sich die Konferenz mit dem Phänomen der „App-ification“ der Gesellschaft. Gemeint ist damit, dass für immer neue Zwecke und Lebenslagen kleine Anwenderprogramme (Applikationen oder „Apps“) insbesondere für mobile Kommunikationsgeräte (sog. Smartphones und Tablets), entwickelt und interessierten Kunden oftmals entgeltfrei zur Nutzung angeboten werden. Dafür muss der Kunde in der Regel allerdings einwilligen, der Applikation Zugriff auf die Daten seines mobilen Endgerätes zu gewähren, was häufig die Standortdaten des Nutzers einschließt und somit das Anfertigen von Bewegungsprofilen ermöglicht. Daher forderte die 35. Internationale Datenschutzkonferenz in ihrer „Warschauer Erklärung zur App-ifizierung der Gesellschaft“, dass auch für diese innovativen Anwenderprogramme die Grundsätze des Datenschutzes, wie Zweckbindung, Erforderlichkeit oder Datensparsamkeit, gelten müssen; zudem müsse für die Nutzer hinreichende Transparenz bei der Erhebung und Verarbeitung ihrer personenbezogenen Daten gewährleistet sein.

Als weitere Orientierungshilfen verabschiedete die Konferenz Entschließungen zu den Themen „Profiling“, „Web-Tracking“ und „Digital Education“ (Alle Entschließungen sind auf meiner Internetseite unter www.datenschutz.bund.de abrufbar).

Darüber hinaus hat die 35. Internationale Konferenz auf Initiative meines Hauses - mit der Unterstützung von Datenschutzbehörden aus Europa, Asien und Amerika - eine Resolution zur Verankerung des Datenschutzes im internationalen Recht beschlossen und die Regierungen weltweit aufgefordert, in Verhandlungen für ein verbindliches internationales Datenschutzabkommen einzutreten. Die Resolution schlägt vor, zu diesem Zweck an Artikel 17 des Internationalen Paktes über Bürgerliche und Politische Rechte der Vereinten Nationen, der u. a. den Schutz des Heims und der Privatsphäre zum Inhalt hat, sowie an die von der Internationalen Datenschutzkonferenz bereits 2009 beschlossenen „Internationalen Standards“ für den Schutz personenbezogener Daten und der Privatsphäre anzuknüpfen. (vgl. auch Nr. 4.1).

Erstmals tagte die Internationale Konferenz anlässlich ihrer 36. Zusammenkunft in der Region Afrika, die auf Einladung der Datenschutzbehörde der Republik Mauritius vom 13. bis 16. Oktober 2014 stattfand.

Als Schwerpunktthema der „closed session“ wurde das „Internet der Dinge“ behandelt (vgl. hierzu auch Nr. 2.2). Durch die fortschreitende Miniaturisierung der Technik ist es möglich geworden, Sensoren, die ständig Daten erfassen können, in immer kleineren Geräten einzusetzen. Beispielhaft genannt seien Fitness-Armbänder, die permanent Schrittfrequenz und Herzschlag des Nutzers aufzuzeichnen und an ein mobiles Kommunikationsendgerät wie ein Smartphone oder ein Tablet übertragen, damit diese Daten dort in einer Gesundheits-App weiter verarbeitet werden. Durch diese ubiquitäre Entstehung und Speicherung personenbezogener Daten werden - insbesondere unter Nutzung der fortgeschrittenen Analysetechniken von „Big Data“ - äußerst detaillierte individuelle Nutzerprofile möglich, die sehr viele und sensible Informationen über den Betroffenen preisgeben können. Daher fordert die „Mauritius Declaration on the Internet of Things“, dass der Schutz der nutzerbezogenen Daten gestärkt werden muss, z. B. durch Nutzung anonymisierter Daten. Insbesondere die Verwendung einmal erhobener Daten zu anderen Zwecken oder die Weiterübermittlung an Dritte („out-of-context-use“) muss streng reglementiert werden. Darüber hinaus sollte spätestens beim Kauf eines Gerätes, das das Internet der Dinge nutzt, der Kunde hinreichend über die vorgesehene Datenverarbeitung informiert werden.

Im Zusammenhang mit dieser Problematik ist auch die Entschließung zu „Big Data“ zu sehen, die ich wie die Resolution zum Schutz der Privatsphäre im digitalen Zeitalter als so genannter Co-Sponsor mitgetragen habe. Letztere nimmt Bezug auf die Resolution der Generalversammlung der Vereinten Nationen vom Dezember 2013 zum gleichen Thema, die vor dem Hintergrund der im Sommer 2013 bekannt gewordenen Massenüberwachungsprogramme einiger Staaten auf Vorschlag Deutschlands und Brasiliens angenommen worden war (vgl. Nr. 4.1).

Darüber hinaus hat die Internationale Konferenz eine Entschließung zur Verstärkung der grenzüberschreitenden Zusammenarbeit der Datenschutzaufsichtsbehörden und ein damit verbundenes „Cooperation Arrangement“ ge-

billigt (Alle Entschließungen sind in Englisch unter www.privacyconference2014.org und auf meiner Internetseite www.datenschutz-bund.de abrufbar).

Die 37. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre wird vom 26. bis 29. Oktober 2015 in Amsterdam stattfinden.

4.4 Verbesserte Zusammenarbeit der europäischen Datenschutzbehörden

Bewährte Instrumente und neue Initiativen haben die Zusammenarbeit der Datenschutzbehörden in Europa gestärkt und vertieft.

Spring Conference Working Group on European Cooperation

Die Konferenz der europäischen Datenschutzbeauftragten hat im Frühjahr 2014 (vgl. auch Nr. 4.2) eine neue Arbeitsgruppe ins Leben gerufen, die sich der Verbesserung der Zusammenarbeit der europäischen Aufsichtsbehörden über den Kreis der EU-Mitgliedstaaten hinaus widmen soll. Den gemeinsamen Vorsitz der Arbeitsgruppe haben die französische Datenschutzbehörde CNIL und der beratende Datenschutzausschuss des Europarates übernommen. Die Ergebnisse der Arbeitsgruppe sollen im Rahmen der Frühjahrskonferenz 2015 vorgestellt werden. Da ich die grenzüberschreitende Zusammenarbeit der Datenschutzbehörden als unerlässlich für eine wirksame Aufsicht erachte, unterstütze ich die Einsetzung der Arbeitsgruppe und beteilige mich an deren Tätigkeit.

Case Handling Workshops

Wie in den Vorjahren fanden auch im Berichtszeitraum zwei unter dem Dach der Europäischen Datenschutzkonferenz organisierte „Case Handling Workshops“ statt - im Oktober 2013 in Sarajevo, Bosnien-Herzegowina, und im Oktober 2014 in Skopje, ehemalige jugoslawische Republik Mazedonien. Das Format dieser Veranstaltung hat sich für den Austausch von Erfahrungen und Kenntnissen zwischen den europäischen Datenschutzbehörden gut bewährt. Auf diese Weise sollen Kohärenz und Homogenität ihres Handelns gefördert werden mit dem Ziel, dass sie bei ähnlich gelagerten datenschutzrechtlichen Problemen zu vergleichbaren Ergebnissen gelangen. Vor allem die Mitarbeiter noch junger Datenschutzbehörden können von diesem Erfahrungsaustausch profitieren und die konkreten Probleme und Fragestellungen der täglichen Praxis kennen lernen. Der Erfahrungsaustausch und die Unterstützung der anderen Datenschutzbehörden in Europa liegen mir sehr am Herzen, weshalb ich das Modell der „Case Handling Workshops“ unterstütze.

Europäische Verwaltungshilfe

Das Instrument der technischen Verwaltungshilfe („Technical Assistance and Information Exchange“ - TAIEX) der Europäischen Kommission hat sich als erfolgreich erwiesen, um Datenschutzbehörden in den Kandidatenländern zum EU-Beitritt im Einzelfall auf deren Bedürfnisse hin „maßgeschneiderte“ Hilfe und Unterstützung zukommen zu lassen. Im Berichtszeitraum habe ich - wie in den Vorjahren - verschiedene Datenschutzbehörden vor allem in Südosteuropa unterstützt. So war ich an Expertenmissionen in Montenegro und in der Republik Mazedonien beteiligt und habe Delegationen der Datenschutzbehörden aus der Republik Moldau und aus Albanien in meiner Dienststelle empfangen.

Zudem habe ich die Dienststelle der Ombudsfrau für Menschenrechte des ukrainischen Parlaments, die zu Beginn des Jahres 2013 die Funktion einer datenschutzrechtlichen Aufsichtsbehörde in der Ukraine übernommen hat, beraten. Ich danke dem Institut für rechtliche Zusammenarbeit (IRZ) in Bonn für die gute Zusammenarbeit im Rahmen dieses Kontaktes.

Neuer Europäischer Datenschutzbeauftragter

Herr Peter Hustinx, der erste Europäische Datenschutzbeauftragte (European Data Protection Supervisor - EDPS), ist Ende 2014 aus seinem Amt ausgeschieden, nachdem das Mandat bereits im Januar 2014 abgelaufen war und er das Amt bis zur Ernennung eines Nachfolgers weiterhin übergangsweise ausgeübt hat. Ich danke Herrn Hustinx für seinen unermüdlichen Einsatz für die Stärkung des Datenschutzes als unveräußerliches Grundrecht in Europa und in aller Welt. Gleichzeitig gratuliere ich Herrn Giovanni Buttarelli**,** dem bisherigen stellvertretenden EDPS, zu seiner Ernennung zum neuen Europäischen Datenschutzbeauftragten. Ich freue mich auf eine auch künftig gute und vertrauensvolle Zusammenarbeit.

4.5 OECD: Arbeitsgruppe für Sicherheit und Privatsphäre in der digitalen Wirtschaft

Die OECD hat - nach intensiven Vorarbeiten der Arbeitsgruppe für Sicherheit und Privatsphäre in der digitalen Wirtschaft - im Sommer 2013 die neu gefassten Richtlinien zum Schutz der Privatsphäre verabschiedet. Derzeit befasst sich die Arbeitsgruppe mit der Aktualisierung der Richtlinien zur Datensicherheit.

Im Berichtszeitraum beschäftigte sich die Arbeitsgruppe zu Internet, Sicherheit und Privatsphäre (Working Party Internet Security and Privacy - WP ISP) der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Cooperation and Development - OECD) mit der Vollendung der Richtlinien zu Datenschutz und zum Schutz der Privatsphäre (OECD Privacy Guidelines; vgl. auch 24. TB Nr. 2.4.5). Nach intensiven Diskussionen innerhalb einer Expertengruppe, an deren Arbeiten ich mich beteiligt habe, wurde entschieden, an den acht bestehenden datenschutzrechtlichen Grundprinzipien, z. B. Transparenz und Zweckbindung bei der Datenverarbeitung, festzuhalten. Neu hingegen sind „Privacy Management"-Programme, mit denen Unternehmen ihren Kunden und Behörden die für den Schutz der Privatsphäre relevanten Informationen zur Verfügung stellen müssen. Auch wurde eine Meldepflicht bei Verletzungen der Datensicherheit oder des Datenschutzes („Data Breach Notification") aufgenommen. Darüber hinaus betonen die neu gefassten Richtlinien die hohe Bedeutung der internationalen Zusammenarbeit angesichts immer größerer globaler Datenströme.

Zu Beginn des Jahres 2014 gab sich die Arbeitsgruppe einen neuen Namen und heißt nun „Working Party on Security and Privacy in the Digital Economy" (WP SPDE - Arbeitsgruppe für Sicherheit und Privatsphäre in der digitalen Wirtschaft). Gemäß dem Auftrag, der in der neuen Bezeichnung zum Ausdruck kommt, beschäftigt sich die Arbeitsgruppe nicht nur mit dem Schutz der Privatsphäre, sondern auch mit der Gewährleistung der Sicherheit dieser Daten. Dementsprechend werden derzeit die aus dem Jahr 2002 stammenden Richtlinien der OECD zur Datensicherheit einer Modernisierung unterzogen. Dabei sollen sowohl die gewachsene Bedeutung des Internets für Wirtschaft und Gesellschaft in den Mitgliedstaaten der OECD als auch neue technologische Entwicklungen, wie z. B. Cloud Computing oder das Internet der Dinge („Internet of Things"), berücksichtigt werden. Die Verabschiedung der aktualisierten Richtlinien zur Datensicherheit ist bis Ende des Jahres 2015 vorgesehen.

4.6 Europarat: Moderne datenschutzrechtliche Grundlagen für Europa

Im Europarat schreiten die Arbeiten zur Modernisierung der Konvention 108 voran. Die Konvention gegen Spielmanipulationen könnte datenschutzfreundlicher gestaltet werden.

Für das 1981 in Kraft getretene Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) ist wegen der zahlreichen technischen Neuerungen auf dem Gebiet der Datenverarbeitung nach 30 Jahren eine Modernisierung überfällig (vgl. 24. TB Nr. 2.4.5). Aufgrund der andauernden Beratungen zur EU-Datenschutz-Grundverordnung (vgl. Nr. 1) konnten die Arbeiten an dem Übereinkommen allerdings noch nicht beendet werden. Denn ein wesentliches Ziel der Modernisierung

der Konvention 108 liegt in der weitgehenden Harmonisierung der rechtlichen Rahmenwerke des Europarates und der EU.

Bereits jetzt zeichnen sich in den Verhandlungen Verbesserungen ab, die ich sehr begrüße. Hervorzuheben sind die Ausweitung des Geltungsbereiches des Übereinkommens auf nicht automatisierte Datenverarbeitungen, die ausdrückliche Erwähnung besonders schützenswerter personenbezogener Daten wie biometrische oder genetische Informationen und - unter gewissen Voraussetzungen - die Öffnung des Übereinkommens für Nichtmitgliedstaaten der EU und des Europarates. Insbesondere der letztgenannte Aspekt gibt zu der Hoffnung Anlass, europäische Datenschutzwerte könnten zukünftig auch außerhalb Europas stärkere Beachtung finden.

Bedauerlicherweise kann ich mich bislang nicht unmittelbar in die Verhandlungen zur Modernisierung der Konvention 108 einbringen, sondern meiner Stimme lediglich indirekt über die Zusammenarbeit mit dem BMI Gehör verschaffen, das Deutschland in der Arbeitsgruppe vertritt. Eine unmittelbare Beteiligung der nationalen Datenschutzbehörden fordert indes die Europäische Datenschutzkonferenz in ihrer Entschließung vom 5. Juni 2014 (vgl. Nr. 4.2).

Das Ministerkomitee des Europarats hat zudem die Konvention gegen Spielmanipulationen angenommen, welche am 18. September 2014 von den Sportministern der Mitgliedstaaten des Europarats unterzeichnet wurde. Im Rahmen meiner Beteiligung durch das federführende BMI habe ich Vorschläge für eine bessere Verankerung des Datenschutzes in der Konvention gemacht.

4.7 Internationaler Datenschutz – Einzelfragen

Neben besonderen Fragen der Mitarbeit in internationalen Organisationen und Gremien habe ich mich im Berichtszeitraum verschiedenen Einzelthemen zum Datenschutz auf internationaler Ebene gewidmet:

Die Entwicklung des Datenschutzes in den USA habe ich, wie in den Vorjahren, aufmerksam beobachtet (vgl. Nr. 4.7.1).

Neue Entwicklungen, für die ich mich zusammen mit einigen europäischen Kollegen eingesetzt habe, ergeben sich auch bei den Bemühungen der EU und der APEC, bestimmte Datenschutzvorschriften aus ihren jeweiligen Geltungsbereichen abzugleichen (vgl. Nr. 4.7.2).

Und nicht zuletzt hat mich die Frage der Verwendung von Fluggastdaten, insbesondere durch die Sicherheitsbehörden, in Europa und in anderen Teilen der Welt weiterhin beschäftigt (vgl. Nr. 4.7.3).

4.7.1 Datenschutzrechtliche Entwicklung in den USA

Trotz vereinzelter ermutigender Signale stagniert im Berichtszeitraum die datenschutzrechtliche Entwicklung in den USA. Die umfassenden und anlasslosen Überwachungsaktivitäten der US-Nachrichtendienste bedrohen die Regelungswerke zum Datenverkehr zwischen den USA und Europa.

Anlass zur Hoffnung auf neue Impulse für den Datenschutz in den USA gab Präsident Obama, der in seiner Rede zur Lage der Nation im Februar 2013 den Wert des Schutzes der Privatsphäre hervorhob. Im Mai 2014 befasste sich der sog. Podesta-Report mit den Auswirkungen von Big Data und unterbreitete der US-Regierung zahlreiche Vorschläge zur Verbesserung des Datenschutzes. Hierzu zählten die Forderung nach einer gesetzlichen Regelung für „Datenpannen“ (Data Breaches) und die Empfehlungen zur Einbeziehung von Nicht-US-Bürgern in den Schutz der Privatsphäre nach US-Recht sowie zur Ausweitung der „Consumer Privacy Bill of Rights“.

Leider ist es bislang bei diesen Ankündigungen geblieben. Weder die bereits im Jahre 2012 vorgestellte Consumer Privacy Bill of Rights (vgl. 24. TB Nr. 2.5.4) noch die Anregungen des Podesta-Reports haben bislang zu gesetzgeberischen Tätigkeiten geführt.

Aufhorchen lässt hingegen die Entscheidung eines New Yorker Bezirksgerichtes vom 25. April 2014, in der die Firma Microsoft auf Antrag einer nicht näher genannten US-Behörde verpflichtet wird, Daten zu einem Kunden-E-Mail-Konto herauszugeben (vgl. Nr. 9.3.2). Besondere Relevanz erfährt diese Entscheidung, weil der Durchsuchungs- und Beschlagnahmebeschluss auch Daten einbezieht, die auf Servern in der EU - in diesem Fall in Irland - gespeichert sind. Das Gericht sieht allein deshalb den Anwendungsbereich des US-Rechts auch für diese Daten als eröffnet an, weil ein Unternehmen mit Sitz in den USA betroffen ist. Neben dieser äußerst weitreichenden Interpretation des Geltungsbereichs des US-Rechts, die die datenschutzrechtlichen Rahmenbedingungen in Europa völlig außer Acht lässt, besteht auch deswegen Anlass zur Sorge, weil die eigentlich für derartige Fälle vorgesehenen internationalen Rechtshilfeabkommen keine Anwendung fanden.

Die durch Edward Snowden im Jahr 2013 aufgedeckten weltweiten Überwachungstätigkeiten der US-Geheimdienste stellen zudem den Datenverkehr zwischen der EU und den USA auf der Basis des Safe-Harbor-Abkommens grundsätzlich in Frage. Aufgrund des nachhaltig erschütterten Vertrauens in einen datenschutzgerechten Umgang auf US-Seite kündigte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Mitte des Jahres 2013 eine Überprüfung an, ob Datenübermittlungen im Rahmen des Safe-Harbor-Systems durch deutsche Unternehmen ausgesetzt werden müssen. Berichte der US-amerikanischen Bürgerrechtsorganisation „Center for Digital Democracy“ (CDD) über erhebliche Verstöße gegen die Safe-Harbor-Prinzipien und eine mangelnde Kontrolle durch die Federal Trade Commission (FTC) nährten zudem die Zweifel an der angemessenen Umsetzung der geltenden Regelung

Die intensive Auseinandersetzung der Europäischen Kommission mit den Safe-Harbor-Prinzipien zum Ende des Jahres 2013 war daher ebenso folgerichtig wie notwendig. Die Europäische Kommission identifizierte neben der Problematik des Datenzugriffs durch US-Geheimdienste weitere, strukturelle Mängel der Safe-Harbor-Prinzipien, u. a. bei der Transparenz, der Aufsicht und der Durchsetzung der Betroffenenrechte, die in 13 Empfehlungen für eine Verbesserung von Safe Harbor mündeten. Entgegen der ursprünglichen Planung dauern die Gespräche der Europäischen Kommission mit den US-Behörden noch immer an. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich daher zum Ende des Jahres 2014 an den Kommissionspräsidenten mit der Bitte um eine Sachstandsmitteilung gewandt.

Ermutigend ist hingegen die Nachricht, die FTC habe Ende des Jahres 2014 ein Bußgeld in Höhe von 200.000 $ gegen die Firma TRUSTe verhängt. Das Unternehmen, das von vielen Teilnehmern auf US-Seite zur Zertifizierung der Einhaltung der Safe-Harbor-Prinzipen beauftragt wird, hatte in den Jahren 2006 bis 2013 in mehr als 1.000 Fällen nicht die jährlich vorgesehenen Datenschutzinspektionen vorgenommen. Auch wenn die Bußgeldhöhe angesichts der Dauer des Verstoßes und der Anzahl der Versäumnisse eher gering erscheint, findet jedes Signal einer spürbaren Datenschutzaufsicht durch die FTC meine Unterstützung.

Eine neue Dynamik erhält die gegenwärtige Diskussion zu Safe Harbor durch eine Vorlage des irischen High Courts an den Europäischen Gerichtshof (EuGH), die sich vor dem Hintergrund der Kompetenzabgrenzung zwischen Kommission und dem irischen Datenschutzbeauftragten auch mit den Auswirkungen der US-Geheimdienstaktivitäten auf die Verlässlichkeit der Safe-Harbor-Prinzipien befasst. Der auch in ihrer politischen Bedeutung nicht zu unterschätzenden Entscheidung des EuGH sehe ich mit großer Spannung entgegen.

4.7.2 BCR und CBPR - schwer in Einklang zu bringen

Ein Vergleich zwischen den Anforderungen der EU und der APEC an die Genehmigung bzw. Zertifizierung von Regelungen zu grenzüberschreitenden Datenübermittlungen durch private Unternehmen zeigt Gemeinsamkeiten, überwiegend aber deutliche Unterschiede. Die von der Artikel-29-Gruppe und der „Data Privacy Sub-

group" der APEC erarbeitete Synopse soll interessierten Unternehmen helfen, die jeweiligen Prüfungsverfahren vorzubereiten.

Für die EU und den Raum der APEC (Asia-Pacific Economic Cooperation)-Länder existieren spezielle Bestimmungen, die für den nicht-öffentlichen Bereich die Übermittlung personenbezogener Daten in Drittstaaten regeln. Auf der Ebene der EU sind dies die so genannten Verbindlichen Unternehmungsregeln (Binding Corporate Rules, BCR), die in § 4c Absatz 2 Satz 1 zweiter Halbsatz BDSG verankert sind und sich vor allem an multinational tätige Konzerne mit einer Vielzahl von Tochtergesellschaften richten; den BCR entsprechen auf der Ebene der APEC die „Cross Border Privacy Rules" (CBPR), die die Vorgaben des bereits 2005 beschlossenen „APEC Privacy Framework" beachten müssen.

Auf Seiten der EU hat sich in den vergangenen Jahren das Verfahren der Genehmigung von BCR bewährt und durch den Prozess der gegenseitigen Anerkennung („Mutual Recognition") erheblich beschleunigt. Inzwischen wurden europaweit einige Dutzend BCR-Verfahren abgeschlossen, so unter anderem auch die Billigung der Verbindlichen Unternehmensregelungen der Deutsche Telekom AG unter meiner Federführung im April 2014 (vgl. auch Nr. 8.8.9).

Für das erst im Jahr 2011 etablierte System der CBPR liegen im Vergleich zu BCR zwar weniger Erfahrungen vor, dennoch wurde eine Reihe von Unternehmen in den USA nach diesem System bereits zertifiziert.

Da zahlreiche Unternehmen sowohl in den Ländern der APEC als auch in der EU geschäftlich tätig sind, äußerten diese den naheliegenden Wunsch, die Verfahren der Genehmigung von BCR und der Zertifizierung nach dem APEC-CBPR-System zu vereinfachen oder idealerweise im Sinne einer Doppel-Zertifizierung zusammenzufassen. Hierzu erarbeitete eine gemeinsame Gruppe aus Vertretern der Artikel-29-Gruppe und der Data Privacy Subgroup - einem Datenschutz-Gremium der APEC - eine Synopse über die Genehmigungsanforderungen für BCR bzw. die Zertifizierungskriterien nach dem CBPR-System. Auf der Seite der EU hat die Artikel-29-Gruppe das entsprechende Papier als Stellungnahme 2/2014 (WP 212 vom 27.02.2014) beschlossen; seitens der APEC wurde das Dokument durch deren „Senior Officials Meeting 1" (SOM1) im Februar 2014 unterstützt. Am Rande des „Global Privacy Summit" der International Association of Privacy Professionals (IAPP) wurde die Synopse schließlich Anfang März 2014 in Washington DC der Öffentlichkeit vorgestellt (vgl. Nr. 3.1.3).

Auch wenn das Ziel der Arbeiten darin bestand, Gemeinsamkeiten beider Prüfungsverfahren herauszuarbeiten, erwies sich rasch, dass die Unterschiede der beiden Verfahren deutlich überwiegen; diese zeigten sich etwa bei dem räumlichen Anwendungsbereich, den Betroffenenrechten oder den Schulungserfordernissen der mit Datenverarbeitungen befassten Mitarbeiter in einem Unternehmen. Dennoch hoffe ich, dass die Übersicht für die interessierten Unternehmen bei der Vorbereitung und Durchführung von BCR-Genehmigungs- oder CBPR-Zertifizierungsverfahren hilfreich sein kann.

Die weitere Aufgabe der EU-APEC-Expertengruppe besteht nun darin, Fallstudien zu der praktischen Durchführung beider Prüfungsverfahren am Beispiel bereits zertifizierter Unternehmen zu erstellen. Auf dieser Grundlage sollen weitere, praktisch orientierte Informationsmaterialien, z. B. in Form von Checklisten, für interessierte Unternehmen erarbeitet werden.

Ich werde die Bemühungen der EU und der APEC, eine größere Interoperabilität ihrer Datenschutzregelwerke herbeizuführen, weiterhin unterstützen und beteilige mich an dem aktuellen Projekt der gemeinsamen EU-APEC-Datenschutz-Expertengruppe.

4.7.3 Fluggastdaten - neue Herausforderungen

Nationale Gesetzgebungen, Begehrlichkeiten von verschiedenster Seite und das Problem der reisenden Dschihadisten bringen die Auseinandersetzungen über die anlasslose polizeiliche Verarbeitung und Nutzung von Fluggastdaten (PNR) erneut auf die politische Agenda. Das Europäische Parlament hat den Europäischen Gerichtshof um Überprüfung des Abkommens mit Kanada ersucht und nach den Attentaten von Paris zugleich den Weg für ein europäisches PNR-System frei gemacht.

Noch vor kurzer Zeit schien es, als gäbe es wenig Neues zu diesem Dauerthema der vorangegangenen Tätigkeitsberichte zu berichten (vgl. 22. TB Nr. 13.5; 23. TB Nr. 13.9; 24. TB Nr. 2.5.2): Die Schaffung eines europäischen Passenger Name Record-Systems (PNR) wurde vom Europäischen Parlament aufgehalten. Die Übermittlungen von Fluggastdaten aufgrund der bestehenden Abkommen mit den USA und Australien verliefen recht geräuschlos. Dann aber haben die Diskussionen über Sinn und Nutzen eines PNR-Systems aus verschiedenen Richtungen neuen Schwung erhalten:

Zum einen setzten verschiedene Mitgliedstaaten nationale Regelungen für die Schaffung von PNR-Systemen ins Werk - pikanterweise mit finanzieller Hilfe der Europäischen Kommission, deren eigener Vorschlag im Europäischen Parlament keine Mehrheit fand.

Zum anderen hatte Russland schon vor der Ukraine-Krise ein Gesetz erlassen, nach dem PNR-Daten sowohl bei Anflügen auf russische Flughäfen als auch bei Überflügen über russisches Territorium zu übermitteln sind. Dieses Ansinnen konnte zunächst auf so genannte API-Daten beschränkt werden, also jene Daten, die aus einem Pass ohnehin auslesbar sind.

Eine neue Zuspitzung hatte die politische Diskussion um Fluggastdaten schon vor den Attentaten von Paris durch den wachsenden Strom von Dschihadisten nach Syrien und in den Irak erlangt. Die Behauptung, Fluggastdaten könnten als Mittel der Terrorbekämpfung von einiger Bedeutung sein, hatte einigen Schwung in die Diskussionen auf europäischer Ebene gebracht. Nach den Attentaten von Paris stand das Thema dann im Mittelpunkt der Maßnahmen, die als Reaktion auf die Attentate erörtert wurden. Das Europäische Parlament hat darauf reagiert. Es hat seinen grundsätzlichen Widerstand mehrheitlich aufgegeben und damit den Weg für die Schaffung eines europäischen PNR-Systems frei gemacht.

Meine Zweifel an der Erforderlichkeit und Verhältnismäßigkeit einer umfassenden, anlasslosen Speicherung der Fluggastdaten aller Passagiere bestehen fort. Ein neuer konkreter Gesetzentwurf liegt bei Redaktionsschluss noch nicht vor. Von zentraler Bedeutung für seine Zulässigkeit wird sein, welche Beschränkungen für die Verarbeitung von Fluggastdaten aus dem Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung von Telekommunikationsdaten folgen (vgl. Nr. 2.3.1). Ich halte das Urteil auch für die Speicherung von Fluggastdaten für äußerst relevant - eine Meinung, die offensichtlich auch die Mehrheit des Europäischen Parlaments teilt: Es hat den Europäischen Gerichtshof um die Überprüfung des PNR-Abkommens zwischen der EU und Kanada ersucht. Es wird deutlich, dass dem Europäischen Gerichtshof nun auch im Bereich der inneren Sicherheit mehr und mehr die Aufgabe zukommt, die das Bundesverfassungsgericht in den vergangenen Jahren nach 9/11 eingenommen hat: Die Grenzen des Zulässigen bei der Terrorbekämpfung zu bestimmen und den Gesetzgeber dabei gelegentlich auch in seine Schranken zu weisen.

5 Innenausschuss

5.1 Die Digitale Verwaltung 2020

Mit dem Programm Digitale Verwaltung 2020 will die Bundesregierung eine effiziente elektronische Verwaltungsarbeit im Bund sowie einfache und schnelle elektronische Dienstleistungen des Staates fördern.

Die Digitale Agenda 2014-2017 der Bundesregierung (vgl. Nr. 18.1) beschreibt unter der Überschrift „Innovativer Staat“ das Ziel, verstärkt digitale Dienstleistungen anbieten zu wollen. Hierbei geht es letztlich um die weitere Modernisierung der Verwaltung. Es werden etwa Maßnahmen aus dem E-Government-Gesetz aufgegriffen und umgesetzt. Meine Dienststelle berät die Bundesregierung bei datenschutzrechtlichen Fragestellungen.

Von datenschutzrechtlicher Relevanz sind vor allem die Themen „Digitale Erklärungen (Normenscreening)“, „Zentraler eID-Service zur Nutzung des neuen Personalausweises“, „De-Mail-Anbindung der Bundesbehörden“, der „Aktionsplan E-Akte“ und das dazugehörige Projekt „Digitales Zwischenarchiv“ (vgl. Nr. 17.1) sowie die Entwicklung eines Geokodierungsdienstes.

Beim Vorhaben „Digitale Erklärungen (Normenscreening)“ sollen alle verwaltungsrechtlichen Formerfordernisse darauf hin geprüft werden, ob sie ersatzlos gestrichen werden können. Dies betrifft beispielsweise das persönliche Erscheinen von Bürgerinnen und Bürgern bei einer Behörde oder die eigenhändige Unterschrift. Bei den geprüften Vorschriften stellt sich auch die Frage, ob alle im Einzelfall verlangten personenbezogenen Daten verarbeitet werden müssen, oder ob entsprechend dem Grundsatz der Datenvermeidung und Datensparsamkeit auf bestimmte Informationen verzichtet werden kann. In diesem Zusammenhang ist die elektronische Identifikationsfunktion des Personalausweises zu erwähnen, die - richtig angewendet - sicherstellt, dass nur die jeweils notwendigen Daten verarbeitet werden. In der Papierwelt werden nämlich oftmals Kopien von Personalausweisen gefertigt, obwohl nicht alle Daten aus dem Ausweis für die jeweilige Verwaltungstätigkeit erforderlich sind.

Bundesbehörden müssen ab 1. Januar 2015 in Verwaltungsverfahren mit Identifizierungserfordernissen im Rahmen der Kommunikation mit den Bürgerinnen und Bürgern den elektronischen Identitätsnachweis des Personalausweises (eID-Funktion) anbieten. Allerdings hat innerhalb dieser Frist nahezu keine Bundesbehörde diese Verpflichtung umgesetzt. Vielleicht weil dies von Anfang an absehbar war, will das BMI den Bundesbehörden eine Unterstützungsleistung anbieten und den notwendigen technischen Service und die technischen Berechtigungszertifikate zentral bereitstellen. Da ich als Aufsichtsbehörde über die Vergabestelle für Berechtigungszertifikate beim Bundesverwaltungsamt einen guten Überblick über das Verfahren und die typischen Probleme habe, verfolge ich diesen zentralen eID-Service mit Interesse. Maßnahmen zur Umsetzung dieses Projekts sind bislang jedoch noch nicht ergriffen worden.

Die Maßnahme „De-Mail-Anbindung der Behörden“ zielt auf die flächendeckende Einführung des Kommunikationsmediums De-Mail ab. Nach dem E-Government-Gesetz müssen Bundesbehörden, die Zugang zum zentral für die Bundesverwaltung angebotenen IT-Verfahren haben, einen elektronischen Zugang durch eine De-Mail-Adresse eröffnen. Dieses zentral angebotene IT-Verfahren, auch als De-Mail-Gateway bezeichnet, soll den Bundesbehörden die Anbindung an De-Mail erleichtern. Im Rahmen der Digitalen Verwaltung 2020 sollen die Bundesbehörden bei der Anbindung ihrer IT-Infrastruktur und bei der Integration von De-Mail unterstützt werden, in dem u. a. Pilotprojekte zur Umsetzung konkreter Einsatzszenarien durchgeführt und Bundesbehörden insgesamt beraten werden. Auch hierzu habe ich meine datenschutzrechtliche Beratung angeboten, diese ist allerdings bislang nicht angenommen worden. Zum einen bin ich als nach dem De-Mail-Gesetz zuständige Zertifizierungsstelle vertraut mit den Datenschutzanforderungen, die die De-Mail-Diensteanbieter einhalten müssen, und kann entsprechende Fragen von Nutzerbehörden beantworten. Zum anderen habe ich bereits mit meiner Handreichung zum datenschutzgerechten Umgang mit De-Mail Hinweise für Bundesbehörden gegeben, wie sie als verantwortliche Stellen mit personenbezogenen Daten bei De-Mail umgehen sollen. Die Handreichung ist auf meiner Internetseite unter www.datenschutz.bund.de abrufbar.

Nach dem E-Government-Gesetz sollen Bundesbehörden ihre Akten elektronisch führen. Zur Unterstützung der Ressorts bei der Umsetzung dieser Verpflichtung sieht die Digitale Verwaltung 2020 einen „Aktionsplan E-Akte“ vor, der die organisatorischen und fachlichen Aspekte und die technischen Angebote bündeln soll. Auch sollen technische Grundlagen erarbeitet werden. Auf die datenschutzrechtlichen Risiken und die insofern notwendigen Schutzmaßnahmen habe ich bereits im letzten Tätigkeitbericht (24. TB Nr. 3.2.1) hingewiesen.

Ab 1. Januar 2015 müssen alle elektronischen Register, die neu aufgebaut oder überarbeitet werden und einen Bezug zu inländischen Grundstücken aufweisen, mit einer bundesweit einheitlichen Geokoordinate für jedes Flurstück versehen werden. Um diese aus dem E-Government-Gesetz folgende Verpflichtung praktisch umzusetzen, entwickelt das Bundesamt für Kartographie und Geodäsie einen Geokodierungsdienst, der klassischen Adressangaben solche standardisierten Geokoordinaten zuweisen kann (vgl. hierzu Nr. 5.5).

5.2 Antiterrordateigesetz - ein (erneuter?) Fall für das Bundesverfassungsgericht

Paukenschlag aus Karlsruhe - auch wenn es manche nicht wahrhaben wollen: Der Datenaustausch zwischen Polizeien und Nachrichtendiensten ist grundsätzlich unzulässig. Die Datenschutzkontrolle ist hierbei von herausragender Bedeutung.

Wieder einmal musste das Bundesverfassungsgericht (Urteil vom 24.04.2013, Az. 1 BvR 1215/07) den Gesetzgeber korrigieren und klare Vorgaben aufstellen - mit weit reichenden Folgen für die Zusammenarbeit der Sicherheitsbehörden. Mit dieser Entscheidung setzt das Bundesverfassungsgericht beharrlich den Schutz der Grundrechte fort.

Nun steht zweifelsfrei fest: Aus dem Grundrecht auf informationelle Selbstbestimmung folgt ein informationelles Trennungsprinzip. D. h.: Daten zwischen den Nachrichtendiensten und Polizeibehörden dürfen grundsätzlich nicht ausgetauscht werden. Warum ist dies so und was bedeutet es? Um es bildlich zu fassen: Rugby und Fußball sind zwar beides Ballsportarten, jedoch mit gänzlich unterschiedlichen Regeln und Spielfeldern. So sind Polizeien und Nachrichtendienste zwar beides staatliche Sicherheitsbehörden; sie haben jedoch gänzlich unterschiedliche Aufgaben und Befugnisse. Durch einen Datenaustausch würden diese Unterschiede gleichsam unterlaufen und damit bedeutungslos. Dem gilt es Rechnung zu tragen. Das Bundesverfassungsgericht hat dies getan. Es hat den Datenaustausch nur in Ausnahmefällen, d. h. zum Schutz herausragender öffentlicher Interessen, für zulässig erklärt. Diese Vorgabe gilt nicht nur für das Antiterrordateigesetz (ATDG), sondern generell.

Zur Begründung des informationellen Trennungsprinzips hat das Bundesverfassungsgericht unmissverständlich auf die unterschiedlichen Rollen und Funktionen von Polizeien und Nachrichtendiensten hingewiesen: Nachrichtendienste sind k e i n e Gefahrenabwehrbehörden. Dies hat das Gericht ausdrücklich betont. Danach ist das Ziel der Nachrichtendienste „nicht die operative Gefahrenabwehr, sondern die politische Information“ (1 BvR 1215/07 vom 24.04.2013, Rdn. 118). Es besteht lediglich ein „auf die politische Vorfeldaufklärung beschränkter Auftrag der Nachrichtendienste“ (a. a. O., Rdn. 119). Dies spiegele sich auch in der Beschränkung ihrer Befugnisse wieder. Vom Aufgaben- und Befugnisprofil der Nachrichtendienste unterscheidet „sich das der Polizei- und Sicherheitsbehörden grundlegend“ (a. a. O., Rdn. 120). Nur der Polizei „obliegt die Verhütung, Verhinderung und Verfolgung von Straftaten sowie die Abwehr von sonstigen Gefahren für die öffentliche Sicherheit und Ordnung“ (a. a. O.).

Das Bundesverfassungsgericht hat den Gesetzgeber ausdrücklich aufgefordert, nicht nur die Regelungen des ATDG, sondern auch das geltende Recht insgesamt (insbesondere die Datenübermittlungsvorschriften für Polizeien und Nachrichtendienste) seinen Vorgaben gemäß zu überprüfen und anzupassen. Dies steht noch aus. So bedarf es auch einer Überprüfung der neuen Sicherheitsarchitektur der Bundesregierung (vgl. 22. TB Nr. 4.2), insbesondere in Bezug auf die Teilnahme der Nachrichtendienste an den gemeinsamen Kooperationsplattformen der Sicherheitsbehörden (GTAZ, GASIM, GIZ, GETZ etc.).

Zwar hat der Deutsche Bundestag am 16. Oktober 2014 (Plenarprotokoll 60. Sitzung, S. 5588) den Gesetzentwurf der Bundesregierung zur Änderung des ATDG (Bundestagsdrucksache 18/1565 vom 28.05.2014) beschlossen, der das Urteil des Bundesverfassungsgerichts umsetzen soll. Meines Erachtens entspricht der Gesetzentwurf nicht den Vorgaben, die das Gericht in Bezug auf die Änderungen des ATDG erlassen hat. Insoweit bestehen gravierende Umsetzungsdefizite. Dies wurde auch in der zu diesem Gesetzentwurf am 22. September 2014 durchgeführten öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages deutlich.

Kritisch zu bewerten ist insbesondere der erfasste Personenkreis. Obgleich das Bundesverfassungsgericht die in § 2 Satz 1 Nummer 3 ATDG normierte Definition der Kontaktpersonen als verfassungswidrig bewertet hat, taucht diese in dem beschlossenen Gesetzentwurf - wenn auch an anderer Stelle - unverändert wieder auf.

Erstaunlich und zu kritisieren ist zudem, dass die Bundesregierung unter Hinweis auf ihren Bericht zur Evaluierung des ATDG vom 7. März 2013 (Bundestagsdrucksache 17/12665) eine gänzlich neue, gravierende Befugniserweiterung (betreffend Analysen und Recherchen) vorgenommen hat (vgl. Bundestagsdrucksache 18/1565, S. 10 f.). Damit wird der Charakter der Antiterrordatei entscheidend verändert. Die Datei ist damit nicht mehr nur eine reine Nachweis- bzw. Hinweisdatei. Das Bundesverfassungsgericht hat seine Entscheidung jedoch auf diese beschränkte Hinweisfunktion gestützt. Ohne diese Funktionsbeschränkung hätte das Gericht nicht nur Teile des ATDG, sondern u. U. das gesamte Gesetz als verfassungswidrig bewertet. Deswegen erstaunt es, wenn die Bundesregierung ihr Vorgehen damit begründet, die bei der Evaluierung des ATDG befragten Nutzer hätten diese Befugnis als „sinnvoll“ (Bundestagsdrucksache 18/1565, S. 12) erachtet. Dies reicht nicht aus. Jede neue Befugnis muss - neben weiteren verfassungsrechtlichen Anforderungen - immer auch zwingend erforderlich sein. Wünsche von Dateinutzern begründen keine verfassungsrechtliche Erforderlichkeit.

Kritisch sehe ich auch den Evaluierungsbericht der Bundesregierung. Denn zu einer wirksamen Evaluierung gehört auch die Prüfung und Beurteilung der Folgen bzw. Auswirkungen der Gesetzesregelungen auf die Grundrechte, insbesondere der unmittelbar betroffenen Bürgerinnen und Bürger. Insoweit verweise ich z. B. auf den von mir vorgestellten „Leitfaden zur Gesetzesevaluation“ (abrufbar auf meiner Internetseite unter www.datenschutz.bund.de). Dieser benennt auch weitere, essentielle Vorgaben für wirksame Evaluierungen. Selbst wenn man diese unberücksichtigt ließe und die Bundesregierung an ihren eigenen Maßstäben messen würde, fehlt eine hinreichende Prüfung zur Wahrung der Grundrechte. So weist die Bundesregierung in ihrem Evaluierungsbericht unter Punkt 4.3.1 (Wahrung der Grundrechte; grundrechtsrelevante Rückschlüsse aus den Evaluierungserkenntnissen - Bundestagsdrucksache 17/12665 (neu), S. 50) ausdrücklich auf Folgendes hin:

„Allerdings kann aus den empirisch ermittelten Nutzungszahlen, die gemäß der gewählten Methodik die Informationsbasis der vorliegenden Evaluierung sind, nicht zwingend die rechtliche Aussage zur Bemessung der verbundenen Grundrechtseingriffe abgeleitet werden. Insoweit wird die Nutzungshäufigkeit im Folgenden als ein Kriterium für die Einschätzung der Intensität eines Grundrechtseingriffs herangezogen; die Auseinandersetzung mit qualitativen Aspekten geht über den Fokus dieser Evaluierung hinaus. Daher sieht das zwischen BMI und BMJ abgestimmte Untersuchungsdesign ein Zweitgutachten mit eben dieser rechtswissenschaftlichen Ausrichtung vor.“

Dieses Zweitgutachten existiert nicht. Damit fehlt die zentrale Grundlage, um die Wahrung der Grundrechte zu beurteilen - und damit eine essentielle Voraussetzung für jede wirksame Evaluierung. Der Evaluierungsbericht der Bundesregierung ist daher eine fragwürdige Legitimation zur Änderung des ATDG.

Schließlich hat das Bundesverfassungsgericht weit reichende, über das ATDG hinausgehende grundsätzliche Aussagen zur Bedeutung, Funktion und Ausgestaltung der datenschutzrechtlichen Aufsicht getroffen und dem Gesetzgeber eindeutige Vorgaben gemacht:

„Eingriffe in das Recht auf informationelle Selbstbestimmung können (…) auch dann unverhältnismäßig sein, wenn sie nicht durch ein hinreichend wirksames aufsichtsrechtliches Kontrollregime flankiert sind. Dies hat

umso größeres Gewicht, je weniger eine subjektivrechtliche Kontrolle gewährleistet ist.“ (1 BvR, a. a. O., Rdn. 207). Gewähren gesetzliche Bestimmungen die Befugnis zu heimlichen, d. h. vom Betroffenen unbemerkten bzw. nicht bemerkbaren Grundrechtseingriffen, liegt die Kontrolle der Ausübung dieser Befugnisse „im Wesentlichen bei der Aufsicht durch die Datenschutzbeauftragten“ (a. a. O., Rdn. 204). Da ein Betroffener von derartigen Eingriffen nichts weiß oder wissen kann, hat er mangels entsprechender Kenntnis faktisch nur eingeschränkte Rechtsschutzmöglichkeiten (vgl. a. a. O.). Deshalb bedarf es einer effizienten Datenschutzaufsicht. Diese Datenschutzaufsicht muss für den Betroffenen gewährleisten (können), dass dessen Grundrechte beachtet und gewahrt werden. Ist ihr dies nicht (ausreichend) möglich, z. B. weil sie daran gehindert oder ihr nicht ausreichende Sachmittel oder Personal zur Verfügung gestellt werden, kann dies ein unverhältnismäßiger Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung sein. Die Betroffenen können diese Grundrechtsverletzung (verfassungs-)gerichtlich rügen.

Folglich ist die Gewährleistung einer effizienten Datenschutzaufsicht von herausragender Bedeutung - auch und insbesondere für die (betroffenen) Bürgerinnen und Bürger. Das Bundesverfassungsgericht hat den Gesetzgeber in seinem Urteil also ausdrücklich verpflichtet, die Aufsichtsinstanzen mit „wirksamen Befugnissen“ (1 BvR, a. a. O., Rdn. 214) auszustatten und die Durchführung effizienter Kontrollen - auch in praktischer Hinsicht - wirksam sicherzustellen (vgl. a. a. O., Rdn. 216).

Es ist daher mehr als nur bedauerlich, dass meinen zahlreichen Forderungen nach dringend notwendiger personeller Verstärkung meiner Behörde bis jetzt nicht entsprochen worden ist.

Ich appelliere daher an den Gesetzgeber, diesem Personalbedarf jetzt zügig und angemessen Rechnung zu tragen, insbesondere auch bei der beabsichtigten Ausgestaltung meines Hauses als oberste Bundesbehörde. Nur dann ist eine effiziente Aufsicht im Sinne der Vorgaben des Bundesverfassungsgerichts zu gewährleisten.

5.3 Scoring: Immer noch viele Fragen offen

Ein Urteil des Bundesgerichtshofs zur Reichweite der Auskunftspflicht von Wirtschaftsauskunfteien und eine Studie zur Evaluation der datenschutzrechtlichen Vorschriften für Scoringverfahren zeigen gesetzgeberischen Nachbesserungsbedarf auf.

Ob jemand an bestimmten Werbeinhalten interessiert ist oder dazu neigt, einen Vertrag vorzeitig zu kündigen, ob ein Kunde pünktlich seine Kreditraten zurückzahlen wird oder aufgrund von Vorerkrankungen zu hohe Gesundheitsrisiken für eine Lebensversicherung aufweist - Scoringverfahren, also die Berechnung eines (punktwertbasierten) Wahrscheinlichkeitswertes aufgrund der Zuordnung der über eine Person bekannten Informationen zu statistischen Vergleichsgruppen, erfreuen sich stetig wachsender Beliebtheit. Auch komplexe Sachverhalte scheinen sich einfach in Zahlenwerten ausdrücken und treffsicher prognostizieren zu lassen.

Fatale Konsequenzen kann es allerdings haben, wenn fehlerhafte oder unvollständige Daten in die Scorewertberechnung einfließen oder wenn der Wahrscheinlichkeitswert trotz zutreffender Datenbasis unerklärlich schlecht ausfällt. Wer einen schlechten Scorewert hat, erhält kein Darlehen oder Girokonto mit Überziehungsmöglichkeit, keinen Mobilfunkvertrag, keine Warenlieferung auf Rechnung, keinen günstigen Sondertarif bei Gas- und Stromlieferanten und gegebenenfalls nicht einmal einen Mietvertrag. Bei einem solchen Bonitätsscoring greifen die verantwortlichen Stellen in aller Regel auf die bei Wirtschaftsauskunfteien gespeicherten Informationen zurück.

Spätestens wenn etwas „schief läuft“, haben Betroffene ein großes Interesse, die bei der Berechnung der Scorewerte zugrunde gelegten Daten prüfen und den errechneten Wahrscheinlichkeitswert nachvollziehen zu können. Ein solcher Auskunftsanspruch „über das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte

einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form“ (§ 34 Abs. 4 Satz 1 Nr. 4 BDSG) ist seit der so genannten BDSG-Novelle I aus dem Jahr 2009 ausdrücklich im BDSG vorgesehen.

Die Grenzen dieses allen Betroffenen einmal im Kalenderjahr unentgeltlich zustehenden Anspruchs hat der Bundesgerichtshof (BGH) in seinem Urteil vom 28. Januar 2014 jüngst konkretisiert (Az. VI ZR 156/13). Danach haben die Betroffen zwar einen Anspruch auf Auskunft über alle in die Wahrscheinlichkeitswerte eingeflossenen Einzeldaten, sie können aber keine Auskunft über die konkrete Gewichtung der in den Scorewert eingeflossenen Merkmale und über die Zusammensetzung der statistischen Vergleichsgruppen zur Scorewertberechnung verlangen. Diese Angaben sind nach Auffassung des BGH als Teil der Scoreformel durch das Geschäftsgeheimnis der Auskunfteien geschützt.

Auch wenn das Urteil des BGH angesichts der mehrheitlichen Rechtsprechung der Instanzgerichte nicht überrascht, bedeutet es, dass Betroffene lediglich die zur Scorewertberechnung genutzte Datenbasis, nicht aber die Scorewertberechnung an sich prüfen können. Ist die Datengrundlage korrekt und fällt der Scorewert trotzdem unerklärlich schlecht aus, können sie nicht nachvollziehen, „woran es gelegen hat“. Das gesetzgeberische Ziel der BDSG-Novelle I aus dem Jahr 2009, mehr Verbrauchertransparenz bei der Scorewertberechnung zu schaffen und den Betroffenen insbesondere die Möglichkeit an die Hand zu geben, ihre Datenschutzrechte ausüben, ihren Standpunkt geltend machen und eine sachgerechte Überprüfung der Entscheidung herbeiführen zu können (Bundestagsdrucksache 16/10529, S. 17), ist nach bestehender Rechtsprechung daher nur unzureichend umgesetzt.

Die bereits im 23. Tätigkeitsbericht (Nr. 10.5) angesprochene Kritik an dem geltenden Rechtsrahmen für Auskunfteien und das Scoring hat sich daher nicht erledigt, sondern ist aktueller denn je. Es ist daher zu begrüßen, dass sich die Bundesregierung mit den Auswirkungen der im Jahr 2009 novellierten datenschutzrechtlichen Regelungen befasst. Die im Dezember 2014 veröffentlichte Studie „Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen“ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und der GP Forschungsgruppe listet eine Vielzahl rechtlicher und praktischer Anwendungsprobleme auf und belegt den Verbesserungsbedarf. Das Gutachten wurde in der letzten Legislaturperiode vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) in Auftrag gegeben und zwischenzeitlich durch das Bundesministerium der Justiz und für Verbraucherschutz federführend begleitet. Die vorgeschlagenen Handlungsempfehlungen an den Gesetzgeber sollten nun zeitnah und mit einem entsprechenden Veränderungswillen analysiert und diskutiert werden. Die gebotene Neujustierung der datenschutzrechtlichen Auskunftei- und Scoringregelungen sollte dann an drei zentralen Punkten ansetzen, nämlich - neben der Verbesserung der Verbrauchertransparenz - an der Beseitigung bestehender Rechtsunsicherheiten und der Sicherstellung hoher Qualitätsstandards für Scoringverfahren, beispielsweise durch konkretere Anforderungen an die nutzbare Datengrundlage und die Aussagekraft (Signifikanz) von Scorewerten.

5.4 Aus dem Düsseldorfer Kreis

Auch in diesem Berichtszeitraum hat sich der Düsseldorfer Kreis aktueller datenschutzrelevanter Entwicklungen im nicht-öffentlichen Bereich angenommen und einer bundesweit einheitlichen Auslegung zugeführt.

Der im halbjährlichen Turnus unter dem Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen tagende Düsseldorfer Kreis übernimmt auch nach seiner Eingliederung in das Gefüge der Datenschutzkonferenz (vgl. 24. TB Nr. 10.3) eine wichtige Informations- und Koordinierungsfunktion. Er stellt die gegenseitige Information der Datenschutzaufsichtsbehörden des Bundes und der Länder über wichtige datenschutzrechtliche Entwicklungen sicher und gewährleistet durch interne oder veröffentlichte Beschlüsse eine bundesweit einheitliche Auslegung des Datenschutzrechts im nicht-öffentlichen Bereich.

Die Themen, mit denen sich der Düsseldorfer Kreis - in enger Abstimmung mit den übrigen Arbeitskreisen der Datenschutzkonferenz - befasst, decken das gesamte Spektrum der Datenverarbeitung durch die Privatwirtschaft

ab. Die thematischen Schwerpunkte unterliegen einem kontinuierlichen Wandel, im Kern geht es aber fast immer um aktuelle Entwicklungen mit großer Breitenwirkung für die Bevölkerung.

Gleich zwei Beschlüsse befassen sich mit dem zunehmenden Einsatz mobiler Videoüberwachungstechnik in und an Fahrzeugen. Der Düsseldorfer Kreis hat betont, dass die Überwachung des öffentlichen Straßenverkehrs zum Zweck vorsorglicher Beweissicherung bei Unfällen oder anderen kritischen Ereignissen weder durch Taxiunternehmen noch durch Privatpersonen datenschutzrechtlich zulässig ist. Auch die im Innenraum von Taxis eingesetzten Kameras zum Schutz vor Überfällen durch Fahrgäste sind nur unter engen Voraussetzungen rechtskonform.

Die vom Düsseldorfer Kreis angenommene Orientierungshilfe zur Videoüberwachung im nicht-öffentlichen Bereich fasst die datenschutzrechtlichen Anforderungen an den zunehmenden Einsatz von Videokameras anschaulich zusammen. Auch die Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“, die die datenschutzrechtlichen Grenzen des Fragerechts von Vermietern gegenüber Mietinteressenten aufzeigt, ist von hoher praktischer Relevanz für die Datenschutzrechte vieler Bürgerinnen und Bürger.

Alle Beschlüsse des Düsseldorfer Kreises im Berichtszeitraum sind aus dem Kasten zu Nr. 5.4 ersichtlich und auf meiner Internetseite unter www.datenschutz.bund.de abrufbar.

Kasten zu Nr. 5.4

Beschlüsse des Düsseldorfer Kreises in den Jahren 2013/2014:

- Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen
- Videoüberwachung in und an Taxis
- Smartes Fernsehen nur mit smartem Datenschutz
- Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)
- Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden
- Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“
- Orientierungshilfe „Videoüberwachung im nicht-öffentlichen Bereich“
- Orientierungshilfe „Datenschutzanforderungen an App-Entwickler und App-Anbieter“

5.5 Georeferenzierung von Registern

Das Bundesamt für Kartografie und Geodäsie entwickelt für die Umsetzung des E-Government-Gesetzes eine technische Lösung für die Geokodierung elektronischer Register.

Entsprechend den Vorgaben des E-Government-Gesetzes des Bundes (EGovG) sind alle elektronischen Register, die einen Bezug zu inländischen Grundstücken aufweisen und ab dem 1. Januar 2015 neu aufgebaut oder überarbeitet werden, mit einer einheitlichen Georeferenzierung zu versehen, sofern diese Register Daten enthalten, die aufgrund einer Rechtsvorschrift des Bundes erhoben und gespeichert werden (vgl. 24. TB Nr. 3.2.3). Diese Verpflichtung trifft daher nicht nur Bundesbehörden, sondern auch Landesbehörden, wenn die Datenerhebung und -speicherung bundesrechtlich angeordnet ist. Dies beträfe beispielsweise ab dem Inkrafttreten des Bundesmeldegesetzes am 1. Mai 2015 die Melderegister (vgl. Nr. 5.15).

Den Adressdaten im Melderegister wären dann geografische Koordinaten zuzuordnen, mit deren Hilfe sich die Lage eines Hauses oder Grundstücks exakt bestimmen ließe. Der Hauptzweck der Georeferenzierung liegt im Erreichen eines höheren Standardisierungsgrades, da das Verwenden von Geodaten mit einer geringeren Fehlerquote verbunden ist, als die Nutzung von Adressdaten, bei deren Schreibweise Fehler auftreten können.

Um die Verpflichtung zur Georeferenzierung von Registern bundesweit einheitlich umzusetzen, entwickelt das Bundesamt für Kartografie und Geodäsie (BKG) ein Verfahren, dessen grundsätzliche Ausgestaltung ich datenschutzrechtlich geprüft habe.

Der technische Ablauf ist so gestaltet, dass die registerführende Behörde zunächst die reinen Adressangaben (Straße, Hausnummer, Postleitzahl, Ort) von ihren übrigen Fachdaten einschließlich unmittelbarer Personenangaben trennt und in einer separaten Tabelle speichert. Gegebenenfalls werden diese Adressdaten mit eindeutigen Kennungen versehen, die der registerführenden Behörde beim Rücklauf die Zuordnung erleichtern. Diese Adressdaten sind zusammen mit den Kennungen weiterhin personenbezogene Daten, da eine Herstellung des Personenbezugs - beispielsweise zur Person des Grundstückseigentümers - weiterhin möglich bleibt.

Die registerführende Stelle übergibt anschließend die Tabelle mit den Adressangaben dem BKG, das diese Daten mithilfe einer Referenzdatenbank mit der Bezeichnung „Georeferenzierte Adressdaten“ mit den exakten Geokoordinaten (geografische Länge und Breite) versieht. Die in dieser Weise geokodierten Adressdaten gehen dann wieder an die registerführende Behörde zurück, die ihrerseits diese Daten wieder mit ihrem Originaldatenbestand zusammenführen kann.

Die nun zusätzlich in den jeweiligen Registern gespeicherten Geokoordinaten stellen für sich genommen zunächst kein erhöhtes datenschutzrechtliches Risiko dar, da sie inhaltlich keine zusätzlichen Informationen im Vergleich zu den Adressdaten enthalten. Der Zugang zu den Geokoordinaten unterliegt beim jeweiligen Register den gleichen rechtlichen Bedingungen wie der Zugang zu den Adressdaten selbst. Die Verwendung standardisierter Geokoordinaten erleichtert allerdings technisch die Verknüpfung und Verschneidung georeferenzierter Informationen und erhöht so potentiell auch die Risiken für das Recht auf informationelle Selbstbestimmung. Dieser Gefahr muss deshalb mit entsprechenden technischen und organisatorischen Maßnahmen begegnet werden.

Angesichts des Personenbezugs der Adressdaten bedarf es für deren Weitergabe an das BKG einer rechtlichen Grundlage. Da das E-Government-Gesetz hierfür keine Übermittlungsbefugnis vorsieht, kann das BKG nur im Rahmen einer Auftragsdatenverarbeitung eingebunden werden. Diese richtet sich grundsätzlich nach § 11 BDSG, sofern die auftraggebende registerführende Behörde eine öffentliche Stelle des Bundes ist. Bei öffentlichen Stellen der Länder sind die entsprechenden Regeln des jeweiligen Landesdatenschutzgesetzes zu beachten.

Für die Datenübertragung habe ich dem BKG geraten, zur Sicherung der Vertraulichkeit ein Verschlüsselungsverfahren einzusetzen. Zur Gewährleistung der Authentizität habe ich eine Authentifizierung der registerführenden Behörde beim BKG empfohlen.

Ich werde das Projekt weiterhin datenschutzrechtlich begleiten.

5.6 Einsatz von Drohnen

Drohnen werden in großem Umfang mit Video- und Fotokameras ausgerüstet und sowohl im behördlichen wie auch im privaten Umfeld eingesetzt. Datenschutzrechtliche Aspekte werden beim Einsatz der Aufzeichnungstechnik häufig nur unzureichend beachtet.

Drohnen (24. TB Nr. 3.3.3) sind unbemannte Flugobjekte (Remotely Piloted Aircraft Systems - RPAS), die sowohl manuell ferngesteuert werden als auch autonom fest einprogrammierte Flugwege einschließlich Start und Landung abfliegen können. Die Größe der Drohnen und damit das Gewicht hängen oft vom Einsatzzweck ab. Entsprechend große Unterschiede gibt es weiter etwa bei der Flugdauer, Flughöhe und der Reichweite oder der Antriebsart.

Die rechtlichen Rahmenbedingungen für die Nutzung von Drohnen und die Zulässigkeit der Flüge im deutschen Luftraum habe ich bereits in meinem 24. Tätigkeitsbericht (Nr. 3.3.3.1) erläutert.

Der Einsatzbereich im behördlichen Umfeld umfasst z. B. die Erkundung und Vermessung von Gebieten, die Überwachung von Personen und Menschenansammlungen oder die Kontrolle der Nutzung von landwirtschaftlichen Anbauflächen. Beim Katastrophenschutz und im militärischen Bereich werden Drohnen für Aufklärungszwecke, z. B. zur Unterstützung von Helfern bei Wasser- und Brandschäden eingesetzt. Im privatwirtschaftlichen Bereich werden Drohnen mittlerweile zum Transport von Waren z. B. zur Versorgung von küstennahen Inseln mit Medikamenten, Kontrolle von Überlandleitungen oder Bahngleisen genutzt.

Für kommerzielle wie auch behördliche Nutzung gelten Drohnen gemäß § 1 Absatz 2 Satz 3 Luftverkehrsgesetz als Luftfahrzeuge, mit allen rechtlichen Vorgaben für deren Einsatz. Drohnen zur Freizeitgestaltung oder zum Sport - häufig werden hierbei Bild- oder Videoaufnahmen des Fluges und der Umgebung gemacht - gelten als unbemannte Luftfahrtsysteme und unterliegen eigenen rechtlichen Vorgaben.

Meine Mitarbeiter haben sich aufgrund einer Eingabe die derzeit bei der Bundeswehr eingesetzten Drohnen und deren Auswertesysteme angesehen. Die aktuell eingesetzten Drohnen, Kameras und Auswertesysteme wurden für spezielle Einsatzzwecke eingeführt und waren zusammen mit den Einsatzvorgaben der Bundeswehr aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Drohnen, die ausschließlich zum Zweck der Freizeitgestaltung genutzt werden, sind in der Regel im Besitz von Bürgern, die häufig weder die Gefahr für die Sicherheit des Luftverkehrs abschätzen können noch die Vorschriften über den zu beachtenden Datenschutz kennen.

Dies führt nicht selten zu Konflikten und neuen rechtlichen Fragestellungen zum Schutz der Privatsphäre.

Das BDSG enthält keine speziellen Regelungen zum Gebrauch einer privaten Drohne. Auch die im Rahmen eines Drohnenfluges angefertigten Foto- und Filmaufnahmen unterliegen nicht bzw. nur bedingt den Regelungen des BDSG, sofern diese Aufnahmen ausschließlich für persönliche oder familiäre Zwecke verwendet werden. Eine Verletzung des allgemeinen Persönlichkeitsrechts liegt allerdings schon bei einer Verbreitung der Aufnahmen vor, die über das persönliche oder familiäre Umfeld hinausgeht. Die Aufnahmen können in erheblichem Maße Persönlichkeitsrechte verletzen, wenn sie gezielt fortlaufend Bild- oder Filmmaterial vom Beobachteten liefern. Hier kann dann zivilrechtlich gegen den Betreiber der Drohne vorgegangen werden. Weiter sind eventuell spezielle Vorschriften wie das Urheberrechtsgesetz bei gewerblichen Aufnahmen zu beachten.

Häufig entstehen Probleme beim Überfliegen abgeschirmter privater Grundstücksbereiche. Dabei kann es zur Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a Strafgesetzbuch) kommen und damit zu strafrechtlichen Sanktionen. Werden Livebilder ausschließlich zur Steuerung der Drohne genutzt und nicht gespeichert, ist allerdings nicht von vornherein von einer Verletzung der Privatsphäre der dargestellten Personen auszugehen.

Grundsätzlich stellt eine „heimliche“ Videoüberwachung im öffentlichen Raum, und dies ist häufig beim Einsatz von Drohnen der Fall, eine Gefahr für die Privatsphäre dar. Besonders zur Überwachung vorgesehene Drohnen sind geräuscharm und fallen selbst aufmerksamen Betroffenen nicht auf. Praktisch hat der Einzelne so-

mit keine Möglichkeit, sich vor einer Überwachung aus der Luft zu schützen. Hinzu kommt, dass eine für die „Überwachung“ verantwortliche Person oder Stelle oft nicht zu erkennen ist.

Da immer mehr Drohnen - sowohl für gewerbliche als auch für private Zwecke - eingesetzt werden, sind strenge datenschutzrechtliche Vorschriften hierfür unumgänglich. Da die europäischen Verkehrsminister eine Harmonisierung des europäischen Luftraumes für den Drohneneinsatz im Sichtflugbereich für 2016 anstreben, bietet sich die Integration datenschutzrechtlicher Vorgaben in die europäische Datenschutz-Grundverordnung (DSGVO) an. Die Bundesregierung geht davon aus, dass bis zur allgemeinen Zulassung von Drohnen die europäische DSGVO in Kraft sein wird. Die Verordnung soll dann auch für Drohnen gelten. Wenn das Inkrafttreten nicht rechtzeitig erfolgen sollte, werde ich mich für geeignete Übergangsregelungen auf der Grundlage des hohen deutschen Datenschutzes einsetzen. Weitere Informationen der Europäischen Kommission zum Thema Drohnen sind unter http://ec.europa.eu zu finden.

Die Arbeiten der Artikel-29-Gruppe, die im Frühjahr 2015 eine Stellungnahme zum Thema Drohnen/Remotely Piloted Aircraft Systems verabschieden wird, unterstütze ich. Die entsprechende Stellungnahme werde ich zu gegebener Zeit auf meiner Internetseite veröffentlichen.

5.7 Neue Entwicklungen im Personaldatenschutz für Beschäftigte des Bundes

Im Berichtszeitraum gab es neue Entwicklungen im Personalaktenrecht für die Beamten. Aber auch bei anderen Fragen des Personaldatenschutzes war meine Beratung gefragt.

5.7.1 Änderungen im Personalaktenrecht der Beamten

Mit dem Entwurf eines Gesetzes zur Änderung des Bundesbeamtengesetzes und weiterer dienstrechtlicher Vorschriften (Bundestagsdrucksache 18/3248) setzt sich der Trend fort, Aufgaben der Personalverwaltung auch im öffentlichen Dienst zu zentralisieren und auszulagern. Dabei sind datenschutzrechtliche Grundsätze einzuhalten, insbesondere darf das Personalaktengeheimnis nicht ausgehöhlt werden.

Bereits in der Vergangenheit (23. TB Nr. 12.6) habe ich über die Einrichtung von Dienstleistungszentren im Bereich der Personalverwaltung des Bundes berichtet. Die Bundesregierung sieht in der Übertragung von Funktionen der Personalverwaltung auf Dienstleistungszentren, wie z. B. das Bundesamt für zentrale Dienste und offene Vermögensfragen, eine Erleichterung u. a. im Sinne einer einheitlichen und gleichmäßigen Rechtsanwendung und -auslegung. Im Vordergrund steht aber eher die - auch von der Bundesregierung eingeräumte - Kostenersparnis und der Effektivitätsgewinn. Allerdings fehlt bislang für die bereits eingerichteten und noch geplanten Dienstleistungszentren eine Rechtsgrundlage, insbesondere für die hierbei erforderliche Übermittlung von Personalaktendaten. Dieses Manko soll die Einfügung eines neuen Absatzes 2 in § 111 sowie eines neuen § 111a Bundesbeamtengesetz (BBG) durch den Entwurf eines Gesetzes zur Änderung des Bundesbeamtengesetzes und weiterer dienstrechtlicher Vorschriften (Bundestagsdrucksache 18/3248) beseitigen. Der vorgeschlagene § 111 Absatz 2 soll für den Fall, dass einzelne Aufgaben von der personalverwaltenden Stelle auf eine andere öffentliche Stelle übertragen werden, dieser die zur Erfüllung der Aufgaben erforderliche Übermittlungsbefugnis für Personalaktendaten gewähren.

Durch den neuen § 111a BBG wird darüber hinaus das Instrument der Datenverarbeitung im Auftrag in das Personalaktenrecht des Bundes eingeführt. Danach soll die Verarbeitung von Personalaktendaten im Auftrag zwar grundsätzlich verboten sein. An gleicher Stelle werden allerdings die Voraussetzungen dargestellt, bei deren Erfüllung gleichwohl die Verarbeitung von Personalaktendaten im Auftrag zulässig sein soll. Von besonderer Bedeutung ist dabei nicht nur, dass eine Datenverarbeitung im Auftrag in diesem Bereich von der Zustimmung der obersten Dienstbehörde (Abs. 2) abhängig gemacht wird und die beauftragende Behörde regelmäßig die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften zu kontrollieren hat (Abs. 1 Nr. 2). Soweit Auftrag-

nehmer eine öffentliche Stelle ist, ist in der zugrundeliegenden Verwaltungsvereinbarung vorzusehen, dass auch der behördliche Datenschutzbeauftragte der Auftrag gebenden Behörde seine sich aus §§ 4f ff. BDSG ergebenden Kontrollrechte beim Auftragnehmer wahrnehmen kann. Soweit die Auftrag nehmende öffentliche Stelle eine solche des Bundes ist, unterliegt diese selbstverständlich auch nach den §§ 24 ff. BDSG meiner datenschutzrechtlichen Kontrolle; soweit es sich um eine öffentliche Stelle des Landes handelt, ist der jeweils zuständige Landesbeauftragte für den Datenschutz kontrollberechtigt. Soweit der Auftragnehmer eine nicht-öffentliche Stelle ist, die nur unter den einschränkenden Voraussetzungen des Absatzes 4 dieser Vorschrift zulässig ist, hat der zugrundeliegende Vertrag vorzusehen, dass der Auftragnehmer eine Kontrolle durch mich nach den §§ 21 und 24 bis 26 Absatz 1 bis 4 BDSG zu dulden hat.

Der vorgesehene § 107 Absatz 1 Satz 2 BBG soll den mit den Aufgaben des ärztlichen Dienstes betrauten Beschäftigten der personalverwaltenden Behörde Zugang zu Personalaktendaten gewähren, soweit dies zur Erfüllung der Aufgaben des ärztlichen Dienstes erforderlich ist. Diese Aufgaben ergeben sich beispielsweise aus dem Arbeitsschutzgesetz, Arbeitssicherheitsgesetz, der Verordnung zur arbeitsmedizinischen Vorsorge sowie aus weiteren spezialgesetzlichen Bestimmungen. In der Gesetzesbegründung wurde klargestellt, dass aus der allgemeinen Fürsorgepflicht des Dienstherren (§ 78 BBG) abgeleitete Aufgaben, insbesondere wenn sie von den Beschäftigten aufgrund ihrer freien Entscheidung in Anspruch genommen werden können (z. B. Beratungsansprüche), den Zugang zu Personalaktendaten dagegen nicht rechtfertigen (Bundestagsdrucksache 18/3248, S. 30). Diese Klarstellung begrüße ich sehr.

Begrüßt habe ich im Hinblick auf Gesichtspunkte der Rechtssicherheit auch, dass nunmehr in § 108 Absatz 1 BBG klargestellt werden soll, dass für Beihilfezwecke personenbezogene Daten erhoben und verwendet werden dürfen, soweit die Daten für diese Zwecke erforderlich sind. Bisher konnte diese naturgemäß erforderliche Datenerhebung und -verwendung nur durch eine sinngemäße Auslegung des § 108 BBG legitimiert werden.

5.7.2 Datenschutzrechtliche Fragen beim sog. Vorgesetztenfeedback

Ich habe Bundesbehörden zum Vorgesetztenfeedback beraten. Das Fazit lautet: Für die Bewertung der datenschutzrechtlichen Zulässigkeit kommt es stets auf die konkrete Ausgestaltung im Einzelfall an.

Vorgesetztenfeedbacks sind eine gute Möglichkeit zur Erhaltung und Förderung der Eignung, Befähigung und fachlichen Leistung der Vorgesetzten. Immer mehr Bundesbehörden zeigen Interesse daran. Solche Verfahren werfen allerdings eine Reihe datenschutzrechtlicher Fragen auf.

Ist die Mitarbeiterbefragung anonym ausgestaltet, bedarf es keiner Rechtsgrundlage für eine verpflichtende Teilnahme der Befragten, denn das Verbot mit Erlaubnisvorbehalt des BDSG greift nur bei personenbezogenen Daten. Erfolgt die Mitarbeiterbefragung allerdings nur pseudonymisiert, ist eine rechtliche Grundlage erforderlich. Ob eine Mitarbeiterbefragung anonym oder pseudonym durchgeführt wird, kann nur anhand der konkreten Umstände des Einzelfalls bewertet werden. Im Falle einer elektronischen Befragung spricht die Versendung eines Links an die personalisierten E-Mail-Postfächer der Beschäftigten gegen die Anonymität der Umfrage. Falls die elektronische Umsetzung gewünscht ist, kommt die Abfrage an Stand-Alone-Computern in Betracht, die keine Rückschlüsse auf den Arbeitsplatz der betroffenen Beschäftigten zulassen. Zu beobachten ist ein Spannungsverhältnis zwischen dem Bedürfnis, Mitarbeiterumfragen anonym auszugestalten, und dem Wunsch nachzuhalten, wer seine Bewertung abgegeben hat, und damit Doppelantworten zu vermeiden. Bei Umfragen in Papierform ist die Anonymität generell leichter zu realisieren. Soweit Anonymität zugesichert ist, muss diese nicht nur bei der Erhebung, sondern auch bei der Auswertung - beispielsweise durch Zusammenfassung von Daten - gewährleistet sein.

Bei einem pseudonymen Verfahren kommt als Rechtsgrundlage grundsätzlich die Einwilligung der Mitarbeiter nach § 4a BDSG in Betracht. Aufgrund des Machtungleichgewichts zwischen Arbeitgeber/Dienstherr und Beschäftigtem kann diese aber in der Regel nur eingeschränkt Grundlage sein. Gleichwohl sehe ich eine entspre-

chende Einwilligung im Rahmen von Mitarbeiterbefragungen als zulässig an, da das Beschäftigungsverhältnis hiervon nicht unmittelbar betroffen ist. Das Risiko der Re-Identifizierung des Beschäftigten muss aber möglichst gering bleiben, beispielsweise durch Auslagerung einer Zuordnungsliste an Personen außerhalb der Behörde und begrenzte Zugriffsmöglichkeiten von Behördenmitarbeitern. Um die Freiwilligkeit zu gewährleisten, dürfen Beschäftigten, die sich gegen eine Teilnahme entscheiden, keine Nachteile entstehen. Personalisierte Mahnungen haben daher zu unterbleiben; allgemeine Aufforderungen zur Teilnahme hingegen sind zulässig. Bereits in meinem 20. Tätigkeitsbericht (Nr. 10.2.4) habe ich darauf hingewiesen, dass bei Mitarbeiterbefragungen subjektive Einschätzungen und Bewertungen abgefragt werden, die ohne eine gesetzliche Rechtsgrundlage nicht verpflichtend erhoben werden dürfen. Wesentliche Bedeutung kommt daher einer vorherigen umfassenden Aufklärung der Mitarbeiter zu. Zudem ist der Hinweis auf die Freiwilligkeit in die Fragebögen selbst aufzunehmen und hervorzuheben. Alternativ kann die verpflichtende Teilnahme auf Grund einer Rechtsvorschrift erfolgen. Ob hierfür eine Dienstvereinbarung ausreicht, hängt vom Einzelfall und der jeweiligen Ausgestaltung ab. Vor der Planung und Durchführung einer Mitarbeiterbefragung ist zudem zu prüfen, ob eine Beteiligung der Personalvertretung erfolgen muss.

Bei der Ausgestaltung des Verfahrens ist neben dem Recht auf informationelle Selbstbestimmung des Beschäftigten auch dasjenige des Vorgesetzten zu berücksichtigen. Die Ergebnisse der Befragung und die einzelnen Bewertungen dürfen nur die Personen und Organisationseinheiten erfahren, für deren Tätigkeit die Kenntnis dieser Informationen unbedingt erforderlich ist, weil es sich bei den personenbezogenen Ergebnissen des Vorgesetztenfeedbacks um Personaldaten handelt, die nach § 32 Absatz 1 BDSG nur genutzt werden dürfen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Im Regelfall trifft dies für die Mitarbeiter der Personalverwaltung zu. Gerne berate ich Bundesbehörden auch in Zukunft zu den datenschutzrechtlichen Rahmenbedingungen ihres geplanten Vorgesetztenfeedbacks.

5.7.3 Elektronische Bewerbungen auf dem Vormarsch

In der Bundesverwaltung setzt sich der Trend zu neuen Verfahren der automatisierten Personaldatenverarbeitung fort (vgl. 24. TB Nr. 13.2). So werden zunehmend elektronische Verfahren zur Auswahl von Bewerbern eingesetzt. Wegen der Risiken für die Persönlichkeitsrechte der Betroffenen sind hierbei bereits im Planungs- und Entwicklungsstadium Datenschutzaspekte zu berücksichtigen.

Das BMVI wurde von mir bei der Einführung eines **elektronischen Bewerbungsverfahrens (EBV)** in der Bundesverkehrsverwaltung beraten. Dabei habe ich zu den unterschiedlichen Entwicklungsstadien dieses modernen E-Rekrutierungs-Verfahrens zu den einzelnen Prozessen (Durchführung von Online-Rekrutierungsmaßnahmen, Pflege und Auswahl von Bewerbern, Löschen von Bewerbungsdaten) datenschutzrechtliche Hinweise und Empfehlungen gegeben (vgl. Kasten zu Nr. 5.7.3). Nach § 106 Absatz 4 BBG und § 32 Absatz 1 Satz 1 BDSG dürfen hierbei nur solche personenbezogenen Daten erhoben werden, die für die Entscheidung über die Begründung eines Beschäftigungs- bzw. Dienstverhältnisses erforderlich sind.

Meine datenschutzrechtliche Beratung ist noch nicht abgeschlossen. So muss noch geklärt werden, welche Personen oder Kommissionen nach einer ersten Vorauswahl im Rahmen der weiteren Bewerberauswahl unter dem Gesichtspunkt der Erforderlichkeit für eine abschließende Entscheidung auf Bewerberdaten zugreifen müssen bzw. zu beteiligen sind.

Abschließend beraten habe ich das BMVI bereits zur Frage der **Löschung von Bewerbungsdaten** nach Abschluss eines konkreten Bewerbungsverfahrens. Strittig ist hier oft, wie lange Bewerbungsunterlagen und personenbezogene Daten von abgelehnten Bewerbern von der verantwortlichen Stelle noch aufzubewahren sind (z. B. für mögliche Rechtsstreitigkeiten) und wann sie konkret gelöscht werden müssen (vgl. 22. TB Nr. 11.3). Argumente aus der Praxis haben mich dazu bewogen, die Frage der Aufbewahrungsdauer dieser Unterlagen neu zu bewerten:

Unterlagen abgelehnter Bewerber sollten spätestens nach einer Frist von sechs Monaten entweder an den Bewerber zurückgegeben oder - soweit die Daten elektronisch eingereicht wurden - gelöscht werden. Um damit tatsächlich Rechtssicherheit zu erreichen, sollte diese Frist mit Absendung der Ablehnungsschreiben beginnen. Nur wenn innerhalb dieses Zeitraums Ansprüche gegenüber dem Arbeitgeber erhoben werden, schließt sich die dreimonatige Frist des § 61b Absatz 1 Arbeitsgerichtsgesetz an, die mit der schriftlichen Geltendmachung des Anspruchs gegenüber dem Arbeitgeber nach § 15 Absatz 4 Satz 1 Allgemeines Gleichbehandlungsgesetz beginnt.

Entscheidend für die Länge der Frist ist die Frage, innerhalb welchen Zeitraums nach Zugang eines Ablehnungsschreibens ein abgelehnter Bewerber noch Kenntnis von einer möglichen Diskriminierung erhalten wird. Ich halte einen Zeitraum von bis zu sechs Monaten für realistisch. In Einzelfällen kann ein Bewerber zwar durchaus sogar noch nach mehreren Jahren von einer Diskriminierung erfahren. Dies dürften aber tatsächlich rare Zufallsfälle sein, die außerhalb der allgemeinen Lebenswahrscheinlichkeit liegen. In diesen Extremfällen muss dem allgemeinen Persönlichkeitsrecht des Betroffenen Vorrang vor dem Rechtsverteidigungsinteresse des Arbeitgebers eingeräumt werden.

Kasten zu Nr. 5.7.3

Elektronische Bewerbungsverfahren - Auswahl wichtiger Datenschutzaspekte

- Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3a BDSG)
- Einrichtung unterschiedlicher Rollen in der Personalbeschaffung
- Bewerbungsunterlagen: Zugriffsrechte und Auswertungsmöglichkeiten in den unterschiedlichen Phasen des Verfahrens
- Festlegung von Verantwortlichkeiten bei zentraler und dezentraler Personalbeschaffung
- Auftragsdatenverarbeitung (§ 11 BDSG)
- Technische und organisatorische Maßnahmen nach § 9 BDSG und dessen Anlage
- Authentifizierung von Bewerbern
- sichere Kommunikation zwischen Bewerber und verantwortlicher Stelle
- Transparenz über das Verfahren und Aufklärung/Information der Bewerber vor einer Bewerbungsentscheidung/Registrierung im System
- Inhalt von Datenschutzerklärungen
- Einwilligung (§ 4a BDSG) und Frage der Freiwilligkeit, z. B. im Hinblick auf zusätzliche Bewerbungsunterlagen/-angaben
- Auskunfts- und Einsichtsrechte der Betroffenen
- Unterbrechung, Abbruch einer Online-Bewerbung und Löschen von Bewerberdaten/Kandidatenprofil
- Beteiligung und Kontrollrechte des zuständigen Beauftragten für den Datenschutz

5.7.4 Immer wieder Verstöße gegen das Personalaktenrecht

Bei mehreren Kontrollbesuchen musste ich Verstöße gegen das Personalaktenrecht, aber auch den Umgang mit Gleitzeitdaten der Beschäftigten beanstanden.

Im Anschluss an drei, in den letzten Jahren im Geschäftsbereich des BMVI durchgeführte Beratungs- und Kontrollbesuche (vgl. 23. TB Nr. 12.4 sowie 24. TB Nr. 13.4) habe ich im Berichtszeitraum Besuche bei den Wasserschifffahrtsämtern (WSA) Freiburg und Nürnberg durchgeführt. Mein Augenmerk galt besonders der Umset-

zung der Erlasse des BMVI zum zulässigen - insbesondere automatisierten - Umgang mit Beschäftigtendaten. Dabei habe ich geprüft, ob neben dem im Geschäftsbereich eingesetzten einheitlichen Personalverwaltungssystem PVS BMVI (PVS), bei dessen Einführung ich das BMVI umfassend beraten hatte, weitere Verfahren verwendet werden.

Kontrolle im Wasser- und Schifffahrtsamt Freiburg

Im WSA Freiburg fand ich erneut in großer Anzahl weitere unzulässige Verfahren der automatisierten Personaldatenverarbeitung. In der Regel waren dort Personal- und Personalaktendaten - auch besondere Arten personenbezogener Daten im Sinne des § 3 Absatz 9 BDSG (z. B. Gesundheitsangaben) - gespeichert, die nach den gesetzlichen Aufbewahrungs-/Löschungsregelungen längst hätten gelöscht sein müssen. Im Ergebnis wurde so das im PVS grundsätzlich gewährleistete gesetzesmäßige Löschen von Personal- und Personalaktendaten durch diesen automatisierten Umgang mit Beschäftigtendaten außerhalb von PVS „unterlaufen".

Dass die Behörden auch beim manuellen Umgang mit Beschäftigtendaten die gesetzlichen Vorgaben, insbesondere der §§ 106 ff. BBG sowie des § 32 BDSG, umzusetzen haben, ist vom BMVI auch im Erlasswege geregelt. Dennoch ergab meine stichprobenartige Prüfung in sehr großem Umfang unzulässig gespeicherte Personal- und Personalaktendaten in Papierform - auch Gesundheitsangaben. Dazu gehörten z. B. mehr als 150 alte „Personalnebenakten", Bezügeabrechnungen bis in das Jahr 2000 und Personal-Stammblätter aus den Jahren 1992 und 1994. Alte Listen betrafen auch ausgeschiedene und teilweise bereits verstorbene Beschäftigte des Amtes. Deren Geburtsdaten reichten bis zum Jahr 1884! Diese unzulässige Speicherung sensibler Personal- und Personalaktendaten im WSA Freiburg in automatisierter und in manueller Form habe ich gegenüber dem BMVI als Verstoß gegen die Regelungen der §§ 106 ff. BBG bzw. gegen § 12 Absatz 4 i. V. m. mit § 32 Absatz 1 BDSG beanstandet. Das BMVI hat meine Kontrollfeststellungen aufgegriffen und in entsprechenden Erlassen umgesetzt.

Kontrolle im Wasser- und Schifffahrtsamt Nürnberg

Auch im WSA Nürnberg waren in Verfahren der automatisierten Personaldatenverarbeitung neben dem PVS zahlreiche alte Personal- und Personalaktendaten gespeichert, die für die Aufgabenerfüllung nicht mehr erforderlich waren und nach den gesetzlichen Aufbewahrungsvorschriften längst hätten gelöscht sein müssen. Auch diesen unzulässigen Umgang mit Personal- und Personalaktendaten im WSA Nürnberg habe ich gegenüber dem BMVI als Verstoß gegen die oben genannten Vorschriften beanstandet.

Weiter habe ich umfassende Verstöße im Umgang mit Beschäftigtendaten bei der automatisierten Gleitzeitverarbeitung festgestellt. So waren z. B. - obwohl der behördliche Datenschutzbeauftragte des Amtes gegenüber den Verantwortlichen schriftlich deren gesetzmäßige Löschung angemahnt hatte - noch alle Zeitbuchungen der Beschäftigten der letzten zwei Jahre gespeichert. Dies steht mit den entsprechenden Regelungen der Verordnung über die Arbeitszeit der Beamtinnen und Beamten des Bundes (Arbeitszeitverordnung - AZV) vom 23. Februar 2006 ebenso wenig im Einklang wie mit dem maßgeblichen Erlass des BMVI. Unzulässig war auch die von mir erneut festgestellte Praxis, täglich eine automatisierte Abwesenheitsliste mit elektronischen Zugriffsmöglichkeiten für alle Beschäftigten des Amtes zu erstellen. Als unzulässige Verhaltenskontrolle habe ich ferner bewertet, dass man an der Pforte des Amtes über ein „Ampelsystem" jederzeit elektronisch erkennen und kontrollieren konnte, welcher Beschäftigte sich wie aktuell im Gleitzeitsystem ein- oder ausgebucht hatte. Die festgestellten Mängel im Umgang mit Beschäftigtendaten bei der Durchführung der Gleitenden Arbeitszeit habe ich gegenüber dem BMVI als Verstoß gegen die Regelungen des § 12 Absatz 4 i. V. m. § 32 Absatz 1 BDSG und § 7 Absatz 7 und 8 AZV beanstandet.

Einen schweren datenschutzrechtlichen Verstoß stellte ich zudem am Arbeitsplatz eines Sachbereichsleiters des WSA Nürnberg fest. Auf seinem Rechner waren noch alle bereits eröffneten und zu den Personalakten genommenen vollständigen Beurteilungen der letzten zehn Jahre - auch noch aus der Zeit seines Vorgängers - gespei-

chert. Diesen Verstoß gegen die Regelungen der §§ 106 ff. BBG, insbesondere gegen § 106 Absätze 1 und 2 BBG, habe ich ebenfalls gegenüber dem BMVI beanstandet.

Im Ergebnis bleibt festzustellen, dass das BMVI zwar meine Kontrollfeststellungen aus den letzten Jahren vollständig aufgegriffen und entsprechende ergänzende Regelungen und datenschutzrechtliche Vorgaben für seinen Geschäftsbereich herausgegeben hat. Die verantwortlichen Stellen setzten diese im Praxisbetrieb jedoch nur sehr unzureichend um. Ich werde mich weiterhin für einen gesetzeskonformen Umgang mit Beschäftigtendaten im Geschäftsbereich des BMVI einsetzen und dies auch stichprobenartig vor Ort kontrollieren.

Kontrolle bei der Bundesfinanzdirektion Nord

Ein Beratungs- und Kontrollbesuch bei der Bundesfinanzdirektion (BFD) Nord zum Umgang mit Personal- und Personalaktendaten der Beschäftigten stand insbesondere im Zusammenhang mit dem dort in Teilkomponenten eingesetzten neuen „einheitlichen Personalverwaltungssystem in der Bundesfinanzverwaltung (PVS)“, bei dessen Entwicklung ich das BMF datenschutzrechtlich beraten habe. Wie ich dabei feststellen musste, erfolgte auf Grundlage eines Erlasses des BMF zur Durchführung der „Gleitenden Arbeitszeit“ in einer Abteilung der BFD Nord zu Testzwecken eine Parallelerhebung und -verarbeitung von Beschäftigtendaten durch das (ursprüngliche) automatisierte Gleitzeitsystem und zusätzlich auch über PVS (Komponente Zeitwirtschaft). Ein „Testbetrieb“ mit Echtdaten ist unzulässig, er wurde ohne Rechtsgrundlage für einen unzulässigen Zweck durchgeführt. Die Vertreter des BMF haben noch vor Ort zugesagt, diesen Parallelbetrieb umgehend einzustellen, auf ein Testen mit Echtdaten in PVS zu verzichten, die unzulässigen Beschäftigtendaten in PVS zu löschen und ausschließlich das bisherige System zu verwenden.

Die stichprobenartige Prüfung des Praxisbetriebs der bisher in der BFD Nord eingesetzten Teilkomponenten von PVS ergab grundsätzlich eine positive und datenschutzfreundliche Umsetzung. An verschiedenen Arbeitsplätzen habe ich jedoch in großer Anzahl alte, unzulässige Dokumente und Excel-Listen außerhalb von PVS festgestellt. Diese wurden ebenfalls für die Zwecke der Personalverwaltung/Personalwirtschaft - für die in der Bundesfinanzverwaltung gerade PVS eingeführt und entwickelt worden ist - betrieben. Für solche automatisierten Verarbeitungen von Personal- und Personalaktendaten greifen nicht die umfassenden, aus datenschutzrechtlicher Sicht positiven und einschränkenden Regelungen zu PVS. In diesem Zusammenhang habe ich auch einen unzureichenden Zugriffsschutz und somit einen nicht gesetzeskonformen Zugang zu Personalaktendaten bemängelt und empfohlen, die Zugriffsrechte im Personalbereich so einzuschränken, dass sie den Vorgaben des § 107 Absatz 1 BBG entsprechen.

Auch beim manuellen Umgang mit Beschäftigtendaten habe ich Personal- und Personalaktendaten festgestellt, die längst hätten gelöscht sein müssen und deren (weitere) Speicherung ohne Rechtsgrundlage unzulässig war. Erschwerend kam hinzu, dass ein Teil dieser Unterlagen in einem unverschlossenen Schrank eines Archivraumes abgelegt war, zu dem auch Beschäftigte der BFD Nord außerhalb des Personalbereiches Zugang hatten. Bezogen auf die gespeicherten Personalaktendaten stellt dies einen Verstoß gegen § 107 Absatz 1 BBG dar. Die BFD Nord hat noch während des Besuches erste notwendige Maßnahmen für einen datenschutzgerechten Umgang mit diesen manuellen Beschäftigtendaten eingeleitet und mir deren Umsetzung anschließend schriftlich bestätigt. Die unzulässige Speicherung von Personalaktendaten sowie weiteren Personaldaten und den mangelnden Zugriffsschutz von Personalaktendaten - sowohl in automatisierter Form, als auch in manueller Form - habe ich gegenüber dem BMF als Verstoß gegen die Regelungen in den §§ 106 ff. BBG, insbesondere § 107 Absatz 1 und § 113 Absatz 2 BBG sowie gegen § 12 Absatz 4 i. V. m. § 32 Absatz 1 BDSG beanstandet.

5.7.5 Personalunterlagen im Hausmüll - immer wieder der Faktor Mensch

Bei der Einhaltung datenschutzrechtlicher Regelungen und Weisungen kommt es auf den einzelnen Beschäftigten an.

Im Berichtszeitraum informierte mich ein Berliner Bürger, er habe in einem frei zugänglichen Papiermüllcontainer seiner Wohnanlage einen Stapel unterschiedlichster personenbezogener Dokumente neueren Datums eines Sozialversicherungsträgers des Bundes entdeckt, offenbar interne Personalvorgänge. Bei einer umgehend durchgeführten Kontrolle durch meine Mitarbeiter konnten zwar keine solchen Unterlagen (mehr) entdeckt werden. Am darauf folgenden Tag gab der Bürger jedoch einen von ihm zwischenzeitlich sichergestellten Teil dieser sensiblen Unterlagen persönlich bei mir ab.

Nach einer ersten Prüfung habe ich den Sozialleistungsträger umgehend über diesen Sachverhalt und die von mir dabei festgestellten Datenschutzverstöße im Umgang mit vertraulich zu behandelnden Personal- und Personalaktendaten von Beschäftigten, aber auch dem Sozialgeheimnis unterliegenden Sozialdaten von Versicherten unterrichtet. Die von mir in Verwahrung genommenen Unterlagen habe ich dann gemeinsam mit Vertretern der verantwortlichen Stelle in Augenschein genommen und ihnen zur umgehenden Prüfung, weiteren Veranlassung und der Bitte um Stellungnahme übergeben.

Wie mir der Sozialleistungsträger dann schriftlich bestätigte, handelte es sich bei den sichergestellten Unterlagen überwiegend um Personal- und Personalaktendaten - u. a. auch um „besondere Arten personenbezogener Daten“ (wie Schwerbehinderteneigenschaft oder Grad der Behinderung) - eigener Beschäftigter, aber vereinzelt auch um Sozialdaten von Versicherten. Die verantwortliche Stelle hat dabei eingeräumt, dass diese Unterlagen von der Leiterin eines Teams in ihrem privaten Umfeld in einer frei zugänglichen Altpapiertonne „unsachgemäß“ entsorgt worden waren und so Dritten unbefugt zur Kenntnis gelangt sind. Ferner hat sie mir detailliert dargelegt, gegen welche bestehenden behördeninternen datenschutzrechtlichen Regelungen die Vorgesetzte im Umgang mit diesen personenbezogenen Daten - dies betrifft nicht nur die Entsorgung der Unterlagen - verstoßen hat und welche aktuellen Maßnahmen sie behördenintern aufgrund dieses Vorfalls veranlasst habe, um solche Datenschutzverstöße in Zukunft zu vermeiden. Bei dem Vorfall handelt es sich um einen Verstoß gegen die Regelungen der §§ 106 ff. BBG bzw. gegen § 12 Absatz 4 i. V. m. § 32 Absatz 1 BDSG sowie um einen unzulässigen Umgang mit Sozialdaten von Versicherten dieses Sozialleistungsträgers (§ 35 Abs. 1 SGB I). Da ich jedoch in diesem Einzelfall ein der verantwortlichen Stelle zurechenbares Organisationsversagen nicht feststellen konnte und aufgrund der sofort eingeleiteten Maßnahmen habe ich nach § 25 Absatz 2 BDSG davon absehen können, den eingeräumten unzulässigen Umgang mit Personal- und Personalaktendaten sowie Sozialdaten förmlich zu beanstanden.

Im Ergebnis zeigt dieser Fall einmal mehr, dass auch die besten internen Regelungen zum datenschutzgerechten Umgang mit personenbezogenen Daten in der Praxis nicht sicherstellen, dass diese auch eingehalten werden. Schwachpunkt ist der Faktor Mensch, der es - sei es aus Bequemlichkeit oder oftmals auch aus Unkenntnis - an Sensibilität und Datenschutzbewusstsein mangeln lässt. Es ist deshalb wichtig, die Beschäftigten in den öffentlichen Stellen des Bundes nicht nur regelmäßig in Datenschutzfragen zu sensibilisieren, zu schulen und immer wieder auf die maßgeblichen Datenschutzvorschriften und behördeninterne Regelungen hinzuweisen, sondern auch, deren Einhaltung in der Praxis stichprobenartig zu kontrollieren.

5.8 Nach dem Zensus ist vor dem Zensus

Der Zensus 2011 hat mit der Veröffentlichung der Zensusergebnisse 2014 seinen Abschluss gefunden. Nun wirft der kommende Zensus 2021 seine Schatten voraus.

Aus Sicht des Datenschutzes ist der Zensus 2011 positiv verlaufen. Das liegt sicher insgesamt auch an der gelungenen Informationspolitik des Statistischen Bundesamts, das für die Bürgerinnen und Bürger ein eigenes Zensusportal im Internet eingerichtet hatte. Der Berichtszeitraum war geprägt durch die Auswertung der Befragungen und Registerauswertungen sowie die Veröffentlichung der aufbereiteten Ergebnisse. Zwar wehren sich in einigen Bundesländern Kommunen gerichtlich gegen die auf Grundlage der Zensusdaten festgestellten Einwohnerzahlen, dies ändert aber nichts am datenschutzrechtlich positiven Fazit. So konnte ich mich davon überzeugen, dass das Statistische Bundesamt innerhalb der gesetzlich festgelegten Frist die dort noch vorhandenen

Hilfsmerkmale - etwa Namens- und Adressdaten der Befragten - aus den Datenbeständen gelöscht hat. Auch das Anschriften- und Gebäuderegister, das ein wichtiger methodischer Baustein des Zensus 2011 war, wird innerhalb der gesetzlich vorgesehenen Frist gelöscht werden. Ich erwarte nun den angekündigten Evaluationsbericht zum Zensus 2011 und die Schlussfolgerungen, die das Statistische Bundesamt und das zuständige Bundesministerium des Innern hieraus für den Zensus 2021 ziehen. Die Vorbereitungen hierfür werden im Laufe des Jahres 2015 beginnen, um frühzeitig die erforderlichen gesetzlichen Grundlagen zu schaffen. Ich gehe davon aus, dass ich auch diesmal wieder mit meinem Rat eingebunden werde und eine gute Arbeitsbeziehung zum Statistischen Bundesamt auch die Begleitung der Vorarbeiten für den Zensus 2021 prägen wird.

5.9 Die BIT-Migration des Statistischen Bundesamts - ein Fall für eine Beanstandung

Der IT-Betrieb der Behörden im Geschäftsbereich des Bundesministeriums des Innern wird schrittweise auf die beim Bundesverwaltungsamt angesiedelte Bundesstelle für Informationstechnik (BIT) übertragen. Dies hat beim Statistischen Bundesamt mangels ausreichenden Datenschutzes zu einer formellen Beanstandung geführt.

Der schrittweise Übergang des IT-Betriebs der Behörden im Geschäftsbereich des BMI auf das Bundesverwaltungsamt ist in vielerlei Hinsicht eine Mammutaufgabe. Dabei ist für mich von großer Bedeutung, dass dieser Übergang datenschutzrechtlich hinreichend begleitet wird. Insbesondere müssen dem faktischen Übergang der IT-Verfahren auf die BIT entsprechende Vereinbarungen, d. h. sogenannte Service Level Agreements zur vertraglichen Sicherstellung von Datenschutz und Datensicherheit, zugrunde liegen. Gerade im Bereich des Statistischen Bundesamts gewinnen diese Anforderungen besonderes Gewicht. Die Datenverarbeitung und damit der IT-Betrieb dieser Behörde unterliegt nämlich aufgrund des Gebots der Abschottung statistischer Daten und des Statistikgeheimnisses besonderen Anforderungen. Deren Erfüllung ist ein Grundpfeiler für das Vertrauen der Bevölkerung in die amtliche Statistik. Ich habe den Prozess des Übergangs lange begleitet und immer wieder auf die datenschutzrechtlichen Erfordernisse hingewiesen (vgl. 24. TB Nr. 4.3). Anfang 2013 ging der IT-Betrieb des Statistischen Bundesamts faktisch auf die BIT über. Als im Herbst 2013 die von mir angemahnten datenschutzrechtlichen Regelwerke immer noch nicht vorlagen, sah ich mich gezwungen, gegenüber dem Bundesministerium des Innern eine formelle Beanstandung auszusprechen. Daraufhin kam es im Laufe des Jahres 2014 zu Gesprächen mit dem Ministerium, dem Statistischen Bundesamt und der BIT. Ich erkenne das ernsthafte Bemühen aller Beteiligten an, substantielle Fortschritte zu machen und das lang Versäumte nachzuholen. Ich werde aber weiter kritisch prüfen, ob die vereinbarten Meilensteine erreicht werden. Insbesondere beabsichtige ich, die Umsetzung der notwendigen technisch-organisatorischen Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit beim Statistischen Bundesamt vor Ort zu prüfen. Ich hoffe in meinem nächsten Tätigkeitsbericht die erfolgreiche Beendigung des Beanstandungsverfahrens mitteilen zu können. Die intensive datenschutzrechtliche Begleitung dieses Projekts ist auch deswegen von großer Bedeutung, weil die Bundesregierung großflächige Umstrukturierungen und Effizienzsteigerungen im Bereich der IT nicht auf den Geschäftsbereich des BMI beschränken wird. Das Vorgehen, wie ich es am Beispiel des Statistischen Bundesamts beobachten musste, darf keine Blaupause für andere Behörden sein.

5.10 Projektgruppe „eID - Strategie für E-Government“ des IT-Planungsrats

Die Projektgruppe hat ihre Arbeit aufgenommen und erste Ergebnisse vorgelegt.

Im Rahmen der E-Government-Strategie des Bundes und der Länder wurde eine Projektgruppe gegründet, die Eckpunkte für ein flächendeckendes Angebot geeigneter elektronischer Verfahren erarbeiten soll, um Identität, Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit (Vertrauensdienste) bei der Abwicklung von E-Government-Dienstleistungen zu gewährleisten.

Die Projektgruppe hat im Berichtszeitraum ein Eckpunktepapier vorgelegt, das im Oktober 2012 durch den IT-Planungsrat angenommen wurde. Auf dieser Basis wurde dann ein Maßnahmenplan erarbeitet. Dieser sieht die Veröffentlichung von Handreichungen und Empfehlungen, die Anpassung von Rechtsvorschriften sowie die

Konzeption sogenannter Bürgerkonten vor. An den Sitzungen der Projektgruppe habe ich teilgenommen und mich für den Datenschutz eingesetzt.

Insbesondere die Maßnahme zu Mindeststandards für den Zugang zu Bürgerkonten begrüße ich. Bürgerkonten sind elektronische Portale, über die der Bürger seine Identifizierungsdaten, wie sie auf dem Chip des Personalausweises vorhanden sind, an Stellen der öffentlichen Verwaltung zur Verarbeitung für einzelne Verfahren weiterleiten kann. Damit wird eine einheitliche Basis für eine sichere sowie datenschutzgerechte Umsetzung von Vertrauensdiensten gelegt. Das BSI hat in Umsetzung dieser Maßnahme eine zweiteilige Richtlinie „Elektronische Identitäten und Vertrauensdienste im E-Government" herausgegeben, die für verschiedene Schutzbedarfsklassen die angemessenen technischen Mittel zur Gewährleistung der notwendigen IT-Sicherheit bei der Gestaltung von Vertrauensdiensten beschreibt. Dabei bilden Bürgerkonten in Bürgerportalen das Leitbild. Die Richtlinie schließt dabei nicht aus, dass entsprechende Portale etwa in kommunalen Rechenzentren betrieben werden, die als Dienstleister für die Behörden arbeiten. Ich habe in diesem Zusammenhang auf § 21 Absatz 1 Personalausweisgesetz hingewiesen, der für die Nutzung der elektronischen Identifikationsfunktion des neuen Personalausweises enge Vorgaben macht. Dabei begrüße ich die Feststellung, dass die Identifizierung einer Person ein flüchtiger Vorgang ist. Dies muss sich auch in der verwendeten Technologie widerspiegeln. Folglich dürfen Bürgerkonten, die ausschließlich für die Identifizierung genutzt werden, grundsätzlich nur als temporäre Konten angelegt sein.

Mit Blick auf die Schutzbedarfsklassen wurde neben einer Schutzbedarfsklasse „hoch" auch eine Schutzbedarfsklasse „hoch+" eingeführt, die sich von der Schutzbedarfsklasse „hoch" allein durch gesetzliche Erfordernisse bei der Identitätsfeststellung unterscheidet und dementsprechend zwingend die Nutzung des neuen Personalausweises, von De-Mail oder den Einsatz qualifizierter elektronischer Signaturen erfordert. Die eigentlichen Bedrohungsszenarien bleiben für beide Schutzbedarfsklassen gleich. Diese Kategorisierung wird aus meiner Sicht noch zu Interpretationsproblemen führen, weil sich das Unterscheidungskriterium „gesetzliche Anforderung" nicht auf Schutzbedarfsanforderungen bezieht, sondern eine „von außen" kommende zusätzliche Anforderung betrifft.

Mit dem Ziel weiterer Standardisierung hat die Projektgruppe überdies auch Eckpunkte für ein interoperables Identitätsmanagement erarbeitet, mit denen zugleich die Grundzüge für Bürgerkonten in Bürgerportalen skizziert werden. Weil Bürgerportale üblicherweise vor allem anonym nutzbare Informationsangebote bereithalten, wurde dies entgegen der eigentlichen Zielstellung des Papiers ebenfalls beschrieben. Ich begrüße es sehr, dass die Möglichkeit zur vollständig anonymen Nutzung von Angeboten ausdrücklich berücksichtigt wurde. Skeptisch bin ich hingegen mit Blick auf das in dem Eckpunktepapier vorgesehene Postfach zur Kommunikation zwischen Behörde und Bürgerkontoinhabern. Damit wird neben De-Mail eine weitere Kommunikationsmöglichkeit geschaffen, die weiteren rechtlichen Regelungsbedarf nach sich zieht, wenn z. B. über diesen Weg zugegangene Bescheide auch im rechtlichen Sinne als zugestellt gelten sollen.

Die Projektgruppe wird sich auch damit beschäftigen, welche Verwaltungsdienstleistungen welcher Schutzbedarfsklasse zuzurechnen sind. Erfreulicherweise beschreibt die Technische Richtlinie „Elektronische Identitäten und Vertrauensdienste im E-Government" auch für die Schutzbedarfsklassen „normal" und „hoch" Mindeststandards zur Gewährleistung der IT-Sicherheit, d. h. Integrität, Unveränderbarkeit und Vertraulichkeit. Im Übrigen sollte für jede Kommunikation mit einer Behörde auch die Möglichkeit einer Ende-zu-Ende-Verschlüsselung angeboten werden.

5.11 De-Mail-Zertifizierung - erst neu, dann bewährt

Die datenschutzrechtliche Zertifizierung von De-Mail-Diensteanbietern gehört seit 2011 zu meinen Aufgaben. Mittlerweile wurden mehrere Verfahren erfolgreich durchgeführt.

Nach dem De-Mail-Gesetz vom 28. April 2011 bin ich für die datenschutzrechtliche Zertifizierung der Anbieter von De-Mail-Diensten zuständig. Über meine ersten Erfahrungen in diesem für mich neuen Aufgabengebiet hatte ich bereits im letzten Tätigkeitsbericht berichtet (vgl. 24. TB Nr. 3.2.4). Nachdem ich seinerzeit bereits der Mentana Claimsoft GmbH, der T-Systems International GmbH und der T-Deutschland GmbH entsprechende Zertifikate erteilt hatte, ist im Jahr 2013 noch die 1&1 De-Mail GmbH dazu gekommen. Alle vier Dienstleister haben seit ihrer erstmaligen Zertifizierung mehrere Re-Zertifizierungen zum Datenschutz durchlaufen, weil wesentliche Änderungen im Betrieb eingetreten sind. Diese Änderungen betrafen vor allem die Einbindung Dritter in die zur Kundenidentifizierung eingerichteten Verfahren. Das De-Mail-Gesetz erlaubt es den De-Mail-Diensteanbietern, sich Dritter zur Erfüllung ihrer gesetzlichen Pflichten zu bedienen. Diese müssen dann aber ihrerseits die Anforderungen des De-Mail-Gesetzes erfüllen. Da die sorgfältige Identifizierung der Kunden einen wesentlichen Bestandteil von De-Mail darstellt, müssen die Anbieter nachweisen, dass auch die Identifizierung durch Dritte den datenschutzrechtlichen Anforderungen genügt.

Der Prozess der Zertifizierung war für meine Dienststelle eine völlig neue Aufgabe, zu der keinerlei Erfahrungen vorlagen. Auch für die Anbieter aus dem Bereich der Telekommunikation war dieses Verfahren Neuland. Gleichwohl konnten die einzelnen Zertifizierungsverfahren insgesamt zeitnah und erfolgreich abgeschlossen werden. Aufgrund der dabei gewonnenen Erfahrungen und nach entsprechenden Rückmeldungen der Anbieter habe ich meinen Kriterienkatalog, der Anhaltspunkte für die datenschutzrechtliche Prüfung geben soll, mehrfach überarbeitet. Mittlerweile liegt er in der Version 1.4 vor und ist auf meiner Internetseite unter www.datenschutz.bund.de abrufbar. Er ist sowohl auf meiner Website als auch im elektronischen Bundesanzeiger veröffentlicht, so dass sich alle De-Mail-Nutzer über die von mir gesetzten Datenschutzstandards informieren können. Bislang hat sich der Kriterienkatalog in der Praxis bewährt. Wie sich aus der sehr geringen Anzahl eingegangener Eingaben ergibt, arbeiten die Anbieter auch in der Praxis datenschutzkonform.

5.12 Das elektronische Passfoto

Passfotos können auch elektronisch an Personalausweisbehörden geschickt werden. Das BSI hat hierzu die Technische Richtlinie „Elektronische Bildübermittlung unter Nutzung von De-Mail“ erarbeitet, die datenschutzrechtlichen Anforderungen genügt.

Bürgerinnen und Bürger, die einen neuen Personalausweis beantragen, bringen bislang ihr Foto ausgedruckt mit ins Amt. Nach der Personalausweisverordnung ist es aber auch möglich, das Foto durch Dritte elektronisch verschlüsselt und signiert zu übermitteln. Das BSI hat hierzu eine Technische Richtlinie (TR) erarbeitet. Dabei kam es nach der Analyse verschiedener elektronischer Übermittlungsmöglichkeiten zu dem Ergebnis, eine Versendung mittels De-Mail stelle die erfolgversprechendste Lösung dar. Zur Vorbereitung eines Pilotprojektes mit Personalausweisbehörden, Fotografen, De-Mail-Diensteanbietern und Verfahrensentwicklern, das im Frühjahr 2014 durchgeführt worden ist, hat mich das BSI vorab um datenschutzrechtliche Beratung gebeten.

Das Verfahren sieht wie folgt aus: Der Fotograf übermittelt mit Einwilligung des Betroffenen das digitale Foto mittels De-Mail an die Personalausweisbehörde. Erscheint dieser dort, um den Ausweis zu beantragen, ist die Behörde anhand einer Bildkennung in der Lage, das Foto dem Antragsteller zuzuordnen. Der Sachbearbeiter in der Behörde kann dann das Foto direkt elektronisch in den Antrag aufnehmen und muss es nicht mehr wie bisher scannen. Dies erhöht die Qualität der Fotos und verringert die Fehlerquote beim Erstellen der Ausweise.

Hierfür musste zunächst eine datenschutzkonforme Einwilligungserklärung entworfen werden, da das Versenden des Fotos vom Fotografen an die Ausweisbehörde eine Datenverarbeitung darstellt, die einer entsprechenden Ermächtigung bedarf. Daneben stellten sich datenschutzrechtliche Fragen bei der Bezeichnung der Fotodateien und deren Speicherdauer. Da die Dateien vom Fotografen mittels De-Mail direkt an die Behörde gesendet werden, müssen die Dateien so benannt werden, dass die Zuordnung des Fotos zum Antragsteller in der Behörde ohne großen Aufwand möglich ist. Auf meine Anregung hin hat sich das BSI dafür entschieden, die Bildkennung aus einem Hashwert über das Foto sowie den Initialen, Geburtstag und Geburtsort des Antragstellers zu

bilden, wobei für die drei letztgenannten Daten alternativ auch jeweils der Ersatzwert „00“ verwendet werden kann. Die Verwendung von personenbezogenen Daten ist damit optional; sie bietet den Vorteil, dass sich der Bürger an diese erinnert, wenn er bei der Behörde nach der Bildkennung gefragt wird. Ich halte diese Vorgehensweise nur dann für akzeptabel, wenn für den Betroffenen klar erkennbar ist, dass er seine personenbezogenen Daten nicht angeben muss und sich für die datenschutzgerechte Variante mit der Dateibezeichnung „00“ entscheiden kann. Da sich nach meinem Kenntnisstand allerdings die Einwilligung nicht ausdrücklich auf den Aspekt der Bildkennung bezieht, bin ich skeptisch, ob aus der „optionalen“ Angabe faktisch nicht doch eine „obligatorische“ wird.

Weiter musste geklärt werden, wie lange die Fotos bei den beteiligten Stellen gespeichert werden dürfen. Ich habe mich für eine Speicherdauer von sechs Wochen sowohl bei der Behörde als auch beim Fotografen sowie eventuell beteiligten Dritten (Betreiber eines entsprechenden Portalsystems, über das der Fotograf die De-Mail versendet) ausgesprochen. Dieser Zeitraum erscheint ausreichend, um dem Bürger Gelegenheit zu geben, nach dem Fotografenbesuch anschließend die Personalausweisbehörde aufzusuchen. Ob die Fotos beim Fotografen ggf. länger gespeichert werden, weil sich der Kunde vorbehält, zu einem späteren Zeitpunkt weitere Abzüge zu kaufen, unterliegt der Absprache zwischen Fotografen und Kunden. Wichtig ist, dass eine vollständige Löschung erfolgt. Das BSI hat sich meiner Einschätzung angeschlossen.

Grundsätzlich ist der Fotograf gegenüber seinem Kunden für die datenschutzgerechte Übermittlung des Passfotos verantwortlich. Diesem gegenüber gibt der Kunde auch seine Einwilligungserklärung ab. Nutzt der Fotograf aber ein „fremdes“ De-Mail-Konto, nämlich das eines Portal-Betreibers (dies könnte z. B. eine Fotografenvereinigung oder ein IT-Dienstleister sein), liegen die Verantwortlichkeiten nicht mehr so klar auf der Hand. Im Ergebnis handelt es sich bei dem Verhältnis zwischen Fotografen und Portalbetreiber wohl um eine Datenverarbeitung im Auftrag nach § 11 BDSG, da die Versendung der De-Mails nach den Vorgaben des Fotografen erfolgt und der Portalbetreiber über die Erbringung dieses Dienstes hinaus kein eigenes Interesse an den Daten oder der Datenverarbeitung hat. Dies bedürfte einer entsprechenden Vereinbarung. An der Ausgestaltung des Verfahrens zur Nutzung des Portalsystems war ich allerdings nicht beteiligt. Darüber hinaus ergibt sie sich nur in Ansätzen aus der Beschreibung in der TR selbst, so dass ich dazu keine Bewertung abgeben kann.

5.13 Datenschutz bei den Sicherheitsbehörden

Auch in diesem Berichtszeitraum hat es wieder kritische Entwicklungen im Bereich der Sicherheitsbehörden gegeben, wie z. B. die Pläne zur Einführung des Polizeilichen Informations- und Analyseverbundes (vgl. Nr. 5.13.2). Bei meinen Kontrollen habe ich u. a. geprüft, wer in welchen Dateien gespeichert wurde (vgl. Nr. 5.13.1, 5.13.3). Hier zeigte sich in der Praxis, wie wichtig der Datenschutz für die Grundrechte der Bürger ist.

5.13.1 Kontrolle der Kriminalakten beim Bundeskriminalamt

Das BKA führt Kriminalakten zu Personen, die polizeilich in Erscheinung getreten sind. Diese Akten habe ich bei einem Beratungs- und Kontrollbesuch vor Ort geprüft.

Kriminalakten dienen der vorbeugenden Gefahrenabwehr und der so genannten Strafverfolgungsvorsorge. Sie dürfen nicht mit den für die Staatsanwaltschaften und das Gericht geführten Strafakten verwechselt werden. Sie sollen der Polizei unter anderem ermöglichen, zu einzelnen Personen Informationen für die Zukunft vorzuhalten und es ihr erleichtern, künftige Kriminalfälle zu lösen. Das BKA legt Kriminalakten aber auch an, um etwa konkrete Anfragen aus dem Ausland zu bearbeiten, etwa wenn eine ausländische Behörde vermutet, ein Verdächtiger halte sich in Deutschland auf. Derzeit führt das BKA ca. 3,6 Mio. eigene Kriminalakten, davon ca. 1 Mio. elektronisch, die übrigen in Papierform. Die Akten werden über die Dateien „Aktennachweis“ (AN) und „Kriminalaktennachweis“ (KAN) verwaltet. Der KAN ist über das polizeiliche Informationssystem (INPOL) bundesweit abrufbar.

Speicherungen, die rein vorsorglich für die Zukunft getroffen werden, unterliegen besonderen Anforderungen. Solche personenbezogenen Daten kann das BKA nicht aufgrund der gesetzlichen Generalklausel speichern, sondern es muss speziellere Vorgaben beachten (vgl. dazu auch 24. TB Nr. 7.4.4). Will es mehr als nur die sog. Grunddaten speichern (insb. Name, Geburtsdatum, Tatzeit, Tatort und Tatvorwurf), muss es auf einer hinreichenden Tatsachengrundlage eine sogenannte Negativprognose aufstellen. Gem. § 8 Absatz 2 BKAG muss es prognostizieren können, wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse bestehe Grund zu der Annahme, dass in Zukunft Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen seien. Daraus ergibt sich: Ein bloßer fortbestehender Verdacht genügt für die Speicherung nicht. Das BKA hat für die Prognose keinen Ermessensspielraum. Deshalb ist sie datenschutzrechtlich und gerichtlich voll nachprüfbar.

Die Negativprognose und die ihr zugrunde liegenden Tatsachen müssen dokumentiert werden. Für die von mir eingesehenen Kriminalakten fehlte jedoch eine solche Dokumentation. Die eingesehenen Kriminalakten enthalten keine Dokumentation darüber, auf welcher Rechtsgrundlage die jeweils verantwortliche Organisationseinheit die Speicherung gestützt hatte und aus welchen tatsächlichen Gründen diese erfolgte. Die Gründe für die Speicherung konnten zwar im Gespräch mit Hilfe des Aktenrückhalts nachvollziehbar dargelegt werden. Die fehlende Dokumentation erschwert aber gleichwohl die datenschutzrechtliche Bewertung. Unabhängig von den geprüften Einzelfällen erhöht sie das Risiko, dass eine Kriminalakte aufgrund fehlerhafter rechtlicher Einschätzungen angelegt wird. Daher sehe ich strukturellen Verbesserungsbedarf.

Neben der Strafverfolgungsvorsorge existiert eine weitere Funktion von Kriminalakten: Unterstützende Ermittlungen des BKA beginnen regelmäßig damit, dass es Meldungen über Sachverhalte erhält, denen es als Zentralstelle des Bundes mit einer konkreten Sachbearbeitung nachgehen muss, ohne selbst die Ermittlungen zu führen. Dies betrifft etwa Fälle, in denen eine ausländische Polizeibehörde über eine geplante Straftat berichtet oder darum bittet, dass die Polizeibehörden des Bundes und der Länder sie bei konkreten Ermittlungen unterstützen. Eine Speicherung muss das BKA in solchen Fällen in der Regel auf die Generalklausel des BKAG zur Datenspeicherung stützen, um den Vorgang abarbeiten zu können (§ 7 Abs. 1 BKAG). Anfragen aus dem Ausland sind oft wenig substantiiert. In diesem Fall bieten sie keinen Spielraum für längerfristige Speicherungen. Zudem bietet die Generalklausel keine Grundlage für Speicherungen zur Strafverfolgungsvorsorge (vgl. 24. TB Nr. 7.4.4). Deshalb muss das BKA in diesen Fällen kurze Prüffristen vergeben. Der Grundsatz der Verhältnismäßigkeit gebietet es darüber hinaus, Daten zu Personen, die selbst keinen Anlass für eine Speicherung gegeben haben, nur mit größter Zurückhaltung zu speichern. Dies betrifft insbesondere Zeugen, Opfer, aber auch Kontakt- und Begleitpersonen, Hinweisgeber etc. Unzulässige Speicherungen habe ich in diesem Zusammenhang aber nicht vorgefunden.

Im Ergebnis habe ich daher insbesondere zwei Verbesserungen gefordert: Aufgrund der verschiedenen Fallgestaltungen sollte das BKA zu jeder Kriminalakte zum einen dokumentieren, auf welcher Rechtsgrundlage sie angelegt wird. Davon hängt letztlich ab, welche Voraussetzungen gelten. Für die Vorsorgespeicherung gelten die strengeren inhaltlichen Vorgaben, für die Speicherung zur Einzelfallbearbeitung als Zentralstelle gelten kürzere Fristen. Ist die Rechtsgrundlage und der Zweck der Speicherung abgesteckt, so ist ggf. eine Negativprognose zu dokumentieren. Dazu sollte bereits in den Dateien „AN“ und „KAN“ technisch eine zwingende Eingabe der Rechtsgrundlage und der Negativprognose vorgesehen sein, ohne die das Anlegen einer Akte nicht möglich ist.

Eine Antwort des BKA zu meinem Bericht liegt noch nicht vor.

5.13.2 PIAV - Polizeilicher Informations- und Analyseverbund

Das BKA wird in seiner Funktion als Zentralstelle weiter gestärkt, seine polizeiliche Datenverarbeitung wächst. Große Systeme führen zwangsläufig zu Fragen, die die Belastbarkeit der bisherigen rechtlichen Regelungen ausreizen. Wie der geplante Polizeiliche Informations- und Analyseverbund (PIAV).

Bereits in den vergangenen Jahren habe ich über tiefgreifende Veränderungen der Datenverarbeitung beim BKA und den damit zusammenhängenden datenschutzrechtlichen Problemen des in der Entwicklung befindlichen PIAV berichtet (24. TB Nr. 7.4.5, 23. TB Nr. 7.2.1 m. w. N.).

Eine gemeinsame Arbeitsgruppe von Mitarbeitern meiner Dienststelle und einiger Landesbeauftragter für Datenschutz hat mit dem BKA und dem BMI das geplante System weiter erörtert.

Es konnten in den folgenden Punkten Klarstellungen erreicht werden:

- Wie das BKA und das BMI mir versichert haben, sollen im PIAV keine Analyse- und Recherchefunktionen enthalten sein. Insbesondere solle es nicht als Big-Data-Anwendung ausgestaltet werden. Gleichwohl sieht das BKA strategische kriminalpolizeiliche Auswertungen und Analysen als notwendig an. Deshalb werde ich weiter verfolgen, welche Funktionalitäten PIAV erhält.

- Alle im PIAV gespeicherten Personen müssen die Voraussetzungen des § 8 BKAG erfüllen. Das haben mir das BKA und das BMI nochmals bestätigt. Insbesondere gilt:
  - Bei Personen, die als Beschuldigte gespeichert werden, muss die speichernde Stelle in jedem Einzelfall eine Negativprognose gemäß § 8 Absatz 2 BKAG erstellen (vgl. dazu Nr. 5.13.1).
  - Für Kontaktpersonen sollen im PIAV die vom Bundesverfassungsgericht aufgestellten Kriterien gelten. Diese dürfen deshalb in den Vorsorgedateien des BKA nur gespeichert werden, wenn konkrete Tatsachen für einen objektiven Tatbezug und damit für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung vorliegen, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten (vgl. dazu auch Nr. 5.13.3).

- Die Funktionalitäten werden zwischen dem Bundessystem und den Landessystemen verteilt, die Protokollierung wird überwiegend in den Landessystemen erfolgen.

- Es erfolgt keine Verknüpfung des Datenbestandes vom PIAV mit anderen Datenbeständen und keine Verarbeitung oder Nutzung der Daten vom PIAV in anderen Systemen, um dort derartige Analysen zu ermöglichen.

Wie ich gegenüber dem BMI und dem BKA deutlich gemacht habe, stehen weitere Fragen an, die dringend geklärt werden müssen. Das BKA hat mir zu seiner Stellungnahme umfassende Unterlagen zur Verfügung gestellt, die ich zurzeit auswerte. Die von mir angesprochenen Aufgaben und Probleme sind:

- Errichtungsanordnungen: Das Verfahren PIAV wird sich in mehrere (logische) Dateien gliedern, in denen die personenbezogenen Daten des jeweiligen Deliktsbereichs gespeichert und ausgewertet werden. Für jede dieser logischen Dateien ist eine Errichtungsanordnung gemäß § 34 BKAG erforderlich, in der die Einzelheiten der Datenverarbeitung zu regeln sind.

- Zweckbindung: Dabei ist es besonders wichtig, die Zweckbeschreibung präzise zu formulieren, denn hieraus folgt die Zweckbindung der Daten. Letztlich geht es darum, die Verhältnismäßigkeit der jeweiligen Datenverarbeitung sicherzustellen. Dabei gilt der Grundsatz: Je intensiver die Polizei in das Grundrecht des Betroffenen bei der Datenverarbeitung eingreift, desto genauer müssen die Datenverarbeitungszwecke beschrieben sein. Daher sind diese Festlegungen sowohl aus rechtlichen Gründen geboten, als auch als grundrechtssichernde Verfahrensvorschrift unentbehrlich.

- Voraussetzungen für die Speicherung von Daten im PIAV: § 8 BKAG nennt die Voraussetzungen, unter denen die Polizeibehörden des Bundes und der Länder personenbezogene Daten in Verbunddateien für Zwe-

cke der Gefahrenabwehr und zur Strafverfolgungsvorsorge speichern dürfen (vgl. auch oben und Nr. 5.13.1, 5.13.3). Wie dargelegt teilen das BMI und das BKA diese Ansicht. Das System dient der Auswertung und Analyse von personenbezogenen Daten. Diese Begriffe sind derzeit noch nicht klar umrissen. Daher müssen im Zweifelsfall die Voraussetzungen des § 8 BKAG restriktiv ausgelegt werden.

- Ein ungelöstes Problem ist die Speicherung von Dokumentanhängen. § 2 der BKA-Daten-Verordnung grenzt die zu speichernden Daten genau ein. Diese gesetzliche Aufzählung der zu speichernden Datenarten führt aber bei Dokumentanhängen zu Problemen. Diese enthalten unstrukturierte Daten, die sich den in der Verordnung genannten erlaubten Datenfeldern nicht zuordnen lassen. Darüber hinaus ist die Auswertung und Analyse der Daten mit einem weiteren erheblichen Grundrechtseingriff versehen, sofern die Daten und deren Verarbeitung über die jeweilige Zweckbindung hinausgehen können. Daher habe ich Bedenken gegen die geplante Speicherung von Dokumentenanhängen.

- Nach dem vorliegenden Konzept können auch personenbezogene Daten aus besonders intensiven Ermittlungseingriffen gespeichert werden; sie stehen somit für Auswerte- und Analysezwecke zur Verfügung. Für diese Daten sieht die StPO Verwendungsbeschränkungen vor, die auch im PIAV beachtet werden müssen. Ich habe daher gefordert, diese Informationen zu kennzeichnen, um durch technische Sicherungen eine unzulässige Verarbeitung auszuschließen. Das BKA verweist darauf, die Verantwortlichkeit liege nach der gesetzlichen Regelung in erster Linie beim Empfänger der Daten. Eine solche Regelung sei überflüssig, wenn die Verwendungsbeschränkung bereits systemseitig berücksichtigt werden müssten.

- Kriterien des § 8 BKAG gegen PIAV-Relevanzkriterien: Es ist geplant, dass die Polizei neben den gesetzlichen Anforderungen aus § 8 BKAG an die Speicherung im PIAV noch eigene, sog. PIAV-Relevanzkriterien, einführt. Dies sehe ich kritisch. Solche zusätzlichen Kriterien dürfen nicht dazu führen, die gesetzlichen Anforderungen zu unterlaufen.

- Prüfung und Übergabe der Daten: Die im PIAV zu speichernden Informationen werden aus Verfahren der Länder und des Bundes (Quellsysteme) angeliefert. Für die Gestaltung des Übertragungsprozesses sind jeweils die Landes- oder Bundespolizeibehörden zuständig. Es gilt den Prozess insgesamt in technisch-organisatorischer Hinsicht zu begleiten, damit eine datenschutzgerechte Ausgestaltung des gesamten Verfahrens sichergestellt werden kann.

- Meldedienste: Mit der Einführung vom PIAV sollen polizeiliche Meldedienste in großen Teilen der Vergangenheit angehören - das gleiche gilt auch für die derzeit noch in INPOL bestehenden Falldateien, die delikts- oder phänomenspezifisch betrieben werden. Bislang sind Landespolizeidienststellen verpflichtet, bestimmte Daten auf einem definierten Weg - Meldedienst - an das BKA zu übermitteln, damit dieses seine Zentralstellenfunktion gemäß § 2 BKAG wahrnehmen kann. Nach § 13 BKAG übermitteln die Länder und einige Behörden des Bundes dem BKA die Daten, die es zur Erfüllung seiner Aufgabe als Zentralstelle benötigt. Es ist noch zu klären, ob PIAV dieser Regelung gerecht wird. Denn derzeit unterscheiden sich die Anforderungen, die für eine Speicherung im PIAV erfüllt werden müssen, von denen, die § 13 BKAG an die Übermittlung stellt. Über PIAV können damit dem BKA mehr Daten zur Kenntnis gelangen als es gesetzlich vorgeschrieben ist.

- Berechtigungsregeln für den Zugriff auf die Daten vom PIAV werden grundsätzlich auf Seiten der Verbundteilnehmer festgelegt; sie müsse sich an den Zwecken der jeweiligen Datei orientieren. Durch technische Vorkehrungen kann verhindert werden, dass dateiübergreifende Zugriffe generell möglich sein werden. Auch hier gilt es, die Erforderlichkeit der Kenntnis von Daten aus einer anderen Datei unter strengen sachlichen Gesichtspunkten zu überprüfen. So erscheint es fraglich, ob Bearbeiter für den Bereich der Eigentumsdelikte auch auf Daten aus dem Deliktsbereich Sexualstraftaten zugreifen dürfen.

- Neben den vorgenannten Details war bisher nicht hinreichend geklärt, welche Funktionen für die Auswertung und Analyse zur Verfügung stehen.

Die Gespräche werden fortgesetzt. Über die Ergebnisse werde ich berichten.

5.13.3 Kontrolle von Kontaktpersonen

Bei der Abteilung Staatsschutz des BKA habe ich in verschiedenen Dateien kontrolliert, ob die Speicherung von Randpersonen aus dem Bereich des Terrorismus datenschutzrechtlich zulässig ist. Unter anderem ging es um Familienangehörige von Verdächtigen, soweit sie als sogenannte Kontakt- und Begleitpersonen gespeichert sind.

Kontakt- und Begleitpersonen sind nicht zwingend selbst verdächtig oder beschuldigt, eine Straftat begangen zu haben. Sie sind auch als solche keine Person, bei der aufgrund bestimmter Tatsachen anzunehmen ist, dass von ihnen eine Gefahr ausgeht. Kennzeichnend ist vielmehr, dass sie mit einem Beschuldigten oder Verdächtigen in Kontakt stehen. Einen Anlass haben sie dafür nicht selbst gegeben. Zusätzliche Eingriffsintensität ergibt sich hier daraus, dass die Polizeibehörden Maßnahmen gegen die Betroffenen veranlassen können, wenn sich Informationen z. B. zu einem Verdacht verdichten.

Nach seinem Wortlaut erlaubt das Gesetz dem BKA, Kontakt- und Begleitpersonen in einem sehr weitgehenden Umfang zu speichern. Die Speicherung ist zulässig, wenn und soweit dies zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich ist (§ 8 Abs. 4 BKAG). Diese gesetzliche Vorgabe ist aber im Lichte der aktuellen Rechtsprechung des Bundesverfassungsgerichts verfassungskonform auszulegen. Insbesondere in seiner Entscheidung zur Antiterrordatei hat das Gericht die verfassungsrechtlichen Anforderungen aufgezeigt (Urteil vom 24.04.2014, Az. 1 BvR 1215/07).

Für die Antiterrordatei hält das Gericht eine Speicherung für möglich, soweit die Kontaktperson Aufschluss über die als terrorismusnah geltende Hauptperson geben kann. In ähnlicher Weise hatte das Gericht bereits früher zu allgemeinen polizeilichen Dateien verlangt, den Begriff der Kontakt- und Begleitperson restriktiv auszulegen. Dies setze „konkrete Tatsachen für einen objektiven Tatbezug und damit für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten“ voraus. In diesem Sinne ist auch § 8 Absatz 4 BKAG restriktiv auszulegen. Bei Familienangehörigen sind zudem bestehende Zeugnisverweigerungsrechte gem. § 52 StPO zu berücksichtigen. Daher habe ich bei meiner Kontrolle diese zusätzlichen Anforderungen zugrunde gelegt. Über den bloßen Kontakt hinaus ist zu fordern, dass zumindest tatsächliche Anhaltspunkte vorliegen, nach denen die jeweilige Person in das Umfeld oder den Hintergrund der Straftatenbegehung verwickelt ist.

Gemessen an diesen Kriterien konnte das BKA in den meisten der stichprobenartig geprüften Fälle die Speicherung rechtfertigen. Lediglich in wenigen Einzelfällen lagen nach meiner Auffassung keine ausreichenden Anhaltspunkte vor. Problematisch war in einigen Fällen zudem, dass der Aktenrückhalt fehlte. Hier handelte es sich um Fälle, in denen die Polizeibehörden der Länder dem BKA Informationen ohne entsprechenden Aktenrückhalt übermittelt hatten. Das BKA hatte die jeweilige Bewertung der Landespolizei zu der Person übernommen. Das ist problematisch, weil das BKA als Zentralstelle in diesen Fällen selbst als verantwortliche Stelle die Informationen in einer eigenen Datei gespeichert hatte. Daher muss das BKA selbst eine Einstufung der Person vornehmen und diese durch einen eigenen Aktenrückhalt belegen können. Noch während meines Beratungs- und Kontrollbesuchs wurde zugesagt, diese Praxis und die von mir angesprochenen Fälle zu prüfen. In einem der Fälle wurde unmittelbar im Anschluss der Prüfung die Löschung zugesagt.

Den Ergebnisbericht meiner Kontrolle habe ich dem BKA erst kurz vor Redaktionsschluss übersandt. Eine Antwort liegt noch nicht vor.

5.13.4 Errichtungsanordnungen - Festlegung Personenkategorien

Datenverarbeitung wird komplexer. Das wirkt sich auch auf die Prozesse innerhalb der Polizeibehörden wie dem BKA aus, wenn diese neue Systeme beschaffen oder bestehende umstrukturieren. Diese sind in Errichtungsanordnungen zu beschreiben.

Der Gesetzgeber fordert wegen der Bedeutung des mit der Verarbeitung oder Nutzung von personenbezogenen Daten verbundenen Grundrechtseingriffs jeden einzelnen Datenverarbeitungsprozess genauestens in einer Errichtungsanordnung zu beschreiben. Die Einzelheiten der Datenverarbeitung sind für jede Datei zu benennen, um eine aussagekräftige Konkretisierung der gesetzlichen Regelungen zu erreichen. So soll im Ergebnis die Rechtmäßigkeit und die Verhältnismäßigkeit der Datenverarbeitung sichergestellt werden. Dies dient der Selbstkontrolle und der Selbstbindung der Verwaltung. Letztendlich ist eine gleichmäßige und fehlerfreie Verarbeitung der personenbezogenen Daten von Beschuldigten, Verdächtigen, Zeugen und Hinweisgebern sowie sonstigen Personen, die beim BKA gespeichert werden dürfen, zu gewährleisten. Um dieses System abzusichern, muss ich nach dem Gesetz vom BMI als Fachaufsichtsbehörde für das BKA zu den Errichtungsanordnungen angehört werden.

Bei den Anhörungen habe ich immer wieder festgestellt, dass meine Anregungen nur zum Teil berücksichtigt worden sind. So besteht beispielsweise bei der konkreten Festlegung des betroffenen Personenkreises der Trend, nur den Gesetzestext zu wiederholen, anstatt diesen zu präzisieren (dazu schon 24. TB Nr. 7.4.5). Hierdurch können sich bei den Anwendern Fehleinschätzungen einschleichen, die im Ergebnis zu einer nicht gesetzeskonformen Verarbeitung der Daten bestimmter Personengruppen führen (vgl. 24. TB Nr. 7.4.4).

Deswegen fragt sich, ob und wieweit das Anhörungsverfahren noch dem vom Gesetzgeber beabsichtigten Zweck entspricht. Die Abstimmungsprozesse für die Planung und Umsetzung von neuen gemeinsamen Datenverarbeitungsverfahren der Polizeien des Bundes und der Länder durchlaufen frühzeitig die polizeilichen Gremien und werden sukzessive je nach Projektstadium wiederholt. Alle beteiligten Stellen haben in die Entwicklung von Datenverarbeitungsprogrammen investiert und die notwendigen organisatorischen Vorbereitungen für die Inbetriebnahme des neuen Verfahrens getroffen. Die Datenschutzbehörden der Länder erhalten den Entwurf der Errichtungsanordnung erst, wenn das Anhörungsverfahren auf Bundesebene abgeschlossen ist und der Entwurf den jeweiligen Landesregierungen übersandt wird.

Dies ist aus meiner Sicht zu spät, um die vom Gesetzgeber vorgesehene Beratung durch die Datenschutzbehörden effektiv leisten zu können. Schließlich geht es um die Gewährleistung von Grundrechtschutz und letztlich auch um den sparsamen Einsatz von Ressourcen.

5.13.5 Der Lagebericht „Innere Sicherheit“

Die Verwendung von personenbezogenen Daten im Lagebericht „Innere Sicherheit“ ist in der bisherigen Form rechtlich unzulässig.

Ein politisch engagierter Bürger hatte aus den Medien erfahren, u. a. sein Name und seine Parteizugehörigkeit seien im Lagebericht „Innere Sicherheit“ (Lagebericht) genannt worden. Das ihm vorgeworfene Delikt sei jedoch nur geringfügiger Natur. Mit dem Lagebericht informiert das Bundesministerium des Innern über wichtige bzw. schwerwiegende Ereignisse auf dem Gebiet der Inneren Sicherheit.

Bei meiner Prüfung stellte ich fest, dass seine Vermutung richtig war. Bereits seine Aufnahme in den Lagebericht entbehrte jeglicher rechtlichen Grundlage. Auch die Verarbeitung und Übermittlung seiner Daten an die Sicherheitsbehörden des Bundes durch das BMI hielt meiner rechtlichen Prüfung nicht stand. So waren seine Daten für einen anderen Zweck erhoben worden als sie später verwendet wurden. Zudem erhielten Behörden

seine Daten, die für Art und Schwere des zur Last gelegten Deliktes offensichtlich völlig unzuständig waren. Dies widersprach dem Grundsatz der Datensparsamkeit (§ 3a BDSG). Auch konnte ich nicht erkennen, inwiefern das BMI bei seiner Arbeit berücksichtigt hatte, dass Informationen zu Menschen die sich politisch betätigen, besonders schutzbedürftig sind (§ 3 Abs. 9 BDSG).

Die „rechtliche Grundlage" für die Aufnahme von personenbezogenen Daten in den Lagebericht in der bisherigen Form halte ich für sehr bedenklich. Obwohl offenkundig in das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung eingegriffen wird, beruht das Vorgehen in diesen Fällen auf einer Entscheidung der Ständigen Konferenz der Innenminister und -senatoren der Länder und damit nicht auf einem formellen Gesetz (Art. 19 Abs. 1 GG). Auch sind die Tatbestände, die festlegen, wer oder was aufgenommen wird, nicht hinreichend genau bestimmt (Bestimmtheitsgebot). Diese Bedenken habe ich dem BMI mitgeteilt. Dieses hat mein Schreiben zum Anlass genommen, die Leitlinien für die Erstellung des Lageberichts „Innere Sicherheit" zu ändern und klarzustellen, dass personenbezogene Daten darin grundsätzlich nicht aufzunehmen sind. Dies ist erfreulich und die Erwähnung des o. g. Bürgers wird damit hoffentlich ein einmaliger Fehler bleiben. Ich habe daher keine Beanstandung (§ 25 BDSG) ausgesprochen, werde aber die weitere Entwicklung des Lageberichts „Innere Sicherheit" kritisch beobachten.

5.13.6 Quellen-Telekommunikationsüberwachung

Das BMI hat zur sogenannten Quellen-Telekommunikationsüberwachung eine Standardisierende Leistungsbeschreibung erstellt und mich dazu angehört.

Über die Kontrolle der Quellen-Telekommunikationsüberwachung habe ich im 24. Tätigkeitsbericht (Nr. 7.4.1) berichtet. Als Reaktion auf die nicht nur von mir geäußerte Kritik an der eingesetzten Software hat das BKA deren Einsatz in der Praxis gestoppt. Das BMI hat eine Standardisierende Leistungsbeschreibung mit Eckdaten für eine künftige Software erstellt. Danach sollen die Softwareanbieter insbesondere verpflichtet werden, den ausreichend kommentierten Quellcode und andere zur Prüfung der Funktionalität der Software relevante Informationen gegenüber dem Auftraggeber - also hier dem BKA - offenzulegen. Sie legt weiter ausdrücklich fest, die Möglichkeit zur Prüfung des Quellcodes durch die jeweilige datenschutzrechtlich zuständige Stelle sei zu gewährleisten. Darüber hinaus bestimmt sie als Reaktion auf die vergangene Kritik Sicherheitsanforderungen und Anforderungen zum Schutz des Kernbereichs privater Lebensgestaltung.

Zu den aktuellen vom BKA zu beschaffenden bzw. neu zu entwickelnden Systemen und Unterlagen hat mir das BMI vollen Zugang, ggf. in den Räumlichkeiten des Anbieters, zugesagt.

5.13.7 Telefonaufzeichnungen beim Bundeskriminalamt

Das BKA möchte an seinen zentralen Rufnummern Gespräche aufzeichnen; hierzu hat es mich um datenschutzrechtliche Beratung gebeten.

Diese Aufzeichnung soll allerdings eng ausgestaltet sein: Das BKA möchte lediglich Anrufe erfassen, bei denen Mitarbeiterinnen und Mitarbeiter bzw. die Behörde und ihre Einrichtungen bedroht oder beleidigt werden. Es erfasst die Gespräche bei den betroffenen Rufnummern in der Regel nur eingeschränkt. Das Telefonsystem startet zu Gesprächsbeginn die Aufzeichnung, löscht die registrierten Daten aber drei Minuten nach Gesprächsende wieder automatisch. Dauerhaft speichert das BKA die Daten nur, wenn die Beschäftigten, die das Telefongespräch geführt haben, den sog. Drohknopf drücken. Dieses Vorgehen wird damit gerechtfertigt, dass Drohungen oft schon im ersten Moment der gegebenenfalls sehr kurzen Gespräche ausgesprochen werden. Würde die Aufzeichnung erst beginnen, wenn der Drohknopf gedrückt wird, wäre der entscheidende Gesprächsinhalt möglicherweise verloren, die Aufzeichnung wirkungslos.

Nach meiner Auffassung war eine solche Gesprächsaufzeichnung nur bei Rufnummern möglich, bei denen der Anrufer bzw. die Anruferin fest mit der Aufzeichnung rechnen muss (16. TB Nr. 10.4.1). Diese Auffassung ist im Hinblick auf Polizeibehörden des Bundes zu präzisieren, auch im Lichte der zwischenzeitlich ergangenen Rechtsprechung. Denn mit einer Gesprächsaufzeichnung können Anrufer nur bei Notrufnummern fest rechnen. Dazu zählen aber die Telefonanschlüsse des BKA als Zentralstelle der Polizeibehörden nicht. Daher ist eine zumindest schlüssige Einwilligung der jeweiligen Anruferin bzw. des jeweiligen Anrufers notwendig. Dafür muss er bzw. sie über die Aufzeichnung informiert sein, z. B. durch eine Bandansage und dann die Gelegenheit haben, zu reagieren. Daran ändert nach meiner Einschätzung die Rechtsprechung des Bundesverfassungsgerichts nichts. Dieses hat in der Entscheidung zum Abgleich von Fahrzeugkennzeichen entschieden, dass nur dann kein Grundrechtseingriff vorliegt, wenn Daten unmittelbar nach der Erfassung technisch spurlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden (Urteil vom 11. März 2008, Az. 1 BvR 2074/05). Hier ist der Personenbezug jedoch während des Gesprächs möglich.

Das BKA hat mir zwischenzeitlich mitgeteilt, dass es meine Rechtsauffassung nicht teilt. Die Kenntnisnahme der nur temporär aufgezeichneten Daten sei technisch ausgeschlossen, weshalb nach der oben genannten Rechtsprechung des Bundesverfassungsgerichts kein Grundrechtseingriff vorliege. Zudem könne die Zwischenspeicherung hilfsweise auf die Generalklausel in § 32 des BKAG gestützt werden, wonach die Speicherung zur Dokumentation behördlichen Handelns zulässig sei.

Hier bin ich nach wie vor anderer Meinung, weil derartige Aufzeichnungen nicht auf eine allgemeine Rechtsgrundlage gestützt werden können, die die Dokumentation behördlichen Handelns zum Gegenstand hat. Schließlich wird hier das gesprochene Wort von Bürgerinnen und Bürgern aufgezeichnet.

Da es an einer bereichsspezifischen gesetzlichen Regelung für die Aufzeichnung von beim BKA eingehenden Telefongesprächen mangelt, halte ich eine gesetzgeberische Entscheidung für geboten.

5.13.8 Unglaublich - aber wahr! Demonstranten als gewaltbereite Extremisten erfasst

Wie schnell man zu Unrecht in Dateien der Sicherheitsbehörden geraten kann - und warum eine effiziente Datenschutzkontrolle unerlässlich ist.

Seit dem Jahr 2006 dürfen Nachrichtendienste und Polizeibehörden auf der Grundlage des Gemeinsame-Dateien-Gesetzes vom 22. Dezember 2006 - neben der Antiterrordatei (vgl. Nr. 5.2) - auch für bestimmte Projekte gemeinsame Dateien führen.

Gegenstand meiner Kontrolle war eine gemeinsame Projektdatei des BfV und des BKA, die vom BfV geführt wurde. In ihr sollten ausschließlich gewaltbereite extremistische Personen gespeichert sein.

Dabei musste ich schwerwiegende Rechtsverstöße feststellen. Denn das BfV hatte eine Vielzahl von Personen gespeichert, die bei einer Anti-Atomkraft-Demonstration lediglich ihr Grundrecht auf Meinungs- und Demonstrationsfreiheit ausgeübt hatten. Dies ist rechtswidrig - selbst wenn bei einer derartigen Demonstration einzelne Personen gewaltbereit gewesen sein sollten. So hat das BfV dann auch im Nachgang zu meiner Kontrolle ausdrücklich eingeräumt, in den von mir festgestellten Fällen hätten die Betroffenen nicht gespeichert werden dürfen. Daher habe man deren Daten bis zum Abschluss meiner Kontrolle sowohl in dieser Projektdatei als auch in einer weiteren, zentralen Datei der Nachrichtendienste des Bundes und der Länder gesperrt. Nach Abschluss des Verfahrens werde man diese Daten löschen. Das Verfahren ist noch nicht abgeschlossen.

Die Erhebung und Speicherung personenbezogener Daten durch einen Nachrichtendienst sind schwerwiegende Grundrechtseingriffe - mit potentiell weit reichenden Folgen für die Betroffenen. Sie sind nur zulässig, wenn tatsächliche Anhaltspunkte beispielweise dafür bestehen, dass der Betroffene gegen die freiheitlich demokrati-

sche Grundordnung handelt. Wann dies der Fall ist, regelt § 4 Bundesverfassungsschutzgesetz (BVerfSchG - vgl. Kasten zu Nr. 5.13.8).

Diese Voraussetzungen darf der Verfassungsschutz für Kernkraftgegner nicht allgemein annehmen. Das BMI hat in seiner Stellungnahme zu meinem Prüfbericht gleichwohl einen Zusammenhang zwischen Kernkraftgegnern und Linksextremismus hergestellt. Es folgert aus der Teilnahme an einer solchen Demonstration, dass die Nutzung der Kernkraft als Ausdruck des menschenverachtenden kapitalistischen Systems kritisiert werde und dementsprechend Kernkraftgegner dieses kapitalistische System überwinden wollten. Dies kann Kernkraftgegnern aber keinesfalls pauschal unterstellt werden.

Wer die Nutzung der Atomkraft etwa aufgrund der potentiellen Risiken dieser Technologie oder der ungeklärten Endlagerung kritisiert, handelt nicht gegen die freiheitlich demokratische Grundordnung. Das Gleiche gilt für diejenigen, die als Betroffene - z. B. eines Zwischenlagers radioaktiv strahlenden Abfalls - gegen diese Lagerung demonstrieren und damit rechtmäßig ihre Grundrechte ausüben. Sofern keine Anhaltspunkte für die oben genannten Bestrebungen existieren, handeln Demonstranten im Rahmen der freiheitlich demokratischen Grundordnung. Entsprechende Anhaltspunkte muss der Verfassungsschutz daher in jedem Einzelfall darlegen können, wenn er eine Person speichern will.

Aber auch Personen, die gewaltsam handeln, in dem sie sich etwa an Schienen, Werkstore etc. ketten oder durch Sitzblockaden den Verkehr behindern und damit eine strafbare Nötigung begehen könnten, dürfen aufgrund dieser Straftat nicht per se vom BfV erfasst werden. Nicht aus jeder Straftat folgt automatisch ein tatsächlicher Anhaltspunkt für eine Bestrebung im Sinne des BVerfSchG gegen die freiheitlich demokratische Grundordnung, der ein Tätigwerden des BfV legitimiert. Andernfalls würde auch jede Körperverletzung, jeder Raubüberfall oder jede Nötigung im Straßenverkehr das BfV zum Tätigwerden berechtigen.

Erforderlich hierfür ist also stets ein qualifizierter tatsächlicher Anhaltspunkt für eine entsprechende Bestrebung. Gibt es diesen nicht, dürfen die Nachrichtendienste - bildlich gesprochen - nicht aufs Spielfeld. Zuständig ist dann allein die Polizei. Erlangt diese bei ihren Ermittlungen Anhaltspunkte für derartige Bestrebungen, darf sie - teilweise muss sie es sogar - die Nachrichtendienste hierüber informieren. Erst dann sind die Nachrichtendienste mit im Spiel.

Indem das BfV die vorgenannten Personendaten nicht nur rechtswidrig erhoben, sondern auch in der Projektdatei gespeichert hat, konnte das an dieser Datei beteiligte BKA hiervon Kenntnis erlangen. Wie der Gesetzgeber eindeutig festgelegt hat, darf ein Beteiligter an einer Projektdatei Daten darin nur speichern, wenn er diese den Projektbeteiligten auch übermitteln darf. Rechtswidrig erhobene Daten können per se nicht rechtmäßig übermittelt werden.

Bei meiner Kontrolle bin ich darüber hinaus auf weitere Verstöße gestoßen. So hatte z. B. ein Landesamt für Verfassungsschutz rechtswidrig lesenden und schreibenden Zugriff auf die Projektdatei, ohne an dieser überhaupt teilzunehmen. Nach dem Gesetz dürfen aber nur die Projekteilnehmer Daten speichern oder abrufen. Ich habe den für die Datenschutzkontrolle dieses Landesamtes zuständigen Landesbeauftragten für den Datenschutz über den Vorgang informiert.

Kasten zu Nr. 5.13.8

§ 4 BVerfSchG - Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind

a) Bestrebungen gegen den Bestand des Bundes oder eines Landes solche politisch bestimmten, ziel- und zweckgerichteten Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf ge-

richtet ist, die Freiheit des Bundes oder eines Landes von fremder Herrschaft aufzuheben, ihre staatliche Einheit zu beseitigen oder ein zu ihm gehörendes Gebiet abzutrennen;

b) Bestrebungen gegen die Sicherheit des Bundes oder eines Landes solche politisch bestimmten, ziel- und zweckgerichteten Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf gerichtet ist, den Bund, Länder oder deren Einrichtungen in ihrer Funktionsfähigkeit erheblich zu beeinträchtigen;

c) Bestrebungen gegen die freiheitliche demokratische Grundordnung solche politisch bestimmten, ziel- und zweckgerichteten Verhaltensweisen in einem oder für einen Personenzusammenschluss, der darauf gerichtet ist, einen der in Absatz 2 genannten Verfassungsgrundsätze zu beseitigen oder außer Geltung zu setzen.

Für einen Personenzusammenschluss handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des § 3 Abs. 1 ist das Vorliegen tatsächlicher Anhaltspunkte. Verhaltensweisen von Einzelpersonen, die nicht in einem oder für einen Personenzusammenschluss handeln, sind Bestrebungen im Sinne dieses Gesetzes, wenn sie auf Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen.

(2) Zur freiheitlichen demokratischen Grundordnung im Sinne dieses Gesetzes zählen:

a) das Recht des Volkes, die Staatsgewalt in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung auszuüben und die Volksvertretung in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl zu wählen,

b) die Bindung der Gesetzgebung an die verfassungsmäßige Ordnung und die Bindung der vollziehenden Gewalt und der Rechtsprechung an Gesetz und Recht,

c) das Recht auf Bildung und Ausübung einer parlamentarischen Opposition,

d) die Ablösbarkeit der Regierung und ihre Verantwortlichkeit gegenüber der Volksvertretung,

e) die Unabhängigkeit der Gerichte,

f) der Ausschluss jeder Gewalt- und Willkürherrschaft und

g) die im Grundgesetz konkretisierten Menschenrechte.

5.14 Technologischer Datenschutz

Mit wachsender Bedeutung der Informationstechnik werden Fragen zum technologischen Datenschutz immer wichtiger.

So ist die Aufarbeitung der sogenannten NSA-Affäre noch längst nicht abgeschlossen; die Bundesregierung, die Wirtschaft und die Öffentlichkeit werden sich weiterhin mit den Konsequenzen befassen müssen.

Neben diesen Gefahren für die Sicherheit informationstechnischer Systeme hat meine Dienststelle gemeinsam mit den Landesbeauftragten für Datenschutz und der Universität Dresden an einem Projekt zur Weiterentwicklung der Grundlagen des technologischen Datenschutzes mitgewirkt (vgl. Nr. 5.14.1) und bei der Erneuerung von Normen zur Vernichtung von Daten (vgl. Nr. 5.14.2 und Nr. 8.4) mitgearbeitet.

Die folgenden Beiträge zum Identitätsdiebstahl (Nr. 5.14.3) und zur Zusammenlegung der IT im Geschäftsbereich des BMI (Nr. 5.14.4) zeigen noch einmal die Spannweite technologischer Themen.

5.14.1 Das Standard-Datenschutzmodell

Seit Jahren entwickeln sich die technisch-organisatorischen Regelungen in den Datenschutzgesetzen des Bundes und der Länder auseinander. 2001 hat ein Gutachten im Auftrag des BMI eine Überarbeitung der technischen und organisatorischen Datenschutzanforderungen für das BDSG vorgeschlagen. Aber nur wenige Bundesländer haben ihre Gesetze bereits auf den neuesten Stand der Technik gebracht.

Seit Jahren ist der Trend zu erkennen, dass die Anwendung der für den Bereich der IT-Sicherheit vom BSI entwickelte Methodik „IT-Grundschutz“ als hinreichend zur Erfüllung der technisch-organisatorischen Maßnahmen nach § 9 BDSG nebst Anlage angesehen wird. Dabei wird allerdings in den meisten Fällen vergessen, dass die Anforderungen des Datenschutzes in vielen Fällen über die IT-Grundschutzmaßnahmen hinausgehen oder - teilweise - diesen sogar widersprechen. Beispielweise kann die Forderungen nach Protokollierung zum Grundsatz der Datensparsamkeit in Widerspruch stehen. Datenschutz bedeutet eben mehr als nur die Umsetzung der IT-Grundschutzmaßnahmen (vgl. z. B. 15. TB Nr. 30.8). Gleichwohl findet in der Praxis nur der IT-Grundschutz als praktikable Lösung Anwendung. Darauf aufbauend müssen aber zusätzliche, relativierende oder auch abweichende Datenschutzmaßnahmen festgelegt werden. Das Standard-Datenschutzmodell, das von einer Arbeitsgruppe des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder entwickelt wurde, ergänzt und erweitert in diesem Sinne die Anforderungen zur IT-Sicherheit.

In der Praxis orientiert sich die Datensicherheit heute unter anderem an der ISO Standard-Reihe 2700x der Internationalen Organisation für Normung (27001 Informationssicherheits-Managementsystem usw.) und an der ISO-Norm 15408 (Common Criteria for Information Technology Security Evaluation, vgl. 19. TB Nr. 4.3). Daraus ergibt sich, dass für die technisch-organisatorischen Regelungen des Datenschutzes ein Augenmerk auf die Aspekte von Planung, Kontrolle, Prüfung, Bewertung und die organisationsinterne Form der Verarbeitung und Nutzung gelegt werden sollte.

Das in einer Arbeitsgruppe entwickelte Standard-Datenschutzmodell greift diese Gedanken auf und definiert unter den vorgenannten Bedingungen die elementaren Schutzziele des Datenschutzes: (vgl. Kasten a und b zu Nr. 5.14.1).

Ich fordere schon seit längerem, dass diese elementaren Schutzziele sowie die ergänzenden Definitionen in das BDSG oder in die neue Datenschutz-Grundverordnung aufgenommen werden sollten. Ich habe die Schutzziele leider erfolglos eingebracht. Die Schutzziele sollten dabei möglichst zutreffend (reliabel/valide), kontrollierbar, entwicklungsfähig, vollständig sowie allgemeinverständlich und normenklar formuliert sein. Die spezifischen Maßnahmen zum Erreichen der Schutzziele müssen ebenfalls rechtlich verankert werden. Über die Schutzbedarf-Feststellung kann dann geklärt werden, welche Maßnahmen zu treffen sind (Konzeptphase) oder welche Maßnahmen hätten getroffen werden müssen (Prüfphase) mit anschließender Bewertung der Maßnahmen (Bewertungsphase). Schließlich habe ich die hier vorgestellten Überlegungen zum Standard-Datenschutzmodell auch in der Artikel-29-Gruppe eingebracht. Hier konnte allerdings bislang keine Einigung über das weitere Vorgehen erzielt werden. Die Ziele lösten bislang nur eine verstärkte Diskussion aus über ihre Definition.

Kasten a zu Nr. 5.14.1

Das Standard-Datenschutzmodell

Das Urteil des Bundesverfassungsgerichts hat den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme als neues Grundrecht aus Artikel 1 und 2 des Grundgesetzes hergeleitet. Damit wurden diese beiden klassischen Schutzziele in ihrer verfassungsrechtlichen Gültigkeit bestätigt. Das dritte klassische Schutzziel, die Verfügbarkeit, ist bereits in der Anlage zu § 9 im BDSG enthalten. Ausgangspunkt der Überlegungen zu einer entsprechenden Weiterentwicklung der technisch-organisatorischen Regelungen in den Datenschutzgesetzen sind nunmehr folgende Randbedingungen, die in einer Arbeitsgruppe des Arbeitskreises der Datenschutzbeauftragten des Bundes und der Länder erarbeitet wurden:

1. Die Grundlage bilden die Definition elementarer Schutzziele, aus denen sich weitere (Schutz-) Ziele systematisch herleiten lassen. Die Schutzziele sollten einfach, verständlich und praxistauglich sein.

2. Die Schutzziele sollten somit soweit wie möglich den elementaren Schutzzielen der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) entsprechen oder zumindest mit ihnen korrespondieren und Überschneidungspunkte aufweisen. Gleichzeitig sollte aber die spezielle Sichtweise des Datenschutzes zum Tragen kommen.

3. Die Schutzziele müssen an den Vorgaben des Datenschutzes gemessen werden und über längere Zeit Bestand haben und dürfen sich nicht ausschließlich an den Vorgaben der IT-Sicherheit orientieren.

4. Auf der Basis der Schutzziele sollte sich ein Katalog von Datenschutzmaßnahmen ableiten lassen, die - ähnlich dem IT-Grundschutzkatalog - in ein flexibles, einfaches, praxistaugliches und durch Software unterstütztes Verfahren umgesetzt werden können und als Kriterien-Katalog eines Datenschutzaudits herangezogen werden könnte.

5. Die elementaren Schutzziele sind technologieunabhängig definiert.

6. Die Nachhaltigkeit der Schutzziele ist gewährleistet. Bei zukünftigen technischen Systemen ist das Modell der Schutzziele vollständig und ausreichend und bleibt weiterhin gültig. Die Schutzziele bleiben, die daraus folgenden Maßnahmen müssen sich dagegen mit der IT weiterentwickeln.

7. Grundsätzliche rechtliche Anforderungen sollen möglichst technisch durchgesetzt werden. Dies greift das Konzept Systemdatenschutz und Datenschutz durch Technik auf (Privacy Enhancing Technology - PET).

8. Die technisch-organisatorischen Maßnahmen, die sich aus dem sich wandelnden technischen Fortschritt ergeben sowie datenschutzfreundliche Techniken, müssen angemessen abgebildet werden können.

9. Technisch-organisatorische Regelungen müssen die Grundlage für ein Datenschutzaudit liefern können.

Kasten b zu Nr. 5.14.1

Das Standard-Datenschutzmodell	
Verfügbarkeit:	Es ist zu gewährleisten, dass personenbezogene Verfahren und Daten zeitgerecht zur Verfügung stehen und diese ordnungsgemäß angewendet werden können.
Vertraulichkeit:	Es ist zu gewährleisten, dass nur befugt auf personenbezogene Verfahren und Daten zugegriffen werden kann.
Integrität:	Es ist zu gewährleisten, dass Daten aus personenbezogenen Verfahren unversehrt, zurechenbar und vollständig bleiben.
Transparenz:	Es ist zu gewährleisten, dass die Erhebung, Verarbeitung in personenbezogenen Verfahren und die Nutzung mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können.
Zweckbindung:	Es ist zu gewährleisten, dass personenbezogene Verfahren so eingerichtet sind, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können.
Intervenierbarkeit:	Es ist zu gewährleisten, dass personenbezogene Verfahren so gestaltet werden, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.

5.14.2 Arbeiten im DIN-/ISO-Umfeld

Auch im Berichtszeitraum habe ich wieder in verschiedenen Arbeitsgruppen (Fachbeirat der Koordinierungsstelle IT-Sicherheit (KITS), Karten und persönliche Identifikation, Identitätsmanagement und Datenschutz-Technologien, Biometrie und Vernichten von Datenträgern) zur Standardisierung von Technologien mitgewirkt. Mein Blick richtet sich dabei insbesondere auf die Schlüsseltechnologien wie Chipkarten und datenschutzfreundliche Technologien (Privacy Enhanced Technology - PET).

Die Arbeiten gestalten sich immer dann besonders schwierig, wenn es bereits gängige Standards gibt und entsprechende Technik schon im Einsatz ist, beispielsweise bei Chipkarten. Hier konzentriert sich meine Mitwirkung in den Arbeitsgruppen (Karten und persönliche Identifikation, Identitätsmanagement und Datenschutz-Technologien, Biometrie) darauf, dass bei zukünftigen Entwicklungen datenschutzrechtliche Aspekte besser in die Standards einfließen. Im ISO-Umfeld (ISO - Internationale Organisation für Normung) ist dies aber nur im begrenzten Maße möglich, da in den Gremien viele Länder vertreten sind, deren Verständnis vom Datenschutz auf anderen rechtlichen und kulturellen Grundlagen beruht. Ich sehe deshalb meine Aufgabe darin, frühzeitig extreme Gefährdungen für den Datenschutz durch die Standardisierung zu verhindern.

Im Bereich der Norm und Standardisierung von Datenschutzprozessen liegen derzeit keine Standards vor. Ich beabsichtige aus deutscher Sicht, die Schutzziele des Standard-Datenschutzmodells (vgl. Nr. 5.14.1) in die Gremien einzubringen und einer Normung zuzuführen. Da andere Länder bis jetzt keine eigenen Vorschläge eingebracht haben, hoffe ich hier die Schutzziele des Modells in eine weltweit gültige Norm einbringen zu können. Der Prozess ist gerade erst angelaufen, sodass ich noch keine abschließende Wertung abgeben kann. Im entsprechenden DIN-Ausschuss (DIN - Deutsches Institut für Normung) arbeite ich in diesen Punkt gut mit dem BSI

zusammen und sehe die Entwicklung auf dem richtigen Weg. Ich hoffe, im nächsten Tätigkeitbericht über weitere Erfolge berichten zu können.

5.14.3 Identitätsdiebstahl wird zur Regel

Im Berichtszeitraum hat die Presse vermehrt über Identitätsdiebstähle großen Ausmaßes berichtet. In einem Strafverfahren wurde das BSI eingebunden, um einen Warndienst zu entwickeln, der Internetnutzern die Prüfung ermöglichen sollte, inwieweit sie von den Identitätsdiebstählen betroffen waren.

Identitätsdiebstähle sind an sich nichts Neues. Als PC-, Smartphone- oder Tablet-Nutzer sollte man deswegen gewisse Regeln bei der Geräte- und Internetnutzung beachten, damit die eigenen Identitätsdaten ausreichend vor Dritten geschützt sind. Durch raffinierte Angriffsmethoden und Ausnutzung von Sicherheitslücken in IT-Systemen gelingt es unbekannten Dritten aber dennoch oft, ganze Systeme zu kapern und diese in ein automatisiertes Netz (sog. Botnetz) von Computern zusammenzuschließen. Über diese können dann umfassend elektronische Identitäten gestohlen und die PCs von Nutzern für eigene Zwecke missbraucht werden, z. B. für den Versand von Spam. Die so gestohlenen Daten setzen sich dabei oft aus Benutzernamen (Login) und Passwort, PIN-TAN-Kombinationen, Bank- oder Kreditkartendaten usw. zusammen. Diese können lukrativ auf dem Schwarzmarkt gegen Bezahlung veräußert werden. Fehlende oder schlecht gewartete Virenscanner erleichtern Dieben zudem ihr Handwerk, und Schadprogramme bleiben so auf den Systemen der Nutzer viel zu oft unentdeckt.

Im Jahr 2014 wurde das BSI im Zuge strafrechtlicher Ermittlungen in zwei Fällen über das Aufdecken umfassender Datensätze mit gestohlenen Identitäten informiert. Es handelte sich zum einen um einen Datensatz mit 16 Millionen Identitäten, der bei einer Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden gefunden worden war. Im zweiten Fall waren es weitere 18 Millionen Identitäten, die bei Ermittlungen durch die Staatsanwaltschaft im Rahmen eines laufenden Verfahrens gefunden wurden. Diese Daten wurden dem BSI zur Verfügung gestellt, damit es die Betroffenen entsprechend informiere.

Das BSI hat daraufhin einen Warndienst für Internetnutzer zur Abfrage der eigenen Betroffenheit auf einer speziell hierfür vorgesehen Website www.sicherheitstest.bsi.de entwickelt und bereitgestellt. Um eigene Identitäten zu überprüfen, werden hierbei lediglich sogenannte Hashwerte der gefundenen Datensätze herangezogen und mit dem Hashwert der abgefragten Identität verglichen. Wird ein Datum erkannt, so wird der Nutzer mittels einer E-Mail hierüber informiert. Das BSI hat diese Art der Meldeverfahren vorab mit mir abgestimmt. Nutzer großer Internetprovider und E-Mail-Dienste in Deutschland wurden im zweiten genannten Fall auch direkt informiert. Zukünftig ist mit weiteren Berichten über Identitätsdiebstähle zu rechnen, und auch bei diesen werden die Internet- und E-Mail-Anbieter voraussichtlich ihre Nutzer entsprechend informieren. Hier ist allerdings zu beachten, dass sich ggf. auch Dritte mit gefälschten Meldungen an Nutzer wenden könnten; Vorsicht ist insbesondere dann geboten, wenn die Meldung fordert, der Nutzer solle (weitere) Daten von sich zur Behebung des vermeintlichen Problems preisgeben. Nutzer sollten solche Meldungen deshalb kritisch hinterfragen und Hinweise in der einschlägigen Fachpresse beachten.

Generell ist es zur Vorbeugung von Missbrauch erforderlich, alle Passwörter bei Internetportalen regelmäßig zu wechseln. Auch wird immer wieder dazu geraten, ein sicheres und ausreichend komplexes, mindestens acht Zeichen langes Passwort, bestehend aus Zeichen, Sonderzeichen und Ziffern zu wählen. Weitere Hinweise hierzu bietet das BSI z. B. unter www.bsi-fuer-buerger.de.

Zum Thema „Sicheres Surfen“ habe ich ein Faltblatt erstellt, welches in meinem Internetangebot unter www.datenschutz.bund.de abgerufen werden kann.

Betreiber von Internetportalen müssen ihre Systeme sicherer machen und z. B. eine Zwei-Faktor-Authentifizierung (Besitz und Wissen) auf ihren Portalen vorsehen. Hierbei wird beim Login-Vorgang ein weiteres Geheimnis z. B. per SMS an den Nutzer zur Eingabe bei der Anmeldung gesendet.

5.14.4 IT-Konsolidierung im Geschäftsbereich des BMI

Die Zusammenfassung der IT-Betriebe innerhalb der Bundesregierung schreitet weiter fort. Das BMI plant seit 2006 die sogenannte IT-Konsolidierung für fast alle Behörden im seinem Geschäftsbereich - ausgenommen sind zurzeit nur Sicherheitsbehörden und das Ministerium selbst.

Das BMI hat für Behörden in seinem Geschäftsbereich vorgesehen, die IT bei der Bundesstelle für Informationstechnik (BIT) im Bundesverwaltungsamt (BVA) zu bündeln. Bereits umgesetzt ist diese Maßnahme für das BVA selbst, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Statistisches Bundesamt (StBA), das Bundesamt für Migration und Flüchtlinge und das Beschaffungsamt des Bundesministeriums des Innern.

Ich habe die Konsolidierung von Anfang an kritisch begleitet und klargestellt, welche datenschutztechnischen und -rechtlichen Rahmenbedingungen vor einer Konsolidierung erfüllt sein müssen. So muss z. B. eine ausreichende Abschottung der IT-Betriebe voneinander gewährleistet sein (Mandantentrennung) und die Weitverkehrsverbindungen und die lokalen Netzwerke müssen ausreichend leistungsfähig sein, damit Verfügbarkeit und Notfallvorsorge gegeben sind. Außerdem müssen sie einen ausreichenden Schutz der Vertraulichkeit durch Verschlüsselung bieten. Diese datenschutzrechtlichen Voraussetzungen sind aber nicht immer erfüllt. So führte eine Kontrolle der Maßnahmen und Vereinbarungen zur Konsolidierung des StBA zu einer Beanstandung gegenüber dem BMI (vgl. Nr. 5.9).

Die Einhaltung der Anforderungen des Datenschutzes werde ich deswegen auch bei den nächsten Maßnahmen zur Konsolidierung bei der Hochschule des Bundes für öffentliche Verwaltung, bei der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, bei der Bundeszentrale für politische Bildung, bei der Bundesanstalt Technisches Hilfswerk, beim Bundesamt für Kartographie und Geodäsie und beim BSI kontrollieren.

5.14.5 Entwurf für ein IT-Sicherheitsgesetz - ein Beitrag zur IT-Sicherheit bei kritischen Infrastrukturen

Mit dem Gesetzentwurf für ein IT-Sicherheitsgesetz plant die Bundesregierung Defizite im Bereich der IT-Sicherheit - insbesondere bei Betreibern kritischer Infrastrukturen - abzubauen.

Mit der digitalen Durchdringung von Staat, Wirtschaft und Gesellschaft entstehen in nahezu allen Lebensbereichen neue Potentiale, Freiräume und Synergien. Gleichzeitig wächst die Abhängigkeit von IT-Systemen in allen Bereichen und damit die Bedeutung der ihrer Verfügbarkeit und Sicherheit. Dabei ist die IT-Sicherheitslage in Deutschland weiterhin angespannt: Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) erhält kontinuierlich eine Vielzahl von Informationen zur aktuellen Bedrohungssituation.

Durch den vom BMI vorgelegten Entwurf des IT-Sicherheitsgesetzes sollen das BSI-Gesetz erweitert und weitere Gesetze angepasst werden. Betreiber kritischer Infrastrukturen in Deutschland werden verpflichtet, angemessene organisatorische und technische Vorkehrungen zum Schutz informationstechnischer Systeme zu schaffen und durch Standardisierungen und Auditierungen zu belegen. Zudem sollen Betreiber kritischer Infrastrukturen IT-Sicherheitsvorfälle, die Auswirkungen auf ihre Funktionsfähigkeit haben können, unverzüglich dem BSI melden. Die Regelungen entsprechen im Grundsatz dem Vorschlag der Europäischen Kommission für eine

Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Europäischen Union.

Kritische Infrastrukturen sind Einrichtungen in solchen Sektoren, die eine wichtige Bedeutung für das Funktionieren des Gemeinwesens haben und durch deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten (z. B. Energieversorgung, Telekommunikation, Ernährung oder etwa Finanzwesen).

Das Gesetz trägt auch dazu bei, das BSI und das BKA rechtlich so aufzustellen, dass sie der steigenden Bedrohungslage durch Cyber-Angriffe angemessen begegnen können.

Das mit dem Gesetzentwurf verfolgte Ziel, das Sicherheitsniveau in Deutschland bei kritischen Infrastrukturen zu stärken, unterstütze ich. Meine Kritikpunkte betrafen Änderungen im Telemedien- und Telekommunikationsgesetz. Die hier ursprünglich für Telemedienanbieter vorgesehene Befugnis, Daten zu Analysezwecken für sechs Monate zu speichern, wurde im Laufe der Beratungen zurückgenommen. Kritisch sehe ich aber weiterhin folgende Punkte: Es muss im Gesetz klar geregelt werden, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Zweckbindungsregelungen müssen für alle Behörden gelten, die nach dem IT-Sicherheitsgesetz Datenerhebungs- und verarbeitungsbefugnisse erhalten. Derzeit sind sie nur für das BSI vorgesehen. Im Zusammenhang mit den Maßnahmen zur Verbesserung der Informationssicherheit bedarf es zudem gesetzlicher Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten. Schließlich müssen die Datenschutzaufsichtsbehörden an der Festlegung von Informationssicherheitsstandards beteiligt und in die Informationswege bei der Meldung von IT-Sicherheitsvorfällen mit einbezogen werden, zumal diese häufig auch mit Datenpannen verbunden sein werden.

Mit dem Kabinettbeschluss vom 17. Dezember 2014 und der Zuleitung an den Bundesrat hat die Bundesregierung das Vorhaben auf den Weg gebracht; ich werde den Gesetzentwurf weiter begleiten.

5.15 Das neue Melderecht

Meldedaten sind personenbezogene Pflichtangaben der Bürgerinnen und Bürger gegenüber dem Staat, deren Übermittlung und Nutzung zu besonderer Sorgfalt verpflichtet.

Auf der Grundlage der Föderalismusreform des Jahres 2006, durch die dem Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen übertragen worden ist, hat der Deutsche Bundestag am 28. Juni 2012 erstmals ein Bundesmeldegesetz (BMG) beschlossen. Auf Vorschlag des Innenausschusses waren darin allerdings Änderungen vorgesehen, die die im Regierungsentwurf enthaltenen Datenschutzbestimmungen deutlich verschlechterten und so das Datenschutzniveau zum Teil sogar hinter das geltende Recht zurückfallen ließen (vgl. 24. TB Nr. 8.2).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wies, auch auf meine Initiative, in einer Entschließung vom 22. August 2012 (vgl. 24. TB Kasten zu Nr. 8.2) sowie in einer Stellungnahme an den Bundesrat auf die erheblichen datenschutzrechtlichen Defizite hin und forderte diesen auf, dem Gesetz nicht zuzustimmen, um über das Vermittlungsverfahren die erforderlichen datenschutzrechtlichen Nachbesserungen doch noch umsetzen zu können.

Der Bundesrat ist dieser Initiative gefolgt. Eine daraufhin vom Vermittlungsausschuss eingesetzte Arbeitsgruppe, in der ich angehört wurde, erarbeitete folgende Veränderungen des BMG:

a) Bei einfachen Melderegisterauskünften für Zwecke der Werbung oder des Adresshandels gemäß § 44 Absatz 3 Nummer 2 muss der Betroffene ausdrücklich seine Einwilligung erklärt haben und

b) eine Zweckbindung der Melderegisterauskunft gemäß § 47 bei Melderegisterauskünften nach § 44 zu gewerblichen Zwecken, bei erweiterten Melderegisterauskünften nach § 45 und bei so genannten Gruppenauskünften nach § 46 sowie bei Vorliegen einer Auskunftssperre nach § 51 Absatz 1: Bei diesen Melderegisterauskünften darf der Empfänger die Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Danach sind die Daten zu löschen. Soweit sie zum Zwecke der geschäftsmäßigen Anschriftenermittlung für Dritte erhoben werden, dürfen sie nicht wiederverwendet werden. Damit gilt auch für ein diesbezügliches Serviceunternehmen die Zweckbindung.

Eine entsprechende Einwilligung zu a) kann gegenüber der Meldebehörde als generelle Einwilligung für einen oder beide der dort genannten Zwecke erklärt und widerrufen werden. Liegt der Meldebehörde keine generelle Einwilligung vor, bedarf es der Einwilligung gegenüber der Auskunft verlangenden Person oder Stelle. Die Einwilligung gegenüber der Auskunft verlangenden Person oder Stelle muss gesondert erklärt werden und sich ausdrücklich auf die Einholung einer Melderegisterauskunft für jeweils diesen Zweck beziehen.

Auf Verlangen sind der Meldebehörde von der Auskunft verlangenden Person oder Stelle Nachweise über die Einwilligungserklärung vorzulegen. Die Meldebehörde hat das Vorliegen von Einwilligungserklärungen stichprobenhaft zu überprüfen. Liegen der Meldebehörde bezüglich der Einwilligungserklärung konkrete Anhaltspunkte für die Unrichtigkeit der Behauptung der Auskunft verlangenden Person oder Stelle vor, hat sie von Amts wegen zu ermitteln. Bis zum Abschluss der Ermittlungen werden der Auskunft verlangenden Person oder Stelle keine Auskünfte erteilt.

Auch bei den bereits mehrfach erforderlichen Folgeänderungen des BMG zur Angleichung des Inkrafttretens des BMG mit verschiedenen Bundesverordnungen, Landesregelungen und Verwaltungsvorschriften und zur Umsetzung der Gleichstellung von Ehen und Lebenspartnerschaften gemäß § 2 Absatz 8 des Einkommensteuergesetzes (EStG) war ich einbezogen, ebenso wie bei der Änderung von Bundesmeldedatenübermittlungsverordnungen und der Schaffung einer Bundesmeldedatenabrufverordnung.

Das BMG vom 3. Mai 2013 wird nach derzeitigem Stand am 1. November 2015 in Kraft treten.

5.16 Eurodac

Fingerabdrücke von Asylbewerbern werden in der europäischen Datenbank „Eurodac“ gespeichert. Eine neue Verordnung ermöglicht den Zugriff der Sicherheitsbehörden auf diese Daten.

Mit dem Namen „Eurodac“ wird eine gemeinsame Datenbank der EU-Mitgliedstaaten und der Europäischen Kommission für Fingerabdrücke von Asylbewerbern und in der EU aufgegriffenen illegalen Einwanderern bezeichnet. Die Datenbank unterstützt die effektive Anwendung des Dubliner Übereinkommens über die Bearbeitung von Asylanträgen. Eurodac ist auf der Grundlage einer Verordnung des Rates der EU eingerichtet worden, die Regelungen zur Gewährleistung des Datenschutzes für die betroffenen Personen einschließt, Die Datenbank ging am 15. Januar 2003 in Betrieb und wird derzeit von den 28 Mitgliedstaaten der EU sowie von Island, Norwegen, Liechtenstein und der Schweiz genutzt.

Der Europäische Datenschutzbeauftragte (EDPS) überwacht die Verarbeitung personenbezogener Daten im Zentralsystem der Datenbank einschließlich der Übermittlung von Daten an die Mitgliedstaaten. Die Datenschutzbehörden in den Mitgliedstaaten überwachen die Verarbeitung der Daten durch die staatlichen Behörden sowie die Übermittlung von Daten an die zentrale Datenbank. Um einen gemeinsamen Ansatz bei der Datenschutzkontrolle zu gewährleisten, treffen sich der EDPS und Vertreter der Aufsichtsbehörden aus den Anwen-

derstaaten mindestens zweimal pro Jahr in einer gemeinsamen Gruppe, an deren Beratungen ich regelmäßig teilnehme.

Im Berichtszeitraum führte die Gruppe eine koordinierte Kontrolle der Verfahrensweisen in den Eurodac-Anwenderländern bei unleserlichen Fingerabdrücken durch. Hierbei ergaben sich erhebliche Unterschiede in den einzelnen Ländern, von der Versagung der Asylanträge wegen mangelnder Kooperation der Betroffenen bis hin zur wiederholten Abnahme der Fingerabdrücke und medizinischen Beratung. Der Bericht der koordinierten Kontrolle empfiehlt den Anwenderländern, klare und faire Regelungen zu entwickeln, die eine mögliche Diskriminierung der Betroffenen ausschließen.

Zudem befasste sich die Gruppe mit der Umsetzung der revidierten Eurodac-Verordnung (nunmehr VO 603/2013) vom Juni 2013, die den Zugriff der Sicherheitsbehörden auf Daten in Eurodac zur Bekämpfung bestimmter schwerer Straftaten ermöglicht. Bereits im Jahr 2012 hatte die Eurodac-Datenschutz-Gruppe dies in einem gemeinsam mit der Artikel-29-Gruppe verfassten Schreiben an die Europäische Kommission kritisiert. Die neue Eurodac-Verordnung soll im Juli 2015 in Kraft treten.

5.17 Europäisches Visa-Informationssystem

Nach dem Start im Oktober 2011 kommt das europäische Visa-Informationssystem nunmehr in fast allen Teilen der Welt zur Anwendung. Strenge Anforderungen sind beim Einsatz externer Dienstleister bei der Bearbeitung von Visumanträgen geboten.

Nach langer Planung und Vorbereitung ist das europäische Visa-Informationssystem (VIS) seit 1. Oktober 2011 im Betrieb (vgl. 24. TB Nr. 2.2.5). Als gemeinsame europäische Datenbank verfolgt das VIS ähnliche Zwecke wie Eurodac (vgl. oben Nr. 5.16), nämlich die Prüfung der Identität einer Person und die Vermeidung von Mehrfachanträgen. Erfasst werden von diesem System Antragsteller für ein Kurzzeitvisum zur Einreise in den Raum der sogenannten Schnengen-Länder (EU außer Großbritannien, Irland, Rumänien, Bulgarien und Kroatien; ferner Schweiz, Liechtenstein, Norwegen, Island). In der VIS-Datenbank werden nicht nur personenbezogene Daten der Antragsteller selbst bis zu fünf Jahre gespeichert, sondern auch Daten von Personen erfasst, die Besuchseinladungen an visumpflichtige Antragsteller ausgesprochen haben. Neben den üblichen alphanumerischen Angaben wie Name, Vorname und Geburtsdatum werden zu den Visumantragstellern auch biometrische Daten (Fotos und Fingerabdrücke) gespeichert. Die Daten werden in der Regel bei Botschaften und Konsulaten der Mitgliedstaaten im Ausland erhoben und über nationale „Kopfstellen“ an die zentrale VIS-Datenbank in Straßburg weitergeleitet. Bis zum Ende des Jahres 2014 war der sog. roll-out des VIS weit fortgeschritten und soll voraussichtlich bis Ende 2015 abgeschlossen sein. Dann wird das VIS auch in Russland und in der Ukraine zur Anwendung kommen, den zwei Ländern mit dem höchsten Visumaufkommen.

Die Datenschutzaufsicht über das VIS folgt einem ähnlichen Modell wie bei Eurodac: Der Europäische Datenschutzbeauftragte (EDPS) kontrolliert die zentrale VIS-Datenbank, während die Datenschutzbehörden der Mitgliedstaaten die jeweiligen nationalen Komponenten des VIS überprüfen. In Deutschland bin ich für die datenschutzrechtliche Kontrolle zuständig, weil das Auswärtige Amt und das Bundesverwaltungsamt für den nationalen Teil des VIS verantwortlich sind. Um die Arbeit und die Kontrollschwerpunkte in den Mitgliedstaaten aufeinander abzustimmen, wurde auch beim VIS eine gemeinsame Kontrollaufsichtsgruppe unter Vorsitz des EDPS geschaffen, die sich mindestens zweimal jährlich trifft. An den Beratungen und Aktivitäten der VIS-Datenschutz-Aufsichtsgruppe nehme ich teil.

Im Berichtszeitraum hat die gemeinsame VIS-Datenschutzgruppe die Qualität der an das VIS-Zentralsystem übermittelten Daten geprüft, da die Verwaltungsbehörde des VIS, die europäische Agentur für große IT-Systeme (European larg-scale Information Systems Agency bzw. euLISA in Tallin, Estland) insbesondere bei biometrischen Daten große Unterschiede gemeldet hatte. Dabei stellte sich heraus, dass in den Anwenderländern des

Visa-Informationssystems die gebotenen modernen Techniken und Verfahren zur Sicherstellung eines hohen Datensicherheitsniveaus immer noch nicht flächendeckend eingesetzt werden.

Einen weiteren Untersuchungsgegenstand bildete der Einsatz von externen Dienstleistern bei der Entgegennahme und Vorbereitung von Visumanträgen bei Vertretungen der Mitgliedstaaten im Ausland. Letztere Maßnahme ist zwar nach Artikel 43 des Visakodex bzw. Verordnung (EG) 810/2009 des Europäischen Parlaments und des Rates grundsätzlich zulässig. Nach Auffassung der VIS-Datenschutz-Gruppe darf dies aber nur unter Bedingungen gelten, die einen angemessenen Schutz der sehr sensiblen personenbezogenen Daten über den gesamten Bearbeitungsprozess hinweg bei allen Beteiligten gewährleisten.

5.18 EU-Staatsangehörige im Ausländerzentralregister

Die Änderung des Ausländerzentralregistergesetzes (AZRG) erfordert eine datenschutzgerechte Umsetzung.

Schon im Jahr 2008 hat der Europäische Gerichtshof (EuGH) die Speicherung von Daten zu Unionsbürgern in einem zentralen Register wie dem AZR sowie deren Übermittlung an andere Behörden nur unter engen Voraussetzungen für zulässig erklärt (Urteil „Huber“ vom 16. Dezember 2008, Az. C-524/06). Wegen der Speicherung und Nutzung von Daten eines freizügigkeitsberechtigten Unionsbürgers im AZR entschied das Gericht seinerzeit, personenbezogene Daten von Unionsbürgern, die nicht Staatsangehörige der Bundesrepublik Deutschland sind, dürften nur dann im Register gespeichert und genutzt werden, wenn sie für die Anwendung aufenthaltsrechtlicher Vorschriften durch die hierfür zuständigen Behörden erforderlich seien.

Der zur Umsetzung dieses Urteils vorgelegte Referentenentwurf zur Änderung des AZRG berücksichtigte die datenschutzrechtlichen Vorgaben zunächst nur unzureichend. Erst im Laufe der Ressortabstimmung konnten unter meiner Mitwirkung deutliche Verbesserungen (vgl. 24. TB Nr. 16.15) erzielt werden. Das Änderungsgesetz zum AZRG vom 20. Dezember 2012 ist am 1. September 2013 vollständig in Kraft getreten (vgl. BGBl. I S. 2745).

Aufgrund dieser gesetzlichen Änderung musste im AZR zwischen freizügigkeitsberechtigten und nicht freizügigkeitsberechtigten Unionsbürgern sowie Drittstaatsangehörigen unterschieden werden. Diese Gruppen weisen nun unterschiedlich viele Speichermerkmale sowie Differenzierungen bei der Datenübermittlung durch und an Dritte auf.

Datenschutzrechtliche Probleme ergaben sich bei Betroffenen, die bisher keine EU-Bürger waren, dies aber zwischenzeitlich geworden sind. So stellte sich die Frage, ob und ggf. wie jetzt nicht mehr zum Datenempfang berechtigte Behörden durch die Registerbehörde im Falle einer Berichtigung, Löschung oder Sperrung (§ 38 Abs. 1 Satz 1 AZRG) benachrichtigt werden können, weil an diese für EU-Bürger keine Übermittlung mehr erfolgen darf. Zur Lösung dieses Problems hatte ich mich in einem ersten Schritt für ein Rundschreiben seitens des Bundesamtes für Migration und Flüchtlinge an die betroffenen Dienststellen eingesetzt, um für eine Übergangszeit ein einheitliches datenschutzgerechtes Verfahren vorzugeben. Seit Ende 2014 besteht eine den neuen Anforderungen entsprechende Lösung in rechtlicher und technischer Hinsicht, deren Umsetzung ich in meinen bereits vorgesehenen Beratungs- und Kontrollbesuch beim Bundesverwaltungsamt einbeziehen werde.

5.19 Visa-Warndatei

Die Visa-Warndatei bedarf angesichts des sensiblen Datenbestandes einer datenschutzfreundlichen Betriebsführung.

Die beim BVA geführte Visa-Warndatei soll den mit Visumverfahren befassten Auslandsvertretungen eine verbesserte Entscheidungsgrundlage bieten. Nutzer sind rund 1.000 öffentliche Stellen. Die Datei ist seit dem Inkrafttreten des Gesetzes zur Errichtung einer Visa-Warndatei (Visa-Warndateigesetz - VWDG vom 22. Dezember 2011) am 1. Juni 2013 in Funktion.

Das Gesetzgebungsvorhaben zum VWDG habe ich datenschutzrechtlich begleitet (vgl. zuletzt 23. TB Nr. 15.1). Gegenüber dem ursprünglichen Entwurf enthält das Gesetz datenschutzrechtliche Verbesserungen, insbesondere eine deutliche Reduzierung der zu speichernden Warnsachverhalte sowie den Verzicht auf Zugriffsbefugnisse der Sicherheitsbehörden und Nachrichtendienste einschließlich der Instrumente der Gruppenauskunft und des Suchvermerksverfahrens (vgl. zuletzt 24. TB Nr. 8.9).

Seit Inkrafttreten des VWDG wird die Visa-Warndatei sukzessive mit den jeweils auflaufenden Fällen befüllt. Es erfolgt somit keine Datenübernahme aus anderen Beständen. Dennoch wird mit der Visa-Warndatei ein sensibler Datenbestand aufgebaut, der ihr eine hohe datenschutzrechtliche Relevanz zukommen lässt.

Ich stehe mit dem BVA in Kontakt, um den Anlaufprozess mit Blick auf Funktionssicherheit, Datenschutz, Datensicherheit und Zugangsschutz zu begleiten. Erste positive oder negative Erfahrungen sollen zeitnah datenschutzfreundlich umgesetzt werden können.

Da das Visumverfahren in eine hochkomplexe „Landschaft“ verschiedener Register, Dateien und Verfahren funktional eingebunden ist (Ausländerzentralregister, Visa-Warndatei, Schengener Informationssystem, Euro-VIS, Datenabgleichverfahren mit der Antiterrordatei u. a.), werde ich mich mit dem Gesamtsystem und dem Zusammenspiel der einzelnen Komponenten weiter befassen.

5.20 Abgleich von Visumsantragsdaten mit der Antiterrordatei

Meine Bedenken gegen die gesetzliche Regelung blieben unberücksichtigt; nun bedarf der Betrieb des Datenabgleichverfahrens besonderer Beobachtung.

Das automatische Abgleichverfahren von Visumsantragsdaten mit der Antiterrordatei (ATD) ist eine wichtige Maßnahme im Visa-Prüfverfahren mit zugleich hoher datenschutzrechtlicher Relevanz. Mit dem Verfahren werden Daten der Visumantragsteller und Referenzpersonen im Inland mit dem visumrelevanten Teilbestand der ATD abgeglichen. Es arbeitet vollautomatisiert, also ohne manuelle fachliche Prüfung. Im Trefferfall werden die speichernden Sicherheitsbehörden beteiligt und die Versagungsgründe oder Sicherheitsbedenken an die jeweilige Auslandsvertretung zurückgemeldet.

Meine bereits im Gesetzgebungsvorhaben zu § 72a Aufenthaltsgesetz geäußerten Bedenken (vgl. 24. TB Nr. 8.9) halte ich aufrecht. Da die Regelung aber am 1. Juni 2013 in Kraft getreten ist, muss es nun darum gehen, die betriebliche Umsetzung der Anforderungen an die Funktionssicherheit, den Datenschutz, die Datensicherheit des automatischen Abgleichverfahrens mit der ATD und dessen Zugangsschutz in den Blick zu nehmen.

Angesichts der betroffenen sensiblen personenbezogenen Daten begrüße ich, dass das Verfahren im administrativen und technischen Hochsicherheitsbereich des BVA erfolgt. Auch der Abgleich von Visumsantragsdaten mit der ATD ist Teil des ineinandergreifenden Registersystems (vgl. oben Nr. 5.19), das neben der Kontrolle seiner einzelnen Bestandteile auch als Gesamtheit datenschutzrechtlich geprüft und bewertet werden muss. Dieser Aufgabe werde ich mich stellen.

5.21 Nationales Waffenregister

Der Betrieb des Nationalen Waffenregisters (NWR) muss auf gesetzlicher Grundlage den Anforderungen des Datenschutzes gerecht werden.

Nach den Vorgaben der europäischen Waffenrichtlinie (2008/51/EG) sind alle EU-Mitgliedstaaten verpflichtet, spätestens bis zum 31. Dezember 2014 auf nationaler Ebene ein computergestütztes Waffenregister zu schaffen und auf aktuellem Stand zu halten. Das nationale Register muss allen zuständigen Behörden Zugang zu den gespeicherten Daten eröffnen.

Wie der deutsche Gesetzgeber in § 43a Waffengesetz festgelegt hatte, war das NWR bereits bis Ende des Jahres 2012 - also zwei Jahre vor Ablauf der in der Europäischen Waffenrichtlinie vorgesehenen Frist - aufzubauen. Die genauen rechtlichen Grundlagen für das NWR schuf das am 1. Juli 2012 in Kraft getretene Gesetz zur Errichtung eines Nationalen Waffenregisters (NWRG - vgl. 24. TB Nr. 8.7; 23. TB Nr. 8.3).

Bei seinem Betrieb war ich u. a. in Fragen der automatisierten Bereinigung der aus ca. 550 örtlichen Dienststellen stammenden Daten eingebunden. Aufgrund der heterogenen Herkunft und Struktur muss der Datenbestand nach Erstaufnahme in das NWR im Hinblick auf für die Speicherung geltende einheitliche Standards bereinigt werden. Dies kann wirtschaftlich nur durch ein automatisiertes Verfahren erfolgen. Die fachliche Leitstelle (FL) bei der Waffenbehörde in Hamburg, die für das Bereinigungsverfahren geeignete Algorithmen entwickeln soll, benötigt zu Test- und Entwicklungszwecken Arbeitsdaten, die aus den Echtdaten des Nationalen Waffenregisters gewonnen werden sollen.

Um datenschutzrechtliche Risiken von vornherein auszuschließen, habe ich mich dafür eingesetzt, dass diese Arbeitsdaten von jeglichem Personenbezug befreit werden, es sich also nicht mehr um personenbezogene Daten im Sinne des BDSG handelt. Hierfür habe ich in Abstimmung mit dem BMI empfohlen, die Generierung der Arbeitsdaten ausschließlich im BVA unter strenger Beachtung von Datenschutz und Datensicherheit durchführen zu lassen. Hierbei sollen die einzelnen Datensätze einen neuen arbeitsbezogenen Ordnungsbegriff, der sich nicht aus dem Echtdatensatz ableitet, erhalten. In den Arbeitsdaten sollen die unter Umständen mit personenbezogenen Daten befüllten Freitextfelder sicherheitshalber ausnahmslos gelöscht werden, ebenso wie personenbezogene Daten in allen Datensätzen. Ferner sollen auch diejenigen Sachdatenfelder gelöscht werden, die für den vorgesehenen Zweck - Analyse und Algorithmusentwicklung - nicht erforderlich sind. Erst der so geschaffene Datenbestand soll der FL zur Verfügung gestellt werden. Eine Anwendung des auf dieser Basis entwickelten Bereinigungs-Algorithmus auf den Echtdatenbestand soll erst nach sorgfältigen Tests erfolgen dürfen.

Bei der Datenbereinigung handelt es sich um einen umfangreichen mehrjährigen Prozess, der voraussichtlich bis zum Ende des Jahres 2017 dauern wird. Ich werde dieses Thema sowie den Betrieb des NWR insgesamt weiter begleiten.

5.22 Selbstauskunft aus dem Nationalen Waffenregister - nicht ohne Identitätsnachweis

Für Auskünfte aus dem Nationalen Waffenregister (NWR) müssen wegen der Schutzbedürftigkeit dort gespeicherter Daten hohe Anforderungen an die Feststellung der Identität des Antragstellers gestellt werden.

Ein Bürger hatte beim BVA eine Auskunft über die ihn betreffenden Daten im NWR nach § 19 NWRG beantragt. Im Antrag nannte er seinen Familiennamen, Vornamen, seine Anschrift sowie Geburtsdatum, Ort und Staat der Geburt. Der Antrag war eigenhändig unterschrieben. Das BVA bat den Petenten um Vorlage einer amtlich beglaubigten Kopie seines Personalausweises/Reisepasses oder Vorlage des ausgefüllten amtlichen Antragsformulars mit einer amtlichen Beglaubigung seiner Unterschrift durch eine siegelführende Stelle. Wegen der Schutzbedürftigkeit der im NWR gespeicherten Daten, so seine Begründung, seien an die Feststellung der

Identität der Antragsteller hohe Anforderungen zu stellen, was die Vorlage der genannten Unterlagen erfordere. Der Petent hielt die Anforderung von Nachweisen vor Erteilung der beantragten Auskunft für rechtswidrig; das Gesetz fordere lediglich im Fall des § 19 Absatz 3 NWRG (elektronische Auskunftserteilung) besondere Identitätsnachweise. Das BVA hielt am geforderten Identitätsnachweis fest, weil die schützenswerten Informationen über den privaten Waffenbesitz auch im Interesse aller gespeicherten Personen nur an Berechtigte übermittelt werden dürften. Die Sensibilität der Daten erfordere eine eindeutige Feststellung der Identität des Antragstellers. Das BVA stellte dem Petenten anheim, im Falle der Vorlage einer amtlich beglaubigten Kopie des Personalausweises oder Reisepasses Schwärzungen nicht benötigter Angaben vorzunehmen; auf Grund der datenschutzrechtlichen Bestimmungen werde die Kopie unverzüglich vernichtet, sobald der mit der Kopie verfolgte Zweck erreicht sei. Auch erfolge keine automatisierte Speicherung übersandter Ausweiskopien.

Nach eingehender rechtlicher Prüfung des Sachverhaltes habe ich mich der Sichtweise des BVA angeschlossen, da es um den Schutz hochsensibler personenbezogener Daten vor unbefugter Übermittlung geht. Meine Ansicht wurde schließlich auch vom Verwaltungsgericht Köln bestätigt, vor dem der Petent Klage gegen das BVA erhoben hatte (Urteil vom 13.03.2014, Az. 13 K 3624/13). Auch nach der Auffassung des Verwaltungsgerichts stand der Erteilung der begehrten Auskunft entgegen, dass der Kläger den zu Recht geforderten Identitätsnachweis nicht eingereicht hat. Das Gericht wies insbesondere darauf hin, je nach Art der Daten, über die Auskunft verlangt wird, seien die schutzwürdigen Belange des tatsächlich Betroffenen in unterschiedlicher Weise zu gewichten: Je heikler die Daten, desto höhere Anforderungen seien an den Identitätsnachweis zu stellen.

5.23 Videoanhörung im Asylverfahren

Videoanhörungen in Asylverfahren müssen dem Persönlichkeitsrecht der Betroffenen gerecht werden.

Durch eine Petition bin ich auf die durch das Bundesamt für Migration und Flüchtlinge (BAMF) in mehreren Bundesländern eingeführte Praxis aufmerksam geworden, Anhörungen in Asylverfahren mittels Videokonferenztechnik durchzuführen. Hierdurch sahen sich betroffene Asylsuchende in ihren Persönlichkeitsrechten verletzt.

Wie meine Überprüfung ergab, wurden Asylsuchende einem Mitarbeiter des BAMF lediglich per Videokonferenz zugeschaltet, obwohl sie gemäß § 24 Asylverfahrensgesetz (AsylVerfG) grundsätzlich persönlich anzuhören sind. Es erscheint nachvollziehbar, dass ein solches Vorgehen geeignet ist, die Betroffenen zu verunsichern oder sogar einzuschüchtern. Auch die bei solchen Anhörungen insbesondere bei besonders belasteten Flüchtlingsgruppen (Folter- und Gewaltopfer sowie Traumatisierte) ausschlaggebende nonverbale Kommunikation kann ohne persönlichen Kontakt erfahrungsgemäß nur unzureichend wahrgenommen werden. Die Befassung des Innenausschusses des Deutschen Bundestages mit dieser Thematik hatte in der vorigen Legislaturperiode zeitweise zu einer Einstellung bzw. Einschränkung der Videoanhörung geführt.

Datenschutzrechtlich klärungsbedürftig war schließlich der Umgang mit den Videoaufzeichnungen nach Abschluss des Asylverfahrens, insbesondere ob es Löschungsfristen gibt und wer Zugriff auf die Aufzeichnungen erhält.

Schließlich erließ das BAMF eine neue Dienstanweisung, die auch Regelungen zu den vorbezeichneten datenschutzrechtlichen Fragen beinhaltet. Diese stellen einen deutlichen Entwicklungsschritt zu mehr Persönlichkeitsschutz im Asylverfahren dar.

5.24 Auswertung von Datenträgern bei Rückführungen?

Die Bundesregierung plant, bei ausreisepflichtigen Ausländern, deren Identität ungeklärt ist, mitgeführte Datenträger für die Rückführung auszuwerten. Dies stößt auf Bedenken.

Seit Mai 2014 wird der Entwurf eines Gesetzes zur Neubestimmung des Bleiberechts und der Aufenthaltsbeendigung diskutiert. Im Zentrum des Entwurfs stehen zum einen das Bleiberecht, zum anderen die Neuausrichtung des Ausweisungsrechts sowie der Abbau rechtlicher Vollzugshindernisse in der Aufenthaltsbeendigung.

Von besonderem datenschutzrechtlichem Interesse ist hierbei die Neuregelung des § 48 Absatz 3 Aufenthaltsgesetz (AufenthG), der die Vorlage- und Überlassungspflicht auf „Datenträger" - also vor allem Mobiltelefone und (Klein-)Computer - erweitern will. Danach haben Ausländer die mitgeführten Datenträger sowie die notwendigen Zugangsdaten für eine zulässige Auswertung zur Verfügung zu stellen. Da oftmals die ungeklärte Identität der Rückführung ausreisepflichtiger Ausländer entgegen steht, sollen so Anknüpfungspunkte für die Bestimmung der Staatsangehörigkeit oder des Heimatlandes gesucht werden. Hinweise für weitere Ermittlungen bei den Behörden des möglichen Heimatstaates lassen sich nicht nur schriftlichen Unterlagen, sondern in zunehmendem Maße mitgeführten Datenträgern entnehmen; so könnten etwa die Adressdaten in einem Mobiltelefon oder die gespeicherten Verbindungsdaten aufgrund der Auslandsvorwahl wesentliche Anhaltspunkte für die Staatsangehörigkeit geben. Gleiches gilt für in (Klein-)Computern gespeicherte Reiseunterlagen.

Mit der vorgesehenen Neuregelung wird datenschutzrechtliches Neuland betreten. Bisher ist eine „Durchsuchung von Datenträgern" nur in zwei Fällen gesetzlich geregelt: Bei dem Verdacht auf bestimmte Straftaten nach der Strafprozessordnung und auf extremistische Bestrebungen nach dem Bundesverfassungsschutzgesetz. Nun soll zusätzlich die Fallgruppe des „nicht kooperierenden Ausländers im Rückführungsverfahren" geschaffen werden. In der Ressortabstimmung habe ich meine Bedenken gegen eine solche Regelung geäußert, denn jede Auswertung von Datenträgern ist mit dem Risiko verbunden, dass auch Daten aus dem Kernbereich der privaten Lebensführung an Dritte gelangen, was verfassungsrechtlichen Bedenken unterliegt. Eine solche Auswertung von Datenträgern ist daher nur in begrenzten Ausnahmefällen zuzulassen. Ich werde das Gesetzgebungsvorhaben weiterhin kritisch begleiten.

5.25 Forschungsprojekt des Bundesamtes für Migration und Flüchtlinge zu einer Repräsentativbefragung ausgewählter Migrantengruppen in Deutschland (RAM 2015)

Die Übermittlung von Meldedaten an das Bundesamt für Migration und Flüchtlinge (BAMF) im Rahmen des Forschungsprojektes begegnet keinen Bedenken.

Das BAMF hat sich an mich gewandt, um datenschutzrechtliche Fragen im Zusammenhang mit einem geplanten Forschungsprojekt zu erörtern. Das BAMF hat als nachgeordnete Behörde des BMI gem. § 75 Nummer 4 Aufenthaltsgesetz den gesetzlichen Auftrag, wissenschaftliche Forschung zu Fragen der Migration und Integration zu betreiben. Vorrangiges Ziel ist die Gewinnung analytischer Aussagen zur Steuerung der Zuwanderung. Für das Jahr 2014 war u. a. die Durchführung eines Forschungsprojektes mit dem Namen „Repräsentativbefragung ausgewählter Migrantengruppen in Deutschland (RAM 2015)" vorgesehen, bei dem türkische, polnische und rumänische Staatsangehörige in Deutschland befragt werden sollten. Außerdem sollten Deutsche mit türkischem Migrationshintergrund berücksichtigt werden. Insgesamt waren 2.400 Interviews geplant, jeweils 600 für jede der vier Befragungsgruppen. Als Datengrundlage schied das Ausländerzentralregister (AZR) aus, da hierdurch lediglich die Gruppe der türkischen Staatsangehörigen hätte bestimmt werden können. Rumänische und polnische Staatsangehörige dürfen als EU-Ausländer aus rechtlichen Gründen nicht zu diesem Zweck aus dem AZR gezogen werden, Deutsche mit türkischem Migrationshintergrund sind im AZR nicht gespeichert. Um unterschiedliche Datengrundlagen bei der Stichprobenziehung zu vermeiden, war daher die Ziehung aller vier Gruppen aus den Einwohnermelderegistern vorgesehen.

Anlässlich eines datenschutzrechtlichen Beratungsgesprächs beim BAMF habe ich darauf hingewiesen, dass die Stichprobenziehung aus den Einwohnermelderegistern nur auf der Basis einschlägiger Rechtsgrundlagen der Meldegesetze der Länder erfolgen darf, wobei Grundlage hierfür grundsätzlich das Melderechtsrahmengesetz (MRRG) darstellt. Ich habe dem BAMF vorgeschlagen, eine gutachterliche Stellungnahme des Fachreferats des BMI einzuholen und auf deren Basis zwecks Einwilligung wieder an mich heranzutreten.

In der Stellungnahme des BMI werden die Datenübermittlungen für die verschiedenen Herkunftsgruppen detailliert rechtlich erörtert. Als zentrale Rechtsgrundlage für die Stichprobenziehung wurde § 18 MRRG identifiziert. Nach Prüfung habe ich mich der Stellungnahme des BMI angeschlossen und dies dem BAMF mitgeteilt. Bezüglich des vom BAMF sodann vorgesehenen Übermittlungsverfahrens der Daten von den Einwohnermeldeämtern an das BAMF erhebe ich daher keine Bedenken - ein gutes Beispiel dafür, dass die frühzeitige Einbeziehung meiner Dienststelle bei der Durchführung von (Forschungs-)Projekten zu datenschutzgerechten Lösungen führen kann.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit
- Arbeitskreis Grundsatzfragen,
- Unterarbeitsgruppe Auftragsdatenverarbeitung/Outsourcing,
- Unterarbeitsgruppe Geodaten,
- Arbeitskreis Verwaltungsmodernisierung,
- Arbeitskreis Beschäftigtendatenschutz,
- Arbeitskreis Statistik,
- Ad-hoc Arbeitsgruppe Zensus 2011,
- Arbeitskreis Sicherheit,
- Unterarbeitsgruppe INPOL,
- Unterarbeitsgruppe Europa,
- Arbeitskreis Technik,
- Unterarbeitsgruppe „Elektronische Gesundheitskarte“

Düsseldorfer Kreis mit
- Arbeitsgruppe Auskunfteien,
- Arbeitsgruppe Kreditwirtschaft,
- Arbeitsgruppe Versicherungswirtschaft,
- Arbeitsgruppe Internationaler Datenverkehr,
- Ad-hoc Arbeitsgruppe Werbung und Adresshandel,
- Workshop der Aufsichtsbehörden,
- Ad-hoc Arbeitgruppe Videoüberwachung

Arbeitsgemeinschaft für Datentransparenz nach § 303b SGB V

NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) mit
- NA 043-01-27-05 AK Arbeitskreis Identitätsmanagement und Datenschutz-Technologien,
- NA 043-01-37 AA Arbeitsausschuss Biometrie,
- NA 043-01-17 AA Arbeitsausschuss Karten und persönliche Identifikation,
- NA 043-01-51 AA Arbeitsausschuss Vernichten von Datenträgern

Arbeitskreis Identitätsmanagement und Datenschutz-Technologien beim DIN
Koordinierungsstelle IT-Sicherheit (KITS) Fachbeirat beim DIN
IT-Sicherheitsmanagement im Geschäftsbereich des Bundesministeriums des Innern
IT-Rat der Bundesregierung mit
- IT-Sicherheitsmanagement der Ressorts (Unterarbeitsgruppe IT-Rat)
- Netz des Bundes (Unterarbeitgruppe IT-Rat)

Arbeitsgruppe 4 des IT-Gipfels: Vertrauen, Datenschutz und Sicherheit im Internet mit
- Unterarbeitsgruppe 1 IT-Gipfel: Cloud Computing,
- Unterarbeitsgruppe 2 IT-Gipfel: Anforderungen an Sichere Identitäten,
- Unterarbeitsgruppe 4 IT-Gipfel: Mobile Sicherheit

IT-Planungsrat

Gemeinsame Kontrollinstanz Europol
Gemeinsame Kontrollinstanz Schengen
Gemeinsame Kontrollinstanz Zoll
Kontroll- und Koordinierungsgruppe des Zollinformationssystems (ZIS)
Eurodac-Koordinierungsgruppe
VIS-Koordinierungsgruppe
Competence Center for Applied Security Technology e. V. (CAST)
Statistischer Beirat nach § 4 BStatG

Mitarbeit in der Ressort-AG Digitale Verwaltung 2020 (beratendes Mitglied)

B. Zudem von besonderem Interesse

Nr. 2.1, 2.2, 2.4, 2.5, 2.6, 6.1, 6.4, 7.11, 8.4, 8.5, 8.6, 16.3, 17.1, 18.1, 22.2, 23.2

6 Ausschuss für Recht und Verbraucherschutz

6.1 Verbandsklagerecht bei Datenschutzverstößen

Die vom Bundesministerium der Justiz und für Verbraucherschutz vorgeschlagene Stärkung der Verbandsrechte bei Verstößen gegen datenschutzrechtliche Bestimmungen nach dem Unterlassungsklagengesetz ist angesichts der staatlichen Datenschutzaufsicht nicht erforderlich und darf nicht zu deren Schwächung führen.

Wie im Koalitionsvertrag vereinbart, sollen Verbraucherverbände künftig datenschutzrechtliche Verstöße abmahnen und Unterlassungsklage erheben können. Der im Juni 2014 vom Bundesministerium der Justiz und für Verbraucherschutz vorgelegte Entwurf eines „Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“ sieht hierzu eine Erweiterung des Unterlassungsklagengesetzes (UKlaG) vor. Datenschutzrechtliche Vorschriften, die die Datenverarbeitung personenbezogener Daten eines Verbrauchers durch einen Unternehmer betreffen, sollen künftig als Verbraucherschutzgesetze im Sinne des UKlaG gelten. Ein datenschutzwidriger Umgang mit „Verbraucherdaten“ berechtigt Verbraucherverbände und andere anspruchsberechtigte Stellen wie Wirtschaftsverbände und Industrie- und Handelskammern, Unternehmen kostenpflichtig abzumahnen und gegebenenfalls Unterlassungsklage vor den Zivilgerichten zu erheben.

So sehr ich Initiativen zur Stärkung des Datenschutzes begrüße, halte ich doch die Erweiterung zivilrechtlicher Verbandsrechte auf datenschutzrechtliche Verstöße für problematisch. Schon von seiner Konzeption her ist das Datenschutzrecht kein Verbraucherschutzrecht. Im Gegensatz zum Verbraucherschutz schützt der Datenschutz nicht die wirtschaftliche Handlungs- und Entscheidungsfreiheit von Verbrauchern, sondern die informationelle Handlungs- und Entscheidungsfreiheit in Ausübung des (Grund-)Rechts auf informationelle Selbstbestimmung. Wo es um die Verarbeitung von „Verbraucherdaten“ geht, entfaltet das Datenschutzrecht zwar mittelbar verbraucherschützende Funktion, diese ist aber eine Nebenfolge und nicht eigentliches Regelungsziel des Datenschutzes. Diese auch in der Rechtsprechung anerkannten unterschiedlichen Zielrichtungen von Daten- und Verbraucherschutz negiert der Gesetzentwurf durch eine gesetzliche Fiktion, mit welcher die datenschutzrechtlichen Vorschriften kurzerhand zu Verbraucherschutzvorschriften gemacht werden.

Bedeutsamer ist jedoch, dass über die Einhaltung der datenschutzrechtlichen Vorschriften unabhängige staatliche Datenschutzbehörden wachen, an die sich jedermann unentgeltlich mit einer Beschwerde wenden kann. Im Gegensatz zu den Verbänden nach dem UKlaG verfügen die Datenschutzbehörden über umfassende Ermittlungs- und Sanktionsbefugnisse. Den Aufsichtsbehörden der Länder stehen weitgehende Auskunfts-, Einsichts- und Prüfungsrechte sowie Anordnungs- und Untersagungsbefugnisse gegenüber den Daten verarbeitenden Stellen zu. In den ganz überwiegenden Fällen sind die Aufsichtsbehörden zuständige Bußgeldbehörden und strafantragsbefugt. Das verwaltungsbehördliche Instrumentarium ist für eine effektive Rechtsdurchsetzung notwendig, aber auch ausreichend.

Zwingend erforderlich sind die Verbandsrechte bei datenschutzrechtlichen Verstößen daher nicht - im Gegenteil birgt die geplante Parallelstruktur zivil- und verwaltungsrechtlicher Rechtsdurchsetzung Nachteile.

Zum einen besteht die Gefahr der Schwächung der behördlichen Datenschutzaufsicht, die nach den Vorgaben der europäischen Datenschutzrichtlinie 95/46/EG institutionell über die Einhaltung der datenschutzrechtlichen Vorschriften durch Behörden und Unternehmen zu wachen hat. Viele Unternehmen - aus meinem Zuständigkeitsbereich vor allem die Telekommunikationsbranche - nehmen bereits im Vorfeld Kontakt zu den Datenschutzbehörden auf, um ihre Verfahren und Geschäftsideen rechtssicher datenschutzkonform auszugestalten. Der gesetzlich vorgesehene Beratungsauftrag der Aufsichtsbehörden (§ 38 Abs. 1 Satz 2 BDSG) würde erheblich geschwächt, wenn Vereinbarungen, die aus Sicht der Aufsichtsbehörden ein ausreichendes Datenschutzniveau gewährleisten, durch Abmahnungen und Verbandsklagen im Nachhinein in Frage gestellt würden. Unternehmen, die davon ausgehen müssen, ihre Verfahren würden ohnehin über das UKlaG einer gerichtlichen Prü-

fung unterzogen werden, dürften sich künftig kaum mehr der mitunter aufwändigen und zeitintensiven Mühe unterziehen, ihre Vorhaben vorab mit der Datenschutzaufsicht abzustimmen. Für einen proaktiven Datenschutz wäre dies von Nachteil. Die Rechtsanwender erwarten im Hinblick auf Investitionssicherheit zu Recht eine hinreichende Verlässlichkeit behördlicher Entscheidungen.

Zum anderen drohen durch die Parallelität zivil- und verwaltungsrechtlicher Rechtsdurchsetzung Friktionen der Rechtseinheit. Während aufsichtsbehördliche Anordnungen von den Verwaltungsgerichten geprüft werden, werden die Ansprüche nach dem UKlaG vor den Zivilgerichten geltend gemacht. Beide Gerichtszweige sind untereinander nicht an die jeweiligen Entscheidungen der anderen Gerichtsbarkeit gebunden, zumal unterschiedliche prozessuale Grundsätze und rechtliche Beurteilungsmaßstäbe gelten. Die bereits heute bestehende Problematik divergierender Entscheidungen von Zivil- und Verwaltungsgerichten würden künftig weiter vertieft werden, wie die beiden nachfolgenden Fälle exemplarisch zeigen:

So bejahte das Kammergericht Berlin (Urteil vom 24.01.2014, Az. 5 U 42/12) in einem Verfahren gegen Facebook die amerikanische Konzernmutter als datenschutzrechtlich verantwortliche Stelle und bejahte die Anwendbarkeit des BDSG (§ 1 Abs. 5 Satz 2), während das Oberverwaltungsgericht Schleswig (Beschluss vom 22.04.2014, Az. 4 MB 11/13) in einem Verfahren des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein gegen Facebook die Anwendbarkeit des BDSG mit dem Argument verneinte, die irische Konzerntochter sei die datenschutzrechtlich verantwortliche Stelle, weshalb irisches Datenschutzrecht anzuwenden sei (§ 1 Abs. 5 Satz 1 BDSG).

Mit Urteil vom 30.04.2013 (Az. 15 O 92/12) erklärte das Landgericht Berlin allein unter Anwendung der Rom-I-Verordnung deutsches AGB-Recht - und somit auch das BDSG - auf die Datenschutzrichtlinie des IT-Anbieters Apple für anwendbar, und zwar unabhängig von § 1 Absatz 5 BDSG, der die Anwendbarkeit des BDSG davon abhängig macht, ob die Datenverarbeitung durch eine Niederlassung in einem Drittland wie den USA (dann BDSG) oder in einem Mitgliedstaat der EU wie Irland (dann irisches Datenschutzrecht) erfolgt.

In jedem Fall sollte der Anwendungsbereich des UKlaG deutlich eingegrenzt werden. Verbandsklagerechte sollten keineswegs dazu führen, dass Unternehmen, die zur Erfüllung ihrer vertraglichen Pflichten mit ihren Kunden oder gar gesetzlichen Verpflichtungen zwingend personenbezogene Daten erheben und verarbeiten müssen, einem Abmahnrisiko ausgesetzt werden. Weiterhin werde ich mich in Anlehnung an die für die Bundesanstalt für Finanzdienstleistungsaufsicht geltende Regelung des § 8 Absatz 2 UKlaG für eine gerichtliche Anhörungspflicht der zuständigen Aufsichtsbehörde für Klagen mit datenschutzrechtlichem Bezug aussprechen, um zumindest einen institutionalisierten und formalisierten Informationsaustausch zwischen Datenschutzbehörden und klagenden Verbänden spätestens in zivilgerichtlichen Verfahren sicher zu stellen.

Der nach Redaktionsschluss am 4. Februar 2015 beschlossene Gesetzentwurf der Bundesregierung greift diese beiden Aspekte auf; meine dargestellten Vorbehalte gegen die Schaffung von Verbandsklagerechten bei datenschutzrechtlichen Verstößen werde ich jedoch weiterhin in das laufende Gesetzgebungsverfahren einbringen.

6.2 Ins Netz gegangen - Öffentlichkeitsfahndung 2.0

Strafverfolgungsbehörden nutzen verstärkt das Internet und soziale Netzwerke, um öffentlich nach Personen zu fahnden. Diese Maßnahme greift intensiv in Grundrechte ein.

Die Justizministerkonferenz möchte die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) ändern. Ein Entwurf der Konferenz will es erlauben, erstmals in großem Umfang Öffentlichkeitsfahndungen in sozialen Netzwerken privater Anbieter zu platzieren. Das ist nach den bisherigen Richtlinien in der Regel nicht möglich. Aber auch die im Entwurf vorgeschlagenen Regelungen sind wenig geeignet, die gesetzlichen Vorgaben und die Verhältnismäßigkeit der Maßnahmen einzuhalten. Dass einige der vorgeschlagenen Formulierungen auch daten-

schutzrechtliche Verbesserungen mit sich bringen, führt angesichts dieser Kritikpunkte nicht zu einer anderen Beurteilung insgesamt.

Die Strafprozessordnung erlaubt eine öffentliche Fahndung schon bei dem Verdacht einer „Straftat von erheblicher Bedeutung“. Diese gesetzlich geregelten Voraussetzungen sind allerdings im Lichte der Verhältnismäßigkeit auszulegen. Das verlangt weitere ungeschriebene Begrenzungen. Deshalb ist stets danach zu differenzieren, auf welchem Weg die Fahndungsdaten veröffentlicht werden. Dies kann ein nur lokal begrenzter Aushang in Tatortnähe sein oder aber die weltweit und dauerhaft abrufbare Öffentlichkeitsfahndung in sozialen Netzwerken. In der Praxis der Bundespolizei führte in einem Einzelfall bereits der Verdacht der Fundunterschlagung eines Mobiltelefons zu einer öffentlichen Fahndung im Internet. Informationen, die einmal im Netz sind, lassen sich nicht wieder zurückholen. Es ist stets damit zu rechnen, dass einmal im Internet publizierte Daten von Dritten kopiert und weiter veröffentlicht werden. Wenn sich später ein Verdacht entkräften lässt, bleibt der Betroffene trotzdem als schon einmal gesuchte Person dauerhaft im Internetgedächtnis. Deshalb dürfte für eine Öffentlichkeitsfahndung im Internet oder in sozialen Netzwerken eine Straftat von erheblicher Bedeutung in der Regel nicht mehr ausreichen, wenn die Verhältnismäßigkeit gewahrt bleiben soll.

„Diskussionsforen“ können den Ruf einer Person ebenfalls nachhaltig beeinträchtigen. Sie gehören daher jedenfalls nicht auf Internetseiten der Strafverfolgungsbehörden. Mit der Kommentierungsfunktion in sozialen Netzwerken stellen die Strafverfolgungsbehörden jedoch ein solches öffentliches Diskussionsforum zur Verfügung. Als erstes stellt sich hier - wie bei jedem Handeln einer Behörde - die Frage, ob die Maßnahme geeignet und erforderlich ist. Ich vermag nicht zu erkennen, wie eine von den Strafverfolgungsbehörden initiierte öffentliche Diskussion für die Aufklärung eines Falles überhaupt dienlich sein kann. Allein der Hinweis, auf diese Weise lasse sich unter Marketingaspekten ein großes Publikum am einfachsten erreichen, genügt nicht.

Aber selbst wenn dieses Mittel geeignet wäre, wäre die Maßnahme jedenfalls nicht erforderlich. Sachdienliche Hinweise können Zeugen auch ohne öffentliche Diskussion der Strafverfolgungsbehörde mitteilen. Deswegen kann es auch nicht darauf ankommen, wie stark das öffentliche Forum moderiert oder kontrolliert wird. Denn ein Hinweis mag auf den ersten Blick als nicht personenbezogen gelten, kann sich aber nach gewisser Zeit aufgrund hinzugekommener Verknüpfungen - etwa durch weitere Leserkommentare - zunehmend auf eine Person oder einen engeren Personenkreis beziehen (und sei es nur auf eine Personengruppe). Fatal wäre es beispielsweise, wenn Nutzer zunächst sehr abstrakt, dann aber immer weniger abstrakt eine Personengruppe umschreiben, die ohnehin Diskriminierungen ausgesetzt ist. An welcher Stelle dann die Polizei die Reißleine ziehen soll, bleibt unklar.

Deswegen habe ich erhebliche Bedenken, die Dienstleistungen sozialer Netzwerke für Öffentlichkeitsfahndungen zu nutzen. Die Ermittlungsbehörden sind für die Fahndungsdaten datenschutzrechtlich verantwortlich. Deshalb dürfen sie es nicht unreglementiert einem Drittanbieter überlassen, diese Daten zu verarbeiten. Sie müssen sich die Einwirkungsmöglichkeiten auf die Daten sichern, insbesondere zur Löschung. Auch müssen sie sicherstellen, dass die Daten auf einem Server im Geltungsbereich deutscher oder europäischer datenschutzrechtlicher Vorschriften bereitgestellt werden. Hindernisse bei der Weitergabe sind zwar nicht schädlich, gleichwohl technisch fragwürdig und ändern nichts daran, dass die Öffentlichkeitsfahndung nur unter restriktiven Voraussetzungen zugelassen werden darf.

Die 87. Datenschutzkonferenz hat dazu eine Entschließung verabschiedet (vgl. Anlage 8). Diese Entschließung habe ich ebenso wie meine vorgenannten Bedenken den innen- und rechtspolitischen Sprechern der Fraktionen des Deutschen Bundestages schriftlich übermittelt.

6.3 Elektronische Akte im Strafverfahren

Die elektronische Akte im Strafverfahren verändert die datenschutzrechtlichen Rahmenbedingungen erheblich und grundsätzlich und erhöht die Gefahren für das Recht auf informationelle Selbstbestimmung. Der vorliegen-

de Gesetzentwurf setzt die Anforderungen an die Grenzen der Verwendungsbefugnis der gespeicherten Daten wie auch die Ausgestaltung der technisch-organisatorischen Maßnahmen nur unzureichend um.

Zwei unterschiedliche Speicherformen bestimmen bislang die Praxis der Datenverarbeitung: Auf der einen Seite gibt es die herkömmlichen Akten. Sie dienen vor allem dazu, das behördliche Vorgehen zu dokumentieren und die jeweiligen Einzelfälle zu bearbeiten. Die Akten sind das „Verwaltungsgedächtnis". Auf der anderen Seite verfügen die Ermittlungsbehörden über automatisierte Dateisysteme zur vorbeugenden Gefahrenabwehr. Damit können sie umfassend und schnell auf Daten aus verschiedensten Verfahren und Zusammenhängen zugreifen, diese recherchieren und abgleichen. Dafür müssen sie aber bei den automatisierten Systemen höhere Schwellen beachten. Mit der elektronischen Akte verschwimmt diese Differenzierung.

Die beiden „Pole" hat das Bundesverfassungsgericht schon im Volkszählungsurteil einander gegenübergestellt. Das Recht auf informationelle Selbstbestimmung bedürfe „unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes". Dieses Recht „ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (…) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind." Es besteht die Gefahr, Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammenzuführen (BVerfGE 65, 1, 42).

Diese vom Gericht bereits 1983 beschriebenen Möglichkeiten und Gefahren sind heute realer denn je. In der Praxis verwenden vor allem die Polizeibehörden Daten aus Strafverfahren über das jeweilige Verfahren hinaus. Dazu haben sie umfassende Dateisysteme errichtet. Die Daten werden nicht nur in den polizeilichen Informationsverbund (INPOL) gespeichert. Die Daten fließen darüber hinaus in viele weitere Einzeldateien (z. B. Zentraldateien oder Arbeitsdateien in Bund und Ländern). Hinzu kommen geplante neue Informations- und Analyseverbünde. Diese sollen sehr große Datenbestände aufnehmen. Mit ihnen sind umfassende Auswertungen und Analysen denkbar. Die Polizeibehörden übermitteln zudem Daten an Nachrichtendienste oder richten gemeinsame Dateien und Zentren mit ihnen ein. Für die bisher bestehenden Dateien hat der Gesetzgeber deshalb Grenzen gesetzt. Dies gilt zumindest für die Frage, welche Daten überhaupt dateimäßig erfasst werden dürfen. So ist nach § 8 Absatz 2 des Bundeskriminalamtgesetzes bzw. nach § 484 Absatz 2 der Strafprozessordnung (StPO) eine sog. Negativprognose notwendig, wenn die Ermittlungsbehörde etwa Daten in eine Kriminalakte oder in INPOL aufnimmt (vgl. Nr. 5.13.1und 5.13.3). Nur dann dürfen die Daten für künftige Strafverfahren zur Verfügung stehen.

Diese Begrenzungen darf der Gesetzesentwurf (abrufbar auf der Internetseite des BMJV unter www.bmjv.bund.de) nicht aushöhlen. Das wäre jedoch der Fall, wenn die elektronische Akte umfassend elektronisch recherchierbar und auswertbar wäre und die Daten ohne weiteres in andere Verfahren überführt werden könnten. Die allgemeinen Datenschutzbedingungen und die entsprechenden der StPO sollen offenbar nicht gelten. Das ist jedenfalls der Formulierung zu entnehmen, die elektronische Akte sei keine „Datei". Der Entwurf sieht dafür vor, dass der automatisierte Datenabgleich nur mit „zuvor individualisierten Akten" durchgeführt werden darf. Nach welchen Kriterien dies geschehen soll, wird nicht geregelt. Zudem enthält der Entwurf keine Begrenzungen für den Abfluss dieser erstmals vollständig elektronisch erfassten personenbezogenen Daten in andere automatisierte Verfahren - etwa die genannten Informationsverbünde.

Unklar ist nach dem Entwurf auch, wie das praktische Umfeld auszugestalten ist. So stellt sich etwa die Frage, welche Stelle die Akten faktisch führen wird. In der Papierwelt heftet häufig der bearbeitende Kriminalbeamte die Akte zusammen und sendet sie an die Staatsanwaltschaft. Diese entscheidet über den weiteren Fortgang und leitet die Akte an das Gericht weiter. Daher ist zu klären, ob der Gesetzentwurf dieses Verfahren auch elektronisch abbilden kann und will. Daran knüpfen sich aber weitere Fragen, beispielsweise:

Welche Stelle und welcher Mitarbeiter haben welche Zugriffsberechtigungen? Welche Recherchemöglichkeiten hat die Polizei in herkömmlichen und in elektronischen Akten? Kann die Polizei sich beim elektronischen Verfahren Schnittstellen zu eigenen Analyseverbünden programmieren und sind weitere Schnittstellen denkbar, etwa zum Verfassungsschutz? Zu all diesen Punkten fehlen noch klare Regelungen.

Auch die vorgesehenen Regelungen zur IT-Sicherheit und zur elektronischen Kommunikation haben Defizite. So überlässt es der Gesetzgeber weitgehend Rechtsverordnungen des Bundes und der Länder, die technische Sicherheit zu regeln. Damit ist nicht einmal ein bundeseinheitlicher Standard geschaffen, obwohl die Begründung des Entwurfs sogar eine bundesweite zentralisierte Speicherung nicht ausschließt, ohne dafür allerdings eine Befugnis zu schaffen.

Die Akte soll auch als Datenverarbeitung im Auftrag geführt werden können. Dazu soll es nach dem Entwurf möglich sein, private Dienstleister einzuschalten. Im Vorentwurf aus dem Jahr 2012 wurde dies noch mit dem Argument verworfen, dass es eine hoheitliche Kernaufgabe sei, die Akte zu führen. Sie müsse im unmittelbaren staatlichen Einflussbereich verbleiben (S. 83 der Begründung 2012). Diese zutreffende Einschätzung wird nun mit dem Argument der „wirtschaftlichen Interessen der Länder an einer Auslagerung von IT-Dienstleistungen auf Privatunternehmen“ verworfen. Wirtschaftlichkeitserwägungen können es aber nicht rechtfertigen, datenschutzrechtliche Belange beiseite zu schieben. Der Entwurf regelt nicht, welche Aufgaben konkret auf Private übertragen werden können, und bleibt sogar hinter den allgemeinen Anforderungen des BDSG zur Auftragsdatenverarbeitung zurück.

Die weitere Entwicklung werde ich kritisch begleiten.

6.4 Marktwächter

Die Verbraucherschutzverbände sollen eine Marktwächterfunktion erhalten. Ihre Aufgabe soll es sein, Marktgeschehen und -entwicklungen zu beobachten und zu analysieren, um frühzeitig im Interesse des Verbraucherschutzes Missstände zu erkennen und Lösungen aufzuzeigen. Dabei sollen die Verbraucherschutzverbände auch mit den staatlichen Aufsichtsbehörden kooperieren, u. a. mit den Datenschutzaufsichtsbehörden des Bundes und der Länder.

Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, die Verbraucherschutzverbände mit einer Marktwächterfunktion in den Bereichen „Finanzmarkt“ und „Digitale Welt“ auszustatten. Nach der Devise „Erkennen - Informieren - Handeln“ sollen die Marktwächter eine strukturierte, proaktive Marktbeobachtung betreiben, um verbraucherschutzrelevante Probleme und Entwicklungen schneller erkennen zu können.

Teil der Marktwächterfunktion ist auch die Weitergabe der Erkenntnisse und Handlungsempfehlungen an die staatlichen Aufsichtsstellen, u. a. an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), das Bundeskartellamt, die Bundesnetzagentur sowie die Datenschutzaufsichtsbehörden des Bundes und der Länder. Beide Marktwächterfunktionen befinden sich in einer Vorprojektierungsphase: Der Finanzmarktwächter soll u. a. in den Bereichen Altersvorsorge, Kredite, Versicherungen und Produkte des Grauen Kapitalmarkts das Marktgeschehen beobachten. Die Digitalen Marktwächter werden in den Bereichen Dienstleistungen in der digitalen Welt (z. B. Buchungs- und Bewertungsportale, Partnervermittlungsportale), Waren in der digitalen Welt (E-Commerce und mobile Commerce), nutzergenerierte Inhalte (Web 2.0-Techonologien wie soziale Netzwerke), digitale Güter (E-Books, mp3 etc.) und im Bereich der Telekommunikationsdienstleistungen tätig. Die Projektphase soll im Februar 2015 abgeschlossen sein, ihren Vollbetrieb sollen die Marktwächter 2017 aufnehmen.

Bei der beabsichtigten Kooperation mit den Datenschutzaufsichtsbehörden des Bundes und der Länder geht es den Verbraucherschutzverbänden nach meinen Informationen darum, Ansprechpartner zu gewinnen, sofern aufgedeckte Missstände Datenschutzbezüge aufweisen. Zudem ist daran gedacht, dem jeweiligen Marktwächter

einen beratenden Beirat zur Seite zu stellen, dem auch Vertreter der Datenschutzaufsichtsbehörden angehören sollen.

Ich begrüße grundsätzlich die angestrebte Kooperation der Verbraucherschutzverbände mit den Datenschutzaufsichtsbehörden, zumal bei Angelegenheiten des Verbraucherschutzes nicht selten auch datenschutzrechtliche Fragestellungen eine Rolle spielen. Besonders relevant ist für mich die beabsichtigte Einrichtung des Digitalen Marktwächters, unterliegen doch Anbieter von Telekommunikationsdienstleistungen meiner datenschutzrechtlichen Aufsicht. Angesichts der bislang sehr unscharfen Konturierung der Funktion und Arbeit der Marktwächter bleiben hingegen noch viele Fragen offen. So ist für mich z. B. nicht nachvollziehbar, warum ausweislich des mir vorliegenden Konzepts der Verbraucherschutzverbände offenbar keine Kooperation mit dem Finanzmarktwächter vorgesehen ist, zumal der Finanzmarkt nicht nur bankaufsichtsrechtliche, sondern auch datenschutzrechtliche Fragen und Problemstellungen aufwirft. Klärungsbedürftig ist auch, wie sich das Kooperationsmodell zu den Verbandsklagerechten verhält, welche den Verbraucherschutzverbänden unmittelbar gegen Wirtschaftsunternehmen bei Datenschutzverstößen eingeräumt werden sollen (vgl. oben Nr. 6.1).

6.5 EU-Kooperationssystem im Verbraucherschutz - Informationsbesuch beim Bundesamt für Verbraucherschutz und Lebensmittelsicherheit

Mit einem Informationsbesuch beim Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL) habe ich mich über die Funktionsweise und die Umsetzung der datenschutzrechtlichen Anforderungen beim Betrieb des Europäischen Kooperationssystems im Verbraucherschutz unterrichtet.

Die besten Verbraucherschutzgesetze nützen wenig, wenn sie sich nicht durchsetzen lassen, weil die Anbieter von Waren oder Dienstleistungen in einem anderen Mitgliedstaat als die geschädigten Verbraucher niedergelassen sind. Wie die Europäische Union früh erkannt hat, bedarf es bei solchen grenzüberschreitenden Verstößen einer besseren Zusammenarbeit der nationalen Verbraucherschutzbehörden bei der Marktüberwachung und Rechtsdurchsetzung im europäischen Binnenmarkt.

Kernstück der „Verordnung über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden“ (Verordnung (EG) Nr. 2006/2004 vom 27.10.2004) ist die Errichtung einer elektronischen Datenbank, die den Verbraucherschutzbehörden aller Mitgliedstaaten als Informations- und Kommunikationsplattform dient (Consumer Protection Cooperation System - CPCS). Mit dem von der Europäischen Kommission betriebenen System können diese gegenseitig um Informationen ersuchen, Warnmeldungen austauschen und auch ein konkretes Einschreiten gegen einen innergemeinschaftlichen Verstoß erwirken.

Eine solche Datenbank kommt nicht ohne die Verarbeitung personenbezogener Daten aus. Die Europäische Kommission hat Anregungen des Europäischen Datenschutzbeauftragten und der Artikel-29-Gruppe aufgegriffen und mit verschiedenen Maßnahmen den datenschutzrechtlichen Erfordernissen an das CPCS Rechnung getragen. So hat die Kommission u. a. im Jahr 2011 eine Empfehlung über „Leitlinien für die Anwendung der Datenschutzbestimmungen“ im CPCS erarbeitet, die zuletzt durch eine Arbeitsvereinbarung zur Sicherstellung der datenschutzrechtlichen Betroffenenrechte ergänzt wurde.

Den Wirkbetrieb des CPCS habe ich mir durch das Bundesamt für Verbraucherschutz und Lebensmittelsicherheit im Februar 2014 erläutern lassen. Das BVL nahm bislang in der Bundesrepublik Deutschland die Funktion der in jedem Mitgliedstaat vorgesehenen „zentralen Verbindungsstelle“ ein, die die aus anderen Mitgliedstaaten eingehenden Amtshilfeersuchen an die zuständige inländische Regulierungsbehörde weiterleitet und die Ersuchen der inländischen Behörden an ihre Schwesterbehörden im EU-Ausland vermittelt. Zugleich war das BVL - neben mehreren Dutzend weiterer deutscher Verbraucherschutzbehörden - in Bereichen wie unlautere Geschäftspraktiken, Haustür- und Fernabsatzgeschäfte, elektronischer Geschäftsverkehr und unerbetene Nachrichten unmittelbar selbst zuständige Regulierungsbehörde. In Folge der Übertragung der Zuständigkeit für Ver-

braucherpolitik vom Bundesministerium für Ernährung und Landwirtschaft auf das Bundesministerium der Justiz und für Verbraucherschutz sind die Zuständigkeiten des BVL mit Wirkung zum 1. Mai 2014 nunmehr auf das BMJV übergegangen.

Bei einem Informationsbesuch im BVL konnte ich mich davon überzeugen, dass im CPCS nur in geringem Umfang unmittelbar personenbezogene Daten verarbeitet werden. In aller Regel sind die ausgetauschten Daten über mögliche Verstöße gegen kollektive Verbraucherschutzinteressen unternehmensbezogen und enthalten keine Angaben über die Identitäten der für das Unternehmen handelnden Personen. Dies entspricht der Empfehlung der Kommission, nach der personenbezogene Daten nur nach sorgfältiger Abwägung der Erforderlichkeit in das CPCS eingestellt und übermittelt werden dürfen.

Wie mir das BVL berichtete, werden die Identitäten von Personen regelmäßig nur dann über das CPCS mitgeteilt, wenn besondere Verdachtsmomente wie der Betrieb einer Vielzahl von Scheinfirmen vorlägen, die die Nennung der Person unerlässlich machten. Auch in diesem Fall würden die Informationen allerdings im System als vertraulich gekennzeichnet und hierdurch nur den konkret zuständigen Behörden - und nicht allen CPCS-Teilnehmern - zur Einsichtnahme zur Verfügung gestellt.

Seit der Einrichtung des Systems im Jahr 2007 belaufen sich die vom BVL bearbeiteten ein- und ausgehenden Informations- und Durchsetzungsersuchen im Jahresschnitt jeweils auf eine niedrige zweistellige Anzahl. Bei den deutschen Behörden wurde bislang - soweit bekannt - noch kein Auskunftsersuchen über die im CPCS gespeicherten Daten gestellt. Dies mag erklären, warum im Wirkbetrieb bislang kaum Erfahrungen zu datenschutzrechtlichen Problemstellungen gesammelt werden konnten. Trotz dieser relativ geringen Fallzahlen werde ich die Entwicklung des CPCS weiter beobachten.

6.6 Staatliche Veröffentlichungsportale

Anders als früher werden Bekanntmachungen in immer mehr staatlichen Registern im Internet veröffentlicht. Auf der einen Seite werden Informationen für den Bürger hierdurch leichter zugänglich, auf der anderen Seite führt diese Entwicklung aber auch zu neuen Herausforderungen für den Datenschutz. Der Gesetzgeber muss hier gesetzliche Rahmenbedingungen schaffen.

Insbesondere muss in jedem Fall genau geprüft werden, welche personenbezogenen Daten gespeichert werden, wer Zugriff auf die Daten erhält und wie ein Missbrauch der Daten verhindert werden kann.

6.6.1 Schwierigkeiten beim gemeinsamen Vollstreckungsportal der Länder

Aufgrund praktischer Schwierigkeiten beim Betrieb des Vollstreckungsportals der Länder plant das BMJV eine Änderung der Schuldnerverzeichnisführungsverordnung.

Am 1. Januar 2013 trat das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung in Kraft. Zeitgleich wurde das gemeinsame Vollstreckungsportal der Länder frei geschaltet. Darüber wird es für jedermann möglich, Einsicht in die Schuldnerverzeichnisse zu nehmen (vgl. 24. TB Nr. 8.12). In der Folge zeigten sich erhebliche qualitative Probleme der Suchauskünfte. Die Fehleranfälligkeit wird auf das für die Suchanfrage vorausgesetzte Identifikationsdatum „Geburtsort“ zurückgeführt, das der eintragende Gerichtsvollzieher häufig nicht kennt. Wenn bei der Suche nun ein Geburtsort eingegeben wird, der im Schuldnerverzeichnis nicht eingetragen ist, wird der Eintrag mangels Übereinstimmung nicht ausgeworfen, obwohl der Schuldner eingetragen ist.

Zur Lösung des Problems wurde unter meiner Beteiligung eine Bund-Länder-Arbeitsgruppe eingerichtet, deren Beratungen zu einem Vorschlag des BMJV führten, § 8 der Schuldnerverzeichnisführungsverordnung (SchuFV) zu ändern. Danach soll das Identifikationsdatum „Geburtsort“ ersatzlos gestrichen werden. Künftig soll es die folgenden zwei Suchmöglichkeiten geben:

- bundesweite Suche mit den Identifikationsdaten „Familienname, Vorname und Geburtsdatum“

- lokale Suche mit den Identifikationsdaten „Name, Vorname und Wohnsitz“. Werden mit dieser Angabe mehrere Treffer erzielt, muss der Benutzer zusätzlich das „Geburtsdatum“ des gesuchten Schuldners angegeben. Erst anschließend erfolgt die Ausgabe aller Treffer.

Wie ich einsehen musste, erhöht sich durch den Wegfall des Identifikationsdatums „Geburtsort“ die Qualität der Suchauskünfte aus dem Vollstreckungsportal deutlich, diese Qualitätssteigerung lässt sich auch nicht durch andere technische Maßnahmen erreichen. Die vorgesehene Streichung des Identifikationsdatums „Geburtsort“ könnte die Gefahr erhöhen, Schuldner zu verwechseln. Dem kann begegnet werden, indem den namensgleichen, aber nicht im Schuldnerverzeichnis eingetragenen Betroffenen ein Recht zugesprochen wird, auf mögliche Verwechslungen vorsorglich hinzuweisen und entsprechende Warnhinweise in das Schuldnerverzeichnis aufnehmen zu lassen.

Ich habe dem BMJV empfohlen, eine entsprechende Regelung in die SchuFV aufzunehmen.

Mehrere Landesjustizministerien fordern zusätzlich die Streichung des Identifikationsdatums „Wohnsitz“. Dies lehne ich ab. Im Gegensatz zum „Geburtsort“ kennt der Gläubiger in der Regel den „Wohnsitz“ seines Schuldners. Fehlerhafte Eintragungen zum Beispiel durch unterschiedliche Schreibweisen und veraltete Daten können den Verzicht auf dieses weitere Datum nicht rechtfertigen. Hier müssen zunächst andere Möglichkeiten zur Fehlervermeidung ausgeschöpft werden, beispielsweise eine in das Programm integrierte Ähnlichkeits- und Umgebungssuche.

Die Neuregelung soll nach zwei Jahren unter datenschutzrechtlichen Gesichtspunkten evaluiert werden. Dies begrüße ich.

6.6.2 Folgen der elektronischen Veröffentlichung von Insolvenzbekanntmachungen

Uneingeschränkte Suchmöglichkeiten und fehlender Kopierschutz führen dazu, dass gesetzliche Löschfristen faktisch ausgehebelt werden.

Im Berichtszeitraum bin ich mehrfach von den Landesbeauftragten für den Datenschutz auf Probleme im Bereich der Insolvenzbekanntmachungen aufmerksam gemacht worden. Die Bekanntmachungen der Insolvenzgerichte erfolgen seit geraumer Zeit ausschließlich elektronisch auf dem länderübergreifend eingerichteten Justizportal www.insolvenzbekanntmachung.de (vgl. 21. TB Nr. 10.8.2). Für die öffentliche Bekanntmachung ist in der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Insolvenzbekanntmachungsverordnung) geregelt, wie lange die Daten auf dem staatlichen Portal veröffentlicht bleiben dürfen. Diese Fristen werden jedoch durch private Unternehmen ausgehebelt, die die veröffentlichten Daten aus dem staatlichen Portal kopieren und für ihre eigenen Zwecke nutzen. Auch wenn das über das eigentliche Veröffentlichungsinteresse hinausgeht, wird dieses Vorgehen von der aktuellen Rechtsprechung noch für zulässig gehalten. So hat das Kammergericht Berlin entschieden, es sei zulässig, die im Internet veröffentlichte Information über die Erteilung einer Restschuldbefreiung aus dem Schuldnerverzeichnis zu erheben und für drei Jahre für Zwecke der Beauskunftung an potenzielle Kreditgeber zu speichern (Kammergericht Berlin, Zeitschrift für Datenschutz 2013, S. 189 ff.).

Ich halte es aber für datenschutzrechtlich problematisch, wenn private Internetportale die auf staatlichen Veröffentlichungsportalen eingestellten Daten erneut veröffentlichen und sich dabei nicht an die Löschfristen des staatlichen Portals halten. Ein solches Verhalten ist durch das Datenschutzrecht nicht mehr gedeckt. Die Veröffentlichung auf privaten Seiten darf nicht weiter gehen, als die auf dem staatlichen Portal. Für private Unternehmen gelten zwar nicht die Fristen der Insolvenzbekanntmachungsverordnung, einer längeren Veröffentlichung der Daten im Internet stehen aber die schutzwürdigen Interessen der Betroffenen entgegen.

Die Problematik wird durch den fehlenden Kopierschutz des staatlichen Portals sowie die Möglichkeit der uneingeschränkten Suche während der ersten zwei Wochen der Veröffentlichung verstärkt.

Ich habe dem BMJV empfohlen, die Insolvenzbekanntmachungsverordnung entsprechend nachzubessern.

6.7 Mehr Rechte für Grundstückseigentümer

Dank des neuen § 12 Absatz 4 Grundbuchordnung kann der Grundstückseigentümer grundsätzlich Auskunft darüber verlangen, wer in die ihn betreffenden Grundbuchblätter Einsicht genommen hat.

Mit dem Gesetz zur Einführung eines Datenbankgrundbuchs wurde das Grundbuchverfahren weiter modernisiert. Im Rahmen des Gesetzgebungsverfahrens wurde meine Empfehlung aufgegriffen, ein Auskunftsrecht des Grundstückeigentümers darüber, wer Einsicht in die ihn betreffenden Grundbuchblätter genommen hat, ausdrücklich zu regeln.

Zuvor beschränkte sich das Auskunftsrecht auf automatisierte Abfragen aus dem Grundbuch. Für die Fälle, in denen vor Ort - z. B. durch private Kaufinteressenten - Einsicht genommen wurde, fehlte hingegen eine ausdrückliche Regelung. Deshalb hatte ich dem Bundesministerium der Justiz empfohlen, auch für diese Fälle ein Auskunftsrecht und eine entsprechende Protokollierungspflicht zu schaffen.

Mit der neuen Regelung kommt es nun nicht mehr darauf an, in welcher Form Einsicht genommen wird. Alle Einsichten Dritter in das Grundbuch werden protokolliert und der Grundstückseigentümer kann hierüber Auskunft verlangen.

Daneben wurde die Dauer der Speicherung der Protokolle über Einsichten ins Grundbuch von einem Jahr auf zwei Jahre verlängert.

6.8 Auskunftsersuchen beim Generalbundesanwalt beim Bundesgerichtshof

Der Generalbundesanwalt beim Bundesgerichtshof (GBA) sollte bei Auskunftsersuchenden den Interessen der Betroffenen stärkeres Gewicht beimessen. Die Rechtsgrundlagen für Auskunftsansprüche im Strafverfahren müssen einfacher gefasst werden.

Wie ich erfahren habe, erteilt der GBA keine Auskunft zu

- bereits abgeschlossenen Ermittlungsverfahren bzw. –maßnahmen oder
- ob er überhaupt zu einer Person ermittelt hat.

Der GBA begründet seine Ablehnung damit, durch die Auskunft könnten Rückschlüsse auf seine Ermittlungstätigkeit gezogen werden. Dies hat mich zu einem Beratungs- und Kontrollbesuch veranlasst. Im Ergebnis hätte der GBA konkreter fassen müssen, inwieweit Daten zu dem Antragsteller gespeichert sind.

Auskunftsansprüche beim GBA stützen sich auf die Strafprozessordnung (StPO), die allerdings ein komplexes Zusammenspiel verschiedenster Vorschriften über die Auskunft und Akteneinsicht enthält. Deshalb ist die Zuordnung der richtigen Rechtsgrundlage oft nicht eindeutig. Auf der einen Seite ist die Auskunftserteilung gem. § 491 StPO spezieller als die nachrangig zu behandelnde Vorschrift des § 19 BDSG. Auf der anderen Seite ist § 491 StPO seinerseits nachrangig gegenüber den weiteren Auskunftsansprüchen nach den §§ 147, 385 Absatz 3, 397 Absatz 1 Satz 2, 406e, 475 StPO. Insbesondere die Abgrenzung zwischen § 491 StPO und § 475 StPO gestaltet sich in der Praxis schwierig, also die Frage, ob jemand in einer Datei oder Akte enthalten ist. Außerdem muss beachtet werden, welche „Rolle" jemand im jeweiligen Verfahren innehat, ob er z. B. Tatverdächtiger oder Zeuge ist. So kann die gleiche Person bei verschiedenen Verfahren unterschiedliche Rollen haben und damit unterschiedliche Auskunftsansprüche. Fehler bei dieser Entscheidung können berechtigte Auskunftsansprüche ins Leere laufen lassen.

Wenn der GBA kein Verfahren gegen eine auskunftsersuchende Person führt oder geführt hat, besteht für diese Person ein Auskunftsanspruch (sog. Negativauskunft) gemäß § 491 Absatz 1 StPO, wobei sich der Inhalt der Auskunft nach § 19 BDSG richtet. Natürlich dürfen der Auskunft keine Verweigerungsgründe gemäß § 491 StPO oder § 19 Absatz 4 BDSG entgegenstehen.

Der GBA ist bei laufenden Verfahren nicht zur Auskunft verpflichtet. Solange die in § 491 Absatz 1 StPO genannte Frist noch nicht verstrichen ist, besteht eine Auskunftssperre. Auskunftssuchenden muss in diesen Fällen mitgeteilt werden, dass Eintragungen, über die eine Auskunft erteilt werden kann, nicht vorhanden sind.

Bei abgeschlossenen Verfahren muss für eine Auskunftsverweigerung einer der Gründe des § 19 Absatz 4 BDSG bzw. § 491 Absatz 1 StPO vorliegen. Die Auskunftserteilung ist der gesetzliche Regelfall, der nur ausnahmsweise durchbrochen werden kann, wenn die jeweiligen Informationen auf Grund konkretisierter Belange geheimhaltungsbedürftig sind und nach einer umfassenden Abwägung die Interessen des Betroffenen zurückstehen müssen.

Der Auskunftsersuchende selbst darf seinen Antrag einschränken. In diesem Fall muss der GBA nur Auskunft zu den erbetenen Inhalten geben. Um einen Irrtum über die Reichweite der Auskunftsbitte zu vermeiden, wäre es in solchen Fällen wünschenswert, wenn der Kern der Anfrage vom GBA bei der Beantwortung wiederholt wird.

Für Auskunftsersuchen sind klare gesetzliche Regelungen wichtig. Gleichzeitig bedarf es stets einer Kontrolle, um Fehlentwicklungen möglichst frühzeitig entgegenwirken zu können. Insbesondere beim GBA kommt mir eine - faktisch - über das übliche Maß hinausgehende Rolle als Kontrollorgan zu, da die Entscheidungen des GBA nach der Rechtsprechung des BGH in der Regel nicht justiziabel sind (BGH NStZ-RR 2009, 145).

Die Auskunftsansprüche in der StPO sind also eher unübersichtlich geregelt. Daher wäre eine sinnvolle Reform vom Gesetzgeber hier wünschenswert.

6.9 Kontrolle des Zentralen Staatsanwaltlichen Verfahrensregisters

Meine Kontrolle des beim Bundesamt für Justiz (BfJ) geführten Zentralen Staatsanwaltschaftlichen Verfahrensregisters (ZStV) hat keine Verletzungen datenschutzrechtlicher Vorschriften ergeben.

Das ZStV wurde seit 1999 bei der Dienststelle Bundeszentralregister (BZR) des Generalbundesanwalts beim Bundesgerichtshof geführt, seit 2007 ist es beim BfJ angesiedelt. Ziel des ZStV ist es, Verfahren zu bündeln, Doppelverfolgungen zu vermeiden, die Durchführung von Strafverfahren effektiver zu gestalten, insbesondere die Ermittlung überörtlich handelnder Täter und Mehrfachtäter zu erleichtern, das frühzeitige Erkennen von Tat- und Täterverbindungen zu ermöglichen und gebotene Verfahrenskonzentrationen zu fördern.

Ganz überwiegend tragen die Staatsanwaltschaften die datenschutzrechtliche Verantwortung dafür, dass die im ZStV gespeicherten Daten inhaltlich richtig und aktuell sind. Gleichwohl muss das BfJ als registerführende Dienststelle das Verfahren strukturell in der Weise ausgestalten, dass die gesetzlichen Vorgaben eingehalten werden. Dem bin ich mit einer Kontrolle nachgegangen. Wie ich dabei festgestellt habe, entspricht das Verfahren den datenschutzrechtlichen Vorgaben.

Das System muss im Falle von Änderungen einzelner Datensätze automatisiert die bei den beteiligten Stellen vorhandenen Informationen synchronisieren bzw. einen solchen Prozess anstoßen. Würde dies unterbleiben, führten Änderungen durch eine verantwortliche Stelle möglicherweise dazu, dass die Daten im Widerspruch zu den durch eine andere Stelle eingepflegten bzw. an anderer Stelle gespeicherten Daten stünden. Insofern ist datenschutzrechtlich zu begrüßen, dass alle beteiligten Behörden und die bisherigen Auskunftsempfänger automatisiert benachrichtigt werden, wenn Personendaten oder die Daten zum Tatvorwurf geändert werden.

Sobald staatsanwaltschaftliche Mitteilungen zum Verfahrensausgang beim BfJ eingehen, löst dies gesetzliche Löschfristen aus. Zulässigerweise wird dabei eine mögliche Verkettung mit anderen Verfahren geprüft, weil der Datensatz nach den gesetzlichen Vorschriften nur gelöscht werden darf, wenn vor Ablauf der Löschfrist kein weiteres Verfahren gegen den Betroffenen eingetragen wurde.

Problematisch ist es, wenn eine der beteiligten Staatsanwaltschaften dem BfJ den Ausgang eines Strafverfahrens nicht mitteilt. Denn dann bleibt möglicherweise eine der genannten Löschfristen unbeachtet. Daher initiiert das System eine automatische Nachfrage bei der zuständigen Staatsanwaltschaft, und zwar erstmals fünf Jahre nach der Speicherung eines Eintrags, sodann jährlich. Dies begrenzt die Gefahr, dass entsprechende Meldungen von den Staatsanwaltschaften versäumt werden.

Ich empfehle aber eine Verbesserung: Wenn eine Eintragung durch fehlende rechtzeitige Mitteilung der Staatsanwaltschaft zu spät aus dem ZStV gelöscht wird, erhalten diejenigen Stellen keine Berichtigungsmeldung, die in der Zeit zwischen dem gesetzeskonformen Löschtermin und der tatsächlichen Löschung Auskunft erhalten haben. Eine solche Mitteilung ist bislang gesetzlich nicht vorgeschrieben und das derzeitige Verfahren deshalb nicht zu bemängeln. Gleichwohl sollte eine solche Mitteilung im Gesetz geregelt werden.

6.10 Europäische Staatsanwaltschaft

Ein zusammenwachsendes Europa braucht eine zusammenwachsende Strafverfolgung. Auch die datenschutzrechtlichen Verfahrensgarantien müssen dann allerdings europaweit gelten.

Im Juli 2013 hat die Europäische Kommission einen Vorschlag für eine Verordnung über die Errichtung einer europäischen Staatsanwaltschaft vorgelegt. Dadurch soll die Bekämpfung von strafbaren Handlungen mit Auswirkungen auf den EU-Haushalt besser und effizienter werden. Unter anderem wird in dem Entwurf das Prinzip der gegenseitigen Anerkennung verankert, das besagt, dass jeder Mitgliedstaat die Regelungen der anderen Mitgliedstaaten grundsätzlich anerkennt, auch wenn diese nicht den eigenen Regelungen entsprechen. Ich halte das für bedenklich, wenn nicht gleichzeitig auch ein datenschutzrechtliches Mindestniveau auf europäischer Ebene geschaffen wird. Die gegenseitige Anerkennung setzt in einem ersten Schritt Mindeststandards voraus, die insbesondere die Grundrechte bzw. Datenschutzrechte der potentiell betroffenen Bürgerinnen und Bürger sicherstellen (vgl. dazu auch Nr. 1.3). Diese Mindeststandards sind auf europäischer Ebene festzuschreiben. Dazu gehören insbesondere Mindesterhebungsschwellen für intensive Ermittlungseingriffe, wie etwa Wohnungsdurchsuchungen, Telekommunikationsüberwachungen sowie den Einsatz verdeckter Ermittler etc. Meine Bedenken habe ich auch dem zuständigen Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages mitgeteilt.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Artikel-29-Datenschutzgruppe
Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem
- Arbeitskreis Technik
- Arbeitskreis Justiz

Düsseldorfer Kreis
NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA)
Arbeitskreis Identitätsmanagement und Datenschutz-Technologien beim DIN
Teletrust Arbeitsgruppe 3 Biometrie

B. Zudem von besonderem Interesse

Nr. 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 3.1.4, 5.2, 5.3, 5.3, 5.4, 5.5, 5.6, 5.14.1, 5.14.2, 5.14.3, 8.4, 8.5, 16.3, 18.1, 19.1, 22.2, 23.2

7 Finanzausschuss

7.1 Beanstandung der Einführung der elektronischen Lohnsteuerkarte zum 1. Januar 2013

Die Einführung der elektronischen Lohnsteuerkarte verlief nicht problemlos. Bereits wenige Tage nach dem Start musste ein Teil des neuen IT-Verfahrens wegen technischer Schwierigkeiten eingestellt werden. Zudem fehlte bis zum Sommer 2013 das für einen sicheren Betrieb zwingend erforderliche verfahrensspezifische IT-Sicherheitskonzept.

Bereits in den vergangenen Tätigkeitsberichten habe ich ausführlich über die nicht reibungslose Einführung der elektronischen Lohnsteuerkarte berichtet (vgl. 23. TB Nr. 9.3; 24. TB Nr. 16.6). Wie ich im zurückliegenden Berichtszeitraum beobachten musste, konnte das IT-Verfahren „elektronische Lohnsteuerkarte“ - das sog. Elster Lohn II - immer noch nicht störungsfrei in den Wirkbetrieb überführt werden. Zwar startete „Elster Lohn II“ nach mehrmaliger Terminverschiebung am 1. November 2012 und ging zum 1. Januar 2013 in den Wirkbetrieb. Die bisherige Papierlohnsteuerkarte wurde damit bis zum Jahresende 2013 nahezu vollständig abgelöst. Arbeitgeber können nun die beim Bundeszentralamt für Steuern (BZSt) gebildeten „Elektronischen Lohnsteuerabzugsmerkmale“ (ELStAM) der insgesamt über 40 Millionen Arbeitnehmer elektronisch abrufen und diese für ihre Lohnabrechnung verwenden.

Schwierigkeiten bereitete aber der Verfahrensteil zur Steuerung der Arbeitgeberauthentifizierung. Bereits kurze Zeit nach dem Start von „Elster Lohn II“ teilte mir das BMF mit, die Arbeitgebereigenschaft könne aufgrund eines technischen Fehlers nicht schon vor einer Abfrage der ELStAM elektronisch überprüft werden. Stattdessen würden die Abrufprotokolle erst im Nachhinein durch die Landesfinanzverwaltungen überprüft. Der Wirkbetrieb des IT-Verfahrens zur Arbeitgeberauthentifizierung wurde daher ausgesetzt, die anderen Teile des IT-Verfahrens aber fortgeführt.

Datenschutzrechtlich ist es außerordentlich bedenklich, wenn die Arbeitgebereigenschaft nicht im Vorfeld überprüft werden kann. Denn damit kann nicht mehr sichergestellt werden, dass ausschließlich zugriffsberechtigte und damit befugte Arbeitgeber die ELStAM abrufen. Durch die technische Panne sind weder eine sichere Vorher-Authentifizierung des Arbeitgebers (§ 39e Abs. 4 Satz 3 Einkommensteuergesetz - EStG) noch dessen Zugriffsberechtigung (§ 39e Abs. 4 Satz 2 EStG) überprüfbar. Die datenschutzrechtlich gebotene Zugangs- und Zugriffskontrolle findet also nicht statt.

Eine unbefugte Abfrage der ELStAM kann damit lediglich nachträglich anhand der Protokolldaten festgestellt und sanktioniert werden. Darüber hinaus bleibt unklar, ob die Arbeitnehmer über einen unberechtigten Abruf benachrichtigt werden und welche weiteren Maßnahmen die vollziehenden Bundesländer treffen. Beruhigend ist allenfalls, dass im Rahmen der bisherigen Überprüfung der Abruflisten noch kein Missbrauchsfall aufgedeckt worden ist.

Als noch bedenklicher aus datenschutzrechtlicher Perspektive bewerte ich jedoch die Prozesssteuerung und die Überführung des neuen IT-Verfahrens in den Wirkbetrieb. Es lag weder das verfahrensspezifische IT-Sicherheitskonzept zum Risikomanagement vor, noch die Festlegungen nach § 8 Steuerdaten-Abrufverordnung, die die schnittstellenbezogenen Regelungen und Verfahrensdokumentationen klären sollen.

Dies habe ich gegenüber dem BMF förmlich beanstandet.

Kasten zu Nr. 7.1

Die Elektronische Lohnsteuerkarte

Seit 2010 plant die Finanzverwaltung die Einführung der „Elektronischen Lohnsteuerkarte“, das sog. Elster Lohn II. Damit setzt sie ihre Anstrengungen fort, die Einkommenssteuererklärungen zunehmend elektronisch bearbeiten zu lassen. Für „Elster Lohn II“ musste ein neues IT-Verfahren entwickelt werden, das über die beim Bundeszentralamt für Steuern (BZSt) bereits gespeicherte Steuer-Identitätsnummer hinaus weitere Daten zu den Lohnsteuerabzugsmerkmalen in der zentralen Datenbank erfassen kann. Rechtsgrundlage dieser Datenerfassung ist § 39e EStG, wonach in die Datenbank die Elektronischen LohnSteuerAbzugsMerkmale (ELStAM) eingespeist werden dürfen.

Zu den ELStAM gehören folgende Merkmale:

- Steuer-Identifikationsnummer (§ 39e Abs. 2 Satz 1 EStG),
- Kirchensteuerabzugsmerkmale des Steuerpflichtigen (§ 39e Abs. 2 Nr. 2 EStG),
- Familienstand, Identifikationsnummer des Ehegatten (§ 39e Abs. 2 Nr. 2 EStG),
- Kinder mit ihrer Identifikationsnummer (§ 39e Abs. 2 Nr. 3 EStG),
- Tag der Geburt (§ 39e Abs. 3 Satz 1 EStG),
- Lohnsteuerabzugsmerkmale (§ 39 Abs. 4 EStG),
  - o Steuerklasse (§ 38b Abs. 1 EStG) und ggf. Faktor (§ 39f EStG),
  - o Kinderfreibetrag (§ 38b Abs. 2 EStG),
  - o Freibetrag und Hinzurechnungsbetrag (§ 39a EStG).

Bereits heute können Arbeitnehmer ihre eigenen ELStAM im ElsterOnline-Portal abfragen (www.elsteronline.de). Sie müssen sich hierfür mit ihrer Steuer-Identifikationsnummer im Portal registrieren. Für die Änderung der Lohnsteuerabzugsmerkmale (z. B. Lohnsteuerklasse, Freibeträge) bleiben jedoch ausschließlich die Finanzämter zuständig. Melderechtliche Datenänderungen (z. B. Heirat, Geburt eines Kindes) werden weiterhin allein von den Meldebehörden in einem automatisierten Verfahren an das BZSt mitgeteilt.

Der Arbeitnehmer hat die Möglichkeit, für die Zukunft einen Datenabruf zu gestatten, zu begrenzen oder auszuschließen (§ 39e Abs. 6 Satz 6 EStG). Sperrt der Arbeitnehmer den Abruf der ELStAM für seinen Arbeitgeber, so hat dieser die Lohnsteuer nach Steuerklasse VI zu ermitteln (§ 39e Abs. 6 Satz 8 EStG).

Um die ELStAM seiner Mitarbeiter abrufen zu können, muss sich der Arbeitgeber einmalig im ElsterOnline-Portal registrieren (Elster-Authentifizierung). Nach erfolgreicher Authentifizierung erhält der Arbeitgeber ein Zertifikat. Dieses kann als Organisationszertifikat bis zu 20 Berechtigungen beinhalten oder als persönliches Zertifikat auf eine konkrete Person beschränkt sein.

Der Arbeitgeber darf die für den Lohnsteuerabzug relevanten Abzugsmerkmale aus der ELStAM-Datenbank nur abrufen, wenn er seinen Arbeitnehmer elektronisch angemeldet hat. Er muss dazu seinen Arbeitnehmer um folgende Datenauskünfte bitten:

- Steuer-Identifikationsnummer (§ 139b Abgabenordnung (AO)),
- Geburtsdatum,
- ob es sich um das erste oder ein weiteres Arbeitsverhältnis handelt,
- ob und in welcher Höhe ein nach § 39a Absatz 1 Satz 1 Nummer 7 EStG festgestellter Freibetrag von diesem abgerufen werden soll (vgl. § 39e Abs. 4 Satz 1 EStG).

Das BZSt übermittelt anschließend zu jedem Arbeitnehmer eine Anmeldebestätigung an den Arbeitgeber. Die Anmeldebestätigung enthält die ELStAM der angemeldeten Mitarbeiter, die für die darauffolgende Lohnabrechnung zur Ermittlung des jeweiligen Lohnsteuerabzugs anzuwenden sind. Da es zwischen den beim BZSt gespeicherten ELStAM-Daten und den in den Lohnabrechnungsstellen vorliegenden Lohnsteuerkarten bzw. Ersatzbescheinigungen häufig zu Abweichungen kam, konnte für einen Zeitraum von sechs Monaten nach dem erstmaligen Abruf weiterhin auf Grundlage der bisherigen Papierbescheinigungen abgerechnet werden.

Bei Beendigung eines Beschäftigungsverhältnisses meldet der Arbeitgeber den ausscheidenden Mitarbeiter bei der ELStAM-Datenbank ab.

7.2 Kontenabrufverfahren

Der Kreis der Abrufberechtigten wurde ständig ausgeweitet, die Zahl der Abrufersuchen steigt weiter stetig an. Das derzeitige Verfahren zeigt datenschutzrechtliche Problemfelder auf.

Für Zwecke der Bekämpfung von Geldwäsche und Terrorismus wurde zum 1. April 2003 im Rahmen des Vierten Finanzmarktförderungsgesetzes ein Kontenabrufverfahren geschaffen (§ 24c Kreditwesengesetz - KWG). Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wurde damals beauftragt, Stammdaten (Kontoinhaber, Bevollmächtigter, Geburtsdatum, abweichende wirtschaftlich Berechtigte und deren Anschrift, Kontonummer, Errichtungs- und Schließungsdatum) zu in Deutschland geführten Konten und Depots zu speichern (vgl. 19. TB Nr. 10.2, 20. TB Nr. 11.3.1). In Deutschland werden etwa 500 Millionen Konten und Depots geführt.

Bereits zwei Jahre später wurde mit dem Gesetz zur Förderung der Steuerehrlichkeit das Kontenabrufverfahren erstmals auf weitere Berechtigte ausgeweitet. Seitdem führt das Bundeszentralamt für Steuern (BZSt) zentral für die Finanzbehörden und gesetzlich bestimmte andere Behörden Kontenabrufe zu steuerlichen Zwecken sowie zu gesetzlich vorgegebenen nichtsteuerlichen Zwecken durch (vgl. 20. TB Nr. 8.2, 21. TB Nr. 8.2).

Mit dem Inkrafttreten des Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung zum 1. Januar 2013 wird den ca. 4.700 Gerichtsvollziehern jetzt ebenfalls gestattet, Kontoabrufersuchen gegenüber dem BZSt zu stellen (§ 802l Zivilprozessordnung - ZPO). Die Ausweitung des Kontenabrufs auf weitere Berechtigte hat zwangsläufig zu einer deutlichen Steigerung der Kontenabrufersuchen geführt. Diese haben sich im Jahr 2013 gegenüber dem Jahr 2012 mit über 143.000 Anfragen nahezu verdoppelt. In 2014 ist es zu einem weiteren erheblichen Anstieg auf über 237.000 Kontenabrufersuchen gekommen. Die Zahl der Ersuchen hat sich somit innerhalb des Berichtszeitraums mehr als verdreifacht (vgl. auch Kasten a und b zu Nr. 7.2).

Die praktische Umsetzung der Kontenabrufe beim BZSt weist zwei datenschutzrechtliche Problemfelder auf.

Zum einen ist es dem BZSt nicht möglich, die Ergebnisse eines Kontenabrufersuchens auf die aktuell bestehenden Konten einer Person zu beschränken. Dem Ersuchenden werden immer auch bereits gelöschte Konten der betroffenen Person mitgeteilt, auch wenn er diese nicht benötigt. Ich halte diese Globalauskunft datenschutzrechtlich für äußerst bedenklich, da sie eindeutig den datenschutzrechtlichen Grundsätzen der Datensparsamkeit und Datenvermeidung zuwiderläuft. Auch nach dem Wortlaut der für Kontenabrufe geltenden Rechtsgrundlagen (§§ 93 Abs. 7 bis 10, 93b Abgabenordnung (AO) i. V. m. § 24c KWG sowie § 802l ZPO und § 3a BDSG) ist eine Globalauskunft rechtswidrig. Danach gestatten diese Vorschriften gerade nicht in jeder Fallkonstellation die Übermittlung aller Kontodaten. Vielmehr wird in den genannten Vorschriften ausdrücklich von einzelnen Daten und soweit erforderlich gesprochen.

Der Gesetzgeber wollte also eindeutig die Kontenabrufersuchen auf das Notwendige begrenzen. Das BMF ist gefordert, Rechtslage und Praxis der Abrufersuchen in Einklang zu bringen.

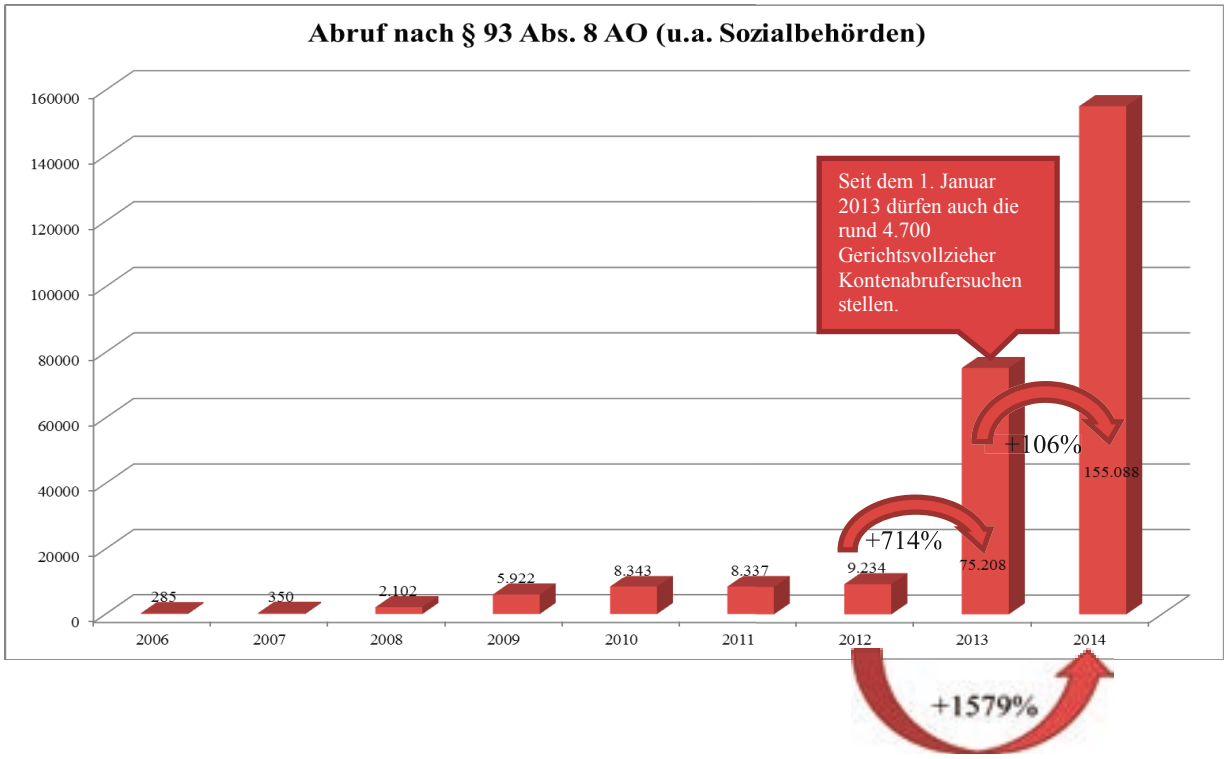
Wie bei mir eingehende Eingaben zeigen, kommt es bei den Kontenabfragen immer wieder zu Personenverwechslungen. Solche Verwechslungen können relativ leicht zustande kommen, da zum Konteninhaber als personenbestimmende Daten nur der Name und das Geburtsdatum gespeichert sind. Ob es aufgrund solcher verfahrensbedingt fehlerhaften Zuordnung von abgerufenen Daten zu folgenschweren Maßnahmen für irrtümlich Betroffene kommen kann, wie z. B. Kontensperren, Pfändungen u. ä., hängt allein von der sorgfältigen Prüfung und Bewertung der abgerufenen Daten durch die ersuchenden Stellen ab. So berichtete mir ein Petent, ihm sei in Folge eines Kontenabrufs zu einer namensgleichen Person sein Girokonto für mehrere Tage gesperrt worden. Dadurch sei es zu Rückbuchungen von Abbuchungen und Überweisungsaufträgen gekommen. Die namensgleiche Person habe den gleichen Nachnamen und das gleiche Geburtsdatum, jedoch einen anderen Vornamen. Der Petent berichtet, in seinem Fall seien Kontendaten zu 24 verschiedenen Personen abgerufen und der ersuchenden Stelle zugeleitet worden. Datenschutzrechtlich ist es deshalb unabdingbar, bei Abrufersuchen Daten nur zu den Konten mitzuteilen, die der tatsächlich betroffenen Person zweifelsfrei zugeordnet werden können. Das derzeitige vom BZSt betriebene Kontenabrufverfahren entspricht diesen Anforderungen jedenfalls nicht.

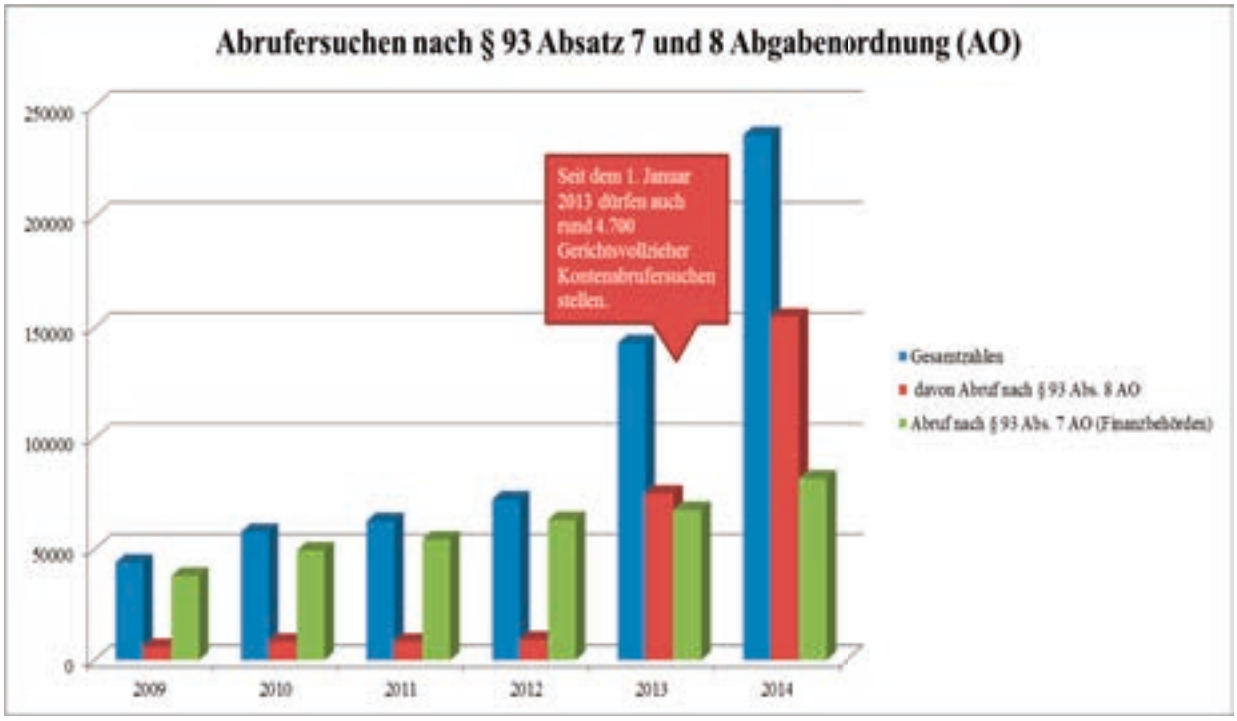
Kasten a zu Nr. 7.2

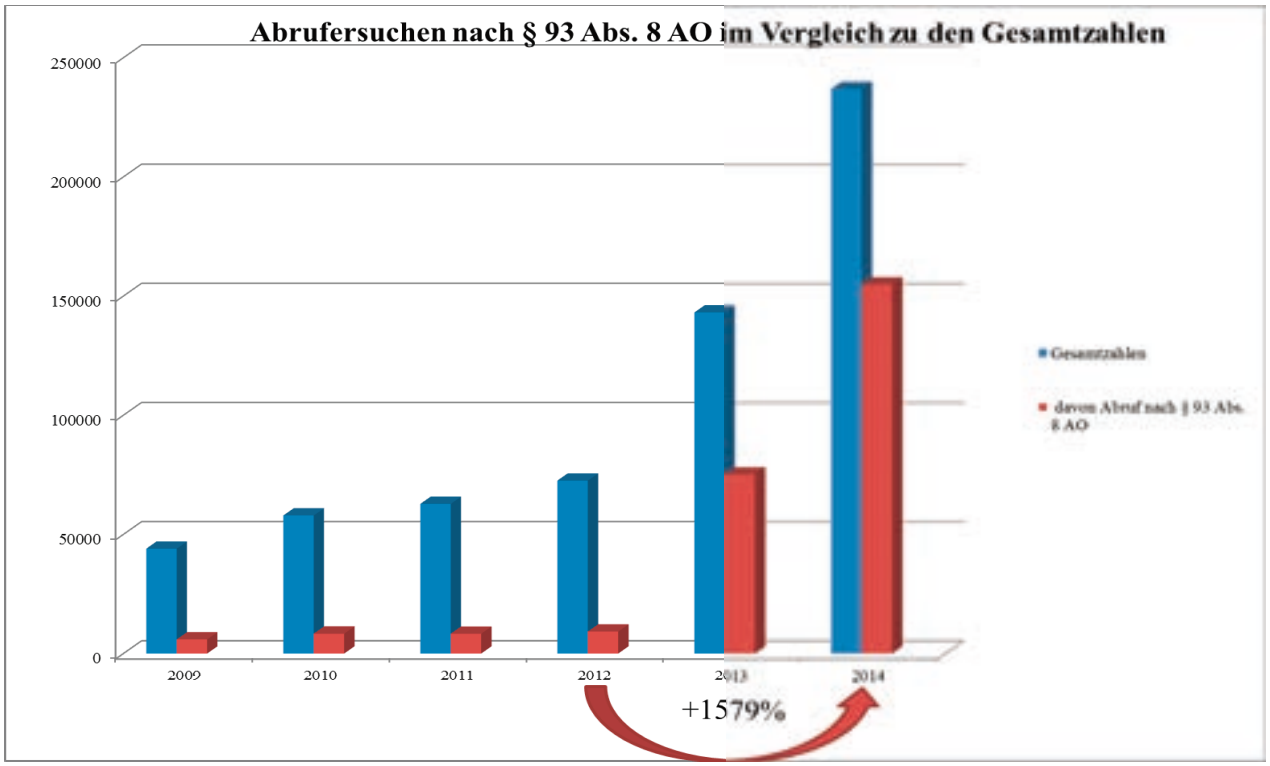
Abrufersuchen nach § 93 Absatz 7 und 8 Abgabenordnung (AO)

Zeitraum	Abruf nach § 93 Abs. 7 AO	Abruf nach § 93 Abs. 8 AO
04/2005 bis 2011	235.637	25.437
2012	63.344	9.234
2013	67.926	75.208
2014	82.038	155.088
Gesamt	448.945	264.967

Kasten b zu Nr. 7.2




Abrufersuchen nach § 93 Absatz 7 und 8 Abgabenordnung (AO)
250000
200000
150000
100000
50000
0
2009
2010
2011
2012
2013
2014
Seit dem 1. Januar 2013 dürfen auch rund 4.700 Gerichtsvollzieher Kontenabrufersuchen stellen.
Gesamtzahlen
davon Abruf nach § 93 Abs. 8 AO
Abruf nach § 93 Abs. 7 AO (Finanzbehörden)


Abrufersuchen nach § 93 Abs. 8 AO im Vergleich zu den Gesamtzahlen
250000
200000
150000
100000
50000
0
2009
2010
2011
2012
2013
2014
+1579%
Gesamtzahlen
davon Abruf nach § 93 Abs. 8 AO

7.3 SWIFT-Abkommen

Erstmals wurde nach dem SWIFT-Abkommen ein Auskunftsersuchen an das amerikanische Finanzministerium gerichtet.

Das 2010 zwischen der EU und den USA geschlossene sogenannte SWIFT-Abkommen, welches der Aufdeckung von Zahlungsströmen zur Terrorismusfinanzierung dienen soll, sieht sowohl ein Recht auf Auskunft (Art. 15) als auch ein Recht auf Berichtigung, Löschung oder Sperrung (Art. 16) der Daten vor, die in diesem Rahmen an die USA übermittelt werden. Diese Rechte stehen zwar dem Betroffenen persönlich zu. Geltend gemacht werden können sie aber nur über die nationale Datenschutzbehörde, die das Ersuchen auf Auskunft, Berichtigung, Löschung oder Sperrung an das amerikanische Finanzministerium, das Department of Treasury (DoT) weiterleitet.

Das umständliche Verfahren wurde 2013 durch eine Verfahrensvereinbarung zwischen der EU und dem DoT dahingehend vereinfacht, dass die nationale Datenschutzbehörde die Feststellung der Identität des Antragstellers überprüft. Ausweiskopien - wie ursprünglich vereinbart - müssen nicht in die USA übersandt werden. Nach Überprüfung der Identität leitet die nationale Datenschutzbehörde den Antrag an das DoT weiter. Die Antwort des DoT wird ebenfalls nicht unmittelbar, sondern über die nationale Datenschutzbehörde dem Antragsteller übersandt.

Wie die Erfahrungen zeigen, ist dieses Auskunftsrecht den EU-Bürgern noch nicht hinreichend bekannt. Obwohl das Abkommen bereits 2010 abgeschlossen wurde, hat Deutschland als bis dahin einziges EU-Land im November 2013 ein Auskunftsersuchen an das DoT gerichtet. Die Antwort fiel zwar unter Hinweis auf Artikel 15 Absatz 2 des Abkommens sehr knapp aus, aber es wurde bestätigt, dass aus datenschutzrechtlicher Sicht keine Rechte des Auskunftsersuchenden verletzt worden seien.

Die Umsetzung des Abkommens werde ich auch weiterhin begleiten und Bürgerinnen und Bürger bei ihren Auskunftsersuchen unterstützen (vgl. 23. TB Nr. 13.6, 24. TB Nr. 2.5.1).

7.4 Einführung eines Mitarbeiter- und Beschwerderegisters

Das Ende 2012 bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eingeführte Mitarbeiter- und Beschwerderegister (MBR) habe ich im Juli 2013 ohne Beanstandungen überprüft.

Mit dem Anlegerschutz- und Funktionsverbesserungsgesetz (BGBl. I 2011, S. 538 ff.) wurde 2012 das von der BaFin geführte Mitarbeiter- und Beschwerderegister (MBR) eingeführt (§ 34d Wertpapierhandelsgesetz (WpHG)).

Die BaFin hat das MBR zu betreiben, die ihr gemeldeten Daten darin bereitzustellen sowie die Speicherfristen einzuhalten. Sie kann Verwarnungen und Untersagungen aussprechen sowie unanfechtbar gewordene Anordnungen auf ihrer Internetseite öffentlich bekannt machen. Aufgrund des europarechtlichen Prinzips der Heimatlandaufsicht werden ausschließlich Daten der von der BaFin kontrollierten inländischen Wertpapierdienstleistungsunternehmen erfasst.

Die Wertpapierdienstleistungsunternehmen übermitteln in das MBR Personendaten ihrer Mitarbeiter, die als Anlageberater, als Vertriebsbeauftragte und als Compliance-Beauftragte (Beauftragte für „rechtskonformes Verhalten“) tätig sind. Beschwerden, die im Rahmen einer Anlageberatung gegen einen Mitarbeiter eingehen, müssen von dem Wertpapierdienstleistungsunternehmen ebenfalls an die BaFin gemeldet werden. Zu melden ist die Anzahl der Beschwerden, das Beschwerdedatum und die alphanumerische Nummer des Mitarbeiters. Der einer

Beschwerde zugrunde liegende Sachverhalt wird zunächst nicht gemeldet. Erst wenn eine Auswertung der Meldungen Anhaltspunkte für ein auffälliges Anlageberatungsverhalten bestimmter Mitarbeiter nahelegt, ist die BaFin befugt, weitere Angaben zu erheben, beispielsweise zu den Sachverhalten.

Die Datenübermittlungen für das MBR werden über die zentrale Melde- und Veröffentlichungsplattform der BaFin (MVP) abgewickelt (§ 7 WpHG-Mitarbeiteranzeigeverordnung - WpHGMaAnzV). Über diese Plattform, die aufwendige IT-Sicherheitsmechanismen vorsieht, registrieren sich die Anwender, beantragen Meldeberechtigungen und verwalten die eigenen Benutzerkonten.

Die Meldungen werden von der BaFin dahingehend überprüft, ob Anhaltspunkte dafür vorliegen, dass nicht sachkundige oder unzuverlässige Mitarbeiter als Anlageberater, Vertriebsbeauftragte oder Compliance-Beauftragte beim Wertpapierdienstleistungsunternehmen tätig sind. Dabei werden sowohl die absoluten Zahlen als auch die Fehlverhaltensmeldungen zu den Mitarbeitern in ein Verhältnis gesetzt. Es liegt im Ermessen der BaFin, ein schriftliches Untersagungsverfahren einzuleiten oder gegebenenfalls Untersagungsanordnungen gegen das Wertpapierdienstleistungsunternehmen zu treffen, dem verboten werden kann, Mitarbeiter in der angezeigten Tätigkeit einzusetzen (§ 34d Abs. 4 WpHG).

Mitarbeiter der Wertpapierdienstleistungsunternehmen haben gemäß § 19 BDSG das Recht, eine Selbstauskunft aus dem MBR anzufordern.

Im Juli 2013 waren in der Datenbank MBR bereits 186.000 Datensätze zu Anlageberatern, Vertriebsbeauftragten und Compliance-Beratern der Wertpapierdienstleistungsunternehmen hinterlegt. Das geprüfte Verfahren und die Sicherheitsmechanismen waren nicht zu beanstanden.

7.5 Foreign Account Tax Compliance Act (FATCA)

2014 sind erstmals Daten von in den USA Steuerpflichtigen nach dem FATCA-Abkommen erhoben worden.

Das bilaterale FATCA-Abkommen zwischen Deutschland und den USA ist am 11. Dezember 2013 in Kraft getreten. Es klärt den Rahmen für einen regelmäßigen Informationsaustausch über private Finanzkonten zwischen deutschen und US-amerikanischen Steuerbehörden, um eine effektive Besteuerung sicherzustellen. Das Abkommen wurde erforderlich, nachdem im März 2010 das US-Steuergesetz Foreign Account Tax Compliance Act - FATCA verabschiedet worden war, das Vermögenswerte von in den USA steuerpflichtigen Personen und Gesellschaften auf Konten im (US-)Ausland erfasst. Seine Umsetzung hatte erhebliche datenschutzrechtliche Probleme in Deutschland und Europa aufgeworfen (vgl. 24. TB Nr. 2.5.5).

Ich war von Beginn an sowohl auf europäischer als auch auf nationaler Ebene in das Verfahren zur Umsetzung von FATCA eingebunden und habe mich für die Einhaltung eines angemessenen Datenschutzniveaus eingesetzt. Dabei habe ich insbesondere auf die Beachtung des datenschutzrechtlichen Erforderlichkeits- und Zweckbindungsgrundsatzes hingewirkt.

Das FATCA-Abkommen zur Förderung der Steuerehrlichkeit bei internationalen Sachverhalten wird jetzt durch § 117c Abgabenordnung (AO) umgesetzt. Ich habe dazu geraten, von der in § 117c AO enthaltenen Verordnungsermächtigung Gebrauch zu machen, um Einzelheiten über Form, Inhalt, Verarbeitung und Sicherung der an das Bundeszentralamt für Steuern (BZSt) zu übermittelnden Daten zu regeln.

Seit dem 29. Juli 2014 ist die FATCA-USA-Umsetzungsverordnung in Kraft, die die Erhebung der erforderlichen Daten durch die Finanzinstitute und deren Übermittlungsform im Einzelnen regelt. Meldende deutsche Finanzinstitute sind verpflichtet, sich bei der amerikanischen Steuerbehörde (Internal Revenue Service - IRS) re-

gistrieren zu lassen und die zu erhebenden Daten zu US-amerikanischen meldepflichtigen Konten an das BZSt zu melden. Die Daten sind jährlich, erstmals 2014 zu erheben und bis zum 31. Juli des Folgejahres an das BZSt zu übermitteln. Dieses leitet die Daten dann an den IRS weiter.

Daten, die der IRS über in Deutschland Steuerpflichtige mit Konten in den USA übermittelt, werden vom BZSt an die zuständigen inländischen Landesfinanzverwaltungen weitergegeben.

Ich werde das Verfahren auch weiterhin datenschutzrechtlich begleiten (vgl. 24. TB Nr. 2.5.5).

7.6 Neues Verfahren zur Erhebung der Kirchensteuer auf Kapitalerträge

Seit 1. Januar 2015 wird die Kirchensteuer auf Kapitalerträge unter Beteiligung der Kreditinstitute erhoben. Um das neue Verfahren vorzubereiten, haben allein die Banken im Herbst 2014 Kirchensteuerabzugsmerkmale zu bis zu 200 Millionen in Deutschland geführten Konten beim Bundeszentralamt für Steuern (BZSt) abgefragt.

Mit dem Unternehmenssteuergesetz von 2008 hat der Gesetzgeber die sog. Quellensteuer auf Kapitalerträge eingeführt. Dieses Gesetz gewährte den Steuerpflichtigen für einen Übergangszeitraum die Wahl, ob sie die Kirchensteuer auf Kapitalerträge über ihre Kreditinstitute oder über ihre Steuererklärung abwickeln wollten. Nur im ersten Fall teilten die Steuerpflichtigen ihre Religionszugehörigkeit freiwillig mit.

Das bisherige Übergangsverfahren ist evaluiert und zum 1. Januar 2015 umgestellt worden (vgl. hierzu Kasten zu Nr. 7.6). An dem Evaluierungsprozess wurde ich erst beteiligt, nachdem er bereits weitgehend abgeschlossen war. Dies habe ich dem BMF gegenüber gerügt, denn nach meiner Einschätzung sind in diesem Prozess die datenschutzrechtlichen Belange im Umgang mit dem besonders sensiblen personenbezogenen Merkmal Religionszugehörigkeit nicht hinreichend beachtet worden. Die Diskussion der Evaluierungsgruppe fokussierte sich überwiegend auf das Procedere der unmittelbaren Abfrage der konkreten Religionszugehörigkeit ihrer Kunden durch die Kreditinstitute beim BZSt. Wäre dieses Verfahren umgesetzt worden, hätten die Kreditinstitute ausnahmslos die Religionszugehörigkeit der Kontoinhaber erfahren. Eine solch umfassende Abfrage derart sensibler Daten führt nicht nur zu Missbrauchsrisiken wegen des Grundsatzes der Datensparsamkeit, sondern ist auch unverhältnismäßig.

In enger Abstimmung mit den Landesbeauftragten für den Datenschutz hatte ich einen Vorschlag für ein sogenanntes Clearingstellenmodell unterbreitet. Danach sollte den Kreditinstituten nur der Prozentsatz des abzuführenden Kirchensteuersatzes bekannt gegeben werden. Der entsprechende Kirchensteuerbetrag sollte an eine Clearingstelle abgeführt werden, die dessen Weiterleitung an die betreffende Religionsgemeinschaft durchführt.

Das BMF ist meinem Vorschlag zwar nur begrenzt gefolgt. Es wurde aber ein IT-Verfahren zur Abfrage der Religionszugehörigkeit sowie der Steuer-Identifikationsnummer (IdNr.) für die Erhebung der auf Kapitalerträge anfallenden Kirchensteuer entwickelt, das zumindest sicherstellt, dass die Kreditinstitute durch Verschlüsselung der betreffenden Informationen keine Kenntnis über die Zugehörigkeit einer Person zu einer bestimmten Religionsgemeinschaft erhalten.

Für datenschutzrechtlich weiterhin bedenklich halte ich die Einbeziehung der Kunden mit Nichtveranlagungsbescheinigung in die Regelabfrage. Dieser Personenkreis wird mangels zu versteuernder Kapitalerträge effektiv nicht besteuert und es darf bis zu drei Jahre auf den Einbehalt der Kapitalertragssteuer und damit auch auf die Kirchensteuer verzichtet werden. Zwar vertritt die Finanzverwaltung die Auffassung, es komme nicht auf die individuellen kapitalertragsteuerlichen Verhältnisse zum Stichtag 31. August an, sondern darauf, ob ein zu versteuernder Vermögenszufluss im Folgejahr zu erwarten sei oder nicht. Diese rein formale Vorgehensweise halte ich jedoch für datenschutzrechtlich nicht gerechtfertigt, weil die beiden datenschutzrechtlichen Grundsätze der Datensparsamkeit (§ 3a BDSG) und des Schutzes besonders schützenswerter personenbezogener Daten (§ 3

Abs. 9 BDSG) hier nicht mehr hinreichend gewahrt werden. Ich rege an, von einer Regelabfrage dann abzusehen, wenn eine Nichtveranlagungsbescheinigung vorliegt oder über einen längeren vergangenen Zeitraum keine Kapitalerträge angefallen sind.

Ich empfehle dem Bundesministerium der Finanzen, Kunden von der Regelabfrage dann auszunehmen, wenn eine Nichtveranlagungsbescheinigung vorliegt oder über einen längeren Zeitraum keine Kapitalerträge angefallen sind

Die Regelabfrage bewegt die Menschen. Seit Ende 2013 haben sich deswegen zahlreiche Petenten an mich gewandt, weil sie vermeiden wollten, dass die Kreditinstitute Informationen über ihre Religionszugehörigkeit erhalten. Wie sich daraus ergibt, ist die Regelanfrage den Betroffenen gegenüber noch nicht transparent und umfassend genug kommuniziert worden.

Kasten zu Nr. 7.6

Das in § 51a EStG geregelte Verfahren verläuft im Einzelnen wie folgt:

- Das BZSt speichert das Kirchensteuerabzugsmerkmal (KISTAM).
- Die Kreditinstitute müssen beim BZSt regelmäßig das Kirchensteuermerkmal (KISTAM) für den Kirchensteuerpflichtigen abfragen.
- Regelanfragen werden jährlich in den Monaten September/Oktober durchgeführt, Anlassabfragen nach Bedarf, z. B. vor der Auszahlung von Versicherungspolicen.
- Das BZSt stellt den Kreditinstituten für den Kirchensteuerabzug gemäß § 139b Abgabenordnung (AO), § 39e Einkommensteuergesetz (EStG) und § 51a Absätze 2b bis e und Absatz 6 EStG drei Merkmale zum Abruf bereit:
  - o die Steuer-Identifikationsnummer (IDNr.),
  - o das Geburtsdatum des Kunden und
  - o das KISTAM.
- Beim Abruf der KISTAM werden drei Fälle unterschieden:
  - o Liegt kein Sperrvermerk vor, wird der „kirchensteuergläubigerscharfe Religionsschlüssel“ und der zugehörige Kirchsteuersatz mitgeteilt.
  - o Hat der Steuerpflichtige einen Sperrvermerkt gesetzt, wird ein „Nullwert“ mitgeteilt.
  - o Gehört der „Steuerpflichtige“ keiner steuererhebenden Religionsgemeinschaft an, wird eben falls ein „Nullwert“ gemeldet.
- Die Kreditinstitute führen bei abgeltend besteuerten Kapitalerträgen die Kirchensteuer ab.
- Vor jeder Abfrage informieren die Kreditinstitute ihre Kunden (§ 51a EStG).
- Steuerpflichtige können schriftlich beim BZSt einen sog. Sperrvermerk setzen lassen. Der Sperrvermerk verhindert die Meldung des KISTAMs an die Kreditinstitute und muss zu bestimmten Fristen dem BZSt vorliegen, um beachtet werden zu können. Das BZSt informiert das zuständige Finanzamt über den Sperrvermerk und benennt das Kreditinstitut namentlich.

7.7 Übergang der Verwaltung der Kraftfahrzeugsteuer auf den Bund

Die Zollverwaltung hat zum 1. Juli 2014 die Verwaltung der Kfz-Steuer von den Ländern übernommen. Zu diesem Zeitpunkt lag weder ein verfahrensbezogenes Datenschutzkonzept noch ein verfahrensspezifisches IT-Sicherheitskonzept vor.

Die Erhebung und Verwaltung der Kraftfahrzeugsteuer wurde 2009 neu geregelt. Die Erträge aus der Kfz-Steuer gingen damals von den Ländern auf den Bund über und auch der Verwaltungsvollzug wurde dem Bund übertragen. Für einen Übergangszeitraum wurde die Steuer noch im Wege der Organleihe durch die Finanzämter eingezogen. Seit dem 1. Juli 2014 wird sie vollständig von den Hauptzollämtern festgesetzt, erhoben und vollstreckt.

Im Zusammenhang mit diesem Zuständigkeitswechsel haben sich zahlreiche Bürger an mich gewandt. Sie waren besorgt, weil ihre persönlichen Daten von den Finanzämtern an die Hauptzollämter übermittelt wurden und äußerten Bedenken wegen der Übertragung der Lastschrifteinzugsermächtigungen von den Finanzämtern auf die Hauptzollämter. Ich habe dies zum Anlass genommen, das Verfahren bei einem Hauptzollamt zu kontrollieren. Wie ich dabei feststellen musste, hat die Finanzverwaltung noch nicht alle organisatorischen und rechtlichen Datenschutzbelange zufriedenstellend geklärt. In organisatorischer Hinsicht fehlen sowohl das verfahrensbezogene Datenschutzkonzept als auch das verfahrensspezifische IT-Sicherheitskonzept. Ich habe das BMF gebeten, diese wesentlichen datenschutzrechtlichen Voraussetzungen zeitnah zu erfüllen. Darüber hinaus konnten zum Zeitpunkt der Kontrolle noch nicht alle Arbeitsschritte in der elektronischen Akte nachvollziehbar abgebildet werden. Insbesondere das Verfahren zur (stichprobenweisen) Zweitprüfung von Festsetzungen, die aus Gründen des Haushaltsrechts erforderlich ist, muss optimiert werden. Die Bearbeiter können innerhalb der elektronischen Akte bislang nicht feststellen, ob die erforderliche Zweitprüfung für die weiterhin Papierbelege vorzuhalten sind, zu einer Festsetzung bereits erfolgt ist. Aus diesem Grund werden auch Kopien von sensiblen Daten, z. B. Schwerbehindertenausweisen, länger aufbewahrt als dies aus datenschutzrechtlicher Sicht geboten wäre. Ich erwarte eine entsprechende Weiterentwicklung der IT-Verfahren, so dass die zugehörigen Papierdokumente zeitnah vernichtet werden können.

Für datenschutzrechtlich problematisch halte ich auch die Weiterverwendung der Lastschriftermächtigungen. Das BMF konnte mir bisher nicht überzeugend darlegen, aufgrund welcher Rechtsgrundlage die den Finanzämtern erteilten Lastschrifteinzugsermächtigungen ohne erneute Ermächtigung durch den Steuerpflichtigen von den Hauptzollämtern als festsetzende Stellen sowie den Bundeskassen als einziehende Stellen umgewidmet und damit weiterverwendet werden durften. Meines Erachtens ergibt sich diese weder aus dem Kraftfahrzeugsteuergesetz noch aus Artikel 7 EU VO Nr. 260/2012 (SEPA-Verordnung), da ein Gläubigerwechsel stattgefunden hat.

Auch wenn die Übermittlung der Daten der Kfz-Steuerpflichtigen von den Finanzämtern an die Hauptzollämter datenschutzrechtlich unbedenklich ist, haben mir die Bürgereingaben gezeigt, dass die Information in die Bevölkerung über den Wechsel dieses Verwaltungsvollzuges nicht transparent und klar genug erfolgt ist. Insbesondere die Kfz-Steuerpflichtigen, die eine Lastschriftermächtigung erteilt hatten, wurden nur unzureichend und teils missverständlich informiert.

Ich empfehle dem Bundesministerium der Finanzen, nochmals öffentlichkeitswirksam über den veränderten Verwaltungsvollzug und das Widerrufsrecht der Lastschrifteinzugsermächtigung informiert.

7.8 Einführung und Nutzung der elektronischen Akte bei den Familienkassen

Die elektronische Akte (E-Akte) wird zunehmend auch von den über 8.400 Familienkassen genutzt. Hinsichtlich des notwendigen Akteninhalts, der Aktenaufbewahrungs- und Löschungsfristen sehe ich Regelungsbedarf.

Die Digitalisierung hat neben dem privaten Alltag der Gesellschaft und den industriellen Produktionsprozessen auch die Verwaltungsabläufe erreicht und bereits tiefgreifend verändert. Die Verwaltung ist dabei gefordert, ihre Papierakten künftig in eine elektronische Aktenführung zu überführen, die nach dem E-Government-Gesetz (vgl. 24. TB Nr. 3.2.3) seit 2013 die Regel sein soll (§ 6 E-Government-Gesetz). Die Umstellung auf die E-Akte verändert sowohl die internen Verwaltungsabläufe als auch die Anforderungen an eine datenschutzgerechte elektronische Schriftgutverwaltung. Bereits 2013 habe ich über das Pilotprojekt zur Einführung der E-Akte in

den Agenturen für Arbeit (AA) berichtet (24. TB Nr. 12.2.1) und greife das Thema auch in diesem Tätigkeitsbericht wieder auf (vgl. Nr. 24.4).

Familienkassen sind für den sog. Familienleistungsausgleich zuständig, d. h. für das Kindergeld (vgl. Kasten zu Nr. 7.8).

Das Bundeszentralamt für Steuern (BZSt) hat für den Umgang mit den sog. Kindergeldakten in der „Dienstanweisung zum Kindergeld nach dem Einkommensteuergesetz (DA-KG)“ verbindliche Regeln zur Aktenführung sowie Aufbewahrungs- und Löschungsfristen festgelegt und auf seiner Internetseite veröffentlicht. Danach können die Familienkassen die Kindergeldakten in Papierform oder elektronisch führen.

Während die DA-KG für die Papierakte konkret festlegt, wie Vorgänge zu führen sind, wie festsetzende Unterlagen aufzubewahren sind und welche Aufbewahrungsfristen gelten, enthält sie für die E-Akte nur rudimentäre Ausführungen. Danach sind Papierdokumente einzuscannen, in der E-Akte abzulegen und danach zu vernichten. Weiterführende Regelungen für die E-Akte enthält die DA-KG nicht.

Wie ich im Rahmen meiner bei den Familienkassen durchgeführten Kontrollen festgestellt habe, wurden die Regelungen der DA-KG zur Aktenführung sowie zu den Aufbewahrungs- und Löschungsfristen in der Praxis häufig nicht datenschutzkonform angewandt. So wurden z. B. Teilvorgänge von Kindergeldakten aufbewahrt, obwohl dies für die Bearbeitung aktueller Kindergeldanträge irrelevant war. Über die Kindergeldakten konnte ich ganze Familienchroniken nachvollziehen.

Das BMF vertritt dazu die Auffassung, eine Kindergeldakte müsse zwingend nach dem Kindergeldempfänger und nicht kindbezogen geführt werden. Zudem handele es sich bei Kindergeldfestsetzungen um Verwaltungsakte mit Dauerwirkung, die teilweise auch bei Festsetzungen zu weiteren Kindern berücksichtigt werden müssten.

Diese Argumente des BMF haben mich nicht überzeugen können. Ich halte es für geboten, dass bei der Bearbeitung von Kindergeldanträgen den datenschutzrechtlichen Geboten der Datensparsamkeit und der Erforderlichkeit der Datenverarbeitung Rechnung getragen wird. Dies setzt allerdings voraus, dass die DA-KG des BZSt überarbeitet wird und deren Regelungen insgesamt auch auf die elektronische Aktenführung erstreckt werden.

Ich empfehle dem Bundesministerium der Finanzen, die „Dienstanweisung zum Kindergeld nach dem Einkommensteuergesetz“ überarbeiten zu lassen und dort datenschutzgerechte Regelungen zu Aktenaufbewahrungs- und Löschungsfristen aufzunehmen

Kasten zu Nr. 7.8

Familienkassen

Bundesweit gibt es 14 überregionale Familienkassen der Bundesagentur für Arbeit und über 8.400 Familienkassen für den öffentlichen Dienst. Familienkassen werden im Wege der Organleihe als Bundesfinanzbehörden tätig und unterstehen grundsätzlich der Fachaufsicht des Bundeszentralamtes für Steuern (BZSt) (§ 5 Abs. 1 Nr. 11 Finanzverwaltungsgesetz - FVG).

7.9 OECD Standard für den automatischen Informationsaustausch über Finanzkonten

51 Staaten unterzeichneten am 29. Oktober 2014 in Berlin ein internationales Abkommen über den automatischen Informationsaustausch in Steuersachen.

Die zunehmende Globalisierung führt auch zu einer verstärkten Verlagerung von privaten Vermögenswerten auf ausländische Konten außerhalb des eigenen Ansässigkeitsstaates. Diese sowie damit erzielte Einnahmen bleiben oft unversteuert. Um dagegen vorzugehen, bedarf es verstärkter Zusammenarbeit der Steuerverwaltungen durch intensiveren Informationsaustausch. Hierzu wurde auf OECD-Ebene gemeinsam mit den G20-Staaten und in enger Kooperation mit der EU ein Modell für einen globalen Standard zum Austausch von Informationen zu Finanzkonten entwickelt und am 15. Juli 2014 von der OECD veröffentlicht. Der Standard orientiert sich weitgehend an Vorgaben des zwischen den USA und anderen Staaten jeweils bilateral abgeschlossenen FATCA-Abkommens (Foreign Account Tax Compliance Act, vgl. Nr. 7.5, 24. TB Nr. 2.5.5).

Der Standard besteht aus zwei wesentlichen Elementen:

a) einer Mustervereinbarung zwischen den zuständigen Behörden über den automatischen Austausch von Informationen über Finanzkonten zur Förderung der Steuerehrlichkeit (Competent Authority Agreement (CAA))

und

b) dem Gemeinsamen Melde- und Sorgfaltsstandard für den automatischen Informationsaustausch über Finanzkonten (Common Reporting Standard (CRS)).

Die zuständigen staatlichen Stellen sollen von den Finanzinstituten die erforderlichen Informationen erhalten und diese einmal jährlich automatisch mit anderen Staaten austauschen. Im Standard ist festgelegt, welche Informationen wann beschafft und ausgetauscht werden müssen und welche Finanzdienstleister und Steuerpflichtigen einbezogen werden. Sämtliche Arten von Kapitalerträgen wie Zinsen, Guthaben und Erlöse aus Veräußerungen von Finanzvermögen werden erfasst.

Im Rahmen des Jahrestreffens des Globalen Forums für Transparenz und Informationsaustausch für Besteuerungszwecke - des weltweit größten Netzwerks für die internationale Kooperation im Bereich von Steuern und Finanzinformationen - haben 51 Länder am 29. Oktober 2014 in Berlin diesen neuen globalen Standard zum automatischen Informationsaustausch zu Finanzkonten in Form eines multilateralen Abkommens gezeichnet.

Diese Gruppe der Erstanwender („Early Adopters“), darunter auch Deutschland, hat darin die frühzeitige Einführung des neuen, einheitlichen und globalen Standards für den automatischen Austausch von Informationen über Steuerpflichtige beschlossen und dessen weltweite Umsetzung vorangebracht. Die Unterzeichnung dieser Rahmenvereinbarungen ist ein weiterer Schritt hin zur tatsächlichen Umsetzung des automatischen Informationsaustausches. Darüber hinaus wurde die Amtshilferichtlinie (2011/16/EU) der Europäischen Union ergänzt. Die Richtlinie 2014/107/EU sieht eine Ausweitung des Anwendungsbereichs für einen verpflichtenden automatischen Informationsaustauch gemäß dem Gemeinsamen Meldestandard im EU-Recht vor.

Der Standard soll auf nationaler Ebene zum Jahreswechsel 2015/2016 eingeführt werden. Ein erster Informationsaustausch soll 2017 für die Erstanwender erfolgen, nachdem der gemeinsame Meldestandard von den einzelnen Staaten in nationales Recht umgesetzt worden ist. In Deutschland bedarf es hierzu eines entsprechenden Gesetzes sowie weiterer anwendungsrechtlicher Regelungen für den automatischen Informationsaustausch. Ich habe im bisherigen Verfahren gegenüber der Bundesregierung auf datenschutzrechtliche Erfordernisse hingewiesen und mich für eine datenschutzkonforme Ausgestaltung des automatischen Informationsaustauschs eingesetzt. Insbesondere muss eine angemessene Datensicherheit gewährleistet werden und es bedarf einer präzisen Zweckbindung hinsichtlich der auszutauschenden Informationen. Ein wesentliches Element wird die Wahrung datenschutzrechtlicher Betroffenenrechte darstellen.

Auf europäischer Ebene hat die Artikel-29-Gruppe festgestellt, der globale Standard selbst enthalte keine ausreichenden Regelungen zum Datenschutz. Sie sieht zwar grundsätzlich die Notwendigkeit des Informationsaustausches zur Bekämpfung der Steuerhinterziehung, hat aber gegenüber OECD, G20, Europäischem Parlament, Europäischer Kommission und Europarat noch einmal auf besonders kritische Punkte aus datenschutzrechtlicher Sicht hingewiesen, um diesbezüglich noch auf Verbesserungen hinzuwirken.

Ich werde das Verfahren aus datenschutzrechtlicher Sicht weiterhin sowohl auf europäischer Ebene im Rahmen der Mitwirkung in den Gremien der Artikel-29-Gruppe als auch bei der Umsetzung in nationales Recht begleiten.

7.10 Vierte Geldwäscherichtlinie

Eine neue Geldwäscherichtlinie soll die Bekämpfung von Geldwäsche und Terrorismusfinanzierung verbessern.

Die Bekämpfung der Geldwäsche wird maßgeblich durch internationale Vorgaben geprägt. Nachdem die bisherigen drei Geldwäscherichtlinien, die vor allem der Bekämpfung der Drogenkriminalität und des Terrorismus dienten, ins nationale Geldwäscherecht umgesetzt worden sind, wird nun auf europäischer Ebene seit 2012 eine 4. Geldwäscherichtlinie (Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung) vorbereitet. Diese soll den Rechtsrahmen für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung vereinheitlichen und die im Februar 2012 von dem wichtigsten internationalen Gremium in diesem Bereich, der FATF (Financial Action Task Force, Arbeitskreis Maßnahmen zur Geldwäschebekämpfung), vorgestellten, neu überarbeiteten internationalen Standards zur Geldwäschebekämpfung berücksichtigen.

Durch die neuen Vorschriften wird man effizienter auf neue Bedrohungen durch Geldwäsche und Terrorismusfinanzierung reagieren können. Die geplante Neuregelung soll den Geltungsbereich der Richtlinie erweitern, die geldwäscherechtlichen Sorgfaltspflichten verschärfen und eine verbesserte Identifizierung von Personen herbeiführen, die hinter einem Unternehmen stehen.

Die Europäische Kommission hat bereits im Februar 2012 den ersten Vorschlag zur Neufassung der 4. Geldwäscherichtlinie verabschiedet. Im März 2014 hat das Europäische Parlament eine rechtliche Vorfestlegung getroffen. Diese enthält einige datenschutzrechtliche Verbesserungen und die Forderung zur Einführung eines Zentralregisters zur Ermittlung wirtschaftlich Berechtigter. Nachdem der Rat der Europäischen Union im Juni 2014 eine inhaltlich vom Parlamentsvorschlag abweichende Allgemeine Ausrichtung zur 4. Geldwäscherichtlinie veröffentlicht hatte, haben sich Rat und Europäisches Parlament auf einen gemeinsamen Vorschlag einigen können. Der Kompromisstext muss nun noch formal durch das Plenum des Europäischen Parlaments und den Ministerrat bewilligt werden.

Der Europäische Datenschutzbeauftragte (EDPS) wurde von der Kommission spät und auch nur informell eingebunden. Erst im Februar 2013 wurde der Richtlinienentwurf der Financial Matters Subgroup der Artikel-29-Gruppe (vgl. Nr. 3.1) und damit den Datenschutzbeauftragten vorgestellt und übergeben.

Die Artikel-29-Gruppe hat in zwei Briefen vom April und November 2013 an das Europäische Parlament ihre datenschutzrechtlichen Bedenken zum Ausdruck gebracht. Der Geltungsbereich der Geldwäscherichtlinie soll weit über die ursprünglichen Regelungsziele Geldwäsche- und Terrorismusbekämpfung hinausgehen und nunmehr auch Steuerstraftaten umfassen. Allerdings werden die Begriffe nicht hinreichend klar definiert. Auch die Zweckbestimmung und die Zweckbindung lassen sich nicht hinreichend klar aus dem Entwurf bestimmen. Ich befürchte zudem, dass die geplanten vereinfachten Sorgfaltspflichten nicht mehr dem bisherigen risikobasierten Ansatz entsprechen. Dadurch könnten übermäßig und willkürlich Daten erhoben werden. Die Artikel-29-Grup-

pe fordert daher, spezielle Regelungen für eine Übermittlung personenbezogener Daten in Drittländer ohne angemessenes Datenschutzniveau zu treffen.

Der EDPS, der den Kommissionsvorschlag ebenfalls kritisch sieht, hat in seiner Stellungnahme vom Februar 2014 Verbesserungen des Datenschutzes empfohlen. Er hat dafür geworben, das EU-Datenschutzrecht anzuwenden, die Zweckbindung der Daten stärker zu beachten und ein Informationsrecht über die Verarbeitung von Daten vorzusehen.

Ich werde das weitere Verfahren sowohl auf europäischer Ebene im Rahmen der Mitwirkung in der Artikel-29-Gruppe als auch im Hinblick auf die nationale Umsetzung konstruktiv kritisch begleiten.

7.11 Persönliche Anwesenheit bei Videoverbindung

Seit März 2014 ist es Banken und Finanzdienstleistern erlaubt, die für eine Kontoeröffnung notwendige Identifizierung des Kunden per Videotechnik durchzuführen. Hiergegen habe ich erhebliche datenschutzrechtliche Bedenken.

Das Geldwäschegesetz (GwG) verpflichtet u. a. Kreditinstitute und Finanzdienstleister zu bestimmten Sorgfaltspflichten, die dem Aufspüren bzw. der Verhinderung von Geldwäsche dienen. So müssen die Kunden vor Vertragsschluss eindeutig identifiziert werden. Dies erfolgt vor Ort beim Dienstleister durch die Vorlage eines Ausweisdokumentes. Ist der Kunde dagegen nicht persönlich anwesend, wie etwa bei der Online-Eröffnung eines Kontos, treffen den Dienstleister besondere Sorgfaltspflichten. Er muss sich z. B. entweder eine beglaubigte Kopie des Ausweises vorlegen lassen oder der Kunde nutzt die elektronische Identitätsfunktion seines Personalausweises. Das BMF hat nun in einem Rundschreiben vom März 2014 der BaFin seine Auslegung des Begriffs „persönliche Anwesenheit“ im Sinne von § 6 Absatz 2 Nummer 2 GwG dargelegt. Unter bestimmten Voraussetzungen soll danach auch dann eine persönliche Anwesenheit angenommen werden können, wenn die am Identifizierungsverfahren Beteiligten zwar nicht physisch, aber im Rahmen einer Videoübertragung visuell wahrnehmbar seien, eine sprachliche Kontaktaufnahme möglich sei und in diesem Zusammenhang eine Überprüfung der Identität des Vertragspartners anhand eines Identifikationsdokuments vorgenommen werden könne. Dabei soll der Kunde sein Ausweisdokument in verschiedenen Positionen in die Kamera halten. Dies soll den Mitarbeiter des Dienstleisters in die Lage versetzen, die Sicherheitsmerkmale des Dokuments wie z. B. Hologramme, zu erkennen. Außerdem muss der Kunde während der Videoübertragung eine an ihn vorab übermittelte Ziffernfolge (TAN) in seinen Computer eingeben und an den Dienstleister senden.

Ein solches Verfahren verstößt nach meiner Auffassung nicht nur gegen das GwG, sondern birgt auch erhebliche datenschutzrechtliche Risiken. Denn Sinn und Zweck einer persönlichen Anwesenheit besteht darin, zweifelsfrei die Übereinstimmung von personenbezogenen Ausweisdaten und anwesender Person sowie Echtheit des Ausweises überprüfen zu können. Ob die Zuverlässigkeit der „Inaugenscheinnahme“ einer Person und ihres Ausweises mittels Videotechnik dem unmittelbaren persönlichen Kontakt gleichgestellt werden kann, erscheint mir mehr als fraglich. Über eine Videoverbindung können beispielsweise Sicherheitsmerkmale des Ausweises wie Hologramme nicht eindeutig als echt erkannt werden. Auch andere Manipulationen am Ausweis sind nicht ohne weiteres so offensichtlich wie bei einer tatsächlichen Inaugenscheinnahme.

Weiter entsteht bei der Aufnahme und Speicherung von Standbildern oder auch der kompletten Videoaufnahme eine vollständige Kopie des Ausweisdokumentes. Dies widerspricht den einschlägigen Bestimmungen des GwG, da nur bestimmte Daten für die Identifizierung zu prüfen und zu dokumentieren sind.

Darüber hinaus enthält das Rundschreiben der BaFin keine Aussagen zu Datenschutz und Datensicherheit. Zwar sollen ungeachtet der Ausführungen des Rundschreibens weiterhin datenschutzrechtliche Regelungen Anwendung finden. Aber was das konkret bedeutet, bleibt der Auslegung des Anwenders überlassen. Ich finde es be-

dauerlich, dass bei der Übermittlung keine Vorgaben an die Datensicherheit gemacht werden, also z. B. keine gesicherte Verbindung erforderlich ist oder nur solche Produkte für die Videoübertragung zum Einsatz kommen dürfen, die sich nicht in ihren Allgemeinen Geschäftsverbindungen vorbehalten, den kompletten Kommunikationsinhalt mitlesen und auswerten zu dürfen.

Ich habe meine datenschutzrechtlichen Bedenken gegen ein solches Verfahren gegenüber der BaFin und auch dem BMF geäußert. Die BaFin hält ihre Vorgehensweise mit Hinweis auf das ihm vorgesetzte BMF für gerechtfertigt. Seitens des BMF stand zum Ende des Berichtszeitraums eine Antwort noch aus.

Ich empfehle der Bundesregierung, für die Identifizierung von Kunden nach dem Geldwäschegesetz auf die Möglichkeiten einer Videoidentifizierung zu verzichten. Es ist weder die Wirksamkeit einer solchen Identifizierung geklärt, noch entspricht dies den Vorgaben des Personalausweisgesetzes. Außerdem ist nicht sichergestellt, dass die anfallenden personenbezogenen Daten datenschutzkonform verarbeitet werden.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Arbeitskreis Steuerverwaltung

OECD Working Party on Information Security and Privacy (WPISP)

B. Zudem von besonderem Interesse

Nr. 5.13.5

8 Ausschuss für Wirtschaft und Energie

8.1 Binnenmarktinformationssystem

Am 6. Mai 2014 fand in Brüssel das erste Treffen der IMI Supervision Coordination Group auf Einladung des Europäischen Datenschutzbeauftragten (EDPS) statt.

Bereits Anfang 2010 startete das Binnenmarktinformationssystem (Internal Market Information System - IMI) und verbindet seitdem nationale, regionale und lokale Behörden grenzüberschreitend miteinander. Zur Umsetzung der EG-Dienstleistungsrichtlinie (RL 2006/123/EG) ermöglicht IMI einen einfacheren und schnelleren Kommunikationsaustausch zwischen den 28 EU-Staaten (22. TB Nr. 3.4.1).

Als Rechtsrahmen dafür dient die IMI-Verordnung ((EU) Nr. 1024/2012-IMI-VO) vom Dezember 2012. Sie ist eine wesentliche Voraussetzung für die verbindliche Anwendung datenschutzrechtlicher Grundsätze bei der Nutzung des IMI, insbesondere im Hinblick auf die Betroffenenrechte (24. TB Nr. 2.3.1).

Inzwischen wird IMI bereits in folgenden Bereichen verwendet:

- Anerkennung von Berufsqualifikationen
- Dienstleistungen
- Entsendung von Arbeitnehmern
- Transport von Euro-Bargeld
- Anerkennung von Fahrerlaubnissen von Triebwerkfahrzeugführern
- Patientenrechte
- als Pilotprojekt für den elektronischen Geschäftsverkehr.

Eine Ausweitung auf weitere Rechtsbereiche ist für die kommenden Jahre geplant.

IMI wird auf europäischer Ebene vom Europäischen Datenschutzbeauftragten überwacht. Er hat am 6. Mai 2014 die nationalen Datenschutzbehörden erstmalig zu einem Treffen der IMI Supervision Coordination Group eingeladen, an dem ich teilnahm.

Neben einem Erfahrungsaustausch der Datenschutzbehörden untereinander hat die Kommission einen Ausblick auf die geplanten Ausweitungen des IMI gegeben. Inhaltlich ging es insbesondere um zwei Fragen: Wie wird die Öffentlichkeit in den einzelnen Mitgliedstaaten über das Instrument IMI informiert? Wie können die Betroffenen besser über die Verarbeitung ihrer personenbezogenen Daten im IMI informiert werden?

National kontrollieren die Datenschutzbehörden die Rechtmäßigkeit der Datenverarbeitung und die Gewährleistung der Rechte der betroffenen Personen im IMI. Um einen persönlichen Eindruck über die mit IMI verbundenen Verfahrensabläufe zu erhalten, habe ich im März 2014 die Bundesfinanzdirektion (BFD) West zur Beratung und Kontrolle besucht. Ich wollte mich über die Umsetzung von IMI im Rahmen der Entsenderichtlinie (96/71 EG) unterrichten lassen, da hier die BFD West die allein zuständige Behörde in Deutschland für IMI-Anfragen ist. Wie ich dabei feststellen konnte, werden die personenbezogenen Daten im Einklang mit den datenschutzrechtlichen Vorschriften verarbeitet und genutzt.

Ich werde die Anwendung der IMI-VO auch weiterhin begleiten und auf die Einhaltung der datenschutzrechtlichen Bestimmungen achten. Dazu stehe ich u. a. auch in Kontakt mit der nationalen, beim Bundesverwaltungs-

amt in Köln angesiedelten IMI-Koordinatorin, die nach Artikel 6 der IMI-VO von jedem Land als nationaler Ansprechpartner für technische Fragen und für die Beratung der IMI-Nutzer in Fragen der Anwendung und Verwaltung einzurichten ist.

8.2 In Erwartung eines besonderen Pakets - Smart Metering

Die Einführung intelligenter Messsysteme für den Stromverbrauch (Smart Meter) steht derzeit still. Alle Beteiligten - darunter auch ich - warten auf das Entscheidende: das „Verordnungspaket Intelligente Netze".

Ich habe in den vergangenen Tätigkeitsberichten bereits mehrfach über meine Einbindung in die Schaffung der rechtlichen und technischen Rahmenbedingungen für die Einführung intelligenter Messsysteme berichtet. Diese aus intelligentem Zähler und Kommunikationseinheit bestehenden so genannten Smart Meter sind ein zweifelsohne bedeutender Baustein einer intelligenten Energieinfrastruktur der Zukunft, ohne die wiederum die gesamtgesellschaftlich gewollten grundlegenden Veränderungen der Energieproduktion nicht denkbar sind. Unbestreitbar ist aber auch, dass die digitale Steuerung und Kommunikationsfähigkeit intelligenter Messsysteme großes datenschutzrechtliches Gefährdungspotential in sich tragen. Daher arbeite ich seit langem eng mit dem zuständigen Bundesministerium für Wirtschaft und Energie (BMWi) und dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) zusammen, um die hinreichende datenschutzrechtliche Flankierung sicherzustellen. Im Berichtszeitraum war ich insbesondere an der AG „Intelligente Netze und Zähler" des BMWi und einer vom BSI koordinierten Arbeitsgruppe beteiligt, die sich intensiv mit konkreten Ablaufszenarien im Zusammenhang mit Wechselprozessen bei der Stromversorgung befasste. Die Arbeitsergebnisse führten zur Aktualisierung einer Technischen Richtlinie des BSI, die Vorgaben für den sicheren Betrieb intelligenter Messsysteme macht. Ganz entscheidend ist aber aus meiner Sicht, dass das BMWi endlich von der in § 21i Energiewirtschaftsgesetz vorgesehenen Verordnungsermächtigung Gebrauch macht, um die Anforderungen an intelligente Messsysteme auch in datenschutzrechtlicher Hinsicht zu konturieren. Konkret wird die Vorlage einer Messsystemverordnung, einer Verordnung über die Messung und Datenkommunikation im intelligenten Energienetz und einer Verordnung über den Rollout intelligenter Messsysteme erwartet. Sobald mir Entwürfe hierzu vorliegen, werde ich prüfen, ob sie den bereits in § 21g Energiewirtschaftsgesetz niedergelegten datenschutzrechtlichen Grundzügen entsprechen. Ein besonderes Augenmerk werde ich darauf legen, dass nicht über den Umweg der Netzentgelt-Berechnung oder für Zwecke der Bilanzierung von Stromtransaktionen an den Netzübergangspunkten der Lastgang (Stromverbrauch) je Haushalt erhoben wird.

8.3 Ein Binnenmarkt für die elektronische Identifizierung und für Vertrauensdienste - die eIDAS-VO

Nach langen Verhandlungen wurden datenschutzrechtliche Forderungen in die EU-Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO) aufgenommen.

Nachdem die Europäische Kommission am 4. Juni 2012 ihren Entwurf der eIDAS-VO vorgestellt hatte, hat sich die zuständige Ratsarbeitsgruppe Telekommunikation & Informationsgesellschaft damit befasst. Das federführende BMWi hat zur Entwicklung der deutschen Position alle relevanten Stellen eingebunden (vgl. bereits 24. TB Nr. 2.3.4). Die Koordination kann ich als vorbildlich bezeichnen.

Ziel der Verordnung soll zum einen die gegenseitige Anerkennung und damit die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel sein. Zum anderen soll die Verbreitung elektronischer Signaturen im Binnenmarkt gefördert sowie ein Regelwerk für sog. Vertrauensdienste geschaffen werden. Als Vertrauensdienste werden neben elektronischen Signaturen auch elektronische Zeitstempel, elektronische Siegel, elektronische Zustelldienste und elektronische Bewahrungs- und Validierungsdienste für Signaturen und Siegel verstanden. Dabei wird zwischen nichtqualifizierten und qualifizierten Diensten bzw. Diensteanbietern unterschieden. Qualifi-

zierte Diensteanbieter unterliegen deutlich strengeren Anforderungen, dafür haben ihre Dienste größere Beweiswirkungen und teilweise weitergehende Rechtswirkungen.

Neben Fragen des richtigen Regelungsinstruments enthielt der Verordnungsentwurf auch aus datenschutzrechtlicher Sicht einige problematische Punkte.

Meine wichtigsten Forderungen waren:

- Die Vorschriften zur gegenseitigen Anerkennung elektronischer Identifizierungsmittel müssen so gestaltet sein, dass der neue Personalausweis mit seiner elektronischen Identifizierungsfunktion (eID-Funktion) weiterhin genutzt werden kann.
- Beim Einsatz von Identifizierungsmitteln müssen generell datenschutzrechtliche Prinzipien wie die Verwendung von Pseudonymen, Datensparsamkeit, Zweckbindung und Erforderlichkeitsprüfung beachtet werden.
- Eine zentrale Datenbank für die Schaffung einer Online-Authentisierung zur Überprüfung elektronischer Identifizierungsdaten sollte vermieden werden.
- Die Verordnung selbst sollte Mindestanforderungen an Datenschutz, Datensicherheit und technische Standards festlegen und dies nicht der Kommission überlassen.
- Das hohe deutsche Niveau in Bezug auf Datenschutz und Datensicherheit sollte beibehalten werden.
- Es sollte klargestellt werden, welche Befugnisse die Datenschutzbehörden neben den Aufsichtsbehörden über die Vertrauensdienste-Anbieter im Falle von Rechtsverstößen haben.
- Elektronische Siegel sollten auch von natürlichen Personen genutzt werden dürfen.

Die Verordnung ist am 28. August 2014 im Amtsblatt der EU veröffentlicht worden (Verordnung Nr. 910/2014 vom 23.07.2014, Amtsblatt L 257/73). Im Laufe der Verhandlungen konnten datenschutzrechtliche Verbesserungen erreicht werden. Elektronische Siegel bleiben allerdings weiterhin nur juristischen Personen vorbehalten. Sie können damit elektronische Dokumente „siegeln“ und so zu erkennen geben, dass das Dokument mit diesem Inhalt aus ihrer Sphäre stammt. Im Gegensatz zur Signatur steht ein Siegel aber nicht für eine Willenserklärung. Die Stellung und die Befugnisse der Datenschutzaufsichtsbehörden sind in der Verordnung nun detaillierter geregelt als zunächst vorgesehen. Die Anbieter von Vertrauensdiensten sind verpflichtet, jeder zuständigen Stelle, wie etwa den Datenschutzbehörden, unverzüglich jeden Vorfall zu melden, der sich erheblich auf den Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt. Außerdem muss auch die Aufsichtsstelle die Datenschutzbehörden unterrichten, wenn sie bei ihren Überprüfungen eines qualifizierten Vertrauensdienstes feststellt, es könnte gegen Datenschutzvorschriften verstoßen worden sein. Auch meine Forderung nach Mindestanforderungen für Datenschutz und Datensicherheit in der Verordnung selbst wurde teilweise erfüllt. Ausdrücklich wird nun an mehreren Stellen die Einhaltung der europäischen Datenschutzrichtlinie 95/46/EG bei der Verarbeitung personenbezogener Daten festgeschrieben. Allerdings werden die notwendigen Konkretisierungen in die sog. Durchführungsbestimmungen verlagert, die von der Kommission erlassen werden. Solche in Komitologie-Verfahren erarbeiteten Vorschriften - die Vorschriften werden durch Expertenausschüsse vorbereitet, die Kommission muss deren Vorschlägen allerdings nicht zwingend folgen - schränken leider die Einflussnahme der Mitgliedsstaaten und damit auch der nationalen Datenschutzbehörden auf den Rechtssetzungsprozess sehr ein. Ich erwarte, dass die Bundesregierung auch hier im Rahmen ihrer Möglichkeiten datenschutzfreundliche Regelungen durchsetzt und mich weiter beteiligt.

8.4 Neue DIN-Norm 66399 zur Vernichtung

Eine neue Orientierungshilfe macht die Anwendung in der Praxis leichter.

Löschen ist gemäß § 3 Absatz 4 Nummer 5 BDSG das Unkenntlichmachen personenbezogener Daten. Personenbezogene Daten sind immer dann zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Aufgabenerfüllung bzw. zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Oft müssen jedoch statt einzelner Datensätze Datenträger insgesamt vernichtet werden. Die Verpflichtung zum Löschen von Daten ist sowohl im BDSG (§ 20 Abs. 2 bzw. § 35 Abs. 2) als auch in spezialgesetzlichen Regelungen (z. B. § 84 Abs. 2 SGB X) verankert. Der Prozess des „Löschens“ oder des „Vernichtens“ muss dauerhaft und irreversibel dazu führen, dass die betreffenden Informationen nicht mehr aus dem Datenträger gewonnen werden können. Dies gilt sowohl für die Daten verarbeitende Stelle selbst, als auch für Dritte, wenn sie beispielsweise im Auftrag Datenträger vernichten.

Das Vernichten von Datenträgern ist gleichzeitig eine technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme personenbezogener Daten durch Unbefugte (Sicherung der Vertraulichkeit). Insofern sind die entsprechenden Regelungen des BDSG (§ 9 sowie dessen Anlage) sowie andere gesetzliche Vorschriften (z. B. § 78a SGB X) zu beachten. Danach muss die Maßnahme dem Schutzbedarf der Daten angemessen sein. Ihre Umsetzung hat sich nach den im Einzelfall zu betrachtenden Risiken und dem Stand der Technik zu richten.

Im Oktober 2012 wurde hierzu die neue DIN-Norm 66399 „Büro- und Datentechnik - Vernichten von Datenträgern“ veröffentlicht (vgl. 24. TB Nr. 4.6). Der zuständige DIN-Ausschuss hat damit einen Standard erarbeitet, der den heutigen Stand der Technik in der Datenträgervernichtung abbildet und die veraltete Norm DIN 32757 ablöst.

In Zusammenarbeit mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder sowie dem Düsseldorfer Kreis habe ich an einer Orientierungshilfe mitgearbeitet, die es den verantwortlichen Stellen leichter macht, die DIN-Norm 66399 in der Praxis anzuwenden. Die Orientierungshilfe steht auf meiner Homepage zum Abruf bereit.

Die DIN-Norm 66399 soll in naher Zukunft durch eine europäische Norm zur Vernichtung von Datenträgern ergänzt werden. Dies unterstütze ich. Mit diesem Ziel kann der deutsche datenschutzrechtliche Standard in Europa verankert werden und damit zur Verbesserung des Datenschutzes beitragen.

8.5 Cloud Computing - wenn dann vertrauenswürdig

Jeder kennt es, fast jeder nutzt es! Cloud Computing ist erwachsen geworden. Verschiedene Stellen und Gremien haben sich mit den rechtlichen und technischen Fragen beschäftigt. Auch an einer Zertifizierung von Cloud-Diensten wird gearbeitet.

Meine Gremienarbeiten zu Cloud Computing, über die ich bereits mehrfach berichtet habe (zuletzt im 24. TB unter Nr. 5.3), ging auch im Berichtszeitraum weiter. Inzwischen drängen die Hersteller mit neuen Cloud-Produkten in den Markt. Als ein Beispiel sind komplette Office-Umgebungen zu nennen, die über die Cloud realisiert werden. Dabei hat sich an den grundsätzlichen Datenschutzanforderungen nichts geändert. Nur wenn die Daten innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) gespeichert und verarbeitet werden, bestehen rechtlich keine Bedenken. Bei einer grenzüberschreitenden Datenverarbeitung in der Cloud, die sich auch über Länder außerhalb der EU oder des EWR erstreckt, ist eine Rechtsgrundlage für die Datenübermittlung sowie ein angemessenes Datenschutzniveau in dem betroffenen Drittstaat erforderlich.

Technologisch gesehen sollten insbesondere (sensible) personenbezogene Daten vor dem Einbringen in die Cloud und bei der Übertragung unter alleiniger Kontrolle des Auftraggebers verschlüsselt werden. Wie die Enthüllungen der Überwachungs- und Spionagetätigkeiten ausländischer Geheimdienste gezeigt haben, hat auch die oftmals vernachlässigte Verschlüsselung der Daten das Cloud Computing als internationales Modell in die Kritik gebracht.

Deswegen wurde die Orientierungshilfe zu Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises überarbeitet. Mit der nun vorliegenden Version 2.0 (Stand 09.10.2014, abrufbar auf meiner Internetseite www.datenschutz.bund.de) wird auf die Rechtsproblematik der bekannt gewordenen Zugriffe ausländischer Nachrichtendienste eingegangen (vgl. Nr. 2.1). Im Zuge dieser Entwicklungen und Erkenntnisse könnte sich ein auf die Bundesrepublik Deutschland beschränktes Cloud-Angebot als Wettbewerbsvorteil auch für die hiesige Wirtschaft erweisen.

Dieser Standortvorteil könnte durch Datenschutzzertifizierungen von Cloud-Diensten weiter ausgebaut werden. In dem Technologieprogramm „Trusted-Cloud“ des BMWi, in das ich eingebunden bin, arbeiten Datenschützer sowie Vertreter der Wirtschaft und von Forschungseinrichtungen/Universitäten in einem Pilotprojekt u. a. daran, Rechtsfragen beim Cloud Computing zu klären und Anforderungen an eine Datenschutz-Zertifizierung von Cloud-Diensten zu definieren. Ziel ist eine Zertifizierung von Cloud-Diensten unter Datenschutzgesichtspunkten. Allerdings wird es noch einige Zeit in Anspruch nehmen, bis solche Zertifikate von unabhängigen Prüfstellen vergeben werden können.

Auch vor dem IT-Grundschutz des BSI macht Cloud Computing nicht halt. Ein neuer Grundschutz-Baustein dazu ist so gut wie fertig gestellt und bereits in einer Vorabversion auf der Internetseite des BSI (www.bsi.de) veröffentlicht.

Zudem arbeitet meine Dienststelle in einer Unterarbeitsgruppe zu Cloud Computing des IT-Gipfels mit, die zuletzt auf dem IT-Gipfel im Jahr 2014 ihre Arbeitsergebnisse veröffentlicht hat. Ziel ist es dabei, über Chancen und Risiken im Umgang mit dem Internet und bei Cloud Computing aufzuklären. Als ein Arbeitsergebnis wurde beim IT-Gipfel eine Broschüre zum Sicherheitsprofil von CRM-Software (Customer-Relationship-Management - Kundenbeziehungsmanagement) nach dem Software-as-a-Service-Modell (SaaS) als exemplarische Cloud-Computing-Anwendung vorgestellt und ein Übersichtspapier über die erarbeiteten Steckbriefe hierzu herausgegeben. Beim SaaS wird die Anwendungssoftware und die dazu notwendige Hard- und Software von einem Dienstleister betrieben. Diese Informationen wie auch das eigentliche Schutzprofil sowie zwei weitere Sicherheitsprofile für eine SaaS Collaboration Plattform und ein SaaS Archivierungssystem können auf der Internetseite des BSI im Bereich Cloud Computing bezogen werden.

8.6 Einsatz von RFID-Systemen - eine datenschutzrechtlich unbefriedigende Situation

Seit 2011 existiert auf europäischer Ebene ein Rechtsrahmen für die Durchführung von Datenschutzfolgeabschätzungen bei RFID-Anwendungen mit personenbezogenen Daten. Diese geht auf eine Empfehlung der Europäischen Kommission vom Mai 2009 zurück. Doch die Praxis sieht anders aus.

RFID-Systeme (Radio Frequency Identifications) durchdringen mittlerweile viele Bereiche und haben dabei unsichtbar für die meisten von uns bereits die Welt erobert (22. TB Nr. 6.7, 23. TB Nr. 5.9). Ob Bezahl- oder Kundenkarten, Fahrkarten für den ÖPNV oder in Textilien eingenäht: RFID-Systeme haben vielfältig Einzug gehalten, und das Taggen bei Kleidung ist heute Standard geworden. Kleidungsstücke werden dabei bereits beim Herstellungsprozess mit den kleinen Funkchips versehen. Doch was passiert nach dem Bezahlen an der Kasse? Werden die RFID-Systeme deaktiviert oder entfernt? Ist dies rechtlich geboten?

Diese Fragen beschäftigen derzeit den Petitionsausschuss des Deutschen Bundestages, den ich berate. Allgemein hat man in den letzten Jahren zum Umgang mit RFID-Systemen eigentlich auf eine Selbstverpflichtung des Handels gehofft, welche jedoch nie gekommen ist. Es ist also weiterhin offen, wie der Handel mit den Tags umgeht und ob vorgesehen wird, RFID-Systeme nach dem Bezahlen an der Kasse von mitführbaren Gegenständen und Textilien zu entfernen oder diese automatisch zu deaktivieren. Denn sind RFID-Systeme nach dem Bezahlen weiterhin aktiv, besteht die Möglichkeit der heimlichen Erstellung von Konsum- oder Bewegungsprofi-

len. Sollte der Handel hier weiterhin nicht zu einer Selbstverpflichtung kommen und dies einheitlich regeln, muss der Gesetzgeber tätig werden.

Anfang 2011 hatte die Artikel-29-Gruppe (WP 180 vom 11.02.2011) den Rahmen für eine Datenschutzfolgenabschätzung bei RFID-Anwendungen geschaffen. Demnach sollten mindestens sechs Wochen vor Inbetriebnahme Berichte über die Folgenabschätzung von RFID-Anwendungen der zuständigen Datenschutzaufsicht vorgelegt werden. Diese Empfehlung ist jedoch nicht bindend. Mit der neuen EU-Datenschutz-Grundverordnung sollen PIAs aber in vielen Bereichen zur Pflicht werden.

In diesem Zusammenhang habe ich innerhalb der Technology Subgroup der Artikel-29-Gruppe und bei meinen Länderkolleginnen und -kollegen nachgefragt, welche Einsatzgebiete und Projekte für RFID-Anwendungen ihnen in ihrer Zuständigkeit bekannt sind, und ob sie diese genauer geprüft haben. Ferner wollte ich wissen, ob ihnen entsprechende RFID PIAs (Privacy Impact Assessment) vorgelegt wurden.

Leider musste ich feststellen, dass den Aufsichtsbehörden der EU wie in Deutschland zwar vereinzelte Fälle von RFID-Anwendungen in ihrem Bereichen bekannt geworden sind, PIAs in Bezug auf RFID-Systeme jedoch so gut wie gar nicht vorgelegt wurden. Vermutlich sind in der Wirtschaft nur sehr wenige PIAs zum Einsatz von RFID-Anwendungen erstellt worden. Lediglich innerhalb des AK Technik habe ich zusammen mit meinen Länderkolleginnen und -kollegen PIAs für Bezahlkarten der Kreditwirtschaft prüfen können. Hierbei haben die Sparkasse sowie die Kreditinstitute Visa und MasterCard ihre PIAs zur Datenschutzfolgenabschätzung bei ihren kontaktlosen Bezahlkarten vorgelegt. Bei diesen Produkten kommt die Nahbereichsfunktechnik NFC (Near Field Communication) zum Einsatz, die nur über sehr kleine Entfernungen arbeitet.

Insgesamt lässt sich sagen, dass diese PIAs den Anforderungen des AK Technik genügt haben und die Privatsphäre der Nutzer bis auf zu tolerierende Restrisiken hin ausreichend gewahrt wird. Die AG Kreditwirtschaft des Düsseldorfer Kreises und der AK Technik fordern jedoch zusätzlich, dass Nutzern der Bezahlkarten kostenlose Schutzhüllen zur Unterbindung unerwünschter Kommunikationsvorgänge zur Verfügung gestellt werden, und dass es möglich sein muss, die Funkschnittstelle/NFC-Funktion auf Wunsch des Karteninhabers zu deaktivieren. Weiterhin werden die Hersteller aufgefordert, Lösungsansätze zu einer angemessenen Verschlüsselung und Randomisierung der Kartennummer weiterhin zu verfolgen.

Die Kommission hat im August 2014 einen Bericht zum Einsatz von RFID-Systemen veröffentlicht (https://ec.europa.eu). Danach kommen RFID-Systeme hauptsächlich beim Taggen von Textilien zum Einsatz, im Einzelhandel dominiert jedoch weiterhin der Strich- bzw. Barcode. PIAs werden nur im geringen Umfang erstellt, weil man die Datenschutzrisiken in den Mitgliedstaaten oftmals als sehr niedrig bewertet.

Ein europäisches Kennzeichen für RFID-Anwendungen existiert seit 2014 (vgl. Kasten zu Nr. 8.6). Es wird jedoch noch sehr selten verwendet. Zudem beabsichtigt die Kommission, im Jahr 2016 eine Neubewertung der Umsetzung der Empfehlung im Lichte der laufenden technischen Entwicklung und Marktentwicklung sowie der damit verbundenen rechtlichen Rahmenbedingungen, beispielsweise für den Datenschutz, durchzuführen.

Abschließend möchte ich noch darauf hinweisen, dass das BSI, das ich hierbei zum Datenschutz berate, zurzeit seine technischen Richtlinien zum Einsatz von RFID-Systemen überarbeitet.

Kasten zu Nr. 8.6

8.7 TTIP

Die Verhandlungen zur „Transatlantic Trade and Investment Partnership“ (TTIP) schreiten ohne Beteiligung der Datenschutzbehörden voran. Sie dürfen nicht die europäischen Datenschutzstandards schwächen.

Die derzeit weitgehend im Verborgenen laufenden Verhandlungen zwischen der Europäischen Kommission und den USA zu TTIP geben für den Datenschutz Anlass zur Sorge. Dies liegt in der Zielrichtung des Abkommens begründet, mit Blick auf die wirtschaftlichen Interessen international agierender Unternehmen Handelshemmnisse abzubauen. Denn schließlich bildete seinerzeit der Abbau sog. nicht-tarifärer Handelshemmnisse den zentralen Grund für die europäische Datenschutzrichtlinie 95/46/EG.

In der Entschließung „Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten“ der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. März 2013 (vgl. Anlage 5) wird von der Kommission gefordert, bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus den Augen zu verlieren und das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards zu wahren.

Gerne würde ich mir selbst ein Bild über die datenschutzrechtlichen Auswirkungen der geplanten TTIP-Regelungen machen. Wie alle anderen Datenschutzbehörden bin ich jedoch von den Verhandlungen ausgeschlossen. Umso mehr bedauere ich, dass mir auch eine Mitwirkung in dem im Mai 2014 einberufenen TTIP-Beirat des BMWi verwehrt geblieben ist, obwohl dort Datenschutzfragen zumindest indirekt eine Rolle spielen. Auch die Bundesregierung ist meiner Bitte um wenigstens rudimentäre Informationen zu datenschutzrechtlichen Fragen bei TTIP bislang nicht nachgekommen.

In dem durch den Europäischen Rat an die Kommission erteilten Verhandlungsmandat zu TTIP findet der Datenschutz keine Erwähnung. Demgegenüber ist der Datenschutz vom Regelungsgehalt des bereits ausgehandelten Freihandelsabkommens mit Kanada (CETA) explizit ausgenommen. Da CETA als Vorbild für TTIP gilt, hoffe ich auf eine Übernahme dieser Regelung.

Ich begrüße, dass der Bundesregierung auf eine Kleine Anfrage im Deutschen Bundestag betont, sie vertrete grundsätzlich in allen Verhandlungen die Position, das Freihandelsabkommen dürfe nicht zu einer Absenkung von Datenschutzstandards führen und müsse nicht nur von der EU sondern auch von den Mitgliedstaaten ratifiziert werden (Bundestagsdrucksache 18/2687, S. 2 und 5).

Ich biete dem Bundestag meine datenschutzrechtliche Beratung im Vorfeld dieser wegweisenden Entscheidungen an.

8.8 Telekommunikation

In den letzten Jahren konnte ich die Anzahl meiner Beratungs- und Kontrollbesuche bei Telekommunikationsdiensteanbietern leicht steigern, nicht zuletzt deshalb, weil es im Bereich des Telekommunikationsrechts keine nennenswerten gesetzgeberischen Aktivitäten zu verzeichnen gab, die meine Arbeitskapazitäten in diesem Bereich gebunden hätten. Dies bedeutet aber leider auch, dass mir gegenüber diesen Unternehmen noch immer keine Sanktionsbefugnisse bei Verstößen gegen das Telekommunikationsgesetz eingeräumt worden sind, sondern ich mich an die Bundesnetzagentur wenden muss, um diese zu einem Tätigwerden zu veranlassen (vgl. 23. TB Nr. 2.1). Auch bei Verstößen gegen das BDSG wurde mir die Zuständigkeit für Bußgeldverfahren nicht übertragen (vgl. 24. TB Nr. 6.9). Wie meine Erfahrungen aus den Kontrollen eindrucksvoll belegen, besteht hier dringender Handlungsbedarf.

Ich empfehle dem Gesetzgeber, mir stärkere Sanktionsmöglichkeiten gegenüber Telekommunikations- und Postdienstunternehmen einzuräumen und die Zuständigkeit für Bußgeldverfahren bei Verstößen gegen das Bundesdatenschutzgesetz zu übertragen.

Kasten zu Nr. 8.8

In der Telekommunikation unterscheidet man folgende Arten von Daten:

Bestandsdaten sind Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Hierzu gehören etwa Name, Adresse, Kontonummer. Es besteht eine Pflicht, für Abfragen von Sicherheitsbehörden bestimmte Bestandsdaten zu erheben, auch wenn diese betrieblich nicht erforderlich sind (vgl. § 111 TKG). Ein unachtsamer Umgang mit diesen Daten oder eine missbräuchliche Nutzung z. B. von Kontendaten kann schwerwiegende Folgen für den Teilnehmer haben.

Standortdaten sind Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden, und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben.

Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden und unterliegen dem Fernmeldegeheimnis (Art. 10 GG, § 88 TKG). Dies sind neben den Daten, die man vom Einzelverbindungsnachweis kennt, auch Standortdaten bei Handygesprächen oder IP-Adressen beim Abruf von E-Mails. Die Aussagekraft dieser Daten ist sehr hoch, da soziale Netze oder Bewegungsprofile erkennbar werden.

Der **Inhalt der Telekommunikation**, also etwa das Telefongespräch, der Text einer SMS oder E-Mail oder übertragene Daten, unterliegen ebenso dem Fernmeldegeheimnis und genießen den höchsten rechtlichen Schutz.

8.8.1 Meldepflicht mit einigen Tücken - der neue § 109a TKG

Wie rasant steigende Fallzahlen belegen, ist die im Jahr 2012 eingeführte Meldepflicht über Datenschutzvorfälle bei den Telekommunikationsunternehmen „angekommen". Der Anwendungsbereich der Meldepflicht bleibt aber in einer wichtigen Frage unklar. Die in Kooperation mit der Bundesnetzagentur erstellten Leitlinien zur Melde- bzw. Benachrichtigungspflicht habe ich überarbeitet.

Nach anfänglich niedrigen Fallzahlen haben sich die bei der Bundesnetzagentur und mir eingehenden Meldungen über Datenschutzvorfälle bei Telekommunikationsunternehmen nach § 109a Telekommunikationsgesetz (TKG) auf aktuell 113 Fälle im Jahr 2014 jährlich jeweils mehr als verdoppelt. Steigen die Fallzahlen weiterhin kontinuierlich, ist zu befürchten, dass eine zeitnahe Bearbeitung aller Fälle mit den zur Verfügung stehenden Mitarbeitern nicht mehr zu gewährleisten ist.

Schon aus diesem Grund ist es wichtig, ein Verfahren zu entwickeln, mit dem die Schwere von Datenschutzverstößen bestimmt werden kann. Mit dessen Hilfe kann dann bei einer großen Anzahl von Meldungen schnell entschieden werden, welche Fälle vorrangig zu bearbeiten sind. Leider wurde ein insoweit hoffnungsvolles Projekt der Artikel-29-Gruppe bis auf weiteres ausgesetzt, da sich die Gruppe nicht auf ein gemeinsames Verfahren verständigen konnte. Ich habe daher zusammen mit den griechischen Kollegen und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) ein entsprechendes Verfahren außerhalb der Artikel-29-Gruppe weiterentwickelt.

Die von der Bundesnetzagentur und mir erstellten Leitlinien zur Melde- bzw. Benachrichtigungspflicht nach § 109a TKG wurden im Berichtszeitraum überarbeitet (vgl. 24. TB Nr. 3.5.3). Dies wurde notwendig, weil die am 25. August 2013 in Kraft getretene Verordnung (EU) Nr. 611/2013 technische Durchführungsmaßnahmen in Bezug auf Umstände, Form und Verfahren der Meldungen an die Aufsichtsbehörden und Benachrichtigungen der Betroffenen vorgegeben hat. Da die Vorgaben der Europäischen Kommission mit dem in unseren Leitlinien festgelegten Verfahren weitestgehend übereinstimmten, beschränkten sich die Änderungen nur auf einige wenige Punkte. Dies dürfte auch das Ergebnis meiner regelmäßigen Mitarbeit in einer Arbeitsgruppe der Kommission zu diesem Thema sein, in deren Rahmen ich bereits zu einem frühen Zeitpunkt das von der Bundesnetzagentur und mir verfolgte Meldekonzept vorstellen konnte.

Die Europäische Kommission bestätigte mir meine im letzten Tätigkeitsbericht dargelegte Rechtsauffassung (vgl. 24 TB Nr. 3.5.3), dass auch dann eine Datenschutzverletzung vorliegt, wenn die betroffenen Daten durch hinreichende technische Vorkehrungen vor unberechtigtem Zugriff geschützt sind.

Weiterhin unklar bleibt eine Gesetzesformulierung des § 109a TKG. So ist die Meldepflicht aufgrund des eindeutigen Wortlauts gegenwärtig auf die Erbringer von Telekommunikationsdienstleistungen im Sinne des § 3 Nummer 6a) TKG beschränkt. Mitwirkende gemäß § 3 Nummer 6b) TKG sind hingegen nicht zu einer Meldung verpflichtet. Damit wäre ein Diebstahl aller Kundendaten, die ihren Vertrag bei einem Vertriebspartner eines Telekommunikationsunternehmens abgeschlossen haben, nicht meldepflichtig, während der Diebstahl derselben Daten bei dem Telekommunikationsunternehmen selbst unter die Vorschrift des § 109a TKG fallen würde. Ich habe das für das Telekommunikationsgesetz zuständige BMWi mehrfach aufgefordert, diesen offensichtlich unbeabsichtigten Wertungswiderspruch durch eine gesetzliche Klarstellung zu beseitigen - bislang leider ohne Erfolg.

8.8.2 Der Bundesgerichtshof und die IP-Adressen

Im Jahr 2014 hat sich der Bundesgerichtshof (BGH) gleich zweimal mit Fragen des datenschutzkonformen Umgangs mit IP-Adressen befasst: Die Frage der Speicherdauer dynamischer IP-Adressen hat der BGH selbst entschieden, die Frage zur Personenbeziehbarkeit von IP-Adressen legte er erwartungsgemäß dem Europäischen Gerichtshof zur Vorabentscheidung vor.

Dürfen Internetzugangsprovider die IP-Adressen ihrer Kunden auch dann über das Ende der jeweiligen Verbindung hinaus speichern, wenn der Vertrag eine pauschale Abgeltung durch eine Flatrate vorsieht? Diese Frage hat seit über zehn Jahren Gerichte verschiedener Instanzen beschäftigt, nun wurde sie endlich durch den BGH mit „Ja“ beantwortet (Urteil vom 03.07.2014, Az. III ZR 391/13).

Ein Nutzer hatte im Klagewege verlangt, dass sein Internetzugangsanbieter die ihm zugeordnete dynamische IP-Adresse unmittelbar nach Beendigung der Internetverbindung löschen müsse. Der beklagte Telekommunikationsanbieter argumentierte, die IP-Adressen unter anderem zum Erkennen und Beseitigen von Störungen in seiner Infrastruktur zumindest für einen gewissen Zeitraum zu benötigen; eine länger währende Speicherung sei daher nach § 100 Absatz 1 TKG für Zwecke der Störungsbeseitigung gerechtfertigt.

Dieser Argumentation schloss sich der BGH zwar an, stellte aber zugleich fest, eine Speicherung für die vorbenannten Zwecke sei zeitlich zu beschränken. IP-Adressen dürften nur bis zu sieben Tagen nach dem jeweiligen Verbindungsende für Zwecke der Störungsbeseitigung gespeichert werden.

Diese Entscheidung hat mich gefreut, insbesondere weil der BGH mit der 7-Tage-Frist ausdrücklich meiner langjährigen Rechtsauffassung folgt, die sich auch in dem gemeinsam mit der Bundesnetzagentur erstellten Leitfaden zur Verkehrsdatenspeicherung findet (vgl. 24. TB Nr. 6.7).

Schon wenige Monate später - im Oktober 2014 - hatte sich der BGH mit der seit langer Zeit umstrittenen Frage zu befassen, ob IP-Adressen auch dann als personenbezogene Daten dem Datenschutzrecht unterfallen, wenn sie von einem Website-Anbieter gespeichert werden (vgl. 23. TB Nr. 4.3.2).

Anlass der Klage war die Speicherung der IP-Adressen auf den Websites der Bundesrepublik Deutschland. Der Kläger erachtete dies als unzulässig: Über die Speicherung der IP-Adresse und des Zeitpunkts (Datum und Uhrzeit) des Aufrufs sei eine Identifizierung seiner Person möglich, so dass es sich um eine Speicherung von personenbezogenen Daten handele, für die keine Rechtsgrundlage bestehe. Die Bundesrepublik Deutschland, vertreten durch das auch für das Datenschutzrecht zuständige BMI, hält die Protokollierung der Aufrufe ihrer Websites hingegen für zulässig, weil es sich bei IP-Adressen zumindest dann nicht um personenbezogene Daten handele, wenn sie von einem Website-Anbieter erhoben würden. Dieser könne einen Personenbezug selbst nicht herstellen. Ohnehin sei die Speicherung für Datensicherheitszwecke erforderlich und daher selbst bei Annahme eines Personenbezugs zulässig. Die Vorinstanzen hatten die Klage abgewiesen, dem Kläger aber auch in einigen Fragen Recht gegeben.

Der BGH hat am 28. Oktober 2014 (Az. VI ZR 135/13) die Frage der Personenbeziehbarkeit von IP-Adressen wegen ihrer grundsätzlichen Bedeutung erwartungsgemäß dem Europäischen Gerichtshof vorgelegt. Die mit Spannung zu erwartende Entscheidung des EuGH zum Personenbezug - dem Schlüsselbegriff des Datenschutzrechts - wird nicht nur für eine einheitliche Auslegung des (noch) geltenden Rechts, sondern auch für die derzeit in Brüssel diskutierte Reform des europäischen Datenschutzrechts (vgl. oben Nr. 1) von herausragender Bedeutung sein.

8.8.3 Kontrollen im Telekommunikationsbereich - nicht nur gute Erfahrungen

Bei Beratungs- und Kontrollbesuchen festgestellte datenschutzrechtliche Defizite sollten in angemessener Zeit behoben werden. Leider geschieht dies nicht immer. Wenn selbst Beanstandungen nicht weiterhelfen, muss mein Sanktionsinstrumentarium erweitert werden.

Bei ca. 3.500 Telekommunikationsanbietern ist eine flächendeckende Überprüfung aller Unternehmen unmöglich. Wie schon in der Vergangenheit habe ich mich deswegen auf einige Anbieter konzentrieren müssen und dabei vielfach positive Eindrücke gewonnen, auch weil Datenschutz immer mehr als Wettbewerbsvorteil gesehen wird. Neben Licht gibt es aber auch immer Schatten, über den im Folgenden berichtet werden soll.

Er bemühte sich stets

Wirklich viel Geduld benötigte ich gegenüber der E-Plus Service GmbH & Co. KG bei einem Sachverhalt, über den ich bereits in meinem 23. Tätigkeitsbericht (Nr. 6.3) berichtet habe. Mitte 2009 hatte der Anbieter mich über Probleme bei der Löschung von Bestandsdaten informiert. Damals ging er von einem Abschluss des Bereinigungsverfahrens im Jahr 2010 aus. In der Folgezeit kam es trotz eines konstanten Bemühens um eine Bereinigung jedoch immer wieder zu Verzögerungen, weil Informationen, etwa über Vertragswechsel oder offene Forderungen, aus verschiedenen Systemen zusammengetragen werden mussten. Nur so war herauszufinden, ob die Daten eines Kunden überhaupt gelöscht werden können. Die alten Bestandsdaten konnten daher überwiegend erst Ende 2014 gelöscht werden, der endgültige Abschluss wird erst im Jahr 2015 erfolgen.

Bei der Verarbeitung von Verkehrsdaten, bei der ich ebenfalls Mängel festgestellt hatte, dauern die Bemühungen allerdings noch länger. Nach aktueller Planung kann mein zusammen mit der Bundesnetzagentur (BNetzA) entwickelter Leitfaden für eine datenschutzgerechte Speicherung von Verkehrsdaten (vgl. 24. TB Nr. 6.7) erst Ende 2016 umgesetzt werden - wenn sich dies nicht aufgrund einer Firmenfusion noch weiter verzögert. Da ich diesen Zeitraum für unangemessen lange halte, habe ich eine Beanstandung gegen die E-Plus Service GmbH & Co. KG ausgesprochen.

Weitere Beanstandungen

Auch die Vodafone GmbH hat sich mit der Umsetzung des bei im Jahre 2011 durchgeführten Beratungs- und Kontrollbesuchen festgestellten Handlungsbedarfs unangemessen viel Zeit gelassen. So wurden Fristen wiederholt nicht eingehalten und Stellungnahmen zum Teil erst nach mehrfacher Aufforderung abgegeben, die dann wiederum zu wichtigen Punkten gar keine oder keine zufriedenstellenden Antworten enthielten. Dies veranlasste mich zu einer Beanstandung der Vodafone GmbH gegenüber der BNetzA. Neben dem Data Warehouse (vgl. Nr. 8.8.4) habe ich die unverhältnismäßige Speicherung zur Datensicherung und die Speicherung von SMS-Inhalten für wenige Tage im Rahmen der Datenerfassung zur Erkennung von Störungen beanstandet (vgl. auch in meinem 24. TB Nr. 6.8.2). Wie mir die BNetzA mitgeteilt hat, hat sie sich hierzu an alle vier Mobilfunkanbieter gewendet und festgestellt, dass eine „maskierte“ Speicherung der SMS-Inhalte zusammen mit den Signalisierungsdaten branchenüblich sei. Ihren Vorschlag, die Inhalte als gesperrte Daten anzusehen, halte ich für problematisch, zumal bereits für die Datenerhebung keine Rechtsgrundlage besteht. Das Thema muss weiter erörtert werden. Wenn selbst Beanstandungen nicht dazu führen, die festgestellten Mängel engagiert anzugehen, ist die gesetzliche Ausweitung meiner Sanktionsmöglichkeiten (vgl. 24. TB Nr. 6.9) unabdingbar.

Eine weitere Beanstandung habe ich gegenüber Telefónica Germany GmbH & Co. OHG aussprechen müssen, weil ich auch hier kein ausreichendes Bemühen feststellen konnte, aufgetretene Mängel zu beseitigen. Gegenstand der Beanstandungen waren zum einen Mängel bei der Verarbeitung von Verkehrsdaten (Data Warehouse und Dauer der Speicherung von nicht abrechnungsrelevanten Verkehrsdaten) und bei der bereits angesprochenen Speicherung von SMS-Inhalten. Zum anderen richtete sich die Beanstandung auch gegen die Datenverarbeitung im Bereich Bestandsdaten. Bei einer bereits im Juni 2012 durchgeführten Kontrolle hatte ich festgestellt, dass die Einwilligung zur Gesprächsaufzeichnung im Callcenter per Opt-Out ausgestaltet war: Nach einem Anruf beim Callcenter konnte der Anrufer nur einen Widerspruch zur Aufzeichnung äußern. Diese Verfahrensweise ist datenschutzrechtlich nicht zulässig (vgl. auch Nr. 8.8.7). Nachdem meine Aufforderung, Abhilfe zu schaffen, erfolglos blieb, habe ich das Verfahren bei der BNetzA beanstandet.

Weiter musste ich beanstanden, dass die Einwilligung zur Nutzung von Verkehrs- und Bestandsdaten für Werbezwecke bei Vertragsabschluss als Widerspruchslösung konzipiert war, weil die Ankreuzfelder im Vertragsformular bereits vorbelegt waren. Wünscht der Kunde keine Nutzung seiner Daten, müssen die Felder gestrichen werden.

Im Rahmen einer Petenteneingabe wurde ich darauf aufmerksam, dass dem Kunden bei einer Ablehnung des Vertrags die wesentlichen Gründe dafür trotz Nachfrage nicht mitgeteilt wurden. Da diese Vertragsablehnung auf einer internen Scorewert-Bildung basierte, ist die Telefónica Germany nach § 6a Absatz 2 BDSG verpflichtet, dem Antragsteller die wesentlichen Gründe für die Ablehnung mitzuteilen. Da die Telefónica dieser Informationspflicht nicht nachgekommen ist, habe ich auch dieses Verfahren formal beanstanden müssen.

Auf Wanderschaft

Noch bevor die Abhör- und Überwachungsaktivitäten ausländischer Geheimdienste in den Fokus der medialen Öffentlichkeit gerieten (vgl. oben Nr. 2.2), war mir bei Kontrollen der Mobilfunk-Netzbetreiber aufgefallen, dass ein amerikanischer Dienstleister mit der Abrechnung von Roaming-Telefonaten beauftragt worden war. Als der digitale Mobilfunk noch in den Kinderschuhen steckte, gab es nur wenige Netzbetreiber in einer überschaubaren Anzahl von Ländern. Durch den großen Erfolg des Mobilfunks auf allen Kontinenten wurde die Zahl der Netzbetreiber schnell unübersichtlich. Dadurch konnten sich Firmen etablieren, die den Austausch der Daten für viele Netzbetreiber übernehmen und die Vorgänge für diese vereinfachen. Solche Dienstleister erhalten eine große Menge an Verkehrsdaten aus verschiedenen Ländern.

Da die Mobilfunk-Netzbetreiber bei meinen Kontrollbesuchen meine Fragen nicht vollständig beantworten konnten, habe ich unmittelbar bei dem Dienstleister - ursprünglich ein deutsches Unternehmen, das aber keine

Kommunikationsdienste anbietet - einen Informationsbesuch durchgeführt. Dabei erfuhr ich, dass die Dienstleistung als Roaming Data Clearing House in Auftragsdatenverarbeitung für alle deutschen Mobilfunk-Netzbetreiber durchgeführt wird und alle Daten für die europäischen Netzbetreiber in Deutschland verarbeitet werden.

Daraufhin habe ich mit einem der Mobilfunk-Netzbetreiber die vertragliche Gestaltung dieses Datenaustauschs erörtert. Es stellte sich heraus, dass dessen Luxemburger Konzerntochter zentral den Vertrag abgeschlossen hat. In den mir zur Verfügung gestellten Teilen des Vertragswerkes - ein vollständiges Exemplar habe ich noch nicht erhalten - war auch eine Regelung zur Übermittlung von Verkehrsdaten für Abfragen von Sicherheitsbehörden enthalten. Bis zum Ende des Berichtszeitraums konnte ich den Vorgang noch nicht abschließen.

Am Kabel

Ein Kabelnetzbetreiber hat - wie ich im Rahmen von Beratungs- und Kontrollbesuchen feststellen musste - die Bestandsdaten der Kunden nach deren Kündigung nicht wie in § 95 Absatz 3 TKG vorgeschrieben gelöscht, sondern lediglich gesperrt. Hier werde ich beobachten, ob die von mir angemahnten Verbesserungen umgesetzt werden, und ggf. weitere Schritte prüfen. Auch Verkehrsdaten wurden verschiedentlich deutlich zu lange gespeichert.

Bei einem anderen Kabelnetzbetreiber, bei dem ich ebenfalls einen Beratungs- und Kontrollbesuch durchgeführt habe, erfolgt die Speicherung von Verkehrsdaten nur an einigen Stellen der Verarbeitungskette zu lange. Hier konnten bereits erste Fortschritte erzielt werden, auch wenn einige Punkte noch der weiteren Diskussion bedürfen.

Sonstiges

Bereits in meinem 23. Tätigkeitsbericht (Nr. 6.3) hatte ich darüber berichtet, dass ein führender Anbieter Verkehrsdaten zur Abrechnung mit anderen Anbietern für die Dauer von sechs Monaten speichert, ich allerdings nur drei Monate für zulässig halte. Die Notwendigkeit der längeren Speicherdauer wurde insbesondere mit den langen Einwendungsfristen im so genannten Interconnection-Vertrag begründet. Diese Interconnection-Verträge sind Gegenstand eines laufenden Beschlusskammerverfahrens bei der BNetzA, in das ich auch die angesprochene Problematik eingebracht habe.

Nachdem im Jahr 2012 die ersten Telekommunikationsanbieter die Zertifizierung eines De-Mail-Angebotes abgeschlossen und den Dienst der Öffentlichkeit zugänglich gemacht hatten (vgl. Anlage 6 zum 24. TB), habe ich mir in der ersten Jahreshälfte 2013 den Wirkbetrieb bei einem großen De-Mail-Anbieter angesehen. Leider musste ich feststellen, dass zu diesem frühen Zeitpunkt - gerade im Privatkundenbereich - die Anzahl der De-Mail-Nutzer noch zu klein war, um die datenschutzrechtlich besonders relevante Verarbeitung von Verkehrsdaten zu Abrechnungszwecken im Praxisbetrieb verlässlich zu beurteilen. Ungeachtet dessen ergab sich ein überwiegend positives Bild. Hervorzuheben war der unter Einbindung der betrieblichen Datenschutzabteilung bei der Produktentwicklung und -umsetzung des De-Mail-Dienstes von Anfang an konsequent verfolgte Privacy-By-Design-Ansatz. Negativ fiel lediglich auf, dass schriftliche Anträge nach der Digitalisierung erst nach mehreren Wochen vernichtet wurden. Dieser zu lange Zeitraum wurde aber zwischenzeitlich erheblich verkürzt.

8.8.4 Große Sammlungen

Big Data und Data Warehouse mit sensiblen Telekommunikationsdaten sind nur unter sehr engen Voraussetzungen zulässig.

Bereits in der Vergangenheit (24. TB Nr. 6.8.2) hatte ich über die Nutzung von Data Warehouse (DWH) bei Telekommunikationsunternehmen berichtet und angekündigt, mich mit diesem Thema näher zu befassen.

In solche DWH von Telekommunikationsunternehmen fließen häufig Standortdaten aus den digitalen Mobilfunknetzen ein, die Aufschluss über den geografischen Standort des Endgeräts des mobilen Nutzers geben, um die Nachrichtenübertragung zu ermöglichen. Solche Daten sind Verkehrsdaten, die entsprechend den dafür geltenden Vorschriften erhoben und verarbeitet werden können, und, wenn sie nicht mehr erforderlich sind, gelöscht werden müssen.

Ein DWH, das mit allen verfügbaren Daten - einschließlich Verkehrsdaten - gefüllt wird, um daraus etwa einen Bericht an den Vorstand oder Statistiken für das Marketing zu erarbeiten, kann mit personenbezogenen Klardaten kaum rechtskonform betrieben werden. Die Unternehmen tun sich oft schwer, ihre DWHs den rechtlichen Vorgaben anzupassen, was auch zu Beanstandungen führte (vgl. Nr. 8.8.3).

Zwar werden - so meine Beobachtung - auch Zwecke verfolgt, für die das TKG eine Nutzung von Verkehrsdaten erlaubt, dies betrifft aber oft nur einen Teil der Daten oder eine begrenzte Speicherdauer. Ein Beispiel hierfür wäre etwa die spezielle Abrechnung für eine Kundengruppe, die nicht mit dem regulären Abrechnungssystem umzusetzen ist.

Eine mögliche Herangehensweise für ein datenschutzkonformes DWH besteht darin, die nach TKG zulässigen Nutzungen zu identifizieren und die Datenspeicherung daran zu orientieren. Weitere Nutzungen, etwa für den tagesaktuellen Bericht für den Vorstand, sind dann möglich, wenn die zulässiger Weise ermittelten Daten anonymisiert werden. Hierzu wurden mir bereits Konzepte vorgelegt.

Da nahezu alle größeren Telekommunikationsunternehmen mit dieser Thematik konfrontiert sind, habe ich mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) nach intensiver Diskussion die nachstehenden Eckpunkte (vgl. Kasten zu Nr. 8.8.4) erarbeitet.

Eine vergleichbare Problematik besteht bei Big Data (vgl. auch Nr. 2.2). Hier wurden mir Projekte vorgestellt, die Standortdaten der Mobilfunkteilnehmer für verschiedene Zwecke nutzbar machen sollen, etwa für Verkehrsplanungen. Dies geht über die Nutzung, die ich bereits in meinem 22. Tätigkeitsbericht unter Nummer 7.8 vorgestellt habe, hinaus. Dabei werden die Bewegungsdaten über 24 Stunden zu einem Teilnehmer zusammenhängend gespeichert. Ein kryptografisches Einwegverfahren soll die Zuordnung der Standortdaten zu einem Teilnehmer verhindern. Dies stellt jedoch noch keine ausreichende Anonymisierung dar. Bei manchen Personen kann bereits die Kombination Funkzelle/Wohnung und Funkzelle/Arbeitsplatz so charakteristisch sein, dass eine relativ sichere Identifizierung möglich ist; beispielsweise kann festgestellt werden, in welcher Gegend sich diese Person abends aufgehalten hat. Erst nach einer Aggregierung, also einer Zusammenfassung von vielen Ergebnissen, kann dies als ausreichend anonymisiert gelten. Die Beurteilung der Verfahren dauerte bei Redaktionsschluss noch an.

Kasten zu Nr. 8.8.4

Zusammenfassung der mit BITKOM erarbeiteten Eckpunkte

Bei solchen Verfahren kommt es entscheidend darauf an, dass personenbezogene Daten, die in einem DWH zusammengetragen und für statistische Auswertungen genutzt werden sollen, umgehend anonymisiert werden. Daten gelten gemäß § 3 Absatz 6 BDSG als anonymisiert, wenn die Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer Person zugeordnet werden können (vgl. auch Nr. 2.2.3, Kasten zu Nr. 2.2.3). Die Anforderungen an eine Anonymisierung im Sinne des Gesetzes sind also erfüllt, wenn die Wiederherstellung des Personenbezugs soweit erschwert ist, dass sie nur

mit unverhältnismäßig großem Aufwand durchgeführt werden könnte. Die Rückgängigmachung der Anonymisierung muss dabei für jedermann unmöglich oder unverhältnismäßig sein. Eine Anonymisierung liegt daher nicht vor, wenn die Person zwar namentlich unbekannt, aber eine Individualisierung möglich ist (Rückschlüsse aus dem Datenpool auf eine konkrete Person). Solange Daten in einem Data Warehouse noch einem Kunden zugeordnet werden können, kann es sich allenfalls um eine Pseudonymisierung handeln. Pseudonyme Daten unterliegen in vollem Umfang den Regelungen des Datenschutzes, da sie als personenbeziehbare Daten im Sinne von § 3 Abs. 1 BDSG gelten.

Zwar ist eine statistische Auswertung personenbezogener Daten, insb. aus verschiedenen Datenbanken, technisch nur durch ein kurzzeitiges Zwischenspeichern möglich. Eine Zwischenspeicherung personenbezogener Daten zum Zweck der Anonymisierung darf aber erst unmittelbar vor der Anonymisierung erfolgen, die ihrerseits unverzüglich durchzuführen ist; keinesfalls dürfen personenbezogene Daten „auf Vorrat" über längere Zeit in einem Zwischenspeicher liegen und ggf. sukzessiv ergänzt werden, um diese bei Bedarf später zu anonymisieren und statistisch auszuwerten. Es ist zudem durch technische und organisatorische Maßnahmen sicherzustellen, dass die Daten im Stadium der Zwischenspeicherung nicht ausgewertet werden können. Selbstverständlich müssen diese zwischengespeicherten personenbezogenen Daten nach erfolgter Anonymisierung unverzüglich gelöscht werden.

8.8.5 Tiefe Blicke

Manche Netzbetreiber wagen einen genaueren Blick auf die Internetpakete. Dafür gibt es viele Gründe.

Für die klassische leitungsbasierte Telefonie gibt es recht klare Regelungen im TKG, die zwischen Verkehrsdaten und Kommunikationsinhalten unterscheiden. Die Kommunikation über das Internetprotokoll gewinnt jedoch zunehmend an Bedeutung und dürfte die leitungsbasierte Kommunikation in vielen Bereichen bald verdrängen, so dass eine praxisgerechte Anwendung des TKG in diesem Bereich ohne Kompromisse oft nicht möglich ist. Über diese Problematik bei der Deep Packet Inspection hatte ich bereits in meinem 23. Tätigkeitsbericht (Nr. 6.5) berichtet.

Bei dieser Thematik bewegt man sich in einem Zwiespalt: Einerseits sind die hier aufgezeigten Verfahren wichtig für die effektive Erbringung der Dienste, andererseits handelt es sich um eine Infrastruktur, die eine tiefgehende Überwachung der Internetnutzung ermöglicht oder diese sogar aufzeichnet. Die Diskussionen zur Verhältnismäßigkeit derartiger Verfahren sind daher noch lange nicht beendet.

Bei zwei Mobilfunkanbietern habe ich im Berichtszeitraum Beratungs- und Kontrollbesuche durchgeführt, um die Auswertung der mobilen Internetnutzung zu untersuchen. Dabei wurde mir erläutert, aufgrund der komplexen Infrastruktur für den mobilen Internetzugang sei eine Fehlersuche nur durch einen Blick auf die Datenpakete an verschiedenen Stellen der Infrastruktur möglich. In der Umsetzung dieser „tiefen Einblicke" habe ich allerdings erhebliche Unterschiede festgestellt:

Bei einem Anbieter werden alle Pakete verkürzt für einige Tage gespeichert. Die spannenden Fragen lauten, ob diese Kürzung ausreicht, um die Kommunikationsinhalte außen vor zu lassen, und - etwas grundlegender - wo die Verkehrsdaten enden und die Kommunikationsinhalte beginnen. So ist etwa der TCP-Header für die reine Übertragung von IP-Paketen nicht erforderlich, zur Analyse von Störungen jedoch sehr nützlich, da er Informationen zur Steuerung der Datenübertragung enthält. Auch http-Fehlermeldungen haben für diese Zwecke eine hohe Aussagekraft.

Bei dem anderen Anbieter musste ich feststellen, dass für viele Internetprotokolle auf eine Kürzung der Pakete verzichtet wurde, also die gesamte Kommunikation gespeichert wird. Wie ich dem Anbieter mitgeteilt habe,

sehe ich darin einen beanstandungswürdigen Sachverhalt und fordere unverzügliche Abhilfe. Eine Verbesserung wurde mir für das erste Quartal 2015 zugesagt.

Ein Mobilfunkanbieter betreibt ein System zur Verhinderung vertragswidriger Nutzungen von Diensten über das Mobiltelefon der Kunden, etwa Internettelefonie. Auch dies geht nicht ohne Prüfung der Kommunikationsinhalte. Was genau automatisiert analysiert wird, ist jedoch Geschäftsgeheimnis des Herstellers. Ob eine Blockade „unerwünschter" Dienste zulässig ist, ergibt sich nicht zweifelsfrei aus dem TKG. Parallelen zu der aktuellen politischen Debatte zur Netzneutralität sind allerdings unverkennbar. Der Gesetzgeber sollte sich bewusst sein, dass eine Steuerung des Netzverkehrs ein Hineinschauen und Bewerten der Inhalte erfordert.

§ 100 Absatz 2 TKG regelt die Störungserkennung bei IP-Kommunikation. Früher konnte ein Post-Techniker ein Aufschalten auf eine analoge Leitung mit einem akustischen Signal anzeigen. Dies funktioniert bei Voice over IP (VoIP) nicht mehr. In der aktuellen Fassung des § 100 Absatz 2 TKG wird in besonderen Fällen eine Aufzeichnung der Kommunikation erlaubt, aufgrund der besonderen Sensibilität ist allerdings eine Information des betrieblichen Datenschutzbeauftragten erforderlich. Dies schien sich jedoch nicht bis zu den verantwortlichen Technikern herumgesprochen zu haben. Ich erwarte, dass die Vorgaben bei den kontrollierten Unternehmen zukünftig korrekt umgesetzt werden und werde auch die Datenschutzbeauftragten weiterer Unternehmen hierfür sensibilisieren.

Auch für Zwecke des Marketings besteht ein hohes Interesse an der Auswertung des Nutzerverhaltens. Ein Mobilfunkanbieter analysiert in einem Projekt die Internetnutzung eines kleinen Teils der Kunden, die in dieses Verfahren eingewilligt haben. Die erfassten Daten der nicht teilnehmenden Kunden werden unverzüglich - nach Angaben des Unternehmens durchschnittlich nach 7,5 Minuten - verworfen. Dies ist eine grundlegende Voraussetzung für die Wahrung der Datenschutzinteressen der nicht teilnehmenden Kunden.

8.8.6 Wie kommt es auf die Rechnung?

Damit Telefonate unter Nutzung anderer Anbieter über die Telefonrechnung abgerechnet werden können, ist ein komplexer Datenaustausch notwendig. Umstritten ist, ob hier zu viele Daten fließen.

Viele Menschen haben sicherlich noch nie darüber nachgedacht, wie die Kosten für einen Anruf bei einem so genannten Mehrwertdienst über eine 0900er Rufnummer - z. B. bei einer Fluggesellschaft - auf ihre Telefonrechnung gelangen. Eigentlich müsste der Anrufer die Fluggesellschaft bezahlen, da diese die Beratungsleistung erbracht hat. Tatsächlich steht der Zahlungsanspruch aber dem Verbindungsnetzbetreiber (VNB) zu, der die 0900er Rufnummer geschaltet hat und seinerseits wiederum mit der Fluggesellschaft abrechnet. Der VNB kennt jedoch den anrufenden Teilnehmer nicht, da dieser in der Regel nur mit seinem Teilnehmernetzbetreiber (TNB) in einem vertraglichen Verhältnis steht. Deshalb wurde ein System für einen Datenaustausch zu Zwecken der Abrechnung geschaffen, das bei der Deutschen Telekom AG (DTAG), dem größten deutschen TNB, betrieben wird.

Zunächst übermittelt der VNB die Verkehrsdaten des Anrufs an die DTAG. Wenn der Anrufer Kunde der DTAG ist, wird die Verbindung bei der nächsten Rechnung aufgeführt. Gleichzeitig mit dem Rechnungsversand werden dem VNB die Verkehrsdaten zusammen mit den Bestandsdaten, u. a. dem Namen und der Adresse des Kunden, der Rechnungsnummer, dem Rechnungsdatum und der Kundennummer zurückgeschickt. Der DTAG-Kunde findet die Verbindung zusammen mit den Kontaktdaten des VNB auf seiner Rechnung, so dass er sich bei Rückfragen an den VNB wenden kann. Zahlt der Kunde nicht, sendet die DTAG eine Information zur Rückbelastung an den VNB, der für Inkassozwecke auch das Geburtsdatum des Teilnehmers enthält. Mit der bereits übermittelten Adresse kann der VNB das Inkassoverfahren betreiben.

Darin erschöpft sich das Verfahren aber nicht. So müssen beispielsweise vorab Stammdaten zur Aufführung in der Rechnung weitergegeben werden. Auch kann eine Nachzahlung des Kunden an den VNB übermittelt werden. Auch bedürfen Fälle einer Lösung, in denen der Anrufer Kunde eines anderen TNB ist. Dann übernimmt die DTAG eine Mittlerfunktion zwischen VNB und TNB. Und schließlich dient das Verfahren auch für die Abrechnung ähnlich abzurechnender Mehrwertdienste und für Call-by-Call.

Um das Verfahren für die VNB zu vereinfachen, organisieren Dienstleister die Abrechnung mit der DTAG, Zahlungserinnerungen und Inkassoverfahren als Auftragsdatenverarbeitung. Der VNB kann sich hierdurch auf die Erbringung der Telekommunikation konzentrieren und seinen Aufwand für Abrechnungen mit Anrufern minimieren.

Bei einem solchen Dienstleister habe ich einen Beratungs- und Kontrollbesuch durchgeführt. Als problematisch erwies sich dabei neben Fragen der organisatorischen Umsetzung der Auftragsdatenverarbeitung, etwa der Trennung der Daten von verschiedenen Auftraggebern, eine überraschend umfangreiche Datenbank der Rechnungs- und Adressdaten. Da bei jedem Anruf bei einem Mehrwertdienstleister oder über Call-by-Call die Adresse übermittelt wird, entstehen umfangreiche Datenbestände, die gesperrt für zehn Jahre vorgehalten werden. Tatsächlich benötigt wird jedoch nur ein kleiner Teil davon - für den Fall einer Zahlungsstörung. Hierzu würde es aber ausreichen, wenn die Adresse erst bei der Rückbelastung übermittelt wird. Für Rückfragen der Kunden würde eine Authentifizierung mit Rechnungsnummer, Rechnungsdatum und Kundennummer genügen.

Ich habe daher Zweifel, ob eine anlasslose Bestandsdatenübermittlung in dieser umfassenden Form überhaupt rechtlich zulässig ist. § 21 Absatz 2 Satz 1 Ziffer 7c TKG sieht als marktregulierende Vorschrift zwar eine Verpflichtung zur Übermittlung der Bestandsdaten auch zur Reklamationsbearbeitung vor, lässt aber offen, ob eine Übermittlung auch bereits im Vorfeld einer Reklamation erfolgen kann. Dagegen spricht die datenschutzrechtliche Vorschrift des § 97 Absatz 5 TKG, der eine Datenübermittlung nur dann zulässt, wenn sie im Einzelfall zur Durchsetzung einer Forderung erforderlich ist. Da Reklamationen der Abrechnung wohl eher selten vorkommen, sollte die bestehende Praxis geändert und die Bestandsdaten des Teilnehmers erst bei einer Zahlungsstörung übermittelt werden. Dies habe ich bereits mit den Telekommunikationsanbietern erörtert, die allerdings an dem bisherigen Verfahren festhalten wollen. Die Diskussion mit den Anbietern ist noch nicht abgeschlossen. Hier werden weitere Überzeugungsarbeiten nötig sein.

Angesichts der Komplexität des Verfahrens und der Anzahl der involvierten Unternehmen dürften Änderungen bei der Bestandsdatenübermittlung kurzfristig nicht zu erwarten sein.

8.8.7 Gesprächsaufzeichnungen in Callcentern

Aufzeichnungen von Telefongesprächen sind nur mit der Einwilligung der Kunden zulässig.

„Aus Gründen der Qualitätssicherung zeichnen wir vereinzelt Gespräche auf …“. Das hören viele Kunden, die sich telefonisch mit ihren Anliegen an Telekommunikations- und Postdienstleister wenden. Dabei betreiben viele Unternehmen eigene Service-Rufnummern, während sich andere Drittanbieter (Callcenter) bedienen. Die Unternehmen begründen die Aufzeichnungen überwiegend mit der Optimierung der Service-Qualität und der Kundenzufriedenheit, aber auch mit Beweis- und Dokumentationszwecken.

Das Aufzeichnen von Telefonaten ist allerdings nur zulässig, wenn hierfür ein Rechtfertigungsgrund vorliegt. Wer eine Tonaufzeichnung unbefugt fertigt, verletzt die Vertraulichkeit des Wortes und begeht damit eine Straftat (§ 201 StGB). Die Unternehmen dürfen deshalb eine Gesprächsaufzeichnung nur mit der Einwilligung des Betroffenen vornehmen. Diese Einwilligung muss ausdrücklich vor der Aufzeichnung - z. B. durch Bestätigung auf der Tastatur oder durch Sprachsteuerung - eingeholt werden. Es reicht nicht aus, dem Betroffenen lediglich

die Möglichkeit einzuräumen, einer Aufzeichnung zu widersprechen, und für den Fall, dass kein Widerspruch erfolgt, dies als Einwilligung zu interpretieren.

Bereits in meinem letzten Tätigkeitsbericht (Nr. 6.10) habe ich auf diese Problematik aufmerksam gemacht. In diesem Berichtszeitraum habe ich stichprobenartig die Verfahrensweise zur Einholung der Einwilligung bei verschiedenen Telekommunikationsdiensteanbieter und Postdienstleister kontrolliert, um mir einen Überblick über die Verfahrensweisen zu verschaffen. Das Ergebnis war durchwachsen, denn neben datenschutzrechtlich vorbildlichen Lösungen bin ich auf bedenkliche Varianten gestoßen. Ich habe die betreffenden Betreiber aufgefordert, die Verfahren umgehend datenschutzkonform auszugestalten.

Seit Jahren strebe ich eine einheitliche Vorgehensweise bei den Gesprächsaufzeichnungen an. Obwohl schon Verbesserungen erkennbar sind, erfüllen noch immer nicht alle Dienstleister die datenschutzrechtlichen Anforderungen. Ein Grund mag sein, dass eine bereichsspezifische Regelung in den für die Telekommunikationsdiensteanbietern und Postdienstleistern geltenden Spezialgesetzen fehlt und oft übersehen wird, dass hier § 4a BDSG zur Anwendung kommt. Sollte es auch im nächsten Berichtszeitraum nicht gelingen, flächendeckend einen rechtskonformen Zustand herzustellen, empfehle ich eine eindeutige gesetzliche Regelung der datenschutzrechtlichen Anforderungen bei Gesprächsaufzeichnungen mit Kunden.

8.8.8 Übersendung von personenbezogenen Daten per unverschlüsselter E-Mail

Der Versand von sensiblen Informationen per unverschlüsselter E-Mail ist nicht zulässig. Leider musste ich im Zuge der SEPA-Umstellung viele Verstöße gegen diese Vorgabe feststellen.

Infolge der Umstellung der nationalen Kontonummern und Bankleitzahlen durch das so genannte SEPA-Verfahren (Single Euro Payments Area, Einheitlicher Euro-Zahlungsverkehrsraum) haben sich viele Bürger an mich gewandt, weil sie von ihrem Telekommunikationsanbieter per unverschlüsselter E-Mail ihre vollständige Bankverbindung erhalten haben. Darin lag ein Verstoß gegen die Anlage zu § 9 Satz 1 BDSG, nach der die Unternehmen zu gewährleisten haben, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen oder kopiert werden können. Die Bankverbindung hätte daher entweder nicht per unverschlüsselter E-Mail oder zumindest in verkürzter Form übermittelt werden müssen. Ich habe die betroffenen Unternehmen auf diesen Verstoß hingewiesen, woraufhin - soweit dies technisch noch möglich war - die Prozesse sofort gestoppt bzw. umgestellt wurden. Wenngleich in diesem Fall keine Wiederholungsgefahr bestand, müssen die Unternehmen zukünftig in ähnlich gelagerten Situationen ihre Prozesse im Vorfeld sorgfältiger prüfen.

Noch in einem weiteren Fall bin ich auf den Versand personenbezogener Kundendaten durch unverschlüsselte E-Mail gestoßen. Ein großer Telekommunikationsanbieter hatte seinen Kunden nach Vertragsschluss in einem „Willkommensbrief“ Name, Anschrift, Kundenkennwort und Bankverbindung in einer unverschlüsselten E-Mail bestätigt. Auch dies war unzulässig und auch nicht durch wirtschaftliche Überlegungen des Unternehmens (Portoeinsparung) zu rechtfertigen. Ich habe mir die Prozesse zum Willkommensbrief von dem Anbieter darstellen lassen und die datenschutzrechtlichen Aspekte verdeutlicht. Bereits während des Gesprächs wurde mir zugesagt, den Willkommensbrief künftig per Post zu versenden. Ein Versand per unverschlüsselter E-Mail erfolgt nur noch, wenn der Kunde vorab über die Risiken umfassend informiert wird und diesem Verfahren ausdrücklich zustimmt.

8.8.9 Binding Corporate Rules - eine sinnvolle Alternative

Konzerndatenschutzrichtlinien ermöglichen die Übermittlung personenbezogener Daten aus der Europäischen Union in Drittstaaten. Erarbeitung und Umsetzung nehmen viel Zeit in Anspruch - die sich aber lohnt.

Die Vorgaben für diese so genannten Binding Corporate Rules (BCR) wurden von der Artikel-29-Datenschutzgruppe entwickelt. Sie garantieren einen datenschutzrechtlichen Standard, der eine konzernweite Datenübermittlung zwischen den Unternehmensteilen unabhängig von dem Datenschutzniveau im Empfängerland ermöglicht. Die konkrete Umsetzung und Gestaltung der BCR wird von der zuständigen Datenschutzaufsichtsbehörde begleitet und kontrolliert. Die Einführung von unternehmensweiten Datenschutzregelungen ist eine sinnvolle Maßnahme, um ein angemessenes Datenschutzniveau bei internationalen Datentransfers sicherzustellen und zu verbessern. Deswegen haben Unternehmen meine Unterstützung, wenn sie sich dazu entschließen, den Genehmigungsprozess zu durchlaufen - insbesondere wenn ihr Kerngeschäft darauf beruht, täglich in hohem Maße personenbezogene Daten zu verarbeiten (vgl. Nr. 4.7.2).

Konzerndatenschutzrichtlinie der Deutschen Post DHL - eine fast unendliche Geschichte

Bereits in meinem 24. Tätigkeitsbericht (Nr. 6.12.1) habe ich über den Abschluss des Genehmigungsverfahrens der verbindlichen unternehmensweiten Datenschutzregelung der Deutschen Post DHL (DP-DHL) im Februar 2011 berichtet. Leider konnte die weltweite Umsetzung dieser Datenschutzrichtlinie noch nicht abgeschlossen werden, obwohl dies im Laufe des Jahre 2013 vorgesehen war. Offenbar gelingt es dem Unternehmen nur unzureichend, die weltweite Vernetzung „datenschutzrechtlich unter einen Hut zu bringen“. Die Gründe hierfür sind vielfältig, aber wenn nach Aussagen der DP-DHL selbst in Europa bislang nur eine Beitrittsquote von 95 Prozent erreicht worden ist, verwundert es nicht, dass sie auch in der Region „Asia Pacific“ nicht höher ist und in Nord- und Südamerika sogar nur bei 33 Prozent liegt. Ich werde das Unternehmen darin bestärken, eine höhere Beitrittsrate bei den zahlreichen Tochter- und Unternehmensgesellschaften zu erreichen und die weitere Umsetzung im Auge behalten.

Binding Corporate Rules der Deutschen Telekom AG

Nach der Deutschen Post DHL hat mit der Deutschen Telekom AG im Jahr 2014 ein weiterer, meiner Aufsicht unterstehender und international agierender Konzern das BCR-Genehmigungsverfahren zu einer unternehmensweit geltenden Konzerndatenschutzrichtlinie erfolgreich abgeschlossen.

Bereits vor über zehn Jahren hatte die Telekom einen konzerninternen Datenschutzkodex entwickelt, der als Grundlage für das bereits im Jahr 2008 initiierte, dann aber immer wieder aus betriebsinternen Gründen verzögerte Genehmigungsverfahren dienen sollte. Im so genannten Verfahren der gegenseitigen Anerkennung konnten die von der Artikel-29-Gruppe festgelegten Vorgaben für das Genehmigungsverfahren unter meiner Federführung und mit der Unterstützung der Datenschutzaufsichtsbehörden aus Österreich und Polen (vgl. oben Nr. 3.1.3) innerhalb eines Jahres umgesetzt und mit Übergabe des Genehmigungsschreibens an den Vorstand der Telekom im Mai 2014 formell abgeschlossen werden. Nunmehr ist es Aufgabe dieses Unternehmens, die Binding Corporate Rules möglichst schnell in den einzelnen Konzernunternehmen zu implementieren. Auch wenn das Unternehmen hierbei nach meinem Eindruck auf einem guten Kurs zu sein scheint, werde ich den Prozess weiterhin beobachten.

8.9 Internet

Auch wenn die Datenschutzkontrolle bei Internet-, Tele- und Mediendienstanbietern im privatwirtschaftlichen und privaten Bereich den Aufsichtsbehörden der Bundesländer obliegt, bin ich sowohl national als auch in internationalen Gremien mit vielfältigen Fragestellungen konfrontiert. Im Rahmen meiner Zuständigkeit für Bundesbehörden kontrolliere ich z. B. deren Internetangebote und setze dabei seit Jahren das Datenschutz-Tool Prividor (Privacy Violation Detector) ein, das in meinem Auftrag entwickelt wurde (vgl. 24. TB Nr. 15.7). Prividor vermag automatisiert datenschutzbedenkliche Vorgänge auf Internetseiten zu erkennen und wurde im Berichtszeitraum weiterentwickelt. So kann das heimliche Ausspähen des Surfverhaltens z. B. durch Cookies, DOM Storage, JavaScript etc. ausfindig gemacht werden.

8.9.1 Cookie-Paragraph

In die Umsetzung des sog. Cookie-Paragraphen in deutsches Recht scheint Bewegung zu kommen.

Auch nach zwei Jahren und weiteren Schreiben an das zuständige BMWi (vgl. 24. TB Nr. 5.4) gibt es noch immer keinen Fortschritt bei der nationalen Umsetzung des Artikels 5 Absatz 3 der E-Privacy-Richtlinie, des sog. Cookie-Paragraphen.

Erfolgreich war allerdings das Einbinden der zuständigen Generaldirektion Digitale Wirtschaft und Gesellschaft der Europäischen Kommission in dieser Frage. Kurz vor Redaktionsschluss wurde bekannt, dass die Generaldirektion das BMWi um Stellungnahme gebeten hat, wie die Verpflichtung zur Einwilligung des Nutzers vor Setzen eines Cookies durch deutsches Recht umgesetzt ist und wie die Vorschrift durch die Aufsichtsbehörden in der Praxis angewendet wird. Die Antwort wird Mitte Februar erwartet.

Ich empfehle dem Gesetzgeber, die Einwilligungslösung vor Setzen eines Cookies durch eine normenklare Regelung im Telemediengesetz umzusetzen.

Wegen der teils unterschiedlichen Auslegung der Regelung hat die Artikel-29-Gruppe im Oktober 2013 ein Papier mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies (WP 208 vom 02.10.2013) und im November 2014 ein ergänzendes Papier zur Anwendbarkeit des Artikels 5 Absatz 3 bei Device Fingerprinting veröffentlicht (WP 224 vom 25.11.2014 - vgl. Kasten zu Nr. 8.9.1, Nr. 3.1.4). Beide Papiere lassen keinen Zweifel daran, dass für das Setzen von Cookies und die Berechnung eines „Fingerabdrucks“ die Einwilligung des Nutzers erforderlich ist. Sie sind auf meiner Website unter www.datenschutz.bund.de verfügbar.

Seitens der EU-Kommission wurde Ende 2014 eine Überprüfung der E-Privacy-Richtlinie angekündigt, die sich insbesondere mit der Regelung in Artikel 5 Absatz 3 befassen wird. Hierbei wird die Kommission die Arbeitsergebnisse der Artikel-29-Gruppe einbeziehen.

Kasten zu Nr. 8.9.1

Beim **device fingerprinting** werden verschiedene nicht-eindeutige Merkmale eines Browsers und/oder PC (z. B. Browser-Version, Bildschirmgröße, Liste der Plugins, Liste der installierten Schriftarten) durch bestimmte technische Verfahren zusammengefügt, so dass sie ein eindeutiges Merkmal für einen bestimmten PC ergeben. Anhand eines solchen „Fingerabdrucks“ lassen sich dann die Aktionen des jeweiligen Nutzers verfolgen.

8.9.2 Noch kein Ende: Kampf mit Giganten

Die Prüfungen der „Google Privacy Policy“ und des „Microsoft Service Agreement“ sind zwar abgeschlossen, doch bei der Umsetzung der von der Artikel-29-Gruppe empfohlenen Maßnahmen müssen beide Unternehmen nacharbeiten.

Im Anschluss an die Prüfung durch die französische Datenschutzbehörde CNIL, die diese im Auftrag der Artikel-29-Gruppe nach europäischem Recht durchgeführt und im Oktober 2012 mit einem Prüfbericht abgeschlossen hatte (vgl. 24. TB Nr. 5.9), haben sechs Datenschutzbehörden aus Frankreich, dem Vereinigten Königreich, Italien, Spanien, den Niederlanden und Deutschland eine Prüfung der „Google Privacy Policy“ nach ihren nationalen Gesetzen durchgeführt. Aufgrund der föderalen Zuständigkeitsverteilung wurde Deutschland durch den Hamburgischen Datenschutzbeauftragten vertreten.

Auf der Basis der Ergebnisse hat die Artikel-29-Gruppe im September 2014 einen Maßnahmen-Katalog an Google übersandt, mit dem die Einhaltung der gesetzlichen Vorschriften sichergestellt werden kann. Diese Empfehlungen betreffen drei Bereiche:

- Die Information der Nutzer muss umfassend und in eindeutiger Sprache verfasst sein sowie alle verarbeiteten Daten und Verarbeitungszwecke benennen. Vorzugsweise sollten die Informationen in einer mehrstufigen Struktur präsentiert werden.

- Die Kontrolle durch die Nutzer muss durch die leichtere Auffindbarkeit des vorhandenen Dashboards verbessert werden, auf dem die Nutzer die Datenschutzeinstellungen nach ihren Vorstellungen vornehmen können. Die Voreinstellungen sollen datenschutzfreundlich sein. Vor allem darf die Verknüpfung der personenbezogenen Daten aus verschiedenen Google-Diensten nur mit informierter Einwilligung des betroffenen Nutzers erfolgen. Denn im Anschluss werden die ausgewerteten Daten für Werbezwecke genutzt. Davon betroffen sind auch Daten von Nutzern, die keinen Google-Account haben und lediglich die Suchmaschine nutzen oder Websites von Dritten mit Google-Cookies besuchen.

- Zuletzt wird Google aufgefordert, Richtlinien für die Speicherung der Nutzer-Daten zu definieren und den europäischen Datenschutzbehörden zu übermitteln.

Eine Stellungnahme von Google stand bei Redaktionsschluss noch aus.

Die Artikel-29-Gruppe hat die Aktualisierung des Microsoft Service Agreement einschließlich der Datenschutzgrundsätze zum Anlass genommen, die Datenschutzbehörden von Luxemburg und Frankreich mit der Prüfung der neuen Privacy Policy zu beauftragen. Von der Aktualisierung sind sämtliche Dienste von Microsoft betroffen, etwa Hotmail, Microsoft-Konto, Windows Live Messenger, Windows-Fotogalerie, Bing, MSN und Office.

Einige der anhand eines Fragenkatalogs erarbeiteten Empfehlungen hat Microsoft bereits umgesetzt, andere - wie die Verbesserung der Information der Nutzer über den gesamten Verarbeitungsprozess ihrer Daten und die transparentere Gestaltung der Datenschutzeinstellungen - stehen noch aus. Microsoft hat angekündigt, eine nutzerfreundliche Datenschutzstruktur in Form eines Dashboards zu installieren, damit Nutzer problemlos auf ihre Daten zugreifen und Einstellungen vornehmen können. Auch hier werde ich den weiteren Fortgang beobachten.

In beiden Verfahren fand eine konstruktive und enge Kooperation unter den europäischen Datenschutzbehörden statt, die hoffentlich zeitnah zu einem erfolgreichen Abschluss der Verhandlungen mit Google und Microsoft führen wird.

8.9.3 Der datenschutzkonforme Betrieb von Websites bei Bundesbehörden ist nicht selbstverständlich

Wie ich bei Kontrollen von Bundesbehörden-Websites feststellen musste, werden grundlegende Datenschutzvorgaben nicht immer eingehalten oder korrekt umgesetzt.

Gemäß § 13 Absatz 1 Telemediengesetz (TMG) muss die Datenschutzerklärung so gestaltet sein, dass ihr Inhalt für den Nutzer jederzeit und von jeder Stelle des Internetangebotes aus direkt abrufbar ist. Diesen Vorgaben wird z. B. dann Genüge getan, wenn sich der Menüpunkt „Datenschutz“ auf der obersten Ebene der Meta-Navigation befindet. Dies war bei einigen Internetangeboten von Bundesbehörden nicht gegeben. Vielmehr wurde - selbst bei neu gestalteten Websites - die Datenschutzerklärung inhaltlich als Teil des Impressums ausgeführt, ohne dass ein direkter Zugriff über die Meta-Navigation möglich war. Ich habe die Bundesbehörden gebeten, ihre Internetangebote zu prüfen und gegebenenfalls anzupassen. Dennoch ist mir bei einer späteren Kontrolle

sogar eine Behördenseite aufgefallen, die überhaupt keine Datenschutzerklärung enthielt. Ich habe diese Behörde aufgefordert, kurzfristig Abhilfe zu schaffen und werde andernfalls eine formale Beanstandung erwägen.

Nachdem ich bereits im 24. Tätigkeitsbericht (Nr. 5.8.3) ausgeführt hatte, die direkte Einbindung von Social Plugins sei datenschutzrechtlich nicht zu vertreten, machte mich eine Eingabe auf eine Website aufmerksam, auf der ein Google-Captcha (reCAPTCHA) verwendet wurde. Obwohl es nachvollziehbare Gründe gibt, die für den Einsatz von Captcha-Lösungen sprechen, etwa um eine missbräuchliche Nutzung von Kontaktformularen durch automatisiertes Ausfüllen zu verhindern, halte ich deren Einsatz für unzulässig. Durch das direkte Einbinden wird nämlich die IP-Adresse an Google übertragen, was ohne ausdrückliche Einwilligung des Betroffenen nicht zulässig ist. Meiner Aufforderung, die Captchas aus den Webangeboten zu entfernen, ist die Betreiberin der Website umgehend nachgekommen.

Die fortlaufende Kontrolle der Internetangebote der Bundesbehörden hat sich als sinnvoll und notwendig erwiesen, um die Einhaltung des Datenschutzes zu gewährleisten.

8.9.4 Bundesbehörden-Apps: Kleine Helfer für das Smartphone

Der mobile Zugriff auf Informationen aus dem Internet mittels Smartphones hat sich längst durchgesetzt. Nützlich sind hierbei mobile Applikationen („Apps"), die auch zunehmend von Bundesbehörden angeboten werden. Doch wie steht es mit der Einhaltung des Datenschutzes?

Zur Beantwortung dieser Frage habe ich sechs Apps untersucht, die derzeit von Bundesbehörden angeboten werden. Besonderes Augenmerk wurde darauf gelegt, ob sich die Nutzer über die Datenerhebung und -nutzung sowohl vor und bei der Installation als auch während des Betriebs informieren können. Wie ich feststellen musste, ist dies meist entweder gar nicht oder zumindest nicht ausreichend möglich. App-spezifische Datenschutzerklärungen fehlten fast durchgängig und nur teilweise fanden sich in der Datenschutzerklärung der Website Hinweise zum Betrieb der App.

Mobile Applikationen unterliegen dem TMG, wenn bei der Nutzung Bestands- und Nutzungsdaten erhoben und übermittelt werden. § 13 Absatz 1 TMG verlangt zudem das Vorliegen einer Datenschutzerklärung. Obwohl vier der getesteten Apps als Telemedienangebot zu werten sind, war nicht eine einzige Datenschutzerklärung verfügbar. Auch die Gestaltung der Einwilligung zum Zugriff auf Standortinformationen, die bei der Installation abgefragt wird, sehe ich kritisch. Es mangelt an Transparenz und ausführlichen Informationen, wann und in welchem Umfang tatsächlich auf diese sensiblen Daten zugegriffen wird.

Hier gilt es, in Zukunft Abhilfe zu schaffen. Eine Leitlinie zur datenschutzkonformen Gestaltung von mobilen Applikationen bietet die „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter" des Düsseldorfer Kreises vom 16. Juni 2014 (abrufbar über mein Internetangebot unter www.datenschutz.bund.de). Aufgrund des Ergebnisses der durchgeführten Kontrolle habe ich die Datenschutzbeauftragten der Obersten Bundesbehörden angeschrieben und gebeten, entsprechend der Orientierungshilfe auf die Einhaltung des Datenschutzes bei den Bundesbehörden hinzuwirken.

Aber nicht erst bei der Nutzung, sondern schon bei der Bereitstellung von Bundesbehörden-Apps lässt sich der Datenschutz verbessern. Bei meiner Überprüfung habe ich festgestellt, dass - bis auf eine Ausnahme - alle untersuchten Bundesbehörden-Apps von den bekannten digitalen Vertriebsplattformen heruntergeladen werden müssen. Lediglich bei der App des Deutschen Bundestages („Bundestag-App") war es möglich, diese alternativ auch direkt von der Website des Deutschen Bundestages zu beziehen. Hier wäre es wünschenswert, wenn auch andere Bundesbehörden diesem positiven Beispiel folgten.

8.10 Post

8.10.1 Erfahrungen bei Kontrollen im Postbereich

Bei Kontroll- und Beratungsbesuchen der Postdienstunternehmen habe ich in der Regel ein hohes Datenschutzniveau festgestellt.

Empfänger nicht zu ermitteln - die Briefermittlungsstelle der Deutschen Post AG/DHL kann weiterhelfen

Wenn der Absender einer Briefsendung die Anschrift des Empfängers nicht korrekt geschrieben oder vergessen hat und gleichzeitig die Angabe des Absenders fehlt, steht die Post vor der Frage: Was nun? Die Briefsendung kann weder ordnungsgemäß zugestellt noch an den Absender zurückgeführt werden. Im Juristendeutsch handelt es sich um eine „unanbringliche Postsendung“, für die gemäß § 39 Absatz 4 Nummer 3 Postgesetz Ausnahmen des Postgeheimnisses gelten. Die Sendungen gelangen zur Briefermittlungsstelle der Deutschen Post AG/DHL im hessischen Marburg, einer seit 1976 existierenden Einrichtung der Post, die nach eigenen Angaben ca. 4,5 Millionen Sendungen pro Jahr bearbeitet und dabei im Jahr 2013 eine „Erfolgsquote“ von rd. 55 Prozent aufweist.

Das Vorgehen der Briefermittlungsstelle, von deren Arbeit ich mir vor Ort einen Eindruck verschafft habe, ist sehr umsichtig: Vor einer Brieföffnung werden zunächst die Möglichkeiten der Adressrecherche in Datenbanken, z. B. der Deutschen Post Direkt GmbH, und in öffentlichen Verzeichnissen genutzt, um zustellfähige Anschriften sowohl der Empfänger als auch der Absender zu ermitteln. Erst wenn dies nicht möglich ist, wird ein Brief geöffnet. Die Mitarbeiterinnen und Mitarbeiter der Briefermittlungsstelle sind angewiesen, nur die Kopf- und Fußzeilen zu lesen, nicht aber die Briefinhalte. Stellt sich trotz aller Bemühungen heraus, dass eine Briefzustellung oder Rückführung unmöglich ist, werden die Sendungen datenschutzkonform vernichtet.

Besonders häufig treten Probleme bei Briefen von Verwaltungsbehörden, größeren Unternehmen und Krankenkassen auf, wenn nur der Unternehmens- oder Behördenname ohne postalische Anschrift als Absender angegeben wird. Ich habe im Rahmen meiner Zuständigkeit darauf hingewirkt, dass diese Stellen gegenüber der Briefermittlungsstelle zentrale Einrichtungen benennen, an welche die Sendungen im Bedarfsfall zurückgesandt werden können.

Postsendungen auf dem Holzweg

Gelegentlich kommt es vor, dass Briefe irrtümlich in den Briefkasten eines „falschen“ Postdienstleisters eingeworfen werden und sich dann im Warenkreislauf eines anderen Postdienstleisters wiederfinden. Solche „Irrläufer“ treten auf, wenn Empfänger nicht für sie bestimmte Briefsendungen in den nächstbesten Briefkasten werfen - oft in der guten Absicht, eine ordnungsgemäße Zustellung an den „richtigen“ Empfänger zu ermöglichen. Fremde Postdienstleister haben allerdings keine Transport- und Zustellpflicht, da ihnen für diese Sendungen kein Entgelt bezahlt wurde. In der Praxis fallen diese Irrläufer meist schon bei der ersten Sortierung oder spätestens im Zustellprozess auf. Während einige Postdienstleister für einen Austausch dieser Irrläufer sorgen, musste ich feststellen, dass solche Rückführungen nicht - wie von mir erwartet - von allen Postdienstleistern vorgenommen, sondern die Briefe nach einer dreimonatigen Lagerung vernichtet werden. Auch wenn die Vernichtung datenschutzrechtlich nicht zu beanstanden ist, habe ich die Postdienstleister aufgefordert, eine kundenfreundlichere Lösung zu suchen, zumal weder Absender noch Empfänger Kenntnis von der Vernichtung erhalten. Da es sich um ein grundsätzliches Problem handelt, sollte eine verbindliche Regelung geschaffen werden, um diesem unbefriedigenden Zustand abzuhelfen; die Bundesnetzagentur habe ich bereits eingebunden.

Fertigung von Sendungsfotografien bei der Sortierung

Sendungsfotografien durch vollautomatische Sortieranlagen ermöglichen zwar eine schnelle und wirtschaftliche Sortierung von Postsendungen, werfen aber auch datenschutzrechtliche Fragen auf.

Auch kleinere Postdienstleister setzen vermehrt vollautomatische Sortieranlagen ein, die mit Sendungsfotografien arbeiten. Dazu werden die Vorderseiten der Sendungen fotografiert und die Empfängeradressen mittels automatisierter Texterkennung aus den Bildern extrahiert. Diese Datenerhebung und -verarbeitung ist zur Sortierung notwendig. Je nach Sortierprozess und verwendetem Maschinentyp werden die zustellrelevanten Daten maschinenlesbar auf die Sendung gedruckt, um weitere automatisierte Sortiervorgänge zu unterstützen. Die nicht mehr benötigten Sendungsfotografien müssen umgehend gelöscht werden, damit das Verfahren datenschutzrechtlich unbedenklich ist.

Einige Postdienstleister speichern und nutzen jedoch die Sendungsfotografien oder die daraus extrahierten Sendungsdaten auch für andere Zwecke, etwa zur Abrechnung bei Groß- oder Geschäftskunden oder zu Qualitätssicherungs- und Nachweiszwecken bei so genannten Mehrwertdiensten. Datenschutzrechtlich ist ein solches Vorgehen nicht unproblematisch: Die Erhebung und Speicherung der Sendungsdaten ist nur unter den engen Bedingungen des § 5 Absatz 4 Postdienste-Datenschutzverordnung zulässig. Personenbezogene Daten dürfen daher ausschließlich erhoben, verarbeitet und genutzt werden, soweit dies für die Zustellung der Postsendung, zum Zweck der Entgeltabrechnung und zum Nachweis der ordnungsgemäßen Zustellung notwendig ist. Bei mehreren Kontrollen habe ich die Einhaltung dieser Vorgaben geprüft und mir die Prozesse detailliert darstellen lassen. Ich habe darauf hingewirkt, dass die Speicherfristen auf das absolut notwendige Maß beschränkt und die Vertragspartner (in der Regel die Absender) vorab über das Verfahren unterrichtet werden.

Zutrittskontrolle bei kleineren Postdienstleistern oft mangelhaft

Gerade bei kleineren Postdienstleistern reicht die Absicherung von Betriebsgebäuden, in denen z. B. die Sortierung der Postsendungen erfolgt, häufig nicht aus.

Viele Betriebsgelände von Postdienstleistern sind nicht umzäunt und Zugangstüren während des Regelbetriebs und insbesondere außerhalb der Betriebszeiten nicht ausreichend gesichert. Auch der Schutz von IT-Anlagen, die im Rahmen der Erbringung von Postdienstleistungen eingesetzt werden, ist häufig nicht ausreichend. Gemäß der Anlage zu § 9 Satz 1 BDSG ist Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Auch wenn den Dienstleistern diese Problematik bewusst ist, scheitert die Umsetzung jedoch häufig an betriebswirtschaftlichen Vorgaben. Dennoch setze ich mich für angemessene Lösungen ein.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit
- Arbeitskreis Technik,
- Ad-hoc Arbeitsgruppe Smart Meter

Düsseldorfer Kreis mit der Arbeitsgruppe Kreditwirtschaft

Jour Fixe Telekommunikation

NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) mit

- NA 043-01-27-05 AK Arbeitskreis Identitätsmanagement und Datenschutz-Technologien
- NA 043-01-17 AA Arbeitsausschuss Karten und persönliche Identifikation
- NA 043-0-51 AA Arbeitsausschuss Vernichten von Datenträgern

Arbeitskreis Identitätsmanagement und Datenschutz-Technologien beim DIN
Arbeitsgruppe 4 des IT-Gipfels: Vertrauen, Datenschutz und Sicherheit im Internet
IT-Planungsrat

Artikel-29-Datenschutzgruppe

B. Zudem von besonderem Interesse

Nr. 2.1, 2.2, 2.5, 3.1.4, 5.3, 5.4, 5.14, 5.14.1, 5.14.2, 5.14.3, 5.14.4, 5.14.5, 6.1, 6.4, 8.6, 16.3

9 Ausschuss für Arbeit und Soziales

9.1 Arbeitsverwaltung SGB II

In den Jobcentern konnten in vielen Bereichen Verbesserungen des Datenschutzes und eine höhere Sensibilität der Mitarbeiterinnen und Mitarbeiter im Umgang mit Sozialdaten erreicht werden. Dennoch gilt es weiterhin, durch intensive Beratungen und Kontrollen das Datenschutzniveau zu erhalten und weiter zu steigern.

9.1.1 Vorlage von Kontoauszügen durch Verfügungsberechtigte

Jobcenter müssen sorgfältig prüfen, welche Mitwirkung von den Leistungsberechtigten nach Durchführung eines Kontenabrufs verlangt werden darf.

Jobcenter können nach § 93 Absatz 8 Satz 1 Nummer 1 der Abgabenordnung (AO) das Bundeszentralamt für Steuern (BZSt) um Durchführung eines Kontenabrufs bitten. Das BZSt teilt im Ergebnis dem anfragenden Jobcenter mit, welche Konten der Leistungsberechtigte bei welchen Banken unterhält oder zuletzt unterhalten hat. Außerdem erhält das Jobcenter Informationen zu Konten Dritter, über die der Leistungsberechtigte verfügungsberechtigt ist. Betroffene haben sich mit der Frage an mich gewandt, ob sie nach Aufforderung ihres Jobcenters verpflichtet sind, diesem über einen Zeitraum von mehreren Monaten oder Jahren Kontoauszüge von Konten vorzulegen, über die sie lediglich verfügungsberechtigt sind. Dies betraf hauptsächlich Kontoauszüge von nahen Angehörigen, in einem Fall allerdings auch die eines Vereins, in dem der Petent Vorstandsmitglied war.

Die geforderte Vorlage der Kontoauszüge durch das Jobcenter war in den von mir geprüften Fällen nicht erforderlich i. S. d. § 67a Absatz 1 Satz 1 SGB X und verstieß insbesondere gegen den Verhältnismäßigkeitsgrundsatz. Eine solche Erhebung der Kontoauszüge kann nur dann ausnahmsweise in Betracht kommen, wenn der konkrete Verdacht eines Leistungsmissbrauchs vorliegt. Besteht ein solcher Verdacht nicht, sind Kontoauszüge von Konten Dritter regelmäßig nicht geeignet, die Hilfebedürftigkeit eines Leistungsberechtigten zu prüfen. Die Auszüge enthalten im Wesentlichen Angaben zum Kontensaldo sowie zu den getätigten Umsätzen. Angaben zur Person, die den Geschäftsvorgang ausgelöst hat, ergeben sich aus ihnen nicht. Somit kann nicht geprüft werden, ob die Buchung vom Kontoinhaber selbst oder vom Verfügungsberechtigten vorgenommen wurde. In den von mir untersuchten Fällen konnten die betroffenen Jobcenter keine belastbaren Verdachtsmomente dafür vorbringen, die jeweiligen Leistungsempfänger hätten zum Zwecke des Leistungsmissbrauchs Gebrauch von den ihnen eingeräumten Verfügungsberechtigungen gemacht.

Die beabsichtigte Erhebung von Kontoauszügen über Konten Dritter war in den geprüften Fällen auch nicht angemessen. Das Jobcenter hätte dadurch einen nicht unerheblichen Einblick in die private Lebensführung der Dritten oder in geschäftliche Aktivitäten juristischer Personen hinsichtlich des Ausgabeverhaltens, vorhandener Einkommenspositionen und Vermögenswerte erhalten, obwohl diese Dritten in keinem Bezug zum Jobcenter standen.

Weiter verstieß das Vorgehen auch gegen den Grundsatz der Datenerhebung beim Betroffenen. Betroffene sind hier die jeweiligen Kontoinhaber, denn bei den Angaben auf den Kontoauszügen handelt es sich um Einzelangaben über ihre persönlichen und sachlichen Verhältnisse bzw. Betriebs- und Geschäftsgeheimnisse. Selbst wenn Leistungsberechtigte im Rahmen ihrer Verfügungsberechtigung den gleichen Zugriff auf die Kontoauszüge haben wie die Kontoinhaber selbst, bleiben sie bei diesem Erhebungsvorgang datenschutzrechtlich Dritte (§ 67 Abs. 10 Satz 2 und 3 SGB X), soweit von ihnen die Vorlage der Kontoauszüge verlangt wird. Eine Rechtsgrundlage für die Abweichung vom Grundsatz der Datenerhebung beim Betroffenen (§ 67a Abs. 2 Satz 2 SGB X) lag in den von mir geprüften Fällen nicht vor.

Ein Jobcenter teilte mir in seiner Stellungnahme zusätzlich mit, es frage bereits bei der Antragstellung auf Leistungen in jedem Einzelfall explizit auch Verfügungsberechtigungen sowie die Gründe dafür ab. Auch diese Abfrage ist nicht erforderlich. Das Vorhandensein einer oder mehrerer Verfügungsberechtigungen hat keine Auswirkung auf die Prüfung der Hilfebedürftigkeit. Weder können Geldeingänge noch Vermögenswerte auf solchen Konten den verfügungsberechtigten Antragstellern zugeordnet werden. Ich habe das Jobcenter aufgefordert, eine Abfrage von Verfügungsberechtigungen ausschließlich im Einzelfall im Rahmen eines Kontenabrufs unter den in § 93 Absatz 8 der AO genannten Voraussetzungen durchzuführen.

9.1.2 Sensibler Papiermüll in der Tiefgarage eines Jobcenters

Die Entsorgung nicht mehr benötigter Unterlagen durch ein Jobcenter erfolgte nicht datenschutzkonform.

In der Tiefgarage eines Jobcenters, die auch von Gästen eines im selben Gebäude befindlichen Hotels genutzt wird, hatte ein Hotelgast offene Säcke gefunden, in denen sich Dokumente des Jobcenters befanden. Der aufmerksame Finder hat diese Unterlagen direkt an sich genommen und unverzüglich an meine Behörde weitergeleitet.

Die Schriftstücke enthielten eine Vielzahl personenbezogener Sozialdaten, auch besonders sensibler Art gemäß § 67 Absatz 12 SGB X. Dazu gehörten Einladungsschreiben zu Vermittlungsgesprächen, Eingliederungsvereinbarungen, Berufsausbildungsverträge, Gesundheitsdaten einschließlich der Angabe des Behinderungsgrades, Zuweisungen an Träger von Maßnahmen zur Eingliederung und Haftzeitübersichten.

Ich habe zunächst die Geschäftsführung des Jobcenters über den Fund der sensiblen Dokumente informiert und eine sofortige Abhilfe gefordert. Weiterhin habe ich mir die vom Jobcenter getroffenen Maßnahmen zur Verhinderung weiterer Datenschutzverstöße im Rahmen der Datenmüllentsorgung in allen seinen Liegenschaften darlegen lassen. Nur aufgrund der hohen Kooperationsbereitschaft und der intensiven Schulung aller Mitarbeiter einschließlich der Reinigungskräfte habe ich von einer Beanstandung abgesehen. Bei meinen regelmäßigen Besuchen der Jobcenter vor Ort ist die datenschutzkonforme Müllentsorgung ein fester Kontrollbestandteil.

9.1.3 Unzulässige Überkreuzprüfungen in vier Jobcentern konnten in letzter Minute gestoppt werden

Eine Agentur für Arbeit hat bei der Überprüfung der Qualität erfasster Sozialdaten datenschutzrechtliche Standards nicht beachtet.

Der Vorsitzende der Geschäftsführung einer Agentur für Arbeit (AA) wollte für alle vier Jobcenter in seinem AA-Bezirk die Qualität der im zentralen IT-Verfahren „VerBIS“ erfassten Sozialdaten anhand von Kriterien überprüfen, die von der BA im Qualitätssicherungskonzept festgelegt worden sind. Die Überprüfungen sollten mittels sogenannter „Überkreuzprüfungen“ jeweils die Teamleiter eines Markt &t Integration-Teams (M&I-Teams) aus einem benachbarten Jobcenter vornehmen. Diese hätten dadurch über die Kenntnis der Sozialdaten aus ihrem eigenen Team hinaus auch Kenntnis von Sozialdaten der Kunden des benachbarten Jobcenters erhalten. Als ich davon erfuhr, war das Vorhaben bereits weitgehend vorbereitet und die erforderlichen Zugriffsberechtigungen für die betroffenen Teamleiter der vier Jobcenter schon beim Regionalen IT-Service der BA beantragt worden. Die Anträge gingen deutlich über die Zugriffsrechte im Berechtigungskonzept für „VerBIS“ hinaus. Damit wäre in allen vier Jobcentern im AA-Bezirk massiv gegen das Sozialgeheimnis (§ 35 SGB I) verstoßen worden.

Zur Wahrung des Sozialgeheimnisses dürfen Sozialdaten vom Leistungsträger nur befugt erhoben, verarbeitet oder genutzt werden und nur die befugten Mitarbeiter dürfen auf die Sozialdaten zur Aufgabenerledigung zurückgreifen. Die BA als verantwortliche Stelle für das zentrale IT-Verfahren „VerBIS“ (vgl. § 50 Abs. 3 Satz 3

SGB II) hat zu diesem Zweck ein Berechtigungskonzept für „VerBIS“ erstellt und mit meiner Behörde abgestimmt. Darin werden die Befugnisse der zuständigen Mitarbeiter im Einzelnen geregelt. Das Berechtigungskonzept gilt verbindlich für alle Jobcenter, die nach § 44b SGB II als gemeinsame Einrichtungen geführt werden, da diese die von der BA zentral verwalteten IT-Verfahren zur Erfüllung ihrer Aufgaben zu nutzen haben (§ 50 Abs. 3 Satz 1 SGB II). Bei der geplanten „Überkreuzprüfung“ der Jobcenter im Bezirk der betroffenen AA wäre den Grundsätzen dieses Berechtigungskonzeptes nicht Rechnung getragen worden.

Auf meine Intervention hin hat der Vorsitzende der Geschäftsführung der AA auf die Einführung der Überkreuzprüfungen verzichtet und bedauert, die behördlichen Datenschutzbeauftragten der Jobcenter nicht frühzeitig eingebunden zu haben.

9.1.4 Beanstandung mehrerer Verstöße bei der Erhebung, Verarbeitung und Nutzung von Sozialdaten

Jobcenter müssen auch bei der Sachverhaltsermittlung das Sozialgeheimnis wahren.

Ein Petent wandte sich an mich, nachdem die regelmäßige Zahlung seiner Miete vom Jobcenter eigenständig auf ein anderes Konto der Vermieterin umgestellt worden war. Wohnungseigentümerin war im vorliegenden Fall die Mutter des Petenten. Der Betroffene versuchte im Anschluss erfolglos beim Jobcenter zu klären, wie es zu dieser, von ihm oder seiner Mutter nicht veranlassten Kontoumstellung gekommen sei. Bei meiner Ermittlung des Sachverhalts stellte sich heraus, dass dem Jobcenter zwei anonyme Anzeigen vorlagen, in denen dem Petenten unterstellt worden war, die Mietzahlungen für den eigenen Lebensunterhalt zu verbrauchen. Er habe angeblich Zugriff auf das Mietkonto der Mutter. Das Jobcenter nahm nach Erhalt der Anzeigen umfangreiche Ermittlungen auf, in denen es beispielsweise Nachbarn befragte, Kontenabrufe durchführte und Banken um Auskunft anschrieb. Außerdem hat das Jobcenter Informationen über die Eigentumsverhältnisse des Mietobjekts aus dem elektronisch geführten Grundbuch abgerufen und mehrfach das für die Mutter zuständige Finanzamt angeschrieben. Bei den Anfragen wurden Sozialdaten des Petenten offenbart und der Verdacht des Leistungsmissbrauchs geäußert.

So akribisch die Behörde ihre Ermittlungen vorantrieb, so ungenau nahm sie auf der anderen Seite ihre Dokumentations- und Informationspflichten war. Mehrfach wurden Ermittlungshandlungen in der Akte überhaupt nicht dokumentiert, beispielsweise die Herkunft der Bankverbindung, auf die das Jobcenter zwischenzeitlich seine Mietzahlung umgestellt hatte. Informationspflichten, die der Behörde bei der Datenerhebung bei Dritten (§ 67a Abs. 5 SGB X) und bei der Durchführung von Kontenabrufen (§ 93 Abs. 9 AO) von Amts wegen oblagen, wurden ignoriert. Sogar zwischenzeitliche Anfragen des Petenten oder seiner Mutter zum Hintergrund der Ermittlungen wurden vom Jobcenter teilweise gar nicht oder falsch beantwortet. Aufgrund der mangelhaften Dokumentation konnte mir das Jobcenter die Rechtsgrundlagen für die durchgeführten Datenerhebungen und -übermittlungen nicht plausibel darlegen. Deswegen musste ich bei der überwiegenden Zahl der Ermittlungshandlungen dieser Behörde Verstöße gegen das Sozialgeheimnis feststellen. Außerdem war das Jobcenter so nicht mehr in der Lage, Ansprüche des Petenten und seiner Mutter auf Auskunft (§ 83 Abs. 1 SGB X) zu erfüllen, obwohl es sich hierbei um unabdingbare Rechte der Betroffenen (§ 84a SGB X) handelt.

Aufgrund der Anzahl der von mir festgestellten Verstöße bei der Erhebung, Verarbeitung und Nutzung von Sozialdaten sowie der mangelhaften Dokumentation, die eine Aufklärung des Sachverhalts wesentlich erschwert hat, habe ich das Verwaltungshandeln des Jobcenters gegenüber dem BMAS förmlich beanstandet. Ich hoffe, dass die vom Jobcenter im Anschluss getroffenen Maßnahmen zur Sensibilisierung seiner Mitarbeiter zukünftig zu einem besseren Verständnis für den Sozialdatenschutz führen werden.

9.1.5 Unzulässiger Zugriff auf ein kommunales Wohngeldverfahren

Ein kommunaler Träger musste den Mitarbeitern des gemeinsam mit der Agentur für Arbeit geführten Jobcenters den Zugriff auf Daten des städtischen Wohngeldverfahrens wieder entziehen.

Durch den Hinweis eines Landesbeauftragten für den Datenschutz (LfD) wurde ich darauf aufmerksam, dass Mitarbeiter eines Jobcenters Zugriff auf ein IT-Verfahren des kommunalen Trägers zur Berechnung und Auszahlung von Wohngeld eingeräumt wurde. Ein kurzfristig durchgeführter Kontrollbesuch vor Ort hat die Hinweise bestätigt. Der Zugriff ermöglichte den Jobcenter-Mitarbeitern einen umfassenden automatisierten Abruf personenbezogener Daten von Wohngeldempfängern, der weit über den für die Bewilligung von SGB II-Leistungen erforderlichen Umfang hinausging. Auf meine Forderung hin wurde den Mitarbeitern des Jobcenters der unzulässige Zugriff auf das Wohngeldverfahren wieder entzogen.

Öffentliche Stellen i. S. d. § 35 SGB I haben die in § 79 SGB X festgelegten gesetzlichen Voraussetzungen vor der Einrichtung eines solchen automatisierten Abrufverfahrens zu erfüllen. Die Kommune als datenliefernde und das Jobcenter als abrufende Stelle hätten ihren jeweils zuständigen Datenschutzkontrollbehörden unter Mitteilung der schriftlichen Festlegungen nach § 79 Absatz 2 SGB X rechtzeitig über die Einrichtung des Abrufverfahrens unterrichten müssen (§ 79 Abs. 3 SGB X). Nur die betroffene Kommune ist ihrer Unterrichtungspflicht gegenüber dem zuständigen LfD nachgekommen. Das Jobcenter als abrufende Stelle hat die Unterrichtung meiner Behörde unterlassen und somit eine Vorab-Kontrolle der Zulässigkeit dieses Verfahrens unmöglich gemacht. Bereits aus diesem Grund war das Abrufverfahren rechtswidrig.

Auch die weiteren Voraussetzungen eines automatisierten Zugriffs auf Daten des städtischen Wohngeldverfahrens fehlten. Im Sozialrecht gilt der Ersterhebungsgrundsatz. Danach sind Sozialdaten grundsätzlich beim Betroffenen zu erheben (§ 67a Abs. 2 Satz 1 SGB X). Die Datenerhebung über den zusätzlichen Informationszugriff auf das Wohngeldverfahren wäre nur dann datenschutzrechtlich gerechtfertigt gewesen, wenn die Ausnahmetatbestände des § 67a Absatz 2 Satz 2 SGB X vorgelegen hätten. Dies war aber nicht der Fall. Die Datenerhebung bei den Betroffenen verursachte keinen unverhältnismäßigen Aufwand und es konnte nicht ausgeschlossen werden, dass überwiegende Interessen der Betroffenen beeinträchtigt werden. Die schutzwürdigen Interessen der Betroffenen an einem Selbst-Nachweis ihrer Kosten für Unterkunft und Heizung haben hier überwogen.

Nur aufgrund der guten Kooperation des Jobcenters und einer sofortigen Einstellung des automatisierten Abrufs von Wohngelddaten beim kommunalen Träger habe ich von einer Beanstandung abgesehen.

9.1.6 Videoüberwachung in Jobcentern

Ansteigende Gewaltbereitschaft und Sachbeschädigungen an Gebäuden sowie Angriffe auf Mitarbeiter und Handgreiflichkeiten unter Kunden haben zum stärkeren Einsatz von Videoüberwachungstechnik im Außen- und Innenbereich von Jobcentern geführt.

In den letzten zwei Jahren haben die Jobcenter verstärkt auf die Videoüberwachungstechnik zum Schutz vor Übergriffen gegenüber Mitarbeitern und Kunden in den Räumen der Liegenschaften und vor Sachbeschädigungen im oder am Gebäude gesetzt.

Die datenschutzrechtliche Zulässigkeit der Videoüberwachung in öffentlich zugänglichen Räumen richtet sich nach § 6b BDSG. Die Beobachtung ist danach zulässig, wenn sie zur Aufgabenerfüllung öffentlicher Stellen oder zur Wahrung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen Betroffener überwiegen. Schutzwürdige Interessen der Betroffenen sind im besonderen Maße berührt bei permanenter und lückenloser Überwachung, der sich die Betroffenen nicht entziehen können, der Möglichkeit einer automatisierten Auswertung der Bilddateien, der Erfassung einer Vielzahl von Personen, die ohne konkre-

ten Anlass überwacht werden oder einer Erfassung von Bereichen, die der ungezwungenen und freien Entfaltung der Persönlichkeit dienen (Kantinen, Raucherecken, Wartebereiche). Die wesentlichen Kriterien bei der Interessensabwägung sind das Ausmaß der konkreten Gefährdungslage und die für die Betroffenen eintretenden Nachteile.

Während eine beobachtende Videoüberwachung als Live-Übertragung an den Sicherheitsdienst im Gebäude zum notwendig werdenden sofortigen Einschreiten in der Regel für die Gefahrenabwehr ausreichend ist, sind die Anforderungen an die Verarbeitung und Nutzung von Videoüberwachungsdaten höher. Diese sind nur dann zulässig, wenn sie zur Beweissicherung erforderlich sind. Im Einzelfall muss die Aufzeichnung zu Beweiszwecken auf bestimmte, besonders gefahrgeneigte Bereiche begrenzt werden. Der Umstand der Beobachtung und die verantwortliche Stelle sind zudem durch geeignete Maßnahmen erkennbar zu machen (§ 6b Abs. 2 BDSG).

Im Rahmen meiner Kontrollbesuche musste ich teilweise auf datenschutzrechtliche Mängel bei der Nutzung der Videotechnik hinweisen. So wurden in der Wartezone eines Jobcenters die Bilder der dort installierten Kamera live auf einen großen Bildschirm in eben dieser Wartezone übertragen. Auf meinen Hinweis hin hat der Geschäftsführer noch am selben Tag die datenschutzwidrige Live-Übertragung abgeschaltet. Andere Jobcenter habe ich aufgefordert, den Schutz der Videoüberwachungsanlage vor Zugriffen unberechtigter Dritter zu erhöhen. Beispielweise wurde in einem Jobcenter der Raum, in dem das Aufzeichnungsgerät stand, gleichzeitig als Aufenthaltsraum für den privaten Sicherheitsdienst genutzt. In anderen Fällen habe ich auf die Einhaltung der Pflicht zur Kennzeichnung öffentlich zugänglicher Räume oder zur Ausblendung etwa von Zugängen zu WC-Räumen gedrungen.

Zu den datenschutzrechtlichen Grundsätzen der Videoüberwachung in der öffentlichen Verwaltung des Bundes verweise ich ergänzend auf Nr. 3.3 meines 24. Tätigkeitsberichts.

9.1.7 Post vom Jobcenter - aber bitte neutral

Ein deutlich sichtbares „Logo“ der Jobcenter auf dem Briefumschlag verstößt gegen den Datenschutz.

Bürgereingaben, Beiträge in einschlägigen Internetforen und entsprechende Anfragen von Mitarbeitern aus den Jobcentern haben mich darauf aufmerksam gemacht, dass eine Vielzahl von Jobcentern ihre Briefe mit einem deutlich sichtbaren Logo versehen hatte. Dies halte ich für datenschutzwidrig. Aufgrund der Größe des Logos können Dritte auch aus einiger Entfernung und bereits bei flüchtiger Betrachtung erkennen, dass der Empfänger der Briefsendung Post vom Jobcenter erhält und damit regelmäßig ein Leistungsempfänger sein wird. Eine solche zusätzliche Kennzeichnung der Briefumschläge ist nicht notwendig, um unzustellbare Briefe sicher an den Absender zurückzusenden. Das Jobcenter druckt in der Regel seine Absenderadresse in kleiner Schriftgröße im Sichtfenster auf. Bei geschlossenen Briefumschlägen reicht einen diskrete Absenderangabe auf der Rückseite des Briefumschlages.

Aufgrund der grundsätzlichen Bedeutung habe ich meine Rechtsauffassung allen Geschäftsführern der meiner Zuständigkeit unterliegenden Jobcenter mitgeteilt und diese aufgefordert, Briefpost an Kunden grundsätzlich ohne Logo oder Aufdrucke mit dem Begriff „Jobcenter“ auf dem Briefumschlag zu versenden. Grundsätzlich haben Betroffene einen Anspruch auf Wahrung des Sozialgeheimnisses durch das Jobcenter (§ 35 SGB I). Die Jobcenter sind daher gesetzlich verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, um diesen Anspruch zu gewährleisten (§ 78a SGB X). Die Verwendung zusätzlicher Merkmale (z. B. Logos, Stempel, Aufdrucke, Aktenzeichen) auf Briefumschlägen selbst würde diesem Anspruch zuwiderlaufen. Die Absenderadresse im Sichtfenster eines Briefumschlages ist demgegenüber datenschutzrechtlich anders zu bewerten. Sie ist erforderlich, um ggf. unzustellbare Post an den Absender zurücksenden zu können. Die Kunden- oder BG-Nummer im Sichtfenster lässt keine Rückschlüsse auf persönliche Daten der Betroffenen zu, sie ist „nicht sprechend“ und damit datenschutzrechtlich nicht zu beanstanden. Insoweit verweise ich auf meine Ausführun-

gen im 18. Tätigkeitsbericht (Nr. 20.2.1). Zwischenzeitlich haben die Jobcenter eine Umstellung der Postversendung auf neutrale Umschläge technisch umgesetzt.

9.1.8 Nachweis der Unterkunftskosten

Jobcenter dürfen Leistungsempfänger nicht verpflichten, vom Vermieter ausgefüllte oder unterschriebene Mietbescheinigung vorzulegen.

Das Jobcenter ist berechtigt, Sozialdaten zu erheben, soweit dies für die Erfüllung seiner Aufgaben nach dem Sozialgesetzbuch erforderlich ist (§ 67a Abs. 1 Satz 1 SGB X). Mit einer Mietbescheinigung werden Daten erhoben, die für die Berechnung der Bedarfe für Unterkunft und Heizung (§ 22 SGB II) benötigt werden. Diese Angaben können jedoch in der Regel mit anderen Unterlagen nachgewiesen werden. Hier bietet sich beispielsweise der zentral von der BA erstellte Vordruck „Anlage Kosten der Unterkunft und Heizung“ an, den jeder Antragsteller vom Jobcenter erhält.

Sozialdaten sind grundsätzlich beim Betroffenen zu erheben (§ 67a Abs. 2 Satz 1 SGB X). Daher muss das Jobcenter jedem Antragsteller die Gelegenheit geben, die erforderlichen Angaben durch geeignete Nachweise selbst zu erbringen. Viele Jobcenter haben in der Vergangenheit die Antragsteller aufgefordert, zum Nachweis der Unterkunftskosten eine Mietbescheinigung vorzulegen, die vom Vermieter ausgefüllt oder zumindest unterschrieben werden sollte. Für die Jobcenter ist die Vorlage solcher Mietbescheinigungen die einfachste Nachweisform, da sie den Aufwand bei der Vorlage aller erforderlichen Daten deutlich vermindern kann. Datenschutzrechtlich problematisch ist in diesen Fällen jedoch, dass der Vermieter dann regelmäßig Kenntnis über eine Antragstellung seines Mieters auf Hartz IV-Leistungen erlangt. Zudem bestehen weder gesetzliche Auskunfts- noch Mitwirkungspflichten des Vermieters gegenüber dem Jobcenter. Dieses muss daher die Antragsteller zwingend auf die freiwillige Mitwirkung von Vermieter und Antragsteller selbst hinweisen. Nur wenn die Betroffenen umfassend über die Freiwilligkeit der Vorlage einer Bescheinigung des Vermieters aufgeklärt wurden, halte ich diesen Weg, Kosten der Unterkunft und Heizung nachzuweisen, datenschutzrechtlich für zulässig.

9.1.9 Manche Jobcenter nehmen die Unterstützungspflicht nicht wirklich ernst

Jobcenter und auch alle anderen öffentlichen Stellen des Bundes sind verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen.

Obwohl ich bereits mehrfach darauf hingewiesen habe, kommen einige Jobcenter ihrer Verpflichtung aus § 50 Absatz 4 Satz 3 SGB II i. V. m. § 24 Absatz 4 BDSG, mich bei der Erfüllung meiner Aufgaben umfassend zu unterstützen, immer noch nicht nach (24. TB Nr. 12.1.1.3).

Jeder, der sich mit einer Eingabe an mich wendet (§ 81 Abs. 1 Nr. 1 SGB X), darf auf eine umfassende und objektive Prüfung seiner Angelegenheit vertrauen. Dazu gehört, der Geschäftsführung des von der Beschwerde betroffenen Jobcenters die Möglichkeit zur Stellungnahme und zur Darstellung der Sach- und Rechtslage aus ihrer Sicht einzuräumen. Leider ist das Interesse einiger Jobcenter an der Aufklärung eines datenschutzrechtlichen Sachverhalts merklich geringer, als das der betroffenen Petenten. Wenn diese Jobcenter grundsätzlich erst auf meine Erinnerungsschreiben oder nur unter Androhung einer Beanstandung gemäß § 25 BDSG reagieren, wird der Datenschutz von ihren Geschäftsführungen offensichtlich noch nicht als Grundrecht der Bürger begriffen.

Ich erwarte von allen Stellen, die meiner Kontrollzuständigkeit unterliegenden, eine pflichtgemäße Unterstützung in angemessener Zeit und mit der gebotenen Sorgfalt. Diesen Anspruch werde ich künftig eine noch stärkere Aufmerksamkeit widmen und ihn gegenüber allen Jobcentern durchsetzen.

Kasten zu Nr. 9.1.9

§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Absatz 4:

Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

9.1.10 Infopost

Weiterbewilligungsanträge dürfen nicht mittels „Infopost" versandt werden.

Zweimal jährlich wird jedem Bezieher von Arbeitslosengeld II ein Weiterbewilligungsantrag (WBA) zugesandt, den dieser ausgefüllt an das zuständige Jobcenter zurücksenden kann. Das Anschreiben zu diesem WBA enthält neben der Bedarfsgemeinschaftsnummer auch den abgelaufenen Bewilligungszeitraum. Zur Versendung dieser WBA wird von der Bundesagentur für Arbeit (BA) das Produkt „Infopost" der Deutschen Post AG (DP AG) genutzt.

Das Produkt „Infopost" ist ein Angebot, bei dem größere Mengen inhaltsgleicher Schreiben zu einem günstigeren Preis versandt werden können. Zur Kontrolle, ob die für die Vergünstigung erforderlichen Bedingungen eingehalten worden sind, können Mitarbeiter der DP AG diese entgeltbegünstigten Postsendungen öffnen. Bei Wahrnehmung dieses Kontrollrechts besteht die Möglichkeit, dass Mitarbeitern der DP AG bekannt wird, wer Sozialleistungen bezieht.

Die BA vertritt die Auffassung, die Mehrkosten für Portogebühren, die durch die Versendung der WBA mit dem Produkt „Kompaktbrief" statt mit dem Produkt „Infopost" entstehen würden (1.902.310,80 Euro im Jahr 2012), seien im Verhältnis zu dem angestrebten Schutzzweck der einschlägigen Datenschutzregelungen nicht angemessen.

Ich teile diese Meinung nicht. Zwar bewertete ich das Produkt „Infopost" der DP AG grundsätzlich als datenschutzrechtlich einwandfrei. Darüber hinaus ist jedoch in jedem konkreten Einzelfall zu prüfen, wie sensibel die personenbezogenen Daten sind, die mit der „Infopost" versandt werden sollen. Genießen die versandten Daten weitergehenden Schutz, wie im konkreten Fall durch das Sozialgeheimnis (§ 35 SGB I), hat eine Versendung mittels „Infopost" zu unterbleiben. Die BA hat beim Postversand grundsätzlich eine Versendungsart zu wählen, die eine Kenntnisnahme der in den Schreiben enthaltenen Sozialdaten durch Dritte ausschließt. Ich erwarte daher, dass künftig alle Schreiben der BA, die Sozialdaten enthalten, nicht mehr mittels „Infopost" versendet wer-

den. Andernfalls behalte ich mir eine Beanstandung des Datenschutzverstoßes gemäß §§ 78a, 81 Absatz 2 Satz 1 SGB X i. V. m. § 25 Absatz 1 Satz 1 Nummer 1 BDSG vor.

9.2 Einleitung Arbeitsverwaltung, SGB III

Im Bereich der Arbeitsförderung standen erneut die Internetplattform JOBBÖRSE der Bundesagentur für Arbeit (BA) sowie die Übermittlung von Gesundheitsdaten im Fokus meiner Beratungs- und Kontrolltätigkeit. Hierzu erreichten mich auch im Berichtszeitraum wieder zahlreiche Eingaben.

9.2.1 Die JOBBÖRSE der Bundesagentur für Arbeit

Die Internetplattform JOBBÖRSE der BA bleibt ein datenschutzrechtlicher Schwerpunkt meiner Arbeit.

Bereits in meinem 22. (Nr. 7.5 und 10.5.1) und 23. Tätigkeitsbericht (Nr. 11.5.4) hatte ich über datenschutzrechtliche Probleme beim Betrieb der JOBBÖRSE durch die BA unter www.arbeitsagentur.de berichtet. Die JOBBÖRSE steht als Internetplattform sowohl Arbeitgebern als auch Arbeit- bzw. Ausbildungsplatzsuchenden zur Verfügung, um Stellen- und Bewerberangebote aufzugeben oder einzusehen. Die BA erfüllt mit der JOBBÖRSE ihre Verpflichtung aus § 35 Absatz 3 Satz 1 SGB III, Ausbildungs- und Arbeitsvermittlung auch über Selbstinformationseinrichtungen nach § 40 Absatz 2 SGB III im Internet durchzuführen.

Insbesondere die folgenden vier Fragestellungen zur JOBBÖRSE waren im Berichtszeitraum relevant:

Übermittlung Kontaktdaten Arbeitsuchender an potentielle Arbeitgeber

Immer wieder haben mich Eingaben von arbeitsuchend oder arbeitslos gemeldeten Personen erreicht, deren Kontaktdaten ohne ihre Einwilligung durch die BA an potentielle Arbeitgeber übermittelt worden sind.

Die örtlichen Agenturen für Arbeit (AA) sind nach § 35 SGB III verpflichtet, Vermittlungsleistungen anzubieten. Das Vermitteln ist weit zu verstehen und umfasst alle Tätigkeiten, die darauf zielen, Arbeitsuchende und Arbeitgeber zur Begründung eines Beschäftigungsverhältnisses zusammenzuführen (§ 35 Abs. 1 Satz 2 SGB III). Zur Vermittlung gehört somit auch die Übermittlung von Daten eines Arbeitsuchenden (Name und Anschrift) an Arbeitgeber. Im Rahmen dieses gesetzlichen Vermittlungsauftrages dürfen die Daten des Arbeitsuchenden ohne dessen vorherige Einwilligung an den potentiellen Arbeitgeber weitergegeben werden, wenn dies nach Maßgabe des § 69 Absatz 1 Nummer 1 SGB X erforderlich ist.

In der Praxis werden häufig die Kontaktdaten des Arbeitsuchenden gemeinsam mit dem Vermittlungsvorschlag an den Arbeitgeber mit übermittelt. Von einer solchen Übersendung der Kontaktdaten kann die Vermittlungsfachkraft der BA jedoch abweichen, wenn sie dies für nicht erforderlich erachtet, so dass dann nur der Arbeitsuchende einen schriftlichen Vermittlungsvorschlag erhält.

Auf der Internetplattform der JOBBÖRSE besteht eine derartige Differenzierungsmöglichkeit nicht. Hier erhält der Arbeitgeber in jedem Fall Kenntnis von den Kontaktdaten, auch wenn dies nicht erforderlich ist.

Es fehlt damit eine datenschutzrechtliche Übermittlungsbefugnis.

Ich habe die BA über meine Rechtsauffassung informiert und um Umsetzung gebeten.

Verwendung von Cookies

Wie mir in einer Eingabe mitgeteilt wurde, werden bei der Nutzung der JOBBÖRSE permanente Cookies verwendet. Da in diesen Cookies die zuletzt angesehenen Stellen abgespeichert werden, konnte ein in der JOBBÖRSE angemeldeter Nutzer auf diese Informationen des vorherigen Nutzers zugreifen.

Die Verwendung von Cookies ist nur zulässig, wenn der Nutzer zu Beginn des Verfahrens hierüber unterrichtet wurde (§ 13 Abs. 1 Telemediengesetz - TMG). Zudem bedarf es einer Rechtsgrundlage oder der Einwilligung des Nutzers (§ 12 TMG).

Bei der JOBBÖRSE wurde allerdings weder in der Datenschutzerklärung auf die Verwendung von Cookies hingewiesen, noch die Einwilligung des Nutzers zu Beginn des Nutzungsvorgangs eingeholt. Außerdem wurde nicht mitgeteilt, ob IP-Adressen erhoben und gespeichert werden. Eine Rechtsvorschrift, die die Verwendung gestattet, gibt es ebenfalls nicht.

Deshalb habe ich die BA gebeten, die entsprechenden Einstellungen der JOBBÖRSE bzw. die Datenschutzerklärung zu überprüfen und datenschutzgerecht abzuändern. Jedenfalls muss sie auf die tatsächlich verwendeten Cookies hinweisen. Insbesondere ist dabei zu beschreiben, welche Cookies verwendet werden (z. B. temporäre Cookies, permanente Cookies), für welche Zwecke sie genutzt werden und welche Lebensdauer sie besitzen.

Von einer Beanstandung habe ich abgesehen, da die BA die Nutzung permanenter Cookies eingestellt und die Datenschutzerklärung im Hinblick auf die Verwendung von sog. temporären Cookies angepasst hat. Ein Zugriff auf die zuletzt aufgerufenen Stellenangebote anderer Nutzer ist nicht mehr möglich.

Speicherung von Vermittlungsvorschlägen in Arbeitgeberaccounts

Sind Arbeitgeber selbst in der JOBBÖRSE mit einem Account gemeldet und bitten sie die Agenturen für Arbeit um Unterstützung bei der Besetzung offener Stellen, erhalten sie in ihrem Account eine Übersicht der ihnen vorgeschlagenen Bewerber und damit auch Zugriff auf deren Kontaktdaten sowie berufliche Werdegänge.

Aufgrund des Hinweises einer Petentin habe ich festgestellt, dass neben den neuen Vermittlungsvorschlägen auch noch zahlreiche alte im Account eines Arbeitgebers in der JOBBÖRSE abgespeichert waren. Die abrufbaren Vermittlungsvorschläge reichten bis zu vier Jahre in die Vergangenheit zurück.

Wie die BA zugegeben hat, ist ein so lange zurückreichender Zugriff auf veraltete Vermittlungsvorschläge nicht erforderlich. Sie hat umgehend eine technische Lösung in Auftrag gegeben, um nur noch aktuelle Vermittlungsvorschläge für Arbeitgeber sichtbar zu machen. Von einer Beanstandung habe ich daher abgesehen, die BA aber aufgefordert, die Arbeitgeber bis zur Abstellung dieses Mangels in der JOBBÖRSE gemäß § 78 SGB X auf die Zweckbindung und Geheimhaltung der offenbarten Bewerberdaten zu verpflichten.

Angaben des Arbeitgebers zu einem abgelehnten Bewerber

Die JOBBÖRSE ist ein interaktives Werkzeug. Über ihren dortigen Account erhalten Arbeitgeber nicht nur Vermittlungsvorschläge, sie können der AA gegenüber auch Rückmeldungen zu den vorgeschlagenen Arbeitsuchenden geben, z. B. kann der Grund einer Absage mitgeteilt werden. Für Rückmeldungen stellt die JOBBÖRSE dem Arbeitgeber ein Menü mit mehreren Vorschlägen sowie ein Freitextfeld für ergänzende Angaben zur Verfügung, z. B. wenn „Sonstige Gründe“ für die Absage auswählt werden. Die Bemerkungen des Arbeitgebers in der JOBBÖRSE werden dann automatisch in das IT-Verfahren VerBIS übertragen und zwar in die elektronische Dokumentation des jeweiligen Vermittlungsvorschlag im Bewerberprofil des Arbeitsuchenden. In diese Dokumentation innerhalb des IT-Verfahrens VerBIS können nicht nur die unmittelbaren Vermittlungsfachkräf-

te, sondern eine Vielzahl weiterer Mitarbeiter der AA einsehen. Bei der Prüfung von VerBIS habe ich sowohl objektive als auch einseitige oder unrichtiger Rückmeldungen der Arbeitgeber festgestellt. So fanden sich Äußerungen wie „Der hat keinen Bock“ oder „Nie telefonisch zu erreichen“.

Wie sich bei der Kontrolle weiter herausgestellt hat, haben die Mitarbeiter der AA keine Möglichkeit, diese Äußerungen zu bearbeiten oder zu entfernen, obwohl den Arbeitsuchenden aus den §§ 84, 84a SGB X das Recht auf Berichtigung falscher oder Löschung unzulässig gespeicherter Angaben zusteht.

Die BA muss Arbeitgeber darauf hinweisen, dass in dem Freitextfeld nur objektive Angaben zum Grund der Ablehnung des Bewerbers eingetragen werden dürfen. Außerdem habe ich darum gebeten, im IT-Verfahren VerBIS eine Möglichkeit zur Korrektur oder Löschung entsprechender Angaben vorzusehen.

Zu meiner Freude hat die BA meine Empfehlungen aufgegriffen und umgesetzt.

9.2.2 Übermittlung von Gesundheitsdaten

Eine Agentur für Arbeit hat ohne eine gesetzliche Übermittlungsbefugnis und ohne eine schriftliche Einwilligung des Betroffenen ein Gutachten des Ärztlichen Dienstes der Agentur für Arbeit an einen Arbeitgeber übermittelt.

Wie ich durch eine Eingabe erfahren habe, hat eine Vermittlungsfachkraft der AA eine Kopie eines ärztlichen Gutachtens, und zwar die sozialmedizinische Stellungnahme, Teil B, ohne schriftliche Einwilligung des Betroffenen an dessen Arbeitgeber übersandt. Der Arbeitgeber wollte für seinen neuen Mitarbeiter einen Arbeitsplatz einrichten, der die vorhandenen gesundheitlichen Einschränkungen berücksichtigen sollte. Dafür hat er eine Förderanfrage an die AA gestellt. Statt eines Hinweises, was bei der Arbeitsplatzeinrichtung zu berücksichtigen wäre, erhielt er eine Kopie des gesamten ärztlichen Gutachtens. Auf meine Nachfrage teilte mir die BA mit, es habe eine mündliche Einwilligung zur Übermittlung des ärztlichen Gutachtens an den Arbeitgeber vorgelegen.

Im geschilderten Fall durfte die AA das ärztliche Gutachten nicht übersenden. Diese Übermittlung ist ein grober Verstoß gegen Datenschutzvorschriften (§ 67b Abs. 1 Satz 1, 67d Abs. 1 SGB X), missachtet den Schutz des Sozialgeheimnisses nach § 35 Absatz 1 Satz 1 SGB I erheblich und verletzt den Arbeitnehmer in seinem Recht auf informationelle Selbstbestimmung. Angaben in einem ärztlichen Gutachten enthalten immer auch Gesundheitsdaten, d. h. besondere Arten personenbezogener Daten i. S. d. § 67 Absatz 12 SGB X, die einem besonderen Schutz unterliegen. Eine solche Übermittlung wäre nur dann gerechtfertigt, wenn der Arbeitnehmer darin schriftlich eingewilligt hätte (§ 67b Abs. 2 SGB X). Eine mündliche Einwilligung reicht hierfür nicht aus.

Angesichts dieses gravierenden Fehlverhaltens habe ich gegenüber der BA eine Beanstandung ausgesprochen (§ 81 Abs. 2 SGB X i. V. m. § 25 Abs. 1 Satz 1 Nr. 4 BDSG).

9.2.3 Beratungs- und Kontrollbesuch beim Institut für Arbeitsmarkt- und Berufsforschung

Zu den Aufgaben der BA gehört auch die Arbeitsmarkt- und Berufsforschung (§ 280 Nr. 2 SGB III), die vor allem durch das Institut für Arbeitsmarkt- und Berufsforschung (IAB) durchgeführt wird. Diesem dürfen die Daten aus dem Geschäftsbereich der BA nach Maßgabe des § 282 SGB III zu Forschungszwecken zur Verfügung gestellt werden.

Aufgrund von Bürgereingaben zu Forschungsvorhaben habe ich einen datenschutzrechtlichen Beratungs- und Kontrollbesuch beim IAB durchgeführt. Wie ich hierbei feststellen musste, wurden bei Tests mit verschiedenen

IT-Programmen Echtdaten von Betroffenen verwendet. Dies habe ich gemäß § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 Satz 1 Nummer 4 BDSG gegenüber dem Vorstand der BA beanstandet.

Darüber hinaus habe ich das IAB dahingehend beraten, die Durchführung der verschiedenen Forschungsvorhaben für die Betroffenen möglichst transparent zu gestalten. So sollten ihnen vor einer Befragung die wichtigsten Informationen über das jeweilige Projekt, insbesondere die Freiwilligkeit ihrer Teilnahme, mitgeteilt werden. Alle Details, sowie die Darstellung der teilweise nicht leicht nachvollziehbaren Rechtsgrundlagen, sollten nach Möglichkeit auf der Internetseite des IAB zu finden sein.

So könnte eine offene und transparente Kommunikation des IAB zu Ausgestaltung und Rechtsgrundlagen der verschiedenen Forschungsvorhaben erreicht werden. Den Betroffenen soll es möglich sein, die Handlungen des IAB und den Weg der eigenen personenbezogenen Daten nachzuvollziehen.

9.3 Beschäftigtendatenschutz

Auch nachdem in der letzten Legislaturperiode der Entwurf eines Beschäftigtendatenschutzgesetzes (hierzu Nr. 9.3.1) gescheitert ist, gab es im Berichtszeitraum doch in verschiedenen Bereichen neuere Entwicklungen.

9.3.1 Auf ein Beschäftigtendatenschutzgesetz kann nicht verzichtet werden

Nach dem Scheitern des Beschäftigtendatenschutzgesetzes in der vergangenen Legislaturperiode, scheint es in der Bundesregierung keine neueren Überlegungen hierzu zu geben. Dabei sind nationale gesetzliche Regelungen zum Beschäftigtendatenschutz dringend notwendig.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt seit langem die Notwendigkeit, umfassende Regelungen für den Datenschutz am Arbeitsplatz zu schaffen - erstmals im Jahre 1984. Das Gesetzgebungsverfahren in der letzten Legislaturperiode hat sie mit Entschließungen aus den Jahren 2009, 2010, 2011 (vgl. 24. TB Nr. 13.1) und zuletzt 2013 begleitet. Auf der 87. Konferenz vom 27. März 2014 forderten die Datenschutzbeauftragten des Bundes und der Länder erneut die sofortige Verabschiedung eines Beschäftigtendatenschutzgesetzes (vgl. Anlage 9).

Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutz-Grundverordnung zu erhalten sowie darüber hinaus gehende Standards zu ermöglichen. Erst wenn mit einer Verabschiedung der Verordnung nicht in absehbarer Zeit gerechnet werden könne, solle eine nationale Regelung geschaffen werden. Für den nationalen Gesetzgeber besteht aber schon jetzt unmittelbarer Handlungsbedarf, denn

- derzeit ist unklar, wann die europäische Datenschutz-Grundverordnung tatsächlich verabschiedet und wie der Beschäftigtendatenschutz darin geregelt sein wird,

- die technische Entwicklung schreitet unaufhaltsam voran und ermöglicht eine immer weitergehende Mitarbeiterüberwachung,

- das hohe Niveau des deutschen Beschäftigtendatenschutzes kann besonders durch eine nationale Regelung erhalten und ausgebaut werden.

Für viele praktisch relevante Fragestellungen im Beschäftigtendatenschutz fehlt es bislang an klaren rechtlichen Regelungen. Auch der aufgrund der Datenschutzskandale 2009 eingeführte § 32 BDSG regelt den Umgang mit

Beschäftigtendaten nur lückenhaft. Entsprechende Regelungen sind jedoch unabdingbar, um Rechtssicherheit zu schaffen und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen der Arbeitgeberinnen und Arbeitgeber sowie dem Recht auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zu gewährleisten. Insbesondere in den folgenden Bereichen sind gesetzliche Regelungen notwendig:

- Videoüberwachung am Arbeitsplatz und in öffentlich zugänglichen Bereichen, bei denen Beschäftigtendaten anfallen;

- Datenschutz im Bewerbungsverfahren, insbesondere die Erhebung und Verarbeitung von Bewerberdaten etwa aus sozialen Netzwerken;

- Private Nutzung dienstlicher Kommunikationsmittel und dienstliche Nutzung privater Kommunikationsmittel;

- Zunehmender Einsatz biometrischer Verfahren;

- Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent machen;

- Personalaktenführung im privaten Bereich;

- Mitarbeiterscreening;

- Einwilligung im Beschäftigungsverhältnis;

- Whistleblowing;

- Erhebung und Verarbeitung personenbezogener Daten im internationalen Konzern unter besonderer Berücksichtigung der Betroffenenrechte.

Ich werde mich weiterhin für die Schaffung eines Beschäftigtendatenschutzgesetzes einsetzen. Auch vor dem Hintergrund europäischer Entwicklungen kann auf eine nationale Regelung nicht verzichtet werden. Es ist höchste Zeit das Projekt „Beschäftigtendatenschutzgesetz“ endlich in die Tat umzusetzen.

9.3.2 Tücken des Cloud Computing bei Personaldaten

Die Verwendung von Cloud-Produkten birgt datenschutzrechtliche Risiken. Dies gilt insbesondere bei der Erhebung und Verarbeitung sensibler Personaldaten.

Das Projekt „Personalbemessung für die Leistungsgewährung bei den gemeinsamen Einrichtungen nach dem SGB II“ soll für den Bereich der Leistungsgewährung Daten erheben und auswerten und auf deren Grundlage eine Entscheidungshilfe für die Personalbedarfsermittlung in den gemeinsamen Einrichtungen nach dem SGB II („Jobcenter“) erarbeiten. Das Projekt des BMAS wird von einer Steuerungsgruppe der Bund-Länder-Arbeitsgruppe Personal begleitet und von einem Beratungsunternehmen durchgeführt. Zu den datenschutzrechtlichen Fragestellungen bei der Datenerhebung und Datenverarbeitung berate ich das BMAS.

Im Rahmen des Projekts sind die Beschäftigten derjenigen gemeinsamen Einrichtungen befragt worden, die sich für eine Teilnahme entschieden hatten. Abgefragt wurden zum einen die aufgabenspezifisch zu schätzenden Ar-

beitszeiten für einen bestimmten vergangenen Zeitraum. Zum anderen sollten die Beschäftigten auf freiwilliger Basis subjektive Einschätzungen hinsichtlich ihres Arbeitsplatzes, ihrer Tätigkeit, etc. abgeben. Die Beschäftigtenbefragung erfolgte mittels eines Webtools. Laut BMAS haben sich mehr als 21.000 Beschäftigte beteiligt. Nachdem die Erhebungsphase abgeschlossen war, wurden seit April 2014 die Antworten aus der Beschäftigtenbefragung sowie weitere Daten der Bundesagentur für Arbeit, des Statistischen Bundesamts und der Jobcenter qualitätsgesichert, aggregiert und ausgewertet.

Während der Erhebungsphase war mir die Trennung der Erhebungsdaten von den personenbezogenen Daten der Beschäftigten wichtig. Wie das BMAS mittlerweile bestätigt hat, standen – wie von mir gefordert - die Listen, mit denen die für die Erhebung verwendeten Identifizierungsnummerns den Namen der Beschäftigten zugeordnet wurden, ausschließlich den zuständigen Projektkoordinatoren zur Verfügung und wurden unmittelbar nach Abschluss der Erhebungsphase in den Jobcentern vollständig gelöscht. Meine Mitarbeiter konnten sich auch persönlich bei Kontrollen einiger Jobcenter davon überzeugen, dass die Befragung im Wesentlichen datenschutzkonform verlief.

Datenschutzrechtlich problematisch war jedoch der Umstand, dass die Antworten der Beschäftigten in der von einem US-amerikanischen Unternehmen bereitgestellten Cloud-Umgebung gespeichert wurden. Zwar wurde mir zugesichert, dass die Speicherung der im Projekt anfallenden Daten auf Servern in einem EU-Mitgliedsstaat erfolge. Nach den Feststellungen der Orientierungshilfe Cloud-Computing der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 2.0, vom 9. Oktober 2014 sind aber US-Behörden auf der Grundlage US-amerikanischen Rechts befugt, auch auf personenbezogene Daten zuzugreifen, die in Europa gespeichert sind. Die Orientierungshilfe ist auf meiner Internetseite unter www.datenschutz.bund.de abrufbar (vgl. auch Nr. 8.5).

Auch wenn die Artikel-29-Gruppe die maßgeblichen Verträge des Unternehmens im Bereich des Cloud-Computing noch Anfang April 2014 ausdrücklich als mit den europäischen Datenschutzregelungen vereinbar erklärt hat, sind meine datenschutzrechtlichen Bedenken nicht vollständig ausgeräumt. So wirft etwa ein Urteil des „United States District Court, Southern District of New York“ vom 25. April 2014 neue Fragen auf, indem es feststellt, dass Durchsuchungsbefehle amerikanischen Behörden das Recht einräumen, von einem Cloud-Service-Provider die Herausgabe aller Daten zu verlangen, die Privatpersonen oder Unternehmen bei ihm gespeichert haben, unabhängig davon, wo sich diese Daten befänden.

Zwar ist das Urteil noch nicht rechtskräftig, da das betroffene Unternehmen Berufung eingelegt hat, es zeigt jedoch, dass der rechtliche Rahmen, der das Cloud-Computing umgibt, noch nicht festgezogen ist. Eine weiterhin kritische Auseinandersetzung mit dem Thema ist aus datenschutzrechtlicher Sicht deshalb dringend geboten.

9.4 Wie viele Daten dürfen für Projekte des Europäischen Sozialfonds erhoben werden?

Zur Förderung der Beschäftigung in den EU-Mitgliedsstaaten hat die Europäische Union den Europäischen Sozialfond (ESF) geschaffen. Immer wieder werde ich dabei gefragt, welche Daten hierzu für den ESF erhoben, verarbeitet und genutzt werden dürfen.

Mit den Förderprojekten des ESF sind viele Stellen befasst: Zwischen den Zuwendungsempfängern, d. h. der Organisation, die das einzelne Projekt plant, organisiert und die Förderung durch den ESF beantragt, und der EU sind mehrere nationale Stellen eingeschaltet. Beteiligt sind auch die im jeweiligen Bundesministerium zuständigen Fachreferate sowie Verwaltungs-, Bescheinigungs- und Prüfbehörden. Darüber hinaus sind verschiedene Prüfinstanzen vorgesehen, etwa der Bundesrechnungshof, der Europäische Rechnungshof sowie das Europäische Amt für Betrugsbekämpfung. Alle diese Stellen erhalten Daten - manche mit Personenbezug andere ohne. Zu Prüf- und Evaluationszwecken werden Daten zum geförderten Projekt selbst, den Zuwendungsempfängern, der Finanzierung und den Teilnehmern erhoben. Was erhoben werden darf, ist in den Verordnungen

auf EU-Ebene festgelegt (für die Förderperiode 2014-2020: VO EU Nr. 1303 und 1304). Auf nationaler Ebene werden diese EU-Vorgaben durch das Zuwendungsrecht und Verwaltungsvorschriften konkretisiert.

Diese Vielzahl von Akteuren und rechtlichen Vorgaben führen zu einer sehr komplexen Struktur. Die Grundsätze des Datenschutzrechtes gelten jedoch auch hier: Jede Datenerhebung, -verarbeitung und -nutzung bedarf einer rechtlichen Grundlage oder einer verständlichen Einwilligung. Die Teilnehmer an den geförderten Projekten, insbesondere Jugendliche, müssen dabei verstehen, was mit ihren Daten geschieht und zu welchem Zweck. Deswegen ist auf eine altersentsprechende Formulierung der Einwilligungserklärung zu achten. Auch muss die Teilnahme freiwillig sein. Die so erhobenen Daten dürfen dann auch nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie ursprünglich erhoben wurden. Eine Nutzung für zusätzliche Auswertungen ist nicht zulässig.

Die Daten sind auf möglichst niedrigster Ebene zu anonymisieren. Sollte ein Personenbezug notwendig bleiben, müsste eine Pseudonymisierung der Daten erfolgen. Der Schlüssel sollte dabei nur der Stelle bekannt sein, bei der die spätere Zuordnung erfolgt, also regelmäßig dem Zuwendungsempfänger.

Wie ich aus Gesprächen mit dem BMAS zu ESF-Programmen für die neue Förderperiode (2014–2020) erfahren habe, will die EU künftig mehr Daten über den Teilnehmenden erheben als bisher. Dem Teilnehmer soll allerdings ein Auskunftsverweigerungsrecht zu bestimmten besonders sensiblen Daten eingeräumt werden. Kritisch sehe ich, dass auch die Umstände des Haushalts („household situation“) eines Teilnehmenden verpflichtend abgefragt werden sollen, weil hier auch Merkmale Dritter erhoben werden, die nicht im Zusammenhang mit der eigentlichen ESF-Förderung stehen. Die Bundesregierung sollte hier eine Änderung des entsprechenden EU-Rechtes anstreben, entweder indem diese Erhebung gestrichen oder zumindest ein Auskunftsverweigerungsrecht eingeräumt wird. Künftig ist bei Rechtsetzungsverfahren der EU stets zu hinterfragen, wofür die Daten erforderlich sind. Ein blindes Sammeln sensibler Daten ist zu vermeiden.

9.5 Ist die Regelung zur wissenschaftlichen Forschung im SGB X noch zeitgemäß?

Häufig werde ich bei Forschungsprojekten um Beratung gebeten, in denen Sozialdaten wissenschaftlich ausgewertet werden sollen. In vielen Fällen sollen bereits von Sozialleistungsträgern übermittelte Daten für weitere Projekte genutzt, in anderen regelmäßig Daten von Sozialleistungsträgern in eine Forschungsdatenbank übermittelt werden.

Sozialdaten unterliegen einem besonderen Schutz. Daher sieht § 75 SGB X für ihre Übermittlung zu Zwecken wissenschaftlicher Forschung besondere Reglungen vor. So haben die Sozialleistungsträger nach § 75 Absatz 2 SGB X vor der Übermittlung an Wissenschaftler oder wissenschaftliche Einrichtungen die Genehmigung der zuständigen obersten Bundes- oder Landesbehörde einzuholen. Mit dem 2. SGB-Änderungsgesetz vom 13. Juni 1994 (BGBl. 1229) wurden in die Vorschrift die Wörter „für ein bestimmtes Vorhaben“ eingeführt, was die Anwendung dieser Norm auf konkrete Projekte beschränken sollte. Dies soll eine generelle Übermittlung zu Forschungszwecken ebenso ausschließen, wie das Sammeln von Sozialdaten auf Vorrat, um sie bei Gelegenheit für ein Forschungsvorhaben zu nutzen. Im Großen und Ganzen hat sich die Regelung in den letzten zwanzig Jahren bewährt.

Gleichwohl wird in den Ländern und in der Wissenschaft Bedarf für eine Modernisierung des § 75 SGB X gesehen, da diese Regelung die Nutzung von Sozialdaten zu gesellschaftlich erwünschter und notwendiger langfristiger Forschung und zum Aufbau von Forschungsdatenbanken verhindere. Weiterhin wird eingewandt, die Regelung führe nach einer vergleichsweise kurzen Zeit zur Vernichtung von für die Forschung wertvollen Daten und setze zudem voraus, dass stets im Vorhinein präzise und abschließend ein nicht mehr veränderbares Forschungsprojekt definiert werden könne. Dies stimme aber weder mit dem heutigen Forschungsalltag überein, noch würden die Fortschritte in der IT-Sicherheit berücksichtigt.

§ 75 SGB X ist zu einer Zeit entstanden, in der die Daten der Sozialleistungsträger noch weitgehend in Papierform vorlagen. Auf Seite der Wissenschaft haben sich durch den technischen Fortschritt die Möglichkeiten der wissenschaftlichen Auswertung von Daten erheblich verändert. Im Gegensatz zu der Zeit als die Vorschrift des § 75 SGB X entstanden ist, liegen die Sozialdaten heute nahezu ausnahmslos elektronisch vor und können auch mit neueren Methoden ausgewertet werden. Dazu gehören etwa auch Big-Data-Anwendungen (vgl. auch Nr. 2.2), die es ermöglichen, riesige Datenbestände wissenschaftlich auszuwerten. Dies hat zum Entstehen von Forschungsdatenbanken geführt, die es erlauben, deutlich mehr wissenschaftliche Fragen zu beantworten als früher. Insbesondere die epidemiologische Forschung hat erhebliche Fortschritte gemacht. Nachdem es in den 1990er Jahren zu Betrugsfällen in der Forschung kam, haben zudem die „Empfehlungen der Deutschen Forschungsgemeinschaft zur Sicherung guter wissenschaftlicher Praxis“ aus dem Jahre 1998 für die Wissenschaft ein flächendeckendes System der Selbstkontrolle eingeführt. So müssen die Rohdaten, mit denen die Forschungsergebnisse erzielt wurden, nach Abschluss des Forschungsprojektes zehn Jahre aufbewahrt werden, um im Zweifelsfall die gefundenen Forschungsergebnisse reproduzieren zu können.

Bei einer möglichen Novellierung der sozialrechtlichen Forschungsvorschrift müssen neben diesen Gegebenheiten aber auch die berechtigten Interessen des Einzelnen geschützt werden, seine zum Teil sehr sensiblen Daten nicht ungeschützt Dritten zu überlassen. Es gibt hier verschiedene Lösungsmöglichkeiten, etwa den Wissenschaftlern nur pseudonymisierte Daten für die Forschung zur Verfügung zu stellen, die keinen Bezug zu einer einzelnen Person mehr zulassen. Die Pseudonymisierung erfolgt bei einer von dem wissenschaftlichen Institut unabhängigen Stelle (Vertrauensstelle), die dabei hinreichend und dem Stand der Technik entsprechend vorgeht. Derartige Lösungen sind auch dafür geeignet, um Langzeitstudien verwirklichen zu können. Die jetzige gesetzliche Regelung lässt derartige Lösungen nicht immer zu.

Ich empfehle dem Gesetzgeber, eine Änderung des § 75 SGB X herbeizuführen, die sowohl die Interessen der Wissenschaft als auch die Rechte der betroffenen Bürgerinnen und Bürger angemessen berücksichtigt.

9.6 Plötzlich Mitarbeiter der Berufsgenossenschaft - die merkwürdige Rolle der sog. beratenden Ärzte in der Unfallversicherung

Vielen Versicherten werden weiterhin die in § 200 Absatz 2 SGB VII genannten Rechte verwehrt. Entgegen den Beteuerungen des zuständigen BMAS hat sich die bisherige Umsetzung durch die Unfallversicherungsträger nicht bewährt.

Seit Inkrafttreten des § 200 Absatz 2 SGB VII zum 1. Januar 1997 habe ich immer wieder darüber berichtet, dass die Unfallversicherungsträger diese Vorschrift in vielen Fällen so auslegen, dass die dort genannten Rechte den Versicherten nicht oder nur unzureichend gewährt werden (zuletzt in meinem 24. TB Nr. 14.4.1). Auch die in vielen datenschutzrechtlichen Fragen grundsätzlichen Urteile des Bundessozialgerichts vom 5. Februar 2008 - B 2 U 8/07 R und B 2 U 10/07 R - haben nicht zu einer Klarstellung des § 200 Absatz 2 SGB VII geführt, da in wichtigen Fragen breite Interpretationsspielräume offen gelassen wurden (vgl. 22. TB Nr. 10.3.1 und 24. TB Nr. 11.41.1). Insbesondere durch den Einsatz sog. beratender Ärzte sind die Verfahren in der gesetzlichen Unfallversicherung intransparent geworden. Die Unfallversicherungsträger holen ärztliche Voten ein, die sich in den Auswirkungen als Beweismittel in den Verfahren kaum von richtigen Gutachten unterscheiden, aber aufgrund der rechtlichen Einordnung den Versicherten die in § 200 Absatz 2 SGB VII genannten Rechte verwehren können.

Die Gutachterregelung des § 200 Absatz 2 SGB VII ist nur dann anwendbar, wenn eine „Übermittlung“ der Daten des Versicherten an einen „Gutachter“ stattfindet. Bei Ärzten, die eine vertragliche Bindung zu einem Unfallversicherungsträger im Hinblick auf eine Beratungstätigkeit oder Zusammenarbeit haben, sollen hingegen kein Gutachterauftrag und vor allem keine Übermittlung vorliegen. Diese „beratenden Ärzte“ gelten nach Auffassung aller Unfallversicherungsträger als „Mitarbeiter“ der jeweiligen Verwaltungen. Wird der „Mitarbeiter“ beauftragt, ein sachverständiges Votum zu dem gesamten Verfahren eines Versicherten abzugeben, das er als

„beratende Stellungnahme“ bezeichnet, handelt es sich nach Auffassung der Unfallversicherungsträger um eine interne Datennutzung. Diese dürfe stets erfolgen, ohne dass dem Versicherten zuvor mehrere Gutachter zur Auswahl benannt werden müssten, er selbst einen Gutachter vorschlagen dürfe oder er auf sein Widerspruchsrecht gegen die Übermittlung seiner Daten hingewiesen werden müsse. Mit dieser Auslegung wird die Absicht des Gesetzgebers konterkariert, der mit der Regelung des § 200 Absatz 2 SGB VII ausdrücklich die Erwartung verbunden hat, die Transparenz der Verfahren zu verbessern (Bundestagsdrucksache 13/4853, S. 22). Es besteht die Gefahr, dass die Rechte der Versicherten ausgehöhlt und unterlaufen werden, obwohl die „beratende Stellungnahme“ regelmäßig in den Verwaltungs- und Gerichtsverfahren wie ein Gutachten als Beweismittel eingesetzt wird.

Die Transparenz der unfallversicherungsrechtlichen Verfahren leidet insbesondere dadurch, dass ein Versicherter über den Einsatz des beratenden Arztes nicht einmal informiert werden muss. Häufig sieht er sich in seinem Verfahren völlig überraschend mit dem Votum eines Sachverständigen konfrontiert. In einem mir bekannt gewordenen Fall wurden einem „beratenden Arzt“, der in einer Klinik arbeitet, die Krankenunterlagen eines Versicherten zugeleitet, obwohl dieser jeder Übermittlung seiner Daten ausdrücklich widersprochen hatte. Der Arzt hatte sodann zur Erstellung seiner Ausarbeitung mehrere Mitarbeiter der Klinik eingeschaltet und ihnen die Daten des Versicherten bekannt gegeben. Auch dies hält der Unfallversicherungsträger durch den Vertrag mit dem Beratungsarzt für gedeckt, da dieser in die Lage versetzt werden müsse, seine Arbeit auszuführen.

Der Auffassung der Unfallversicherungsträger folgend, dass beratende Ärzte als „Teil der Verwaltung“ ansehen sind, habe ich Kontrollen bei zwei Beratungsärzten durchgeführt. Wie sich dabei zeigte, hatten die jeweiligen Unfallversicherungsträger keine Regelung für eine Abschottung der Daten der Versicherten von den Daten anderer Patienten des beauftragten Arztes getroffen. Es bestanden auch keine Vorgaben für die verwendeten Server, Sicherheitsregelungen für die Praxissysteme oder Löschungskonzepte. Ein beratender Arzt lehnte eine Prüfung seiner EDV vollständig ab. Die Berufsgenossenschaft Handel und Warendistribution wurde daraufhin beanstandet. Bei einem beratenden Arzt der Berufsgenossenschaft Holz und Metall sowie bei einem beratenden Arzt der Berufsgenossenschaft der Bauwirtschaft und der Berufsgenossenschaft Rohstoffe und chemische Industrie wurden die gleichen Mängel festgestellt. Von einer Beanstandung wurde zunächst nur abgesehen, da zugesagt wurde, die festgestellten Mängel abzustellen.

Die Unfallversicherungsträger zeigten sich von den Kontrollen bei ihren „Mitarbeitern“ alles andere als erfreut. Sie haben mir gegenüber zum Ausdruck gebracht, dass sie meine Zuständigkeit für die datenschutzrechtliche Kontrolle der beratenden Ärzte als nicht gegeben sehen, obwohl sie stets die Auffassung vertreten, diese Sachverständigen seien „Teil der Verwaltung“, wenn es um die Anwendbarkeit des § 200 Absatz 2 SGB VII geht.

Ich empfehle dem Gesetzgeber, eine klarstellende Änderung des § 200 Absatz 2 SGB VII auf den Weg zu bringen, damit eine Umgehung des Regelungsgehalts zum Nachteil der Versicherten künftig ausgeschlossen ist.

9.7 Gemeinsame Servicestellen der Rehabilitationsträger

Für diese zentralen Anlaufstellen für Versicherte bei Fragen zur Rehabilitation bestehen noch keine datenschutzrechtlichen Regelungen.

Bei der Einfügung des Rechts der Rehabilitation und Teilhabe in das Sozialgesetzbuch (als SGB IX) wurden gemeinsame Servicestellen nach §§ 22 ff. SGB IX als zentrale Anlaufstellen für Versicherte bei allen Fragen zur Rehabilitation eingerichtet. Aufgabe der gemeinsamen Servicestellen ist eine umfassende, qualifizierte und individuelle Beratung behinderter oder von Behinderung bedrohter Menschen sowie deren Angehörigen. Diese Aufgaben nehmen die Rehabilitationsträger (gesetzliche Krankenkassen, gesetzliche Rentenversicherungsträger, gesetzliche Unfallversicherungsträger, Agenturen für Arbeit, Träger der Kriegsopferversorgung und Kriegsopferfürsorge und öffentliche Jugend- oder Sozialhilfeträger) trägerübergreifend wahr. Eine Servicestelle ist dabei organisatorisch jeweils einem Rehabilitationsträger zugeordnet. In Kooperation und Koordination mit den betei-

ligten Rehabilitationsträgern gewährleistet die Bundesarbeitsgemeinschaft für Rehabilitation (BAR) durch „Gemeinsame Empfehlungen“, dass die Leistungen der Rehabilitation nach gleichen Grundsätzen zum Wohle der behinderten und von Behinderung bedrohten Menschen durchgeführt werden. In einem Turnus von drei Jahren wird über die Tätigkeiten der BAR und die Arbeit der Servicestellen berichtet. Für den Berichtszeitraum vom 1. Juli 2010 bis zum 30. Juni 2013 gab die BAR eine Steigerung der Beratungsfälle in den Servicestellen auf über 30.000 Fälle an.

Dies habe ich zum Anlass genommen, stichprobenhaft die Arbeitsweise von zwei Servicestellen zu prüfen. Da das SGB IX keine eigenen Datenerhebungs- oder Datenverarbeitungsbefugnisse enthält, können in den Servicestellen Daten nur nach den bereichsspezifischen Regelungen des jeweiligen Sozialgesetzbuches erhoben, verarbeitet oder genutzt werden. Meine Informationsbesuche der Servicestelle galten einer Berufsgenossenschaft und der Servicestelle einer Krankenkasse in Berlin, um vor Ort Informationen über die Einhaltung datenschutzrechtlicher Regelungen bei den Tätigkeiten der Servicestellen zu erhalten. Die Servicestellen hatten von der BAR ein Dokumentationsformular zur Verfügung gestellt bekommen, in dem persönliche Daten (Name, Geburtsdatum, Geschlecht), Art der Leistung, Grund für die Einschaltung der gemeinsamen Servicestelle sowie die Beratungsschwerpunkte und betroffenen Rehabilitationsträger vermerkt werden können. Wieso dieser Personenbezug für statistische Erhebungen erforderlich sein soll, ist aus datenschutzrechtlicher Sicht jedoch nicht erkennbar. Auch fehlt noch eine Regelung zur Löschung der erhobenen personenbezogenen Daten.

Ich werde weiterhin mit der BAR in Kontakt bleiben und mich für eine datenschutzgerechte Handhabung der Verfahren bei den gemeinsamen Servicestellen einsetzen.

9.8 Erhebung von Daten aus den Reha-Entlassungsberichten

Die Deutsche Rentenversicherung (DRV) Bund sieht jetzt die Bekanntgabe von Reha-Entlassungsberichten von privaten Rehabilitationseinrichtungen oder von Reha-Einrichtungen anderer Rentenversicherungsträger als Datenübermittlung und nicht mehr als interne Weitergabe an. Dies stützt auch die Rechte der Versicherten.

Wer einen Reha-Entlassungsbericht erhalten darf, hat mich bereits in den letzten Jahren beschäftigt (vgl. 22. TB Nr. 10.4). Bisher ging die DRV Bund davon aus, nicht eigene Reha-Einrichtungen, in denen die Versicherten behandelt wurden, würden lediglich im Wege der Datenverarbeitung im Auftrag für die DRV Bund als verantwortlicher Stelle tätig. Infolgedessen wäre die Übersendung von Reha-Entlassungsberichten durch die Reha-Einrichtungen an sie keine Datenübermittlung, da der Auftragnehmer bei der Datenverarbeitung im Auftrag kein Dritter ist (§ 3 Abs. 8 Satz 3 BDSG, § 67 Abs. 10 Satz 3 SGB X). Deswegen sei die Weitergabe der Unterlagen an die DRV Bund auch ohne Einwilligung des Versicherten zulässig. Diese Auffassung hat die DRV Bund nun aufgegeben. Wie sie zu Recht annimmt, steht bei der Behandlung von Versicherten (Rehabilitanden) in den privaten Rehabilitationseinrichtungen (Vertragseinrichtungen) die medizinische Behandlung des Patienten im Vordergrund, die in eigener Regie und Verantwortung erfolgt. Es handelt sich nicht um unselbständige Hilfstätigkeiten bei der Datenverarbeitung im Sinne des § 80 SGB X oder des § 11 BDSG, es liegt also keine Datenverarbeitung im Auftrag vor.

Damit unterliegt der Datenverkehr zwischen der DRV Bund und der Vertragseinrichtung den gesetzlichen Vorgaben für eine Datenübermittlung. Soweit die privaten Vertragseinrichtungen während der Reha-Maßnahme weitere personenbezogene Daten zur Erbringung der Reha-Maßnahme und zur Erfüllung der ärztlichen Dokumentationspflicht erheben, handelt es sich überwiegend um medizinische Daten und damit um besondere Arten personenbezogener Daten nach § 3 Absatz 9 BDSG. Ein Teil dieser von den Vertragseinrichtungen erhobenen personenbezogenen Daten fließt in den Reha-Entlassungsbericht ein. Dieser wird von der privaten Vertragseinrichtung für die DRV Bund als Reha-Träger im Rahmen seiner Beauftragung nach § 97 SGB X erstellt und nach § 28 i. V. m. § 39 BDSG an sie übermittelt. Insbesondere darf die Vertragseinrichtung Gesundheitsdaten des Versicherten im Reha-Entlassungsbericht nach § 28 Absatz 7 Satz 1 BDSG an den Reha-Träger übermitteln.

Soweit die Reha-Einrichtung in der Trägerschaft eines anderen Rentenversicherungsträgers steht, ist sie Teil dieser verantwortlichen Stelle, bei der sowohl die von der DRV Bund ursprünglich übermittelten als auch die im Rahmen der Durchführung der Reha-Maßnahme hinzugekommenen Daten Sozialdaten sind. Hier gilt, dass die Übermittlung von Sozialdaten nur zulässig ist, wenn die Voraussetzungen des § 35 SGB I in Verbindung mit §§ 67 ff. SGB X vorliegen. Bei diesen Reha-Einrichtungen ergibt sich die Befugnis zur Übermittlung von Reha-Entlassungsberichten aus § 69 Absatz 1 Nummer 1 3. Alternative SGB X, da die Datenübermittlung zur Erfüllung einer gesetzlichen Aufgabe der empfangenden Stelle - hier zur Erbringung von Leistungen zur Teilhabe im Sinne des § 23 Absatz 1 Nummer 1 Buchstabe a SGB I i. V. m. § 15 Absatz 1 SGB VI - erfolgt. Darüber hinaus lässt § 67b Absatz 1 Satz 2 i. V. m. § 67a Absatz 1 Satz 2 bis 4 SGB X die Übermittlung medizinischer Sozialdaten ohne Einwilligung der Betroffenen zu, sofern es sich um eine Übermittlung zwischen den Trägern der gesetzlichen Rentenversicherung handelt und zu deren gesetzlicher Aufgabenerfüllung erforderlich ist.

Einer besonderen Einwilligung des betroffenen Versicherten bedarf es daher weder für den Fall, dass der Reha-Entlassungsbericht von einer privaten Vertragseinrichtung, noch für den Fall, dass er von einer Reha-Einrichtung eines anderen Rentenversicherungsträgers übermittelt wird.

9.9 OMS - Optimierte Meldeverfahren in der Sozialen Sicherung

In Einzelfällen konnten beim Projekt OMS datenschutzrechtliche Lösungen erarbeitet werden. Es fehlte aber der Mut, auch grundsätzliche Fragen anzugehen.

Bereits im 24. Tätigkeitsbericht (Nr. 4.2.3) hatte ich über das Projekt OMS (Optimierte Meldeverfahren in der Sozialen Sicherung) berichtet und dabei befürchtet, angesichts der teilweise sehr kleinteilig ausgerichteten Fragestellungen könnte grundlegender Reformbedarf unberücksichtigt bleiben.

Ich selbst hatte als Optimierungsvorschlag die Angleichung der verschiedenen Einkommensbegriffe angeregt. Nach Auffassung des federführenden BMAS werde die grundsätzlich dahinter stehende Idee allerdings in bereits anderweitig betrachteten Optimierungsvorschlägen berücksichtigt. Gemeint ist offenbar der Vorschlag eines Data Dictionary, das sich u. a. zum Ziel gesetzt hat, gleiche Datensatz-Feldinhalte zu standardisieren. Das Data Dictionary ist ohne Zweifel ein wichtiger Meilenstein, der zur Vereinheitlichung der bestehenden und künftigen Datensatzbeschreibungen in den Verfahren der Sozialen Sicherung beitragen wird. Allerdings sehe ich derzeit speziell bei den Einkommensbegriffen noch keinen Fortschritt. Darüber hinaus gilt das Data Dictionary nur für den Bereich der Sozialversicherung. Daher wurde nicht geprüft, ob auch rechtsbereichsübergreifend eine Angleichung sinnvoll bzw. möglich ist, z. B. mit dem Entgeltbegriff im Steuerrecht.

Einige der bearbeiteten Optimierungsvorschläge hat sich die Bundesregierung bereits zu Eigen gemacht und etwa den Entwurf für ein SGB-IV-Änderungsgesetz (Bundestagsdrucksache 18/3699) vorgelegt. Darin ist geplant - in Anlehnung an das Projekt Bea (vgl. Nr. 23.8) - ein elektronisches Verfahren auch für Bescheinigungen einzuführen, mit denen das Zusammentreffen von Renten und Entgeltzahlungen der Versicherten festgestellt wird. Darüber hinaus wird erstmalig der gesamte Ablauf des Datentransfers zwischen Arbeitgebern und Sozialversicherungsträgern beschrieben, der bislang nicht gesetzlich definiert ist.

Es gab auch datenschutzrechtlich bedenkliche Vorschläge, wie etwa für bestimmte Verfahren eine monatliche Meldung einzuführen, in denen bislang nur anlassbezogen oder jährlich gemeldet wird. So sollte als erstannehmende Datenannahme- und Verteilstelle (DAV) eine „Super DAV“ eingeführt werden, die die monatlichen Meldungen für die jeweiligen Empfänger aufbereitet und an diese weiterleitet. Bei der monatlichen Meldung würden teilweise auch Daten übermittelt, die der Empfänger in vielen Fällen nicht regelmäßig oder erst zu einem späteren Zeitpunkt benötigt. Unter den Aspekten der Datensparsamkeit und der Erforderlichkeit ist eine solche Speicherung daher kritisch zu bewerten. Im Übrigen fehlte es an konkreten Aussagen zur IT-Sicherheit, zu Verantwortlichkeiten und Zugriffsberechtigungen, so dass der Vorschlag nicht weiter verfolgt wurde.

Dagegen wurde der Optimierungsvorschlag, die Nutzung von elektronischen Zertifikaten der Arbeitgeber im Bereich der Sozialversicherungsmeldungen auch für den Bereich der Steuererklärungen und umgekehrt zu ermöglichen, mit entsprechenden Vorkehrungen datenschutzkonform ausgestaltet. Dieser Optimierungsvorschlag zielt auf eine Wiederverwendung einmal erworbener digitaler Zertifikate für möglichst viele Einsatzfälle. Wesentlich bei der gemeinsamen Nutzung von Zertifikaten ist, dass dabei keine Personenkennzeichen des einen Verfahrens für das andere offenbart werden, weil dies sonst die Verknüpfung von Daten des Sozialversicherungswesens mit solchen des Steuerwesens ermöglichen würde.

Der Vorschlag, auch die elektronische Gesundheitskarte (eGK) zur Identifizierung im Sozialversicherungswesen einzusetzen, wurde als nicht umsetzbar bewertet. Die eGK enthält zur eindeutigen Identifizierung die Krankenversichertennummer, die bei einer sektorübergreifenden Nutzung offengelegt würde. Auch deshalb ist die Nutzung der eGK gemäß § 291a SGB V streng zweckgebunden; deswegen wäre allenfalls in der Kommunikation mit den Krankenkassen ein Einsatz der eGK denkbar, nicht jedoch im gesamten Sozialversicherungsbereich.

Ein weiterer Vorschlag sieht vor, zur Abwicklung der Umlageverfahren U1 (Entgeltfortzahlung im Krankheitsfall) und U2 (Ausgleich der finanziellen Belastungen aus dem Mutterschutz nach dem Gesetz über den Ausgleich der Arbeitgeberaufwendungen für Entgeltfortzahlung - Aufwendungsausgleichsgesetz - AAG) eine gemeinsame Stelle einzurichten. Mit § 8 Absatz 2 AAG hat der Gesetzgeber grundsätzlich den Krankenkassen die Möglichkeit gegeben, die Durchführung der ihnen nach dem AAG obliegenden Aufgaben auf eine andere Stelle zu übertragen. Damit soll das bis 2006 im Bereich des BKK-Landesverbandes Ost durchgeführte Verfahren, an dem ca. 60.000 Arbeitgeber und ca. 160 Krankenkassen teilnahmen, eine Rechtsgrundlage erhalten.

Bedenken habe ich allerdings dagegen, dass eine zentrale Stelle geschaffen werden soll, in der alle Arbeitsunfähigkeitsbescheinigungen (AU-Bescheinigungen) zusammenlaufen. Nach dem vorgeschlagenen Verfahren sollen die entsprechenden Daten anonymisiert sein, allerdings mit nur pseudonymisierten Angaben zu Arbeitgeber und Krankenkasse. Bei einem mittelständischen Unternehmen sind damit auch die AU-Daten lediglich pseudonymisiert, weil aufgrund der mitgelieferten Daten zu Arbeitgebern über das Pseudonym feststellbar ist, welcher Arbeitnehmer in welchem Zeitraum erkrankt bzw. im Mutterschutz war. Ich gehe daher davon aus, dass auch die AU-Daten insoweit angesichts der geringen Beschäftigtenzahlen in den weitaus meisten Betrieben als lediglich pseudonymisiert zu betrachten sind. Damit liegen personenbezogene Daten vor. Diese sind überdies dem Wesen nach Gesundheitsdaten und damit „besondere Arten“ von Daten im Sinne von § 3 Absatz 9 BDSG. Falls eine derartige zentrale Sammelstelle für AU-Daten geschaffen werden soll, müsste diese entsprechend rechtlich und technisch abgesichert sein.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Arbeitskreis Beschäftigtendatenschutz

B. Zudem von besonderem Interesse

Nr. 8.6, 19.1

10 Ausschuss für Ernährung und Landwirtschaft

10.1 Gute Zusammenarbeit mit dem Bundesministerium für Ernährung und Landwirtschaft

Im Berichtszeitraum habe ich das Bundesministerium für Ernährung und Landwirtschaft bei seinen Rechtsetzungsvorhaben datenschutzrechtlich beraten.

Datenschutz gelingt immer dann besonders gut, wenn ich von den zuständigen Stellen frühzeitig beteiligt werde und meine Empfehlungen im Rahmen vertrauensvoller Zusammenarbeit insbesondere in Rechtsetzungsvorhaben dann auch berücksichtigt werden.

Das BMEL verfolgt diesen Ansatz: So wurde ich beispielsweise bei dem mittlerweile im Bundesgesetzblatt verkündeten „Gesetz zum Erlass und zur Änderung von Vorschriften zur Durchführung unionsrechtlicher Vorschriften über Agrarzahlungen und deren Kontrollen in der Gemeinsamen Agrarpolitik“ bereits in einer frühen konzeptionellen Phase eingebunden, deutlich vor der förmlichen Beteiligung im Rahmen der entsprechenden Ressortabstimmung. Dieses Gesetz stellt die rechtlichen Rahmenbedingungen für die Abwicklung von EU-Hilfen an Landwirte auf eine neue Grundlage. Aufgrund meiner frühzeitigen Beteiligung konnte ich erreichen, dass in der in Artikel 2 dieses Gesetzes enthaltenen Novelle des „Gesetz über die Verarbeitung und Nutzung von Daten im Rahmen des Integrierten Verwaltungs- und Kontrollsystems nach den unionsrechtlichen Vorschriften für Agrarzahlungen“ datenschutzrechtliche Regelungen aufgenommen wurden. Das Gesetz enthält nunmehr abschließend festgelegte Datenkränze sowie die entsprechenden datenschutzrechtlichen Erhebungs-, Verarbeitungs-, Nutzungs- und Löschungsvorschriften sowie Zweckbindungsregeln.

10.2 Datenschutz und Transparenz gehen Hand in Hand

Veröffentlichung der Namen von Agrarsubventionsempfängern ist datenschutzgerecht umgesetzt.

Die Mitgliedstaaten der EU sind verpflichtet, die Begünstigten von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des Ländlichen Raumes (ELER) nachträglich im Internet zu veröffentlichen. Damit verfolgt die EU das Ziel, die Verwendung der EU-Gemeinschaftsmittel stärker zu kontrollieren sowie die Transparenz der Verwendung von Gemeinschaftsmitteln und die Öffentlichkeitswirkung und Akzeptanz der Europäischen Agrarpolitik zu verbessern.

Der EuGH hatte mit Urteil vom 9. November 2010 (Az. C-92/09, C-93/09) die Veröffentlichung von Agrarsubventionsempfängern bei juristischen Personen für uneingeschränkt zulässig erklärt. Bei natürlichen Personen hielt er deren Veröffentlichung grundsätzlich zwar ebenfalls für zulässig. Der Gerichtshof hatte dabei allerdings moniert, die Veröffentlichung personenbezogener Daten sei hinsichtlich aller Empfänger vorgeschrieben, ohne nach einschlägigen Kriterien wie den Beihilfe-Zeiträumen, der Häufigkeit oder auch Art und Umfang dieser Beihilfen zu unterscheiden.

Mit den Artikeln 111 - 114 der EU-VO 1306/2013 ist die EU auf die gerichtlichen Vorgaben eingegangen und hat diese umgesetzt. Die auf zwei Jahre beschränkte Veröffentlichung enthält im Hinblick auf natürliche Personen folgende Informationen:

a) Vorname und Nachname;

b) die Gemeinde, in der der Begünstigte wohnt oder eingetragen ist, sowie gegebenenfalls die Postleitzahl bzw. den Teil der Postleitzahl, der für die betreffende Gemeinde steht;

c) für jede aus dem EGFL und aus dem ELER finanzierte Maßnahme die Beträge der Zahlungen, die der Begünstigte in dem betreffenden Haushaltsjahr erhalten hat;

d) Art und Beschreibung der aus dem EGFL bzw. dem ELER finanzierten Maßnahmen unter Angabe des Fonds, aus dem die Zahlungen gemäß Buchstabe c) gewährt werden.

Ausgenommen von der Veröffentlichung des Namens sind Begünstigte, deren Gesamtbeihilfebetrag aus beiden Fonds unterhalb eines Schwellenwertes von 1.250 EUR liegt. In diesem Fall erfolgt eine codierte Bekanntgabe des Begünstigten. Sollte die Identifizierung des Betroffenen dennoch (ausnahmsweise) möglich sein, werden die Informationen nur unter Angabe der nächstgrößeren kommunalen Verwaltungseinheit, zu der diese Gemeinde gehört, veröffentlicht und damit die Identifizierung verhindert.

Die Veröffentlichungspflicht besteht erstmals im Jahr 2015 für alle ab dem EU-Haushaltsjahr 2014 (16.10.2013-15.10.2014) getätigten Zahlungen aus den o. g. EU-Agrarfonds. Ich habe das Bundesministerium für Ernährung und Landwirtschaft sowohl bei seinen Verhandlungen auf europäischer Ebene als auch bei der Umsetzung der europäischen Vorgaben in nationales Recht beraten. Die vom Bundeskabinett mittlerweile beschlossene Novelle des Agrar- und Fischereifonds-Informationen-Gesetzes (Bundestagsdrucksache 18/4278) enthält von mir empfohlene Erhebungs-, Verarbeitungs- und Nutzungsregelungen sowie die Verpflichtung zur Löschung von Daten nach dem Ablauf des oben erwähnten zweijährigen Veröffentlichungszeitraums.

10.3 Datenschutz bei der Bundesanstalt für Landwirtschaft und Ernährung

Die Bundesanstalt für Landwirtschaft und Ernährung (BLE) hat meine Empfehlungen zur Erarbeitung eines Datenschutzkonzepts und zur Optimierung ihrer IT-Sicherheitsrichtlinie umgesetzt.

Bei einem Informations-, Beratungs- und Kontrollbesuch bei der zum Geschäftsbereich des Bundesministeriums für Ernährung und Landwirtschaft gehörenden BLE habe ich mir einen Überblick über den dortigen Umgang mit personenbezogenen Daten verschafft:

Die BLE stellte zum Zeitpunkt meines Besuchs erste Überlegungen zu einem Datenschutzkonzept an. Ich habe sie bei der Erarbeitung des Konzepts beraten und beispielsweise empfohlen, darin ein Löschkonzept zu verankern sowie Hinweise zum Umgang mit besonderen personenbezogenen Daten nach § 3 Absatz 9 BDSG zur Rechtslage bei Übermittlungen ins Ausland nach den §§ 4b und 4c BDSG aufzunehmen. Das mittlerweile vorliegende Datenschutzkonzept entspricht diesen Anforderungen. Ferner habe ich die BLE bei der Fortschreibung ihres IT-Sicherheitskonzepts unterstützt. Meine Empfehlungen wurden umgesetzt, so dass das Konzept jetzt den Anforderungen entspricht.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

11 Verteidigungsausschuss

11.1 Gesundheitsdaten in der Bundeswehr

Ein wesentlicher Schwerpunkt meiner Beratungs- und Kontrolltätigkeit bei der Bundeswehr betraf den Umgang mit Gesundheitsdaten. Hierzu hatten mich im Berichtszeitraum vermehrt Hinweise über datenschutzrechtliche Defizite erreicht.

11.1.1 Das Institut-Informationssystem des Zentrums für Luft- und Raumfahrtmedizin der Luftwaffe

Bei der Einführung eines IT-Verfahrens zur Verarbeitung besonders sensibler Gesundheitsdaten durch die Bundeswehr wurde gegen datenschutzrechtliche Grundsätze verstoßen.

Im Berichtszeitraum erhielt meine Dienststelle einen Hinweis auf ein bei dem Zentrum für Luft- und Raumfahrtmedizin der Luftwaffe (ZentrLuRMedLw) der Bundeswehr eingesetztes IT-Verfahren. Dort wird ein Institut-Informationssystem (IIS) betrieben, in dem Gesundheitsdaten von ca. 60.000 Piloten über die Tauglichkeitsuntersuchungen zum Führen eines Luftfahrzeugs (im militärischen Sprachgebrauch Wehrfliegerverwendungsfähigkeit) gespeichert sind. Die Datenbank enthält nicht nur Einträge von aktiven und ehemaligen Piloten der Bundeswehr, sondern auch von zivilen Luftfahrzeugführern, da das ZentrLuRMedLw aufgrund seiner fachlichen Kompetenz als Flugmedizinisches Begutachtungszentrum auch Untersuchungsaufträge aus dem zivilen Bereich übernimmt.

Die Bundeswehr entschied sich dazu, das IT-Verfahren IIS auch den Fliegerärzten seiner fliegenden Verbände außerhalb des Zentrums zur Verfügung zu stellen, denen die Überwachung der Wehrfliegerverwendungsfähigkeit der Piloten in den Einsatzverbänden obliegt. Bei der Ausbildung des medizinischen Personals der Fliegerarztstellen wurde der vollständige Inhalt der Datenbank zu Übungszwecken gespiegelt. In der Schulungsdatenbank sollte das medizinische Personal den Umgang mit dem IT-Verfahren an echten Probandendatensätzen üben, ohne dabei die Datensätze der Produktivversion ändern zu können. In einem Fall wurde dem Personal einer Fliegerarztstelle sogar das Üben in der Schulungsdatenbank über einen Administratorenzugang gewährt. Damit konnte das Personal der Fliegerarztstelle nicht nur Zugriff auf die Probandendatensätze der Piloten des eigenen Verbandes, sondern auf den gesamten Datenbestand der Schulungsdatenbank mit echten Gesundheitsdaten militärischer und ziviler Piloten nehmen. Dies stellt einen Verstoß gegen das Zweckbindungsgebot von Personalaktendaten dar.

Unmittelbar nach der Feststellung dieser umfassenden Zugriffsmöglichkeit und der Information der behördlichen Datenschutzbeauftragten in der Bundeswehr (BfDBw) hat diese im Rahmen einer eigenen Kontrolle empfohlen, den Zugang zur Schulungsdatenbank zu unterbinden und diese zu löschen. Dem ist das ZentrLuRMedLw nachgekommen. Von einer Beanstandung habe ich deshalb abgesehen.

Bei einer anschließenden gemeinsamen Kontrolle meiner Mitarbeiter und der BfDBw im ZentrLuRMedLw Köln/Wahnheide habe ich festgestellt, dass das IT-Verfahren IIS bei seiner Inbetriebnahme entgegen den gesetzlichen Bestimmungen der BfDBw weder zur Vorabkontrolle vorgelegt, noch in das Verfahrensverzeichnis des ZentrLuRMedLw aufgenommen worden war. Wichtige verfahrensbezogene Dokumente wie das IT-Sicherheitskonzept sowie das Rollen- und Berechtigungskonzept waren jahrelang nicht fortentwickelt und dem aktuellen Stand angepasst worden. Diese Verstöße habe ich gegenüber dem Bundesministerium der Verteidigung förmlich beanstandet.

In einem zweiten Schritt haben meine Mitarbeiter die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes beim Einsatz des IT-Verfahrens IIS im Standort Fürstenfeldbruck des Zen-

trLuRMedLw geprüft. Wie sich auch hier zeigte, wäre eine frühzeitige Einbindung der zuständigen Datenschutzbeauftragten wichtig gewesen, um die erforderlichen technischen und organisatorischen Maßnahmen für den Betrieb des IT-Verfahrens zu treffen. So wurde erst im Zuge der Datenschutzkontrollen damit begonnen, die Nutzer- und Rechteverwaltung zu überarbeiten, eine Dokumentation dieser Verwaltung einzuführen oder ein Löschkonzept für die im IT-Verfahren und in Papier gespeicherten Gesundheitsdaten zu entwickeln. Da das ZentrLuRMedLw meine Hinweise dankbar aufgegriffen und mit der Umsetzung bereits begonnen hat, habe ich von einer weiteren Beanstandung abgesehen.

11.1.2 Kontrolle des Instituts für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr

Bereits zu Beginn einer Archivierung medizinischer Unterlagen müssen die technischen und organisatorischen Maßnahmen getroffen werden, damit diese nach Ablauf der Archivierungsfrist vernichtet werden.

Im Jahr 2013 kontrollierten meine Mitarbeiter das Institut für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr in Andernach. Das Institut ist die zentrale Einrichtung der Bundeswehr für die Langzeitaufbewahrung von Gesundheitsunterlagen und nach eigenen Angaben das wohl größte Krankenarchiv Deutschlands. Im Institut werden unter anderem die Gesundheitsunterlagen der gedienten Wehrpflichtigen, Gesundheits- bzw. Musterungsunterlagen der ungedienten und untauglichen Wehrpflichtigen und Freiwilligen, ärztliche Unterlagen über ambulante und stationäre Behandlungen und Untersuchungen in Sanitätszentren und Bundeswehrkrankenhäusern sowie betriebsärztliche Unterlagen von Soldaten und zivilen Bundeswehrbeschäftigten aufbewahrt.

Die eingehenden Unterlagen werden im Institut für die Archivierung aufbereitet. Sie werden zum Teil mikroverfilmt und im Übrigen im Original aufbewahrt. Bei der Verfilmung werden mehrere Gesundheitsunterlagen verschiedener Personen in der Reihenfolge ihres Eingangs aus unterschiedlichen Quellen und mit unterschiedlichen Archivierungsfristen jeweils auf einem Mikrofilm gespeichert. Eine im Institut geführte Fundstellendatenbank ermöglicht dabei, die einzelnen Gesundheitsunterlagen auf den Mikrofilmen wiederaufzufinden. Mit der Archivierung werden die gesetzlichen Speicherfristen erfüllt. Zudem können auch Auskünfte zu länger zurückliegenden ärztlichen Untersuchungen erteilt werden.

Bei ihrem Besuch stellten meine Mitarbeiter fest, dass die Beachtung der Archivierungsfristen und die Aussonderung der zu vernichtenden Unterlagen insbesondere bei den mikroverfilmten Dokumenten Schwierigkeiten bereitet.

So ist es nicht möglich, einzelne Gesundheitsunterlagen, deren Archivierungsfrist abgelaufen ist, auf den Mikrofilmen zu löschen. Denn ein Mikrofilm kann und darf nicht bereits dann vernichtet werden, wenn die Aufbewahrungsfrist für nur eine der dort abgefilmten Gesundheitsunterlagen abgelaufen ist. Entscheidend ist die Aufbewahrungsfrist derjenigen Dokumente, die die längste Aufbewahrungsfrist haben. Auch die Alternative, den Eintrag in der Fundstellendatenbank zu löschen, um damit ein Wiederauffinden der eigentlich zu löschenden Gesundheitsunterlage auf dem Mikrofilm zu verhindern, ist derzeit nach Angaben des Bundesministeriums der Verteidigung technisch noch nicht umsetzbar.

Während des Besuches haben mir die Mitarbeiter des Instituts glaubhaft versichert, sie würden keine Auskünfte aus Gesundheitsunterlagen geben, deren Archivierungsfristen abgelaufen seien.

Gleichwohl halte ich das derzeitige Verfahren für datenschutzrechtlich unzureichend.

Ich empfehle dem Bundesministerium der Verteidigung, eine technische Lösung zur Datenlöschung nach Ablauf der Archivierungsfristen entwickeln zu lassen.

11.1.3 Einzelfälle:

Versendung von Datenträgern mit Gesundheitsdaten

Ein Petent wurde in einem Bundeswehrkrankenhaus behandelt. Die Untersuchungsergebnisse wurden nach dem Ende der Behandlung auf eine CD gebrannt und sollten ihm per Post zugesandt werden. Der Versand erfolgte mit einfacher Post. Allerdings kam es dabei zu einer Verwechslung, denn in dem Briefumschlag befand sich nicht die CD mit seinen Untersuchungsergebnissen, sondern mit denen eines anderen Patienten. Die CD war mit dem Patientennamen, dem Geburtsdatum sowie Angaben zur Untersuchung gekennzeichnet. Auf seine Beschwerde beim Bundeswehrkrankenhaus hin sei ihm mitgeteilt worden, er solle die fälschlich zugesandte CD einfach wegwerfen. Er würde eine neue CD mit den eigenen Daten erhalten. Aber auch der Versand der zweiten CD war fehlerhaft. Sie wurde nämlich nicht dem Petenten unmittelbar, sondern seiner früheren Dienststelle übermittelt. Der Petent war zu diesem Zeitpunkt bereits seit mehr als zehn Jahren pensioniert. Erst mein Tätigwerden führte dazu, dass der Petent seine CD erhielt, die fälschlich zugesandte CD des anderen Patienten abgeholt und dieser vom Bundeswehrkrankenhaus über die fehlerhafte Versendung informiert wurde.

Darüber hinaus wurden die Angehörigen der betroffenen Fachabteilung des Bundeswehrkrankenhauses nochmals über ihre datenschutzrechtlichen Pflichten belehrt. Das Bundeswehrkrankenhaus wird die Versendung von Gesundheitsdaten an Privatadressen künftig restriktiv handhaben und Gesundheitsunterlagen nur noch per Einschreiben mit Rückschein versenden.

Zu meinem Bedauern konnte das Bundeswehrkrankenhaus jedoch nicht mehr abschließend aufklären, ob die erste CD mit den Gesundheitsdaten des Petenten ebenfalls an einen falschen Adressaten abgesandt oder ein Versand vergessen worden war.

Führt die Bundeswehr in Auswahlverfahren Schwangerschaftstests durch?

Mir wurde berichtet, bei den Einstellungsuntersuchungen zum Auswahlverfahren bei der Bundeswehr würden auch Schwangerschaftstests durchgeführt. Weibliche Bewerber, deren Schwangerschaftstest positiv ausfalle, seien vom weiteren Bewerbungsverfahren ausgeschlossen. Daraufhin habe ich das Einstellungsverfahren bei der Bundeswehr einer Prüfung unterzogen.

Wie ich dabei allerdings feststellen konnte, wird im Eignungsfeststellungsverfahren weder nach Schwangerschaften der Bewerberinnen gefragt noch gezielt nach Frühschwangerschaften gesucht. Es ist auszuschließen, dass bei der Bundeswehr gezielt Daten über Schwangerschaften im Einstellungsverfahren erhoben werden.

Kasten zu Nr. 11.1.3

Eignungsfeststellungsverfahren

Das Eignungsfeststellungsverfahren verläuft in mehreren Schritten. Zu Beginn des Verfahrens nehmen die Bewerberinnen und Bewerber gemeinsam an einem Einführungsvortrag teil. Dabei erläutert der Prüfoffizier, was auf die Kandidaten an sportlichen Aktivitäten zukommt (Sporttest, Herz-Kreislaufprüfung unter Belastung - Ergometrie). Vollständigkeitshalber wird auch auf die möglichen fruchtschädigenden Einflüsse und deren Folgen bei Fortführung der Eignungsfeststellung aufmerksam gemacht. Nach dieser Ersteinführung erhalten alle Bewerberinnen ein dreiseitiges Formblatt mit der Bitte, dieses im Ärztlichen Dienst abzugeben. Damit werden die Bewerberinnen zu Beginn des Eignungsfeststellungsverfahrens aktenkundig darüber belehrt, dass die Feststellung der Verwendungsfähigkeit für militärische Anforderungen durch eine bestehende Schwangerschaft erschwert oder unmöglich gemacht werden könnte. Mit diesem Formblatt bestätigen die Bewerberin-

nen, dass sie die Belehrung zur Kenntnis genommen habe. Die Hinweise im Einführungsvortrag und in dem Formblatt dienen ausschließlich dem Schutz der Bewerberinnen und der ungeborenen Kinder. Soweit eine Bewerberin eine Schwangerschaft offenbart oder diese als Nebenbefund bei der ärztlichen Untersuchung festgestellt wird, erhält nur der Ärztliche Dienst Kenntnis davon. Die seitens der Bewerberin gemachten Angaben unterliegen ebenso wie die Dokumentation in den Gesundheitsunterlagen, die ausschließlich beim Ärztlichen Dienst geführt werden, der ärztlichen Schweigepflicht. Unbefugte Personen haben keinen Zugriff auf diese Daten.

Außerhalb des Ärztlichen Dienstes können keine Rückschlüsse auf eine Schwangerschaft von Bewerberinnen gezogen werden. Sollte eine Schwangerschaft festgestellt worden sein und die Bewerberin aus diesem Grunde die Eignungsfeststellung abbrechen, wird dieser Grund weder vermerkt, noch der Prüfgruppe zur Kenntnis gegeben. Sollte die Bewerberin die Eignungsfeststellung trotz bestehender Schwangerschaft fortsetzen wollen, so wird das Eignungsfeststellungsverfahren ohne Sporttest durchgeführt. Der Ärztliche Dienst teilt nur mit, der Sporttest könne aus gesundheitlichen Gründen nicht durchgeführt werden. Dies entspricht dem allgemein üblichen Verfahren bei allen gesundheitlichen Ausschlussgründen von Bewerberinnen und Bewerbern für den Sporttest. Eine Wiederholung des Sporttests ist zu einem späteren Zeitpunkt ohne Nachteile möglich.

11.2 Mobiles Geschütztes Fernmeldeaufklärungs-System der Bundeswehr - Testeinsatz in Daun

Befürchtungen über eine Aufzeichnung ziviler Kommunikation durch die Bundeswehr konnten zerstreut werden.

Die Bundeswehr beabsichtigt, ein neues mobiles Fernmeldeaufklärungssystem für den Einsatz in Krisengebieten zu beschaffen. Zu Testzwecken wurden dafür im Oktober 2013 drei Fahrzeuge der Bundeswehr mit dem System ausgestattet.

Insbesondere die Herstellerangaben über die Leistungsfähigkeit des Systems haben in der Öffentlichkeit für Aufregung gesorgt. Es wurde die Befürchtung geäußert, mit dem eingesetzten System könne die Bundeswehr auch während der Tests jeglichen Funkverkehr im Testgebiet auslesen und damit auch Handygespräche abhören sowie private und geschäftliche E-Mails lesen.

Ich habe dies zum Anlass genommen, das mobile Fernmeldeaufklärungssystem am Bundeswehrstandort Daun in der Eifel zu kontrollieren. Dabei konnte ich feststellen, dass das Testsystem keine zivile Kommunikation erfasst. Die in Daun vorgesehenen Tests wurden ausschließlich auf militärischen Frequenzen durchgeführt. Die Bundeswehr hatte durch technische und organisatorische Vorkehrungen den Empfang regulärer ziviler Kommunikation ausgeschlossen. Sollten Bürger dagegen missbräuchlich über die Funkfrequenzen der Bundeswehr miteinander kommunizieren, greifen diese technischen und organisatorischen Vorkehrungen allerdings nicht. Für solche Fälle hat die Bundeswehr Vorkehrungen getroffen, solche als Beifang bezeichneten Daten unverzüglich zu löschen.

Eine datenschutzrechtliche Gefährdung der Bevölkerung durch den Testeinsatz konnte ich nicht feststellen. Gleichwohl beabsichtige ich, die verschiedenen Entwicklungsphasen des Mobilen Geschützten Fernmeldeaufklärungs-Systems weiterhin zu begleiten.

11.3 Überraschende Kontrolle bei der Wehrbereichsverwaltung Nord in Hannover

Durch die Kooperation der Dienststelle konnten die festgestellten Datenschutzverstöße bereits während des Kontrollbesuchs beseitigt werden.

Durch eine Eingabe erfuhr ich 2013, Soldaten- und Personalakten wurden in nicht verschlossenen Schränken in Kopierräumen bei der Wehrbereichsverwaltung Nord (WBV Nord) aufbewahrt. Diese sensiblen Daten wurden nicht nur offen aufbewahrt, es hatten auch andere Dienststellen als die WBV Zugang zu den Räumen und damit zu den Akten. Ich habe unverzüglich nach Kenntnis einen Kontrollbesuch bei der WBV Nord in Hannover durchgeführt, bei dem erhebliche datenschutzrechtliche Mängel bei der Aufbewahrung personenbezogener Daten festgestellt wurden.

Die mir zugegangenen Informationen trafen zu: In mehreren unverschlossenen Räumen mit Kopier- und Faxgeräten habe ich in meist unverschlossenen Schränken Akten mit personenbezogenen Daten aus dem Personalbereich, dem Bereich der Familienkassen (Kindergeldakten) sowie Unterlagen aus dem Bereich der Aus- und Fortbildung (Bewerbungsunterlagen) vorgefunden. Die Aktenschränke stellten aufgrund ihrer Beschaffenheit auch in verschlossenem Zustand kein ausreichendes Zugriffshindernis dar, da sie ohne nennenswerten Kraftaufwand hätten geöffnet werden können. Zudem standen die Türen des Kopierraums regelmäßig offen. Kopierer und Faxgeräte in diesen Räumen waren betriebsbereit und boten so die Möglichkeit einer Vervielfältigung und Verbreitung der Daten. Hinzu kam, dass die Liegenschaft der WBV Nord noch von weiteren Dienststellen genutzt wurde und nur im Eingangsbereich eine zentrale Zugangskontrolle stattfand. Es hatten folglich auch die Mitarbeiter der anderen Dienststellen und deren Besucher Zugang zu den Kopierräumen. Dies stellte einen erheblichen Verstoß gegen datenschutzrechtliche Bestimmungen dar.

Öffentliche Stellen sind nach § 9 BDSG gehalten, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um eine unberechtigte Kenntnisnahme der bei ihr vorliegenden personenbezogenen Daten durch unbefugte Dritte zu verhindern. Die Anforderungen an den Schutz vor einer unbefugten Kenntnisnahme variieren und richten sich nach der Schutzbedürftigkeit der Daten. Bei den vorgefundenen Unterlagen handelte es sich um sensible und besonders geschützte Daten, zu denen ausschließlich die zuständigen Mitarbeiter der Personalstellen und Familienkasse Zugang hätten haben dürfen (vgl. § 29 Abs. 3 Soldatengesetz, § 30 Abgabenordnung, § 106 Abs. 1 und § 107 Bundesbeamtengesetz). Da die Dienststelle umgehend alle erforderlichen Maßnahmen ergriff, um den Datenschutzverstoß zu beseitigen und vergleichbare Verstöße künftig zu vermeiden, habe ich von einer Beanstandung abgesehen.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

B. Zudem von besonderem Interesse

Nr. 5.14.1

12 Ausschuss für Familie, Senioren, Frauen und Jugend

12.1 Onlinewahl beim Bundesfreiwilligendienst

Die Sprecherinnen und Sprecher des Bundesfreiwilligendienstes werden online gewählt. Dies ist auch eine datenschutzrechtliche Herausforderung.

Am 29. März 2013 ist die Verordnung zur Wahl der Sprecherinnen und Sprecher des Bundesfreiwilligendienstes in Kraft getreten. Diese sind Interessenvertreter der Bundesfreiwilligen. Sie werden jährlich über die Internetseite www.bundesfreiwillgendienst.de gewählt. Es handelt sich nach meiner Kenntnis um die erste gesetzlich geregelte Onlinewahl auf Bundesebene.

Eine Wahl über das Internet abzuwickeln, birgt auch datenschutzrechtliche Risiken. Denn wie bei einer Wahl in herkömmlicher Form müssen auch bei einer Onlinewahl sowohl die Wahlgrundsätze ausreichend berücksichtigt als auch das Recht auf informationelle Selbstbestimmung der Wählerinnen und Wähler geschützt werden.

Das Bundesministerium für Familie, Senioren, Frauen und Jugend hat im Rahmen des Verordnungsverfahrens viele von mir in meiner Beratungsfunktion gegebene Empfehlungen aufgegriffen. In einzelnen Punkten hätte ich mir jedoch strengere Regelungen zum Datenschutz gewünscht. So erfolgt die Kommunikation zwischen dem Wahlvorstand und den Wählerinnen und Wähler ausschließlich per E-Mail. Insbesondere für den Versand des Transaktionscodes hätte ich eine sicherere Übermittlungsform bevorzugt. Nach Wunsch des BMFSFJ sollte jedoch das gesamte Verfahren als reine Onlinewahl ausgestaltet werden.

Inzwischen haben die ersten Wahlen stattgefunden. Beschwerden haben mich dazu nicht erreicht. Gleichwohl behalte ich mir vor, das Wahlverfahren noch einer datenschutzrechtlichen Prüfung zu unterziehen.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

13 Ausschuss für Gesundheit

Auch in diesem Berichtszeitraum gab es zahlreiche Datenschutzprobleme im Bereich des SGB V. Zudem beginnen sich neue Problemfelder beim Umgang mit Versichertendaten durch die gesetzlichen Krankenkassen abzuzeichnen.

13.1 „Gesundheits-Apps“ der Krankenkassen

Die gesetzlichen Krankenkassen müssen beim Einsatz sogenannter Gesundheits-Apps die datenschutzrechtlichen Vorgaben beachten.

Zunächst nur am Rande haben mich die von verschiedenen Anbietern und teilweise auch von Krankenkassen zur Verfügung gestellten sogenannten Gesundheits-Apps beschäftigt, die sich die Versicherten bereitwillig auf ihre Smartphones und Tablets laden oder die sich auf sogenannten Smartwatches befinden. Smartwatches sind Armbanduhren, die über ein Display, Sensoren, die z. B. die Herzfrequenz erfassen, sowie zusätzliche Computerfunktionalitäten und Internetzugriff verfügen. Mit Hilfe dieser Gerätschaften übermitteln die Betroffenen „freiwillig“ zum Teil sehr sensible Gesundheitsdaten an unterschiedliche Stellen.

Nach einer Studie gab es in den USA im Sommer 2013 bereits mehr als 43.000 mobile Applikationen („Apps“), die den Themen Gesundheit und Fitness zuzuordnen waren. Ca. 23.000 Apps davon konnten unmittelbar als Gesundheits-Apps bezeichnet werden. Nach einer Online-Umfrage der IKK classic nutzen 22 Prozent der Bundesbürger über ihre Smartphones Medizin- oder Gesundheits-Apps. Auch bei den gesetzlichen Krankenkassen ist eine wachsendes Interesse an Gesundheits- und Fitnessdaten ihrer Versicherten zu beobachten. So sind mir zwei Fitness-Apps großer gesetzlicher Krankenkassen bekannt, die mit einem angebotenen Bonusprogramm gekoppelt sind. Hierbei werden zwar noch keine Gesundheitsdaten der Versicherten von den Krankenkassen über die App erhoben - die Kasse erhält lediglich die Meldung, dass eine bestimmte Anzahl von Bonuspunkten erreicht wurde, ohne Kenntnis, durch welche Aktivitäten/Maßnahmen die Bonusberechtigung ausgelöst wurde -, ein gewisses gesundheitsförderliches Verhalten wird bei der Bonusberechnung dennoch zumindest mittelbar transparent.

In einer nach deutschen Datenschutzstandards derart unsicheren Umgebung, mit der Apps verbunden sind, sollten sich Krankenkassen als Sozialversicherungsträger und Körperschaften des öffentlichen Rechts ihrer Verantwortung gegenüber den Versicherten bewusst sein. Zwar darf es einer Krankenkasse nicht verwehrt sein, moderne Medien zum Zwecke der Neukundenwerbung und Bestandskundenbindung zu nutzen. Aber ihre gesetzliche Verantwortung für die Sozialdaten ihrer Versicherten erstreckt sich auch auf eben diese Kommunikationswege, umso mehr als sich die Nutzer der Konsequenzen ihrer Aktivitäten und deren Adressaten vielfach nicht bewusst sind.

Überlegungen, mit Hilfe des Smartphones, eines Tablets oder einer Smartwatch mit einer integrierten Gesundheits-App den Krankenkassen den jeweiligen Fitnesszustand des Versicherten zu übermitteln, sehe ich daher sehr kritisch. Zu dem Argument, der Versicherte handele schließlich freiwillig, möchte ich darauf hinweisen, dass gesetzliche Krankenkassen für jegliche Form der Datenerhebung, -verarbeitung und -nutzung eine gesetzliche Grundlage benötigen. Zwar sieht das SGB V in vielen Bereichen vor, dem Versicherten freiwillig Leistungen einzuräumen, wenn dieser hierfür seine Daten bereitstellt. Wo es eine solche Regelung aber nicht gibt, bleibt im Bereich des SGB V für eine gesetzliche Krankenkasse keine Möglichkeit, (sensible) personenbezogene Daten auf freiwilliger Basis vom Versicherten zu erhalten.

Ich werde diese neueren Entwicklungen in den nächsten Jahren kritisch im Auge behalten.

13.2 Die elektronische Gesundheitskarte ist da - jetzt beginnt das Warten auf die Erprobung

Die elektronische Gesundheitskarte ist zwar flächendeckend ausgegeben, aber noch nicht in der Praxis erprobt. Auch die medizinischen Anwendungen lassen weiter auf sich warten.

„Der Datenschutz hat dabei höchste Priorität und wird durch rechtliche und technische Maßnahmen sichergestellt“ betont die Bundesregierung in ihrer Antwort auf eine Kleine Anfrage der Fraktion DIE LINKE zur Einführung der elektronischen Gesundheitskarte am 18. November 2014 (Bundestagsdrucksache 18/3225). Ob diese Aussage auch in der Praxis belastbar ist, wird sich in den nächsten Jahren erweisen.

Die Vergangenheit hat gezeigt, wie komplex der Aufbau einer Telematikinfrastruktur ist, die im ganzen Land ständig verfügbar sein, den höchsten Datenschutzansprüchen gerecht werden und gleichzeitig den Nutzern eine hohe Servicequalität bieten muss. Diese Aufgabe wurde den Organisationen der Selbstverwaltung im Gesundheitswesen gesetzlich übertragen, die hierfür 2005 die Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) gegründet haben. In den letzten Jahren wurden die elektronischen Gesundheitskarten mit Lichtbild nahezu flächendeckend an alle Versicherten ausgegeben und Kartenlesegeräte in Arzt- und Zahnarztpraxen sowie Krankenhäusern installiert. Ab dem 1. Januar 2015 gilt beim Arzt- und Zahnarztbesuch nur noch die elektronische Gesundheitskarte als Versicherungsnachweis und nicht mehr die Krankenversichertenkarte. Wie das Bundessozialgericht Ende 2014 entschieden hat, verletzen weder die Lichtbildpflicht noch der eingebaute Speicherchip die Patienten in ihrem Recht auf informationelle Selbstbestimmung (vgl. Nr. 13.3).

Nach europaweit ausgeschriebenen Vergabeverfahren hat die gematik zwei großflächige Erprobungsvorhaben vergeben. Diese Erprobungsmaßnahmen mit ca. 1.000 Ärzten in den Testregionen Nordwest (Schleswig-Holstein, Nordrhein-Westfalen, Rheinland-Pfalz) und Südost (Bayern und Sachsen) sollen in der zweiten Jahreshälfte 2015 beginnen. Zum Testumfang gehören der Aufbau der Telematikinfrastruktur, die Online-Aktualisierung der Versichertenstammdaten sowie Anwendungen mit einer qualifizierten elektronischen Signatur zur sicheren Kommunikation zwischen den Ärzten. Die elektronische Kommunikation wird sich zwar in der sicheren Telematikinfrastruktur abspielen, ohne aber die elektronische Gesundheitskarte einzubinden. Dadurch entfällt in Zukunft der unsichere Transport von Gesundheitsinformationen über Telefax, E-Mail oder der zeitaufwendigere Weg über die Post, so dass dieses Projekt zu einer deutlichen datenschutzrechtlichen Verbesserung führen wird.

Offen ist die Frage, wie die sog. Sicheren Netze der Kassenärztlichen Vereinigungen an die Telematik-Infrastruktur angebunden werden können (vgl. Nr. 13.14).

Seit Jahren bereitet die gematik die Einführung erster medizinischer Anwendungen wie Notfalldaten oder Daten zur Verbesserung der Arzneimitteltherapiesicherheit vor. So sollen möglichst rasch die Voraussetzungen für die Einführung flächendeckender medizinischer Anwendungen für eine bessere Versorgung von Patientinnen und Patienten geschaffen werden.

Spätestens zu diesem Zeitpunkt müssen auch die sog. Anwendungen der Versicherten realisiert sein. Die Möglichkeiten der Versicherten, auf ihre mittels der elektronischen Gesundheitskarten gespeicherten Daten zuzugreifen, sind zwar gesetzlich normiert (§ 291a Abs. 4 Satz 2 SGB V), befinden sich aber im Planungsstand weit hinter den sonstigen Projekten. Es ist geplant, dass Versicherte in einer geschützten Umgebung (Arztpraxis oder Apotheke) an einem Terminal (E-Kiosk) ihre Daten einsehen können. Darüber hinaus ist in § 291a Absatz 3 Satz 1 Nummer 5 SGB V als freiwillige Anwendung vorgesehen, ein sog. Patientenfach des Versicherten einzurichten. Hierin können Versicherte nicht nur eigene Daten einstellen, sondern auch Kopien sämtlicher anderer medizinischer Daten, die mittels der elektronischen Gesundheitskarte gespeichert sind, einfügen lassen. Da für dieses Patientenfach erleichterte Zugriffsmöglichkeiten gelten, weil der Heilberufsausweis des Arztes nicht erforderlich ist, könnten Versicherte auch am heimischen PC auf ihre Daten zugreifen, wenn sie über eine eigene Signaturkarte verfügen.

Ebenfalls im Hintergrund scheinen die Arbeiten der gematik für die Erweiterung der elektronischen Gesundheitskarte um die elektronische Dokumentation der Organspendeerklärung zu verlaufen. War ich in meinem letzten TB (Nr. 4.1) noch davon ausgegangen, die ersten Tests könnten bereits im Jahre 2014 anlaufen, lässt der von der gematik dem Deutschen Bundestag vorgelegte Bericht vom 3. Juli 2013 (Bundestagsdrucksache 17/14326) den Schluss zu, dass noch weitergehende Untersuchungen und Evaluationen erforderlich sind, ehe an eine konkrete Umsetzung zu denken ist.

Ich werde auch im kommenden Berichtszeitraum die Entwicklung der elektronischen Gesundheitskarte aufmerksam und kritisch begleiten und dabei die eingangs zitierten Worte der Bundesregierung zum Maßstab nehmen.

13.3 Das Lichtbild auf der Krankenversichertenkarte

Ab dem 1 Januar 2015 wird die alte Krankenversichertenkarte endgültig von der elektronischen Gesundheitskarte (eGK) abgelöst. Im Vorfeld wandten sich wieder einige Versicherte an mich, weil sie ihrer gesetzlichen Krankenkasse kein Lichtbild für die neue eGK zu senden wollten.

Bereits im letzten Berichtszeitraum erreichten mich zahlreiche Eingaben zu diesem Thema. Das setzte sich im Berichtszeitraum fort. Im 24. Tätigkeitsbericht (Nr. 11.1.5) konnte ich von einem ersten erstinstanzlichen Urteil eines Sozialgerichts (Sozialgericht Düsseldorf, Urteil vom 28. Juni 2012, Az. S9 KR 111/09) berichten, dass die eGK in ihrer jetzigen Form - einschließlich der Verpflichtung zur Vorlage eines Lichtbildes – für rechtmäßig erklärt hatte. In der Folgezeit haben sich eine Reihe von Sozialgerichten und Landessozialgerichten mit entsprechenden Klagen von Versicherten beschäftigen müssen und unisono die Rechtmäßigkeit des Verlangens nach einem Lichtbild eines Versicherten für die eGK festgestellt. Diese Rechtsprechung der unteren Instanzen hat mittlerweile das Bundessozialgericht (BSG) bestätigt. Mit seinem Urteil vom 18. November 2014 (Az. B 1 KR 35/13 R) hat es eine Klage eines Versicherten zurückgewiesen, der von seiner Krankenkasse eine Versichertenkarte ohne Lichtbild und ohne eGK-Chip verlangte. In seiner Entscheidung führt das BSG aus, das Lichtbild auf der eGK einer gesetzlichen Krankenkasse verletze nicht das Recht der Versicherten auf informationelle Selbstbestimmung. Es überwiege zudem der durch das Bild verbesserte Schutz vor Missbrauch gegenüber dem Interesse des Einzelnen. Die freiwilligen, vom Einverständnis des Betroffenen abhängigen Anwendungen der eGK begegnen danach auch keinen verfassungsrechtlichen Bedenken. Bereits jetzt würden die gesetzlichen Vorschriften die entsprechenden Daten der Versicherten vor unbefugtem Zugriff Dritter und vor missbräuchlicher Nutzung schützen.

13.4 Ein Leitfaden zum Datenschutz in medizinischen Forschungsprojekten

Der überarbeitete Leitfaden der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF) beschreibt neue generische Modelle zum Datenschutz in medizinischen Forschungsprojekten.

Die generischen Datenschutzkonzepte der TMF bilden seit ihrer ersten Version aus dem Jahr 2003 die Grundlage für die Planung und Umsetzung medizinischer Forschungsprojekte. Sie wurden 2006 noch einmal überarbeitet und ebenso wie bereits 2003 mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt. Allerdings hat sich in den letzten Jahren die Technik, das Datenschutzrecht, aber auch die medizinische Forschung deutlich weiterentwickelt, die zunehmend vernetzt und einrichtungsübergreifend arbeitet. Dies hat die TMF veranlasst, die generischen Datenschutzkonzepte grundlegend zu überarbeiten und fortzuschreiben. Sie decken jetzt weitere Anwendungsfälle ab und wurden zudem modularisiert, indem für viele Projekte passgenaue Lösungen vorgeschlagen werden. Sie sind in einen umfassenden Leitfaden zum Datenschutz in der medizinischen Forschung eingebettet und in der Schriftenreihe der TMF veröffentlicht. Eines der ersten Anwendungsbeispiele, bei denen das Datenschutzkonzept auf der Basis der neuen generischen Datenschutzkonzepte erstellt wurde, ist das Datenschutz- und IT-Sicherheitskonzept der Nationalen Kohorte e. V. (vgl. hierzu Nr. 13.5).

Ich begrüße sehr, dass die TMF auch bei der Neufassung seiner generischen Datenschutzkonzepte und des „Leitfadens zum Datenschutz in medizinischen Forschungsprojekten“ das Gespräch mit den Arbeitskreisen Technik, Wissenschaft sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gesucht hat. Im Rahmen ihrer Frühjahrstagung 2014 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossen, die neuen generischen Datenschutzkonzepte der TMF zustimmend zur Kenntnis zu nehmen und den medizinischen Forschungseinrichtungen und -verbünden als Basis für die konkrete Ausgestaltung von Datenschutzkonzepten zu empfehlen.

13.5 Der „Nationale Kohorte e. V.“ nimmt seine Arbeit auf

Epidemiologische Langzeitstudien wie die Nationale Kohorte bieten neuartige datenschutzrechtliche und technische Herausforderungen und erfordern eine kontinuierliche datenschutzrechtliche Begleitung.

Über die Nationale Kohorte habe ich bereits in meinem 24. Tätigkeitsbericht (Nr. 11.5.4) berichtet. Es handelt sich um eine epidemiologische Langzeitstudie von Wissenschaftlern der Helmholtz-Gemeinschaft, der Leibniz-Gemeinschaft sowie von Universitäten und anderen Forschungseinrichtungen in Deutschland. Koordiniert wird diese Studie durch den Nationale Kohorte e. V., der sich im Jahr 2012 gegründet hat. Ziel ist die Entwicklung von Volkskrankheiten, wie Herz-, Kreislauf- und Gefäßerkrankungen, Krebs und Atemwegserkrankungen sowie deren Vorbeugung, Früherkennung und die Identifizierung von Risiken zu untersuchen. Dafür werden 200.000 Studienteilnehmer zwischen 20 und 69 Jahren ausgewählt und in 18 deutschlandweit verteilten Studienzentren umfassend zu ihren allgemeinen Lebensgewohnheiten befragt sowie medizinisch untersucht. Es werden auch Bioproben entnommen. Nach fünf Jahren werden alle Teilnehmer erneut zu einer Untersuchung und zweiten Befragung in die Studienzentren eingeladen. Die Nachbeobachtung soll zunächst über 10-20 Jahre laufen. Geplant ist die Zusammenführung der in den Studienzentren gewonnenen Befragungs- und Gesundheitsdaten mit regelmäßig aktualisierten Sekundärdaten, z. B. von den gesetzlichen und privaten Krankenversicherungen, der Deutschen Rentenversicherung Bund, von den epidemiologischen und klinischen Krebsregistern sowie Behandlungsdaten von behandelnden Ärzten. Die Anschrift der Teilnehmer soll über Abfragen bei den Meldeämtern aktualisiert werden. Weiter soll bei verschiedenen Registern regelmäßig abgefragt werden, ob die Teilnehmer noch leben. Im Todesfalle soll die Todesursache recherchiert und die Todesbescheinigung vom Gesundheitsamt angefordert und gespeichert werden.

Einzigartig ist dabei nicht nur die Größe der Kohorte und die Dauer der Datenspeicherung, die bis über den Tod der Studienteilnehmer hinausgehen soll, sondern auch der Umfang und die Detailtiefe der gesammelten Daten. So soll der teilnehmerspezifisch zusammengeführte Studiendatensatz neben den in den Studienzentren erhobenen medizinischen Daten, zu denen auch genetische Informationen gehören, und der lebenslangen Krankengeschichte auch Diagnose- und Abrechnungsdaten von den Krankenversicherungen, Informationen zu den verschriebenen Medikamenten, die kombinierten Informationen aus den epidemiologischen und klinischen Krebsregistern, den beruflichen Lebenslauf sowie Geolokalisierungsdaten zu den jeweiligen Wohnorten enthalten. Aus den gesammelten Daten und aufgetretenen Krankheiten sollen Rückschlüsse auf genetische Faktoren, Umweltbedingungen, soziales Umfeld und Lebensstil als Ursachen für die jeweiligen Erkrankungen ermöglicht werden.

Sowohl für die Erhebung der Studiendaten unmittelbar beim Studienteilnehmer als auch für die Erhebung der Daten bei den Sozialleistungsträgern und den weiteren Sekundärquellen ist wesentliche Rechtsgrundlage die Einwilligung der Studienteilnehmer, die grundsätzlich fünf Jahre gilt und dann erneut eingeholt werden muss. Die Einwilligung kann jederzeit widerrufen werden. Im Falle des vollständigen Widerrufs werden die Daten aus der Studiendatenbank gelöscht. Sowohl die unmittelbar bei den Probanden erhobenen Daten als auch solche aus Sekundärquellen stehen den Wissenschaftlern nur pseudonymisiert zur Auswertung zur Verfügung. Das Pseudonym wird bei einer Vertrauensstelle gebildet und lässt einerseits zu, die Daten einer bestimmten Person immer demselben Falldatensatz zuzuordnen. Andererseits wird das Pseudonym so gestaltet, dass eine Identifizierung des Einzelnen durch einen an der wissenschaftlichen Forschung Beteiligten nicht wahrscheinlich ist. Datenschutzrechtlich verantwortlich ist die „Nationale Kohorte e. V.“, die, obwohl als privater Verein organisiert,

nach § 2 Absatz 3 BDSG datenschutzrechtlich eine öffentliche Stelle des Bundes ist. Sie schließt Verträge zur Datenverarbeitung im Auftrag mit den 18 Studienzentren und weiteren Einrichtungen der Nationalen Kohorte.

Ich begleite das Projekt, das auch bei verschiedenen Sitzungen des Arbeitskreises Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder auf der Tagesordnung stand, seit längerem. Auch wenn ein abgestimmtes Datenschutzkonzept noch nicht vollständig vorliegt, hat der Nationale Kohorte e. V. meine Anregungen zum Datenschutzkonzept in konstruktiver Zusammenarbeit aufgenommen. So konnten wesentliche Verbesserungen des Datenschutzniveaus erreicht werden. Dieses Konzept hat der Nationale Kohorte e. V. Ende des Jahres 2014 grundlegend überarbeitet und sich am Leitfaden zum Datenschutz in medizinischen Forschungsprojekten der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF) sowie den generischen Datenschutzkonzepten der TMF orientiert, die mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt sind (vgl. hierzu Nr. 13.4). Angesichts der langen Laufzeit der Nationalen Kohorte werde ich die Studie noch lange datenschutzrechtlich begleiten.

13.6 Beratung des Gemeinsamen Bundesausschusses

Der Gemeinsame Bundesauschuss (G-BA) hat mir in zahlreichen Fällen Gelegenheit zur Stellungnahme nach § 91 Absatz 5a SGB V gegeben. Ich kann aber den G-BA nur dann effizient beraten, wenn ich über die vorab getroffenen datenschutzrechtlichen Überlegungen hinreichend informiert werde.

Im Rahmen der neuen Aufgabe nach § 91 Absatz 5a SGB X (vgl. 24. TB Nr. 11.1.4), habe ich in den letzten beiden Jahren u. a. Stellung genommen

- zur Veröffentlichung von wenigen Fallzahlen in einem Tabellenfeld beispielsweise in den Regelungen zum Qualitätsbericht der Krankenhäuser nach § 137 Absatz 3 Satz 1 Nummer 4 SGB V, die analog § 16 Absatz 4 Bundesstatistikgesetz erst ab ≥ 3 dargestellt werden sollten, um einen Rückschluss auf bestimmte Patientinnen und Patienten auszuschließen.

- zu den datenschutzrechtlichen Regelungen in der Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung, insbesondere zur Art der betroffenen Daten und zu den erforderlichen Regelungen über das Erheben, Verarbeiten und Nutzen von Daten,

- zu den datenschutzrechtlichen Anforderungen an die Vorlage einer pseudonymisierten Dokumentation des indikationstellenden Arztes an eine Beratende Kommission der Kassenärztlichen Vereinigungen bei Apheresen im Rahmen der vertragsärztlichen Versorgung.

Darüber hinaus wurde ich um Beratung nach § 26 Absatz 3 BDSG gebeten zur Durchführung von Patientenbefragungen in der sektorenübergreifenden Qualitätssicherung und zur Evaluation strukturierter Behandlungsprogramme. Meine datenschutzrechtlichen Stellungnahmen können sowohl im Falle des § 91 Absatz 5a SGB V als auch nach § 26 Absatz 3 BDSG aufgrund der komplexen medizinischen und tatsächlichen Sachverhalte im Zweifel nur dann alle wesentlichen Belange berücksichtigen, wenn die bis zu meiner Einbeziehung gemachten datenschutzrechtlichen Erwägungen mir ebenfalls mitgeteilt werden. Dies wurde im Rahmen einer nach § 91 Absatz 5a SGB V mir gegebenen Gelegenheit zur Stellungnahme mit der Begründung abgelehnt, solche Hinweise des G-BA würden den Zweck meines „Stellungnahmerechts konterkarieren, indem sie durch ihre unvermeidliche Lenkungswirkung die erforderliche Freiheit der Prüfung letztlich auf eine ‚Supervision' der rechtlichen Bewertung erkannter Probleme beschränkten." Dass ich mein Amt unabhängig und mit spezifischen Fachkenntnissen ausübe und mich dabei durch datenschutzrechtliche Überlegungen Dritter nicht „lenken" lasse, ist selbstverständlich. Solche Überlegungen lenken nur von der Verantwortung des G-BA für die datenschutzrechtlichen Bestimmungen in seinen Beschlüssen ab, die ich nach dem Gesetz in meinen Stellungnahmen zu bewerten habe. Entsprechend dieser Verantwortung muss der G-BA die wesentlichen Aspekte des Datenschutzes

selbst erarbeiten. Meine Beteiligung ist dann darauf gerichtet, diese Überlegungen zu stützen, zu ergänzen oder ihnen ggf. auch zu widersprechen. § 91 Absatz 5a SGB V ist eine Konkretisierung meiner Beratungsaufgabe nach § 26 Absatz 3 BDSG. Meine dort bei datenschutzrelevanten Regelungen immer vorgesehene Stellungnahme entbindet den G-BA nicht von der Verpflichtung, selbst datenschutzrechtlich tätig zu werden. Andernfalls würde sich die Stärkung des Datenschutzes, die der Gesetzgeber mit der Einfügung von § 91 Absatz 5a SGB V erreichen wollte, in ihr Gegenteil verkehren. Es ist weder meine Aufgabe, zu vermuten, welche datenschutzrechtlichen Erwägungen der G-BA zu einzelnen Regelungen angestellt hat, noch ist es meine Aufgabe, diese selbst zu erarbeiten. Die innerhalb des G-BA vorgenommenen datenschutzrechtlichen Erwägungen sollten mir auch dann mitgeteilt werden, wenn sie nicht im Konsens von allen Trägerorganisationen mitgetragen werden. Meine Stellungnahmen erfolgen in fachlicher Unabhängigkeit und werden nicht davon bestimmt, welche datenschutzrechtlichen Ausführungen im Einzelnen dazu bereits aus dem G-BA vorliegen. Die Kenntnis dieser Überlegungen zeigt nicht nur, dass der G-BA seine datenschutzrechtliche Verantwortung wahrnimmt, sondern ermöglicht mir auch eine darauf aufbauende Beratung.

Ich empfehle dem Gesetzgeber, durch eine Ergänzung des § 91 Absatz 5a SGB V klarzustellen, dass, wenn der G-BA mir Gelegenheit zur Stellungnahme gibt, die aus seiner Sicht maßgeblichen Erwägungen zum Datenschutz beizufügen sind.

13.7 „Fallmanagement“ - der Trend zur ganzheitlichen Betreuung durch die gesetzliche Krankenkasse

In den letzten Jahren hat bei den gesetzlichen Krankenkassen der Trend zugenommen, sich über ihren gesetzlichen Auftrag hinaus um ihre Versicherten zu kümmern. Dies darf aber nicht zu rechtswidrigem Umgang mit personenbezogenen Daten von Versicherten führen.

Bereits in der Vergangenheit (24. TB Nr. 11.1.8) hatte ich beim „Krankengeldfallmanagement“ auf den bedenklichen Umgang mit personenbezogenen Daten von Versicherten durch gesetzliche Krankenkassen hingewiesen. Bedauerlicherweise hat der Trend zur Erhebung von Versichertendaten für sog. Fallmanagement weiter zugenommen (vgl. Kasten zu Nr. 13.7). Dies betrifft nicht nur das sog. Krankengeldfallmanagement (hierzu Nr. 13.7.1), sondern auch andere Formen, z. B. die „psychosoziale Komfortbetreuung“ (hierzu Nr. 13.7.2). Gesetzliche Krankenkassen weisen auf ihren Internetseiten selbst darauf hin, beim Fallmanagement oder Case Management in der gesundheitlichen Versorgung handele es sich ursprünglich um eine amerikanische Management-Strategie mit dem Ziel, die Versorgung von Versicherten in einer akuten Krankheitsepisode so zu steuern, dass in einem abgestimmten Prozess die individuell notwendigen Gesundheitsleistungen zeitnah zur Verfügung gestellt werden. Das Fallmanagement soll den Versorgungsbedarf eines Versicherten in einem bestimmten Zeitraum unabhängig von unterschiedlichen Zuständigkeiten von Einrichtungen, Ämtern und Dienstleistungen planen, koordinieren, implementieren, überwachen und evaluieren. Letztlich verfolgen die Krankenkassen mit dem Fallmanagement das Ziel, die Qualität der Versorgung zu sichern und dadurch auch langfristig entstehende Kosten zu senken.

Durch dieses Aufgabenverständnis der Krankenkassen könnte allerdings das in der gesetzlichen Krankenversicherung grundsätzlich geltende Sachleistungsprinzip in Frage gestellt werden, nach dem die Krankenkassen ihren Versicherten Sachleistungen zur Verfügung stellen, die sie aber nicht selbst erbringen und über deren Notwendigkeit sie auch nicht selbst entscheiden. Vielmehr beauftragen sie Dritte (Ärzte, Krankenhäuser, etc.) und rechnen die erbrachten Leistungen direkt mit diesen Vertragspartnern ab (§§ 2, 69 SGB V). Die umfangreiche Erhebung personenbezogener Daten der Versicherten in diesem Bereich bedeutet einen weiteren Schritt in Richtung „gläserner Patient/Versicherter“. Zudem handelt es sich beim Fallmanagement in der Regel nicht um Aufgaben, die den Krankenkassen gesetzlich, insbesondere durch das SGB V, übertragen worden sind. Auf die fehlende Rechtsgrundlage für diese Tätigkeit der gesetzlichen Krankenkassen hatte ich bereits in meinem 24. Tätigkeitsbericht hingewiesen. Zwar berufen sich die Krankenkassen weiterhin auf § 11 Absatz 4 SGB V, dies aber offensichtlich nur, weil dort das Wort „Versorgungsmanagement“ auftaucht. Versorgungsmanagement im Sinne des § 11 Absatz 4 SGB V, auf das die Versicherten einen Anspruch haben, betrifft jedoch die Hilfe beim Über-

gang in verschiedene Versorgungsbereiche (stationär zu ambulant oder von dem Bereich der Kranken- in die Rentenversicherung) und verpflichtet die Krankenkassen, die Leistungserbringer - und nicht die Versicherten - bei deren Aufgabe zu unterstützen, für eine sachgerechte Anschlussversorgung zu sorgen.

Die Bundesregierung hat kurz vor Ende des Berichtszeitraums den Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz, Bundesratsdrucksache 641/14) verabschiedet (hierzu Nr. 13.7.1), der zwei Bereiche eines Fallmanagements gesetzlich regeln möchte: das Entlassmanagement zur Unterstützung einer sektorenübergreifenden Versorgung der Versicherten (§ 39 Abs. 1a SGB V-E) und das Krankengeldfallmanagement (§ 44 Abs. 4 SGB V-E). Selbst wenn diese Regelungen Gesetz werden sollten, betreiben die Krankenkassen weiterhin eine Reihe von Fallmanagement-Anwendungen, denen die gesetzliche Grundlage fehlt.

Kasten zu Nr. 13.7

Sozialdaten bei den gesetzlichen Krankenkassen - ein kurzer Überblick

Im Bereich des Sozialversicherungsrechts gelten besondere Datenschutzregeln. Diese finden sich vor allem im Zehnten Buch Sozialgesetzbuch (SGB X) und den speziell für den jeweiligen Sozialverwaltungsbereich geltenden Gesetzbüchern. Beispielhaft seien hier genannt für die gesetzliche Krankenversicherung das Fünfte Buch Sozialgesetzbuch (SGB V), für die gesetzliche Rentenversicherung das Sechste Buch Sozialgesetzbuch (SGB VI) und für die gesetzliche Unfallversicherung das Siebte Buch Sozialgesetzbuch (SGB VII).

Was sind Sozialdaten?

Nach § 67 Absatz 1 Satz 1 SGB X sind Sozialdaten

- personenbezogene Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (z. B. Name, Geburtsdatum, Diagnosen),
- die von einem Sozialleistungsträger, d. h. einer in § 35 SGB I genannten Stelle,
- im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch

erhoben, verarbeitet oder genutzt werden.

Welche Sozialdaten hat meine Krankenkasse über mich gespeichert?

Zentrale Vorschrift im Bereich des Krankenversicherungsrechts ist § 284 SGB V. Die Norm legt abschließend fest, zu welchen Zwecken und in welchem Umfang Krankenkassen Sozialdaten erheben, verarbeiten und nutzen dürfen. Einige wichtige genannte Zwecke sind dabei:

- die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft,
- die Ausstellung der Krankenversichertenkarte,
- die Feststellung der Beitragspflicht und der Beiträge,

- die Abrechnung mit den Leistungserbringern (Ärzte, Krankenhäuser, Apotheken, Heil- und Hilfsmittelhersteller) und anderen Leistungsträgern (z. B. gesetzliche Renten- oder Unfallversicherung).

Uneingeschränkt unterliegen diese Datenerhebungsbefugnisse dem Grundsatz der Erforderlichkeit, d. h. Sozialdaten dürfen immer nur in dem Umfang erhoben und gespeichert werden, wie dies für die Aufgabenerfüllung der Krankenkasse erforderlich ist und sind zu löschen, sobald die Daten für die genannten Zwecke nicht mehr benötigt werden.

Darf meine Krankenkasse darüber hinausgehende Sozialdaten speichern?

Häufig versuchen Krankenkassen über Selbstauskunftsbögen zum Gesundheitszustand oder eine Schweigepflichtentbindungserklärung für die Anforderung von Arztunterlagen (Befundbrief, Krankenhausentlassungsbericht) an zusätzliche Versichertendaten zu gelangen. Diese Vorgehensweise ist immer dann datenschutzrechtlich unzulässig, wenn keine spezielle gesetzliche Vorschrift die Datenerhebung legitimiert. Auch eine Einverständnis- und/oder Schweigepflichtentbindungserklärung ist in diesen Fällen nicht ausreichend um die Datenerhebung zu rechtfertigen. In medizinischen Zweifelsfällen, in denen die Krankenkasse auf Grundlage der zulässig erhobenen Daten keine sachgerechte Leistungsentscheidung (Ist z. B. ein elektrischer Rollstuhl erforderlich?) treffen kann, hat sie den Medizinischen Dienst der Krankenversicherung (MDK) zur Begutachtung des Sachverhalts zu beauftragen. Dazu darf der MDK - soweit im Einzelfall erforderlich - zusätzliche medizinische Daten erheben. Der beauftragenden Krankenkasse darf er nur das Ergebnis seiner Begutachtung mitteilen, nicht aber die Informationen, aufgrund derer der MDK zu seinem gutachterlichen Ergebnis gekommen ist.

Muss mir die Krankenkasse Auskunft über die über mich gespeicherten Sozialdaten geben?

Ja, als Versicherte steht Ihnen gegenüber Ihrer Krankenkasse gemäß § 83 Absatz 1 SGB X auf Antrag ein Auskunftsanspruch über

- die zu Ihrer Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

- die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden und

- den Zweck der Speicherung

zu. Außerdem können Sie nach § 305 Absatz 1 Satz 1 SGB V bei Ihrer Krankenkasse einen Antrag auf Unterrichtung über die in einem Zeitraum von mindestens 18 Monaten vor Antragstellung in Anspruch genommenen Leistungen und deren Kosten stellen.

13.7.1 „Krankengeldfallmanagement“ durch die Krankenkassen - bald auf gesetzlicher Grundlage?

Mit dem Gesetzentwurf zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung ebnet die Bundesregierung den Weg für die datenschutzrechtlich gefährliche Legitimierung eines von den gesetzlichen Krankenkassen durchgeführten „Krankengeldfallmanagements“.

Schon mehrfach (zuletzt im 24. TB Nr. 11.1.8) habe ich die Praxis verschiedener gesetzlicher Krankenkassen als datenschutzrechtlich unzulässig bewertet, Sozialdaten ihrer arbeitsunfähigen Versicherten zu erheben, die

Krankengeld beziehen oder bei denen ein solcher Bezug droht. In Gesprächen mit dem BMG und dem GKV-Spitzenverband habe ich mich um datenschutzgerechte Lösungen bemüht. Diese fanden mit dem im Herbst 2014 vom BMG vorgelegten Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz) zumindest vorübergehend ein Ende. Der Gesetzesentwurf schafft nämlich unter anderem mit dem neuen § 44 Absatz 4 SGB V eine gesetzliche Grundlage für die datenschutzrechtlich kritische Vorgehensweise der Krankenkassen. Eine erste Formulierung des § 44 Absatz 4 SGB V-neu sah zunächst vor, dass Versicherte „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung durch die Krankenkasse, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind" haben. Mit dieser neuen Aufgabe einher geht eine umfassende Datenverarbeitungsbefugnis: „Die Krankenkasse darf die dazu erforderlichen personenbezogenen Daten nur mit Einwilligung und nach vorheriger Information des Versicherten erheben, verarbeiten und nutzen".

Diese Regelung ist im Kontext des Normengefüges des Krankenversicherungsrechts unter besonderer Berücksichtigung des datenschutzrechtlichen Schutzbedarfs äußerst bedenklich. Nach Maßgabe des § 275 Absatz 1 Nummer 3a und b SGB V sind Krankenkassen verpflichtet, bei Arbeitsunfähigkeit in bestimmten Fällen eine gutachterliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung (MDK) einzuholen. Wie der Gesetzgeber damit entschieden hat, sollen die Krankenkassen keine über die üblichen, im Katalog des § 284 Absatz 1 Satz 1 SGB V abschließend normierten Sozialdaten hinausgehenden Daten über den Gesundheitszustand ihrer Versicherten erheben. Diese Datenerhebungsbefugnis ist dem MDK, der den Krankenkassen lediglich das Ergebnis seiner Begutachtung mitteilen darf, vorbehalten. Zugleich schützt die strikte Aufgabenteilung und Datentrennung zwischen Krankenkassen und MDK den Versicherten vor der Schaffung eines Pools sensibler Gesundheitsdaten und der sich hieraus ergebenden Option, umfassende und dem Versicherten möglicherweise zum Nachteil gereichende Gesundheitsprofile zu erstellen.

Diese Aufgabenteilung zwischen Krankenkassen und MDK hat sich aus datenschutzrechtlicher Sicht bewährt, daher sehe ich für die vorgesehene Gesetzesänderung keinen Bedarf. Die angemessene Reaktion auf die Praxis vieler Krankenkassen, sich die begehrten Versichertendaten unter Umgehung der Zuständigkeit des MDK und durch häufig bedrängende Ansprache der Versicherten rechtswidrig zu beschaffen, kann aus meiner Sicht nicht sein, den derzeitigen Zustand zu legalisieren und damit verbunden das Datenschutzniveau zu senken. Vielmehr sollte das gesetzeswidrige Verhalten der Krankenkassen durch ein konsequentes Tätigwerden der Aufsichtsbehörden unterbunden werden. Die vorgesehene Einführung des § 44 Absatz 4 SGB V-neu stellt einen weiteren Schritt in Richtung des „gläsernen Versicherten" dar. Hier hilft auch nicht die vorgesehene Einwilligungslösung, da die hierfür erforderliche Freiwilligkeit innerhalb eines nicht gleichberechtigten Rechtsverhältnisses, wie es zwischen Krankenkasse und Versichertem besteht, stets in Frage zu stellen ist.

Meine grundsätzlichen datenschutzrechtlichen Bedenken, die von den Datenschutzbeauftragten der Länder geteilt werden (vgl. Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014, Kasten zu Nr. 13.7), habe ich im Gesetzgebungsverfahren immer wieder zum Ausdruck gebracht. Bedauerlicherweise konnte ich mich damit im bisherigen Gesetzgebungsverfahren nicht durchsetzen. Aber ich konnte zumindest erreichen, dass der durch die Befugnisnorm legitimierte Eingriff in das Recht auf informationelle Selbstbestimmung der Versicherten minimiert wurde. So werden nach der Formulierung des § 44 Absatz 4 SGB V-neu in der vom Bundeskabinett am 17. Dezember 2014 beschlossenen Fassung eine Übertragung des „Krankengeldfallmanagements" auf private Stellen ausgeschlossen, die Worte „umfassende Prüfung" zum Zwecke der eindeutigeren Abgrenzung zu den Aufgaben des MDK gestrichen und klargestellt, dass die erforderlichen personenbezogenen Daten nur auf Grundlage einer schriftlichen Einwilligung und einer vorausgehenden schriftlichen Information des Versicherten erhoben, verarbeitet und genutzt werden dürfen. Im weiteren Verlauf des Gesetzgebungsverfahrens werde ich gegenüber dem Deutschen Bundestag meine datenschutzrechtlichen Bedenken weiter zur Geltung bringen.

13.7.2 „Psychosoziale Komfortbetreuung“ ohne Rechtsgrundlage

Auch außerhalb des „Krankengeldfallmanagements“ war im Berichtszeitraum bei den gesetzlichen Krankenkassen die Tendenz zu beobachten, jenseits der gesetzlichen Kernaufgaben den Versicherten medizinische Betreuungsangebote zu machen. Die datenschutzrechtlichen Vorgaben werden dabei nicht immer beachtet.

Eine große bundesunmittelbare Krankenkasse bietet ihren Versicherten bei bestimmten Krankheiten spezielle Betreuungsprogramme an. Deren Ziel ist es nach Aussage der Krankenkasse, die medizinische Versorgung der Versicherten zu ergänzen, eine wirtschaftliche Versorgung sicherzustellen sowie vorhandene Ressourcen effizienter zu nutzen. Dabei befasst sich ein Programm ausschließlich mit psychisch erkrankten Versicherten, ein zweites richtet sich an Versicherte, die an schwerwiegenden Erkrankungen, wie Diabetes, Hypertonie, Herzinsuffizienz, Schlaganfall oder Rückenschmerzen leiden. Zur Datenselektion findet monatlich eine Auswertung von pseudonymisierten Abrechnungs- und Krankenhausdaten nach den verschlüsselt hinterlegten Diagnosen (sog. ICD-10-Code) statt. Die für ein Programm in Frage kommenden Fälle werden im Zuge eines standardisierten Prozesses repseudonymisiert, der entsprechende Schlüssel liegt bei der Controllingabteilung der Krankenkasse. Die ausgewählten Versicherten erhalten Informationsmaterial sowie eine Teilnahme-/Einwilligungserklärung zum Datenschutz. Nach deren Unterzeichnung übermittelt die Krankenkasse folgende Versichertendaten an einen privaten Dienstleister, der die telefonische Betreuung der Versicherten durchführt:

- Vor- und Zuname
- Anschrift
- Geburtsdatum und Versichertennummer
- Name, Adresse und ggf. Telefonnummer der behandelnden Ärzte (optional)
- Name, Adresse und ggf. Telefonnummer nahe stehender Personen/Angehöriger (optional)

Die Betreuung erfolgt über einen Zeitraum von zwölf Monaten und umfasst u. a. regelmäßige Telefongespräche, die Erstellung eines persönlichen Versorgungsplanes sowie die Unterstützung bei der Organisation von Therapien. Von den im Rahmen der Betreuungsgespräche von dem Dienstleister erhobenen Gesundheitsdaten des Versicherten oder Gesprächsergebnissen erhält die Krankenkasse keine Kenntnis.

Bei den beschriebenen Programmen handelt es sich um ein datenschutzrechtlich unzulässiges Fallmanagement. Eine erforderliche gesetzliche Grundlage für die mit der Durchführung der Programme einhergehende Datenerhebung, -verarbeitung und -nutzung ist nicht vorhanden. Insbesondere können diese nicht auf § 11 Absatz 4 SGB V gestützt werden (vgl. Nr. 13.7). Da sich die Krankenkasse selbst auf keine einschlägige Rechtsgrundlage für die Datenerhebung, -verarbeitung und -nutzung berufen kann, ist auch die Betrauung eines privaten Dritten mit dieser Aufgabe im Wege der Auftragsdatenverarbeitung nach § 80 SGB X unzulässig.

Während einer Vor-Ort-Kontrolle habe ich die Krankenkasse auf die datenschutzrechtliche Unzulässigkeit der geschilderten Betreuungsprogramme hingewiesen und erwarte, dass diese von ihr eingestellt werden - so wie es eine andere Krankenkasse mit einem vergleichbaren Betreuungsprogramm bereits getan hat.

13.8 „Good Will“ des Datenschutzes führte zu Fehlentwicklungen beim sog. Umschlagsverfahren

Das sog. Umschlagsverfahren konnte in der Praxis nicht verhindern, dass medizinische Unterlagen nur vom Medizinischen Dienst der Krankenversicherung (MDK) zur Kenntnis genommen werden. Zukünftig sind die Leistungserbringer verpflichtet, die erforderlichen Unterlagen direkt dem MDK zu übersenden.

Hat der MDK für Krankenkassen gutachtliche Stellungnahmen abzugeben oder Prüfungen durchzuführen, für die er bei den Krankenkassen nicht vorhandene medizinische Unterlagen (Sozialdaten) benötigt, sind diese von den Leistungserbringern unmittelbar dem MDK zu übermitteln (§ 276 Abs. 2 SGB V). Bisher hatte ich bei der Anforderung von Krankenhausentlassungsberichten durch Krankenkassen nicht widersprochen (vgl. 18. TB Nr. 21.3), wenn diese Unterlagen an die Krankenkasse selbst zur Weiterleitung an den MDK in einem gesonderten, verschlossenen Umschlag übersandt werden, der mit der Anschrift des MDK sowie einem Vermerk „ärztliche Unterlagen - nur vom MDK zu öffnen“ versehen ist (sog. Umschlagsverfahren). Damit wäre eine unzulässige Einsichtnahme in Krankenhausentlassungsberichte durch eine Krankenkasse ausgeschlossen. Wie ich bereits in meinem 20. Tätigkeitsbericht (Nr. 17.1.5) dazu feststellen musste, werden diese datenschutzrechtlichen Vorgaben in der Praxis jedoch häufig nicht beachtet. In der Zwischenzeit durchgeführte Kontrollen haben dies leider erneut bestätigt. Wie mir zudem bei Kontrollen aufgefallen ist, werden vom MDK in einem verschlossenen Umschlag erhaltene Unterlagen an die Krankenkasse zur dortigen Ablage offen zurückgegeben; spätestens zu diesem Zeitpunkt erhielt die Krankenkasse Kenntnis vom Inhalt der Unterlagen. Meine bisherige Auffassung kann ich deshalb nicht aufrechterhalten: Sozialdaten sind nach § 276 Absatz 2 Satz 1 zweiter Halbsatz SGB V unmittelbar an den MDK zu übermitteln, soweit dies für die gutachterliche Stellungnahme und Prüfung erforderlich ist; der MDK muss sicherstellen, dass die Sozialdaten nur Personen zugänglich sind, die sie zur Erfüllung ihrer Aufgaben benötigen (§ 276 Abs. 2 Satz 6 SGB V). Die Bedeutung des Begriffes „unmittelbar“ liegt auf der Hand und schließt im Gegensatz zu „mittelbar“ die Einbeziehung Dritter aus. Deshalb kommt eine Übermittlung von Sozialdaten zwischen Leistungserbringern und MDK nur auf direktem (Post)Weg und ohne Einschaltung der Krankenkassen in Betracht. Weiter dürfen die Unterlagen auch zu einem späteren Zeitpunkt vom MDK nicht den Krankenkassen zugeleitet bzw. von ihnen zur Kenntnis genommen werden. Die vom MDK erhobenen und gespeicherten Sozialdaten müssen in seinem Zuständigkeitsbereich verbleiben und sind nach fünf Jahren zu löschen. Die Krankenkassen meines Zuständigkeitsbereichs und den MDK habe ich deshalb gebeten, künftig § 276 Absatz 2 Satz 1 zweiter Halbsatz SGB V einzuhalten. Erforderliche Umstellungen werden bis zum Ende des ersten Quartals 2015 erfolgen können. Sollte ich bei Kontrollen ab Mitte 2015 feststellen, dass das bisherige Verfahren weiterhin zur Anwendung kommt, werde ich dies wegen Verstoßes gegen § 276 Absatz 2 SGB V förmlich beanstanden.

13.9 Private Zusatzversicherungen - ein grauer Markt im Bereich der gesetzlichen Krankenversicherungen

Gesetzliche Krankenkassen dürfen private Zusatzversicherungen vermitteln. Doch zwischen zulässiger Vermittlung und unzulässiger Datenübermittlung liegt ein schmaler Grat.

Die gesetzlichen Krankenkassen dürfen nach § 194 Absatz 1a SGB V in Verbindung mit ihrer Satzung private Zusatzversicherungen zwischen ihren Versicherten und einem privaten Krankenversicherungsunternehmen vermitteln. Damit ist ihnen aber nicht erlaubt, Daten der Versicherten zu übermitteln, auch nicht mit dessen Einwilligung. In der Begründung zu Artikel 1 Nummer 136 GKV-Modernisierungsgesetz vom 14. November 2003, mit dem § 194 Absatz 1a SGB V mit Wirkung zum 1. Januar 2004 eingefügt wurde, hat der Gesetzgeber unmissverständlich ausgeführt: „Die Vorschriften des Sozialgesetzbuches zum Schutz der Sozialdaten bleiben unberührt. Eine Weitergabe von Versichertenadressen an den Kooperationspartner ist daher nicht zulässig“ (Bundestagsdrucksache 15/1525, S. 138). Der Begriff „Vermittlung“ schließt von vornherein aus, auf die allgemeinen oder speziellen Regelungen zur Verarbeitung von Sozialdaten zurückzugreifen. Deshalb kann nur der Versicherte selbst seine Daten an den Kooperationspartner übergeben. Ein weiteres, wesentliches datenschutzrechtliches Anliegen: Beide Unternehmen müssen eindeutig getrennt sein, was für die Versicherten auch klar erkennbar sein muss. Die gesetzliche Krankenkasse und das private Versicherungsunternehmen sind sowohl räumlich als auch technisch und organisatorisch so voneinander abzugrenzen, dass eine Datenübermittlung ausgeschlossen ist.

Wie ich bei meinen Kontrollen jedoch immer wieder feststellen musste, folgen die gesetzlichen Krankenkassen diesem Willen des Gesetzgebers nicht konsequent. Im Sinne eines falsch verstandenen Services übernehmen sie die Anmeldungsformalitäten für ihre Versicherten. Oder sie vermerken den Abschluss einer Zusatzversicherung

in ihren Datensätzen, um den Versicherten nicht abermals mit dem gleichen Produkt zu bewerben. Manche gehen noch darüber hinaus und teilen sich mit einem privaten Versicherungsunternehmen eine Geschäftsstelle: Der Datenaustausch erfolgt dann quasi direkt von Schreibtisch zu Schreibtisch. Je nach Ausgestaltung der „Kooperation“ mit den privaten Versicherungsunternehmen und dem damit einhergehenden Schweregrad der Datenschutzverstöße habe ich die gesetzlichen Krankenkassen im Nachgang zu dort durchgeführten Kontrollen aufgefordert, den unsachgemäßen Umgang mit den Sozialdaten einzustellen. Die weitere Entwicklung werde ich beobachten. Im Fall der mhplus BKK war eine Beanstandung erforderlich. Im Zuge der Kooperation mit einem privaten Versicherungsunternehmen übermittelte die gesetzliche Krankenkasse, nachdem ein dortiger Mitarbeiter einen Versicherten telefonisch akquiriert hatte, einen „Überleitungsbogen“, der Sozialdaten (Name, Adresse) enthielt, an ihren Kooperationspartner. Diese bereits unzulässige Datenübermittlung erfolgte zudem per unverschlüsselter E-Mail und damit auf einem unsicheren Übertragungsweg. Die mhplus BKK hat mir zugesichert, diese Verfahrensweise zum 31.12.2014 zu beenden.

13.10 Fehlende Löschkonzepte bei gesetzlichen Krankenkassen

Daten sind zu löschen, wenn sie nicht mehr benötigt werden. Fast alle gesetzlichen Krankenkassen ignorieren diesen Grundsatz der Datensparsamkeit.

Nach § 84 Absatz 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis nicht mehr erforderlich ist, um die jeweiligen Aufgaben zu erfüllen. Konkretisiert wird dieser gesetzliche Auftrag für die gesetzlichen Krankenkassen in § 304 SGB V. Anlässlich meiner Kontrollen bei gesetzlichen Krankenkassen habe ich festgestellt, dass die Programme zur elektronischen Erfassung und Verwaltung der Versichertendaten häufig deren Löschung nicht vorsehen. Vielfach besteht lediglich die Möglichkeit, die Daten auf unbestimmte Zeit zu sperren. Teilweise existieren noch nicht einmal Konzepte, wann welche Daten zu löschen sind. Damit verstoßen diese Krankenkassen auch gegen § 78a SGB X, der organisatorische Maßnahmen vorschreibt, um die Ausführung der Vorschriften des Sozialgesetzbuches zu gewährleisten.

Wie konnte es zu dieser Missachtung datenschutzrechtlicher Grundsätze kommen? Die Krankenkassen nutzen zur Speicherung und Verarbeitung ihrer Versichertendaten unterschiedliche Softwaresysteme. Bei der Entwicklung und Einführung der Software haben sie aus Zeit- und Kostengründen oft auf Löschroutinen verzichtet. Bei Zusammenschlüssen von Krankenkassen, aber auch bei der „normalen“ Migration auf neuere Systeme oder Versionen wurde vielfach der Altdatenbestand (ausgeschiedene oder verstorbene Versicherte) nicht in das aktuelle Softwaresystem der Krankenkasse übernommen. Als Folge führen die Krankenkassen zum großen Teil ihre aktuellen Daten und ihre Altdaten auf ganz unterschiedlichen Systemen. Überdies rangiert die Einführung datenschutzrechtlich angemessener Löschkonzepte bei vielen Krankenkassen ganz unten auf der Skala der zu erledigenden Aufgaben.

Inzwischen wurden von einigen Softwarefirmen oder Krankenkassen selbst Programme entwickelt, die das Löschen der Versichertendaten nach den gesetzlichen Vorschriften ermöglichen. Deswegen habe ich alle gesetzlichen Krankenkassen auf die Dringlichkeit hingewiesen, datenschutzgerechte Löschkonzepte zu entwickeln und Löschroutinen einzuführen. Eine Missachtung der datenschutzrechtlichen Regelungen durch fehlende Konzepte oder technische Anwendungen werde ich ab Juli 2015 konsequent beanstanden.

13.11 Beratung in der Pflegeversicherung

Seit dem 1. Januar 2009 hat jeder Pflegebedürftige des § 7a SGB XI einen Anspruch auf individuelle Beratung und Hilfestellung durch einen Pflegeberater bei den Pflegekassen. Stichprobenartige Kontrollen ergaben keine gravierenden datenschutzrechtlichen Mängel.

Da sich die allgemeinen Aufklärungs- und Beratungspflichten der Pflegekassen nach § 7 SGB XI im Einzelfall als nicht ausreichend erwiesen hatten, wurde durch das Pflege-Weiterentwicklungsgesetz vom 28. Mai 2008 (BGBl. I S. 874) § 7a in das SGB XI eingefügt. Nach dieser Vorschrift hat ein Pflegebedürftiger einen einklagbaren Anspruch auf individuelle Beratung und Hilfestellung durch einen Pflegeberater oder eine Pflegeberaterin bei der Auswahl und Inanspruchnahme von bundes- und landesrechtlich vorgesehenen Sozialleistungen sowie sonstigen Hilfsangeboten, die auf die Unterstützung von Menschen mit Pflege-, Versorgungs- oder Betreuungsbedarf ausgerichtet sind. Die Aufgaben der Pflegeberatung sind in § 7a Absatz 1 Satz 2 SGB XI beispielhaft aufgeführt. Nach Absatz 2 der Regelung erfolgt die Pflegeberatung auf Wunsch unter Einbeziehung von Dritten, insbesondere Angehörigen und Lebenspartnern und in der häuslichen Umgebung oder in der Einrichtung, in der der Anspruchsberechtigte lebt.

Wie ich bei der Kontrolle der Pflegekasse der KKH festgestellt habe, werden die gesetzlichen Vorgaben im Wesentlichen eingehalten. Die Pflegeberatung wurde Personen angeboten, die entweder vom MDK dafür vorgeschlagen oder von Servicezentren oder Pflegesachbearbeitern benannt worden sind. Die so ausgewählten Versicherten wurden nach einem ersten telefonischen Kontakt und einer allgemeinen Information um eine Teilnahme- und Einwilligungserklärung gebeten. Erst wenn diese vorlag, wurde ein Versorgungsplan mit einer zielgerichteten Therapieempfehlung entwickelt. Die Mitarbeiter der Pflegeberatung waren ausschließlich mit dieser Tätigkeit und nicht mit anderen Aufgaben der Pflegekasse befasst.

Bei der Kontrolle habe ich festgestellt, dass die Einwilligungserklärung - wie bei Formularen in der Sozialversicherung üblich - auch auf die Mitwirkungspflichten nach § 60 SGB I verweist. Dies ist jedoch nicht zulässig. Die in § 66 SGB I vorgesehene Sanktion wegen „fehlender Mitwirkung“ gilt im Rahmen der Pflegeberatung nicht. Der entsprechende Hinweis wurde von der Pflegekasse umgehend aus dem Formular entfernt.

13.12 Die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau und der Einsatz von Dritten

In der landwirtschaftlichen Sozialversicherung besteht keine hinreichende Rechtsgrundlage dafür, Dritte mit Beratung zu beauftragen.

Die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG) wurde zum 1. Januar 2013 als Körperschaft des öffentlichen Rechts errichtet und ist der zuständige Leistungsträger nach dem Sozialgesetzbuch für die landwirtschaftliche Kranken- und Pflegekasse, die landwirtschaftliche Berufsgenossenschaft und die landwirtschaftliche Alterskasse. Mit der regelmäßigen Wahrnehmung laufender Verwaltungsaufgaben in der landwirtschaftlichen Sozialversicherung kann die SVLFG „Dritte beauftragen, soweit dies einer wirtschaftlichen Aufgabenerfüllung und einer sachgerechten Betreuung der Versicherten dient und diese nicht durch eine Zusammenarbeit mit den Versicherungsämtern gewährleistet werden kann“ (§ 8 Abs. 1 Satz 1 des Gesetzes zur Errichtung der Sozialversicherung für Landwirtschaft, Forsten und Gartenbau - SVLFGG). Die Wahrnehmung von Verwaltungsaufgaben durch Dritte muss von der Aufsichtsbehörde genehmigt werden (§ 8 Abs. 1 Satz 3 SVLFGG).

Ein Landtagsabgeordneter machte mich darauf aufmerksam, die SVLFG beabsichtige, Verwaltungsstandorte zu schließen und vermehrt Dritte insbesondere mit Aufgaben der Beratung nach § 14 SGB I zu beauftragen. Damit ist die SVLFG der einzig bekannte Sozialleistungsträger, der eine Kernaufgabe, wie die Beratung, durch Dritte wahrnehmen lassen will. Als Dritte sollen im Wesentlichen rechtlich selbstständige Untergliederungen des Deutschen Bauernverbandes e. V. beauftragt werden. Ich habe dazu die SVLFG um Stellungnahme gebeten und dabei im weiteren Verlauf auch das BMAS, das BMEL und das Bundesversicherungsamt (zuständige staatliche Aufsichtsbehörde) einbezogen. Die mir gegebenen Erläuterungen können meine datenschutzrechtlichen Einwände nicht ausräumen:

Zum einen ist § 8 Absatz 1 SVLFGG in Verbindung mit dem Recht auf informationelle Selbstbestimmung keine hinreichende Rechtsgrundlage dafür, Dritte für die Beratung von Versicherten einzusetzen. Insbesondere kann dies nicht aus der Formulierung „Wahrnehmung laufender Verwaltungsaufgaben“ hergeleitet werden. Zum anderen wäre dies auch ein Widerspruch zu § 26 Absatz 2 des Zweiten Gesetzes über die Krankenversicherung der Landwirte (KVLG 1989), der für die Aufgabenerledigung durch Dritte § 197b SGB V für entsprechend anwendbar erklärt. Nach § 197b Satz 2 SGB V dürfen wesentliche Aufgaben zur Versorgung der Versicherten nicht in Auftrag gegeben werden; dazu zählt auch die Beratung nach § 14 SGB I. Soll der SVLFG die Möglichkeit eingeräumt werden, Dritte für die Beratung von Versicherten einzusetzen, so bedarf es angesichts der getroffenen Feststellungen einer normenklaren gesetzlichen Regelung, um damit auch dem Recht auf informationelle Selbstbestimmung zu genügen.

Weiterhin habe ich mich mit der Frage befasst, ob als Dritte rechtlich selbstständige Untergliederungen des Deutschen Bauernverbandes e. V. beauftragt werden können. Auch bei vertraglich geregelter Zweckbindung ist zu berücksichtigen, dass bei Dritten, die parallel eigene Geschäftszwecke verfolgen, die in einem engen Zusammenhang zu den beauftragten Aufgaben bestehen, die Einhaltung der Zweckbindung Risiken ausgesetzt ist. Ein Missbrauchsrisiko ist deutlich geringer, sofern die vom Dritten verfolgten Geschäftszwecke keinen inhaltlichen Bezug zu den Aufgaben haben, die ihm im Rahmen des Sozialgesetzbuches übertragen werden sollen. Exemplarisch kann diese Problematik am Beispiel des (internen) Beauftragten für den Datenschutz nach § 4f BDSG, der für öffentliche und nicht-öffentliche Stellen zu bestellen ist, verdeutlicht werden. So ist in den häufigen Fällen, dass ein Beauftragter für den Datenschutz seine Aufgabe nicht hauptamtlich wahrnimmt, darauf zu achten, dass ihn die anderen Aufgaben nicht in einen Interessenkonflikt bringen können und damit seine unabhängige Stellung gefährden (im Einzelnen BfDI-Info 4, Die Datenschutzbeauftragten in Behörde und Betrieb, Oktober 2014, 1.4). Übertragen auf die hier nach § 8 Absatz 1 SVLFGG nach pflichtgemäßem Ermessen auszuwählenden Dritten, soweit eine Zusammenarbeit mit den Versicherungsämtern nicht in Betracht kommt, sollte neben der erforderlichen Fachkunde auch darauf geachtet werden, dass der eigene Geschäftszweck des Dritten nicht in einem solchen Spannungsverhältnis zu den Aufgaben steht, mit denen er beauftragt werden soll, dass bei den für den Dritten handelnden Personen nicht schon von vornherein Interessenkonflikte bestehen können. Zur Wahrung der Neutralität sollte jeder Anschein eines möglichen Interessenkonfliktes vermieden werden. Deshalb habe ich den verantwortlichen Stellen nahegelegt, im Bereich der landwirtschaftlichen Sozialversicherung auf die Beauftragung von Untergliederungen des Deutschen Bauernverbandes e. V. als Dritte zu verzichten. Die weitere Entwicklung werde ich verfolgen.

13.13 Einsatz von Hilfsmittelberatern ohne Rechtsgrundlage

Zahlreiche Bürgereingaben betreffen die von Krankenkassen beauftragten „Hilfsmittelberater“.

Den Einsatz von externen Hilfsmittelberatern hatte ich als datenschutzrechtlich problematisch beschrieben (zuletzt 24. TB Nr. 11.1.10). Wie ich feststellen musste, waren viele „Hilfsmittelberater“ Mitarbeiter von Leistungserbringern - wie beispielsweise Hersteller von speziell angepassten Rollstühlen oder Prothesen. So wurde in Verträgen mit Hilfsmittelberatern eine Honorarzahlung nur für den Fall vorgesehen, dass durch die Tätigkeit eine Einsparung für die Krankenkasse realisiert werden kann. Wie die Verträge mit externen Hilfsmittelberatern zeigen, können Krankenkassen in diesen Fällen gerade nicht eigenständig darüber urteilen, ob ein Hilfsmittel medizinisch notwendig oder wirtschaftlich sinnvoll verordnet wurde.

In der Antwort der Bundesregierung auf eine entsprechende Kleine Anfrage der LINKEN (Bundestagdrucksache 18/2549) teilt die Bundesregierung leider nicht meine Auffassung, nach der immer dann, wenn medizinischer Sachverstand zur Beurteilung der Leistungspflicht in der Hilfsmittelversorgung erforderlich ist, ein Gutachten vom Medizinischen Dienst der Krankenversicherung (MDK) einzuholen ist. Vielmehr soll in diesen Fällen sowohl ein Prüfauftrag an den MDK, als auch eine Prüfung durch privatrechtlich beauftragte „Hilfsmittelberater“ auf der Grundlage des § 197b SGB V erfolgen können. Die Bundesregierung verweist darauf, dass die Krankenkassen die ihnen obliegenden Aufgaben nach § 197b SGB V durch Arbeitsgemeinschaften oder durch Dritte mit deren Zustimmung wahrnehmen lassen können, wenn die Aufgabenwahrnehmung durch die Arbeits-

gemeinschaft oder den Dritten wirtschaftlicher ist, es im wohlverstandenen Interesse des Betroffenen liegt und Rechte der Versicherten nicht beeinträchtigt werden. Wesentliche Aufgaben zur Versorgung der Versicherten dürfen nicht in Auftrag gegeben werden.

Die staatlichen Aufsichtsbehörden des Bundes und der Länder haben bereits im April 2011 das Arbeitspapier zur „Beauftragung privater Gutachterdienste durch die gesetzlichen Krankenkassen im Bereich der Hilfsmittelversorgung“ erarbeitet, das ebenfalls auf § 197b SGB V verweist. Nach ihrer Auffassung soll die Einschaltung externer Hilfsmittelberater nur unter bestimmten Voraussetzungen im Einzelfall zulässig sein, wenn die Krankenkasse diese Aufgabe nicht selbst fristgerecht wahrnehmen, der MDK im Einzelfall keine zeitnahe Begutachtung vornehmen kann und der Versicherte der Beauftragung und der Datenübermittlung zugestimmt hat.

Auch nach Auskunft des Spitzenverbandes Bund der Krankenkassen sollen externe Hilfsmittelberater von den Krankenkassen nur in Ausnahmefällen eingesetzt werden.

In der Antwort auf die Kleine Anfrage räumt die Bundesregierung auch ein, dass dem Bundesversicherungsamt (BVA) weiterhin Beschwerden über die Beauftragung externer Hilfsmittelberater vorliegen, wenn auch nicht in erheblicher Anzahl. Auch an mich wenden sich weiterhin zahlreiche Versicherte mit Beschwerden über externe Hilfsmittelberater.

Ich sehe weiterhin für die Beauftragung von externen Hilfsmittelberatern keinen Raum, da die Krankenkassen in Einzelfällen, in denen es zur Prüfung der Voraussetzungen sowie Art und Umfang der Leistungspflicht erforderlich ist, nach § 275 Absatz 1 Nummer 1 SGB V eine gutachterliche Stellungnahme des MDK einzuholen haben. Die Prüfung ist also keine Aufgabe der Krankenkassen, sie kann diese erst recht nicht nach § 197b SGB V durch Dritte wahrnehmen lassen. Sollte der MDK diese Aufgabe nicht fristgerecht erfüllen können, worauf das Arbeitspapier der staatlichen Aufsichtsbehörden abstellt, wäre zunächst der MDK so auszustatten, wie es seine gesetzlichen Aufgaben erfordern. Sensible Gesundheitsdaten der Versicherten dürfen jedenfalls nur dort gespeichert werden, wo es das Gesetz vorsieht - und dies ist der MDK und nicht ein privater externer Hilfsmittelberater. Im Übrigen hat der MDK - und nicht die Krankenkassen - auf der Grundlage der §§ 276 Absatz 2b, 279 Absatz 5 SGB V vorrangig externe Gutachter zu beauftragen.

13.14 Die Telematik-Infrastruktur steht - Was geschieht mit den Bestandsnetzen?

Die Einbindung der Bestandsnetze der Kassenärztlichen Vereinigungen in die Telematik-Infrastruktur des Gesundheitswesens ist noch offen. Das BSI pocht zu Recht auf definierte und überprüfbare Sicherheitsbedingungen.

Im Jahr 2015 beginnt der Probebetrieb der Telematik-Infrastruktur mit einem noch sehr begrenzten Angebot an Anwendungen (vgl. Nr. 13.2). Derzeit werden Anwendungen vorwiegend über das Netz der Kassenärztlichen Vereinigungen (KV-SafeNet) bereitgestellt, die über sogenannte Konnektoren angebunden und in einem weiteren Migrationsprozess dauerhaft integriert werden sollen. Dabei ist von großer Bedeutung, dass über alle sektoralen Netze hinweg ein einheitlich hohes Niveau an IT-Sicherheit gewährleistet wird. Ob dabei die Bestandsnetze erhalten bleiben oder Anwendungen aus diesen Netzen heraus in die Telematik-Infrastruktur migriert werden, ist letztendlich eine Frage der Wirtschaftlichkeit und Praktikabilität. Wesentlich ist dabei die Einhaltung eines einheitlich hohen Sicherheitsniveaus. Die Rahmenbedingungen für einen koordinierten Betrieb von Bestandsnetzen und Telematik-Infrastruktur werden derzeit noch zwischen den Gesellschaftern der Telematik-Infrastruktur-Betreibergesellschaft gematik und dem BSI unter meiner Mitwirkung erörtert. Ich werde dabei darauf hinwirken, dass das datenschutzrechtlich erforderliche und vorgesehene hohe IT-Sicherheitsniveau eingehalten wird.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit
- Arbeitskreis Gesundheit und Soziales,
- Unterarbeitsgruppe „Elektronische Gesundheitskarte“

Datenschutzgruppe der gematik/Beirat der gematik GmbH/Statusgespräche mit der gematik (BMG)

14 Ausschuss für Verkehr und digitale Infrastruktur

14.1 Moderne Kraftfahrzeuge - rollende Datenspeicher?!

Das Themenfeld „Datenschutz im Kraftfahrzeug“ bildete im letzten Jahr einen Schwerpunkt der datenschutzrechtlichen und -politischen Diskussion mit Technologiebezug. Automobilindustrie, Datenschutzaufsichtsbehörden und auch Fahrzeugnutzer müssen sich neuen Herausforderungen stellen.

Die Deutschen hegen von jeher eine besondere Beziehung zu Automobilen. So war es nicht verwunderlich, dass im Jahr 2014 zwischen Industrie, Politik, Datenschützern und Gesellschaft verstärkt über den Umfang und die Art der Erhebung und Verarbeitung personenbezogener Daten in modernen Kraftfahrzeugen diskutiert wurde, nachdem sich der 52. Verkehrsgerichtstag Anfang des Jahres der Frage widmete: „Wem gehören die Fahrzeugdaten?“

Kurz darauf nahmen sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Düsseldorfer Kreis der Datenschutzaufsichtsbehörden der Thematik an. Wie sich schnell zeigte, ist die Situation äußerst komplex. In modernen Fahrzeugen erfassen zahlreiche Steuergeräte Betriebszustands- und Umgebungsdaten, um komplexe Assistenzsysteme funktionsfähig machen zu können. Diese Daten werden in unterschiedlicher Weise und Dauer gespeichert und verarbeitet. Insbesondere in jüngster Zeit verbleiben solche Daten nicht mehr nur im Fahrzeug. Zunehmend werden sie über dauerhafte Funkverbindungen nach außen kommuniziert, z. B. zum Hersteller oder zu Anbietern von Servicediensten. Um die datenschutzrechtliche Komplexität der ablaufenden Vorgänge erfassen zu können, muss unterschieden werden zwischen unterschiedlichen Datenkategorien, den Schnittstellen, über die Daten auslesbar oder kommunizierbar sind, den unterschiedlichen Betroffenen (Halter, Fahrer, Arbeitnehmer bei Dienstfahrzeugflotten, Nutzer von Mietwagen), den Lebenszyklen eines Fahrzeugs (Kauf, Leasing, Weiterveräußerung) sowie den Beteiligten, die Interesse an den anfallenden Daten haben (Versicherer, Anbieter von Servicediensten, Multimediaanbieter, öffentliche Stellen, Infrastrukturbetreiber). Deswegen wird mich dieses Thema sicher noch einige Zeit begleiten. Dennoch kann bereits jetzt Folgendes festgehalten werden:

- Alle bei der Nutzung von Fahrzeugen anfallenden Daten sind personenbezogen, keine der Daten sind deshalb datenschutzrechtlich irrelevant.

- Ich sehe die Automobilindustrie in der Verantwortung, ihre Produkte datenschutzgerecht zu gestalten und entsprechend auf Zulieferer und Anbieter von Zusatzdiensten, die die technische Autoinfrastruktur nutzen, einzuwirken.

- Dementsprechend ist auch die Automobilindustrie auf die datenschutzrechtlichen Grundsätze von privacy by design und privacy by default verpflichtet.

- Fahrzeugnutzern gegenüber müssen die im Fahrzeug ablaufenden Datenerhebungs- und -verarbeitungsvorgänge absolut transparent sein.

- Die Kommunikation zwischen Fahrzeug und Hersteller muss nach dem aktuellen Stand der Technik sicher gestaltet sein.

Nach Vorarbeiten des Arbeitskreises Verkehr hat die Datenschutzkonferenz auf ihrer Herbstsitzung 2014 in einer Entschließung datenschutzrechtliche Forderungen an die Automobilindustrie formuliert (vgl. Anlage 12). Fast zeitgleich und daher unabhängig hiervon veröffentlichte auch der Verband der deutschen Automobilindustrie (VDA), der Hersteller wie Zulieferer vertritt, eigene „Datenschutzprinzipien“. Kurz vor Ende des Berichts-

zeitraums begannen direkte Gespräche zwischen dem Arbeitskreis Verkehr und dem VDA. Bislang erfolgte ein Austausch grundlegender datenschutzrechtlicher Positionen. Ich bin zuversichtlich, dass der eingeleitete Dialog zu konkreten Ergebnissen führen wird, die den berechtigten Datenschutzinteressen genauso gerecht werden wie den Erfordernissen der technologischen Entwicklung.

Daneben hat sich das BMVI mit Themen befasst, die ohne Beachtung von Datenschutz und Datensicherheit nicht sinnvoll bearbeitet und gedacht werden können und die das Thema „Datenschutz im Kraftfahrzeug“ noch erweitern (zum künftig EU-weit vorgeschriebenen E-Call vgl. Nr. 14.6). So berate ich den sogenannten Runden Tisch „Automatisiertes Fahren“. Dieser versammelt im Wesentlichen Industrie, Wissenschaft, Versicherer und Verbraucherschützer, um die Herausforderungen abzustecken und erste Antworten auf Fragen zu formulieren, die sich aus der Entwicklung automatisierter Fahrsysteme ergeben können. Auch Datenschutz- und Datensicherheitsaspekte sind hierbei frühzeitig zu bedenken. Schon jetzt erscheint klar, dass solche Systeme die Erhebung und Verarbeitung einer noch nicht überschaubaren Anzahl an personenbezogenen Daten notwendig machen werden. Dafür notwendige Vorkehrungen in rechtlicher und technologischer Hinsicht sind frühzeitig zu bedenken, um den datenschutzrechtlichen Grundsatz von Privacy by Design umsetzen zu können.

Zum anderen hat mich die Entwicklung der so genannten Car-to-Car-Kommunikation beschäftigt. Sie soll es Fahrzeugen ermöglichen, über spezielle Funkverbindungen Informationen auszutauschen, um sich z. B. gegenseitig vor Gefahrenstellen zu warnen oder selbständig Kollisionen in Kreuzungsbereichen zu vermeiden. Soweit mir Informationen vorliegen, wächst in mir die Sorge, bei der Entwicklung der Kommunikationsstandards und der Festlegung von Art und Umfang der zu übermittelnden Datenkategorien könnte der Grundsatz von privacy by design nicht ausreichend beachtet werden. Insbesondere scheinen keine ausreichenden Vorkehrungen dafür getroffen zu werden, dass im Car-to-Car-Netz befindliche Fahrzeuge nicht verfolgbar sind und das Netz ausreichend gegen Angriffe von außen geschützt ist. Wie auch im Bereich der herstellereigenen Online-Kommunikation von Fahrzeugen lassen sich hier Datenschutz- von Datensicherheitserwägungen nicht sinnvoll trennen. Die Sicherheit der Verkehrsinfrastruktur ist von überragender Bedeutung. Daher müssen Bedrohungspotentiale analysiert und technische Vorkehrungen darauf abgestimmt werden. Ich werde die Entwicklung weiter beobachten und Datenschutz- und Datensicherheitsstandards einfordern, wenn die staatliche Verkehrsinfrastruktur das Kommunikationsnetz zwischen den Fahrzeugen für eigene Zwecke nutzen will.

Mir sind die positiven Wirkungen des technologischen Fortschritts in der Automobilindustrie durchaus bewusst. Neuartige Systeme, für deren Funktionalität viele beim Fahrzeugbetrieb entstehende Daten verarbeitet werden müssen, können in Punkto Sicherheit und Effizienz der Verkehrslenkung vorteilhaft sein. Die Industrie muss dabei aber auch ihrer datenschutzrechtlichen Verantwortung nachkommen. Wichtig sind Transparenz, Datensparsamkeit und weitestgehende Erhaltung der Datenherrschaft beim Betroffenen. Die oft gestellte Frage danach, wem die Daten „gehören“, führt in die Irre, da das deutsche Datenschutzrecht nicht auf der Idee von „Eigentum an Daten“ fußt. Mitilfe der datenschutzrechtlichen Grundsätze der Betroffenheit und der verantwortlichen Stelle lässt sich auch die beschriebene Thematik in den Griff bekommen.

Ich sehe es als große Chance für die deutsche Autoindustrie, ihre Marktposition im globalen Kontext durch datenschutzfreundliche Gestaltung ihrer Produkte zu sichern bzw. auszubauen. Ihre technologische Führungsposition kann dazu führen, dass sich solche Technologien auch herstellerübergreifend durchsetzen. Ich bin überzeugt, Kunden werden zunehmend datenschutzfreundliche Technologien nachfragen und den Grad ihres Vertrauens in die Hersteller daran messen.

14.2 Keine Papiervignette für die geplante PKW-Maut

Die Bundesregierung setzt auf eine elektronische Mauterhebung; eine Papiervignette wäre die datenschutzfreundlichere Lösung.

Mit der PKW-Maut sollen finanzielle Mittel für Erhalt und Ausbau der Straßenverkehrsinfrastruktur der Bundesfernstraßen gewonnen werden.

Bei der Ressortabstimmung zum sogenannten Infrastrukturabgabegesetz, mit dem die PKW-Maut eingeführt werden soll, habe ich mich für die Erhebung der PKW-Maut in Form einer Papiervignette eingesetzt. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Stellung bezogen und sich in einer Entschließung ebenfalls für die Erhebung der PKW-Maut mittels Papiervignette ausgesprochen (vgl. Anlage 13). Denn für diese Form der Mauterhebung brauchen keine personenbezogenen Daten der Mautpflichtigen erhoben zu werden.

Die Bundesregierung ist meiner Empfehlung nicht gefolgt und hält in ihrem mittlerweile dem Deutschen Bundestag vorliegenden Gesetzentwurf an der Mauterhebung durch elektronische Vignetten fest.

Unabhängig von der Entscheidung gegen die Papiervignette enthielt der ursprüngliche Gesetzentwurf auch im Übrigen datenschutzrechtlich problematische Vorschriften. Dies betraf etwa den Umfang der elektronischen Kontrollen, deren Ausgestaltung sowie die Frist zur Löschung von Daten nach der Durchführung von Erstattungsverfahren. Insoweit hat die Bundesregierung meine entsprechenden Empfehlungen im Gesetzentwurf umgesetzt und die Kontrollen der Einhaltung der Mautpflicht auf Stichproben beschränkt. Auch wurde festgeschrieben, dass das bei der Mautkontrolle aufgenommene Bild des Kraftfahrzeuges nicht die Fahrzeuginsassen wiedergeben darf. Ferner werden die bei der Stichprobenkontrolle erhobenen Daten sofort gelöscht, wenn die Mautzahlung nachgewiesen ist.

14.3 Rechtskonforme Löschung dient der Verwaltungseffizienz - auch bei der Untersuchung von Seeunfällen

Die rechtskonforme Löschung personenbezogener Daten spart Verwaltungskosten und setzt die gesetzlichen Prinzipien von Datenvermeidung und Datensparsamkeit um - eine „Win-Win-Situation" für Verwaltung und Datenschutz.

Mit einem Kontrollbesuch beim Seeamt Kiel habe ich mir den Umgang mit personenbezogenen Daten bei der Untersuchung von Seeunfällen nach dem Seesicherheits-Untersuchungs-Gesetz (SUG) angesehen.

Bestehen nach einem Seeunfall hinreichende tatsächliche Anhaltspunkte, dass eine Berechtigung zu entziehen oder die Ausübung der mit ihr oder einem Befähigungszeugnis oder einer Fahrerlaubnis verbundenen Befugnisse zu beschränken ist, prüft die Generaldirektion Wasserstraßen und Schifffahrt Außenstelle Nordwest in Aurich als sog. Vorprüfstelle unverzüglich das Untersuchungsinteresse. Ist eine der obigen Maßnahmen wahrscheinlich zu erwarten, beantragt sie beim Seeamt, den Fall zu untersuchen. Es erhält von ihr die hierfür erforderlichen wasserschutzpolizeilichen und staatsanwaltschaftlichen Unterlagen. Diese werden vom Seeamt kopiert und die Originale zurückgegeben. Die Kopien sind Teil der Seeamts-Akte.

Optimierungsbedarf bestand bezüglich der rechtskonformen Löschung der Seeamts-Akten. Sie werden zehn Jahre lang ab Beginn des jeweiligen seeamtlichen Verfahrens aufbewahrt und dann vernichtet. Der vorgefundene Aktenbestand reichte jedoch bis 2002 und damit mehr als zehn Jahre zurück. Mittlerweile hat das Seeamt entsprechend meiner Auffassung die mehr als zehn Jahre aufbewahrten Akten komplett vernichtet. Zudem hat es für die seeamtlichen Verfahren ab 2003 ein entsprechendes Löschkonzept erarbeitet.

Wie die stichprobenartige Sichtung von Akten ergab, enthielten diese auch Daten von Personen (in der Regel weitere Besatzungsmitglieder am Unfall beteiligter Schiffe), bei denen spätestens bei Eintritt der Rechtskraft des seeamtlichen Spruchs feststand, dass ihre Speicherung nicht mehr erforderlich war. Das Seeamt hat bis zum Ende des Berichtszeitraums den Aktenbestand gesichtet und diese Unterlagen aus fast allen Akten entfernt und

vernichtet. Die Prüfung einer Teilvernichtung der Akten bei Eintritt der Rechtskraft ist mittlerweile ebenso Bestandteil des seeamtlichen Löschkonzepts, wie der Umgang mit Auskünften aus dem Bundeszentralregister und dem Verkehrszentralregister zu Beteiligten des seeamtlichen Verfahrens, die auch wegen ihrer Löschfristen in einschlägigen Fachgesetzen (Bundeszentralregistergesetz und Straßenverkehrsgesetz) zu vernichten sind, sobald sie für die Durchführung des seeamtlichen Verfahrens nicht mehr benötigt werden.

Unanfechtbare seeamtliche Sprüche können nach § 49 Absatz 8 SUG einschließlich der Schiffsnamen in einer amtlichen Entscheidungssammlung veröffentlicht werden, wenn Namen natürlicher Personen anonymisiert werden. Der Schiffsname erlaubt jedoch Rückschlüsse auf Besatzungsmitglieder, aber auch auf einen zum Unfallzeitpunkt ggf. an Bord befindlichen Lotsen. Der Schiffsname muss nach der gesetzlichen Regelung nicht zwingend veröffentlicht werden. Das Seeamt hat mir mitgeteilt, meiner Empfehlung nachzukommen und künftig die Schiffsnamen nur dann zu veröffentlichen, wenn ein allgemein bekannter Seeunfall und ein erkennbar breites öffentliches Interesse vorliegen und die Veröffentlichung im Interesse der Förderung der Seesicherheit zweckdienlich ist.

Das Seeamt nimmt seit 2010 an dem Pilotprojekt „AdeBA“ (Ablaufoptimierung durch elektronische Bearbeitung und Aktenverwaltung) der Wasser- und Schifffahrtsverwaltung des Bundes teil. Ziel ist die ausschließlich elektronische Aktenführung. Zum Zeitpunkt des Kontrollbesuchs hat die für das Seeamt zuständige Registratur ihr von der Poststelle zugeleitete Schriftstücke zwar eingescannt, anschließend aber die Originale in Papierform weitergeleitet. Das Seeamt konnte den Vorgang nun elektronisch und in Papierform bearbeiten. Die Möglichkeit elektronischer Vorgangsbearbeitung wurde nur als Hilfsmittel zur Ablage von Informationen genutzt, so dass nur redundante, nicht revisionssichere Teilbestände vorhanden sind. Dies ist hinnehmbar, wenn es der Arbeitserleichterung dient und technisch-organisatorische Maßnahmen nach § 9 BDSG und dessen Anlage getroffen sind. Da bisher systemseitig keine Löschroutinen vorgesehen sind, ist eine manuelle Löschung nicht mehr erforderlicher kompletter Ordner und einzelner Dateien vorzunehmen. Ich habe diesbezüglich empfohlen, bei der weiteren Durchführung des Pilotprojekts und eines möglichen Rollouts eines anschließenden Wirkbetriebs sicherzustellen, dass datenschutzrechtlichen Erwägungen (insbesondere Revisionssicherheit sowie technisch-organisatorische Maßnahmen nach § 9 BDSG und dessen Anlage) Rechnung getragen wird. Dabei sind Dateien auch vor unbefugtem Zugriff zu schützen; sie dürfen nicht mehr Informationen enthalten als die Papierakte. Meine Empfehlungen wurden durch eine Verfahrensanweisung inzwischen umgesetzt.

14.4 Fahrleistungserhebung 2014

Die Bundesanstalt für Straßenwesen (BASt) ermittelte die Fahrleistung von Kraftfahrzeugen innerhalb eines Jahres auf Deutschlands Straßen. Die damit verbundenen datenschutzrechtlichen Probleme haben die BASt und das Kraftfahrtbundesamt (KBA) hervorragend gelöst.

Die BASt hatte vom BMVI den Auftrag erhalten, die Inanspruchnahme der Straßeninfrastruktur aktuell zu erheben. Um aussagekräftige Ergebnisse zu erhalten, wurde das Projekt in zwei parallel durchgeführte Teile gegliedert. Fahrzeuge mit ausländischem Kennzeichen sollten auf allen deutschen Straßen gezählt werden. Aussagen über den deutschen Individualverkehr sollten hingegen durch eine Befragung von Haltern in Deutschland zugelassener Kraftfahrzeuge getroffen werden. Die BASt hat frühzeitig die mit der Durchführung beider Projektteile verbundenen datenschutzrechtlichen Fragen erkannt und mich bereits im Vorfeld um Beratung gebeten.

a) Zählung des ausländischen Individualverkehrs

Um festzustellen, wie viele ausländische Kraftfahrzeuge auf deutschen Straßen (Autobahn, Bundes-, Land-, Kreisstraßen) unterwegs sind, mussten diese Daten in Form einer vorher definierten Stichprobe gewonnen werden. Frühere Auswertemethoden, wie z. B. Zählungen beim Grenzübertritt, waren wegen des Wegfalls der Kontrollen an den Binnengrenzen nicht mehr möglich. Neben einer datenschutzrechtlich unproblematischen reinen

Zählung sollte auch die Art des Kraftfahrzeugs und seine Herkunft erfasst werden. Dies ist nur mit dem Einsatz von Videotechnik möglich.

Die BASt hatte vor Beginn der Zählung ein umfangreiches Datenschutzkonzept entwickelt, das die Speicherung und Auswertung personenbezogener oder -beziehbarer Daten ausschloss. Das hierfür ausgesuchte Videosystem erfüllte diese Voraussetzungen: Die Zählungen konnten mittels automatisierter Videobeobachtung des fließenden Verkehrs an zufällig ausgewählten Straßenabschnitten und Tagen stattfinden. Das System erfasst das Kennzeichen mittels einer Front- und einer Rückkamera, wobei die Herkunft des Fahrzeuges anhand der Kennzeichensyntax erkannt wird. Durch den Einsatz besonderer Videotechnik ist eine Durchsicht durch die Scheiben der Fahrzeuge und somit ein Erkennen der Fahrzeuginsassen ausgeschlossen. Nur die Nationalität, nicht aber das komplette Kennzeichen wird im System gespeichert und mit einem Zeitstempel versehen. Zusätzlich erfolgt eine Fahrzeugklassifizierung (LKW, Pkw, Motorrad etc.) durch Radardetektoren.

Meine Empfehlungen zur Anonymisierung, zum Ausschluss der Personenerkennbarkeit und nicht zuletzt zur Transparenz durch Kennzeichnung der Erhebungsstelle und Information der Verkehrsteilnehmer durch Hinweisschilder und Erläuterungen im Internet wurden umgesetzt. Trotz der Dauer der Erhebung von einem Jahr, an 520 zufällig ausgewählten Standorten in 52 Landkreisen jeweils über 24 Stunden, sind mir keine größeren Probleme bei der Durchführung bekannt geworden.

b) Inländerfahrleistung

Um die Fahrleistung von in Deutschland zugelassenen Kraftfahrzeugen zu ermitteln hatte die BASt das KBA beauftragt. Dort stehen Informationen über alle Halter im Zentralen Fahrzeugregister (ZFZR) zur Verfügung, das als Grundlage für die Befragung diente. Ich habe mir im Rahmen eines Kontrollbesuchs beim KBA ein Bild von der Umsetzung des Auftrags gemacht, dem ein umfängliches Datenschutzkonzept zugrunde liegt.

Bei der Inländerfahrleistung handelt es sich um eine empirische Erhebung in sechs Wellen über den gesamten Zeitraum des Jahres 2014. Der Erhebungszeitraum einer Welle betrug zehn Wochen, in denen die insgesamt 156.000 zufällig ausgewählten Fahrzeughalter einen inhaltlich mit mir abgestimmten Fragebogen erhalten haben. Zehn Wochen nach der ersten Kontaktaufnahme erhielt der Halter dann einen Schlussfragebogen mit weiteren Fragen zur Fahrleistung des Fahrzeugs.

Aufgrund einer festgelegten Schichtung nach Fahrzeugklassen, Antriebsart, Krafträder, Lastkraftwagen usw. hatte die Abteilung „Statistik“ des KBA eine Projektdatei auf der Grundlage des aktuellen ZFZR erstellt, um die Halter anzuschreiben. Die zufällig ausgewählten Personen konnten den übermittelten Fragebogen schriftlich oder elektronisch ausfüllen. Ich habe mich vom datenschutzgerechten Umgang bei Herstellung und Versand der Fragebögen überzeugt. Hierbei war mir wichtig, die Aufgaben der Abteilung „Statistik“ räumlich und personell von den Aufgaben der Abteilung „Register“ zu trennen, um Personenverwechslungen auszuschließen. Auch die Rückläufe der ausgefüllten Fragebögen wurden ausschließlich von den Mitarbeiterinnen und Mitarbeitern der Abteilung „Statistik“ bearbeitet. Wie neben dieser strikten Trennung besonders hervorzuheben ist, hat das KBA durch eine interne Qualitätssicherung Fehler bei der Zuordnung der eingehenden Antworten nahezu ausgeschlossen. Alle schriftlich oder elektronisch eingegangenen Antworten wurden nach einer Erhebungswelle anonymisiert und einem von der BASt beauftragten Institut zur Berechnung des Ergebnisses weitergeleitet.

Die im Auftrag der BASt und im Datenschutzkonzept des KBA vereinbarten bzw. niedergeschriebenen Regelungen zum Schutz personenbezogener Daten sind in vorbildlicher Weise umgesetzt worden.

14.5 Kontrollbesuch beim Bundesamt für Seeschifffahrt und Hydrographie

Das Seeleute-Befähigungsverzeichnis (SBV) und hiermit im Zusammenhang stehende Verwaltungsvorgänge sind getrennt voneinander zu führen. Dies gilt auch bezüglich der frühestmöglichen Löschung von Vorgangsinhalten.

Mein Besuch beim Bundesamt für Seeschifffahrt und Hydrographie (BSH) galt dem Umgang mit personenbezogenen Daten bei der Führung des SBV, der hiermit zusammenhängenden Vorgangsbearbeitung, zu der auch die Ausstellung der Seeleute-Ausweise zählt, sowie der Führung des Internationalen Seeschifffahrtsregisters. Das SBV ist das Verzeichnis erteilter, abgelaufener oder erneuerter, ausgesetzter, widerrufener oder als verloren oder vernichtet gemeldeter Befähigungszeugnisse einschließlich der zugehörigen Vermerke sowie der sonstigen Nachweise über Befähigungen im Schiffsdienst von Seeleuten. Im Rahmen der Vorgangsbearbeitung werden die für das Verwaltungsverfahren erforderlichen Informationen und die Daten, die Bestandteil des SBV sind, gemeinsam gespeichert. Der Datenkranz der im SBV zu speichernden Daten ist abschließend gesetzlich geregelt. Weitere, für den Verwaltungsvorgang erforderliche Daten müssen also separat gespeichert werden. Das BSH hat schon während meines Besuchs angekündigt, dies künftig durch entsprechende technisch-organisatorische Maßnahmen sicherzustellen. Das begrüße ich.

Die Vorgangsbearbeitung erfolgt formulargestützt. Ich habe dem BSH empfohlen, die hierin aufgrund der gesetzlichen Verpflichtung zur Speicherung in das SBV zu machenden Angaben besonders zu kennzeichnen und den Antragsteller auf die elektronische Speicherung im SBV hinzuweisen. Auf freiwillige Angaben, die z. B. der erleichterten Kontaktaufnahme bei Rückfragen dienen, sollte ausdrücklich hingewiesen werden.

Wie bei der Prüfung deutlich wurde, werden alle Vorgangsbestandteile bis zum Ende der allgemeinen Aufbewahrungsfrist von zehn Jahren gespeichert. Ich habe dem BSH empfohlen, die Unterlagen zu löschen, die schon vorher für die Aufgabenerfüllung nicht mehr erforderlich sind. Das BSH hat sein Löschkonzept selbst als überarbeitungsdürftig angesehen und angekündigt, dies zeitnah in Angriff zu nehmen.

Das BSH arbeitet auch mit Freitextfeldern, die vom jeweiligen Bearbeiter befüllt werden können. Freitextfelder bergen das prinzipielle Risiko nicht für die Aufgabenerfüllung erforderlicher Eintragungen. Zur Verringerung dieses Risikos haben meine Mitarbeiter empfohlen, die Freitextfelder im Umfang zu minimieren und darüber hinaus mit einer katalogartigen Aufzählung eintragungsfähiger, also für die Aufgabenerfüllung erforderlicher Einträge zu verknüpfen.

Nach § 62 Seeleute-Befähigungsverordnung können Seeleute einen sog. Seeleute-Ausweis beantragen. Dieser gilt in Verbindung mit einem gültigen Reisepass oder Personalausweis und stellt keinen eigenständigen Identitätsnachweis dar. Dennoch wird ein solcher Ausweis in vielen Häfen weltweit insbesondere als Legitimation zum Verlassen oder Betreten eines Schiffes benötigt. Die früher ausgeteilten Ausweise in Papierform tauscht das BSH gegenwärtig sukzessive gegen Plastikkarten im Scheckkartenformat aus. Entsprechende Kartendrucker und Kartenrohlinge befinden sich in einem Raum, der zum Zeitpunkt des Besuchs nicht abgeschlossen und somit für jeden zugänglich war. Das BSH hat dies auf meine Empfehlung noch während des Besuchs abgestellt. Durch vorhandene elektronisch gesicherte Schlösser können jetzt nur noch zuständige Mitarbeiter den Raum betreten.

Die Führung des Internationalen Seeschifffahrtsregisters (ISR) durch das BSH begegnete hingegen keinen datenschutzrechtlichen Bedenken.

14.6 E-Call - Leben retten mit personenbezogenen Daten

Das E-Call-System ist geeignet, durch ein schnelleres Auslösen der Rettungskette viele Menschenleben zu retten. Es birgt aber auch datenschutzrechtliche Risiken, denen der europäische Gesetzgeber grundsätzlich angemessen Rechnung trägt.

Aufgrund einer Änderung der EU-Typengenehmigungsvorschriften müssen voraussichtlich ab 2018 in allen neu entwickelten Autos sog. E-Call-Systeme verbaut werden. Bei einem Unfall wird dann ein vordefinierter Datensatz automatisch oder von einem Fahrzeuginsassen manuell ausgelöst und über Mobilfunk an die nächstgelegene Rettungsleitstelle gesandt. Diese kann unverzüglich die Rettungskette in Gang setzen und zusätzlich eine Sprachverbindung zum Fahrzeug herstellen.

Zu den übermittelten Daten gehören die Geokoordinaten, die Uhrzeit, die Fahrtrichtung sowie die Fahrzeugidentifikationsnummer. Eine solche - in aller Regel automatische, d. h. von einer konkreten Willensbekundung des Betroffenen unabhängige - Datenübermittlung birgt aber auch datenschutzrechtliche Risiken. An dem zugehörigen Rechtsetzungsprozess auf EU-Ebene bin ich durch das BMVI eingebunden worden. Zudem habe ich an den Sitzungen der nationalen E-Call-Implementierungsplattform teilgenommen.

Regelungen zu E-Call finden sich einerseits in einem Beschluss, nach dem Mitgliedstaaten ein System aus Notrufleitstellen aufbauen müssen, das die über E-Call eingehenden Notrufe verarbeiten kann. Die an die Leitstellen übermittelten Daten dürfen ausschließlich für die mit dem Beschluss verfolgten Rettungszwecke genutzt werden. Die Verantwortung für den Aufbau und den - datenschutzgerechten - Betrieb dieser Leitstellen liegt in Deutschland bei den Bundesländern.

Neben diesem Beschluss wird eine EU-Verordnung die Spezifikationen für die im Fahrzeug verbaute Technik regeln. Diese Verordnung war bei Redaktionsschluss noch nicht abschließend behandelt, der maßgebliche Text liegt mir also noch nicht vor. Er wird aber wohl relativ ausführliche datenschutzrechtliche Regelungen enthalten. Insbesondere geht es darum, dass Fahrzeuge im Normalbetrieb - d. h. außerhalb eines E-Call-auslösenden Unfallereignisses - durch Nutzung der E-Call-Module nicht verfolgbar sein dürfen. Leider konnte nicht erreicht werden, Haltern bzw. Nutzern die Möglichkeit einzuräumen, das verbaute E-Call-System abzuschalten.

Ebenfalls bei Redaktionsschluss noch nicht abschließend geklärt war die Art und Weise, wie sich künftig das Zusammenspiel zwischen E-Call, das in jedem Fahrzeug verbaut sein wird, und herstellereigenen Notrufdiensten gestalten wird. Allerdings werden wohl E-Call und solche Dienste nicht gleichzeitig aktiv sein. E-Call soll aber jedenfalls dann einspringen, wenn der jeweilige Zusatzdienst vom Kunden nicht gebucht ist oder nicht funktionieren sollte. Letztlich und unabhängig von der technischen Ausgestaltung müssen aber solche Angebote für Autofahrer klar vom E-Call-Dienst unterscheidbar bleiben. Nur so können Fahrer und Nutzer entscheiden, ob sie statt des E-Call-Dienstes einen Herstellerdienst nutzen wollen, der möglicherweise mehr Daten aus dem Fahrzeug übermittelt als notwendig.

14.7 Nationale Plattform Elektromobilität

Wenn sich Deutschland zum Leitmarkt und Leitanbieter für Elektromobilität entwickeln soll, darf der Datenschutz nicht vergessen werden.

Am 3. Mai 2010 wurde die Nationale Plattform Elektromobilität gegründet, um Deutschland als Leitmarkt und Leitanbieter für Elektromobilität zu etablieren. Vertreter aus Industrie, Wissenschaft und Politik erarbeiten in mehreren Arbeitsgruppen Strategien zur Umsetzung dieses ehrgeizigen Ziels. Im Rahmen eines nationalen Entwicklungsplanes gibt es eine Vielzahl von geförderten Forschungsprojekten und Modellregionen rund um das Thema Elektromobilität.

Elektromobilität wird eng in die elektronischen Kommunikationsnetze eingebunden sein. Aufgrund großer Standzeiten einzelner Fahrzeuge könnten Elektromobile darüber hinaus auch eine Rolle als Zwischenspeicher zur Aufnahme von temporären Überkapazitäten in der Energieerzeugung beim Smart Grid spielen, dem neuen intelligenten Stromnetz (vgl. Nr. 8.2). Auch weitergehende Szenarien wie etwa bei der Heimvernetzung sind denkbar. Die Infrastruktur aus Ladesäulen, die Anbindung an das intelligente Stromnetz und an elektronische Kommunikationsdienste sowie deren Verknüpfung mit Navigationshilfen und anderen Fahrunterstützungssystemen sind mit einer umfangreichen Datenerhebung und -verarbeitung verbunden. Daher gibt es viele Stellen, die Interesse an den dabei anfallenden Daten haben, um etwa Energieleistungen abrechnen zu können. Dies stellt eine große Herausforderung für den Datenschutz dar. Ein datenschutzgerechtes Konzept wird nach meiner Überzeugung ein wesentlicher Erfolgsfaktor des Projekts.

Auf meine Anregung hat sich das Karlsruher Institut für Technologie (KIT) in einer Studie unter datenschutzrechtlichen Aspekten und Berücksichtigung der unterschiedlichen energiewirtschaftlichen Marktrollen mit möglichen Szenarien beim Bezug von Fahrstrom in einer öffentlichen Ladeinfrastruktur und dessen Abrechnung befasst. Die Vorschrift des § 21g Energiewirtschaftsgesetz aus dem Jahr 2011 enthält zwar grundsätzliche datenschutzrechtliche Vorgaben. Jedoch fehlen insoweit spezielle Normen für den Bereich der Elektromobilität. Daher müssen die für den Datenschutz maßgeblichen Regelungen aus den allgemeinen Vorgaben des Energiewirtschaftsgesetzes abgeleitet werden. Mit einer aus dieser Studie Anfang 2013 hervorgegangenen Bachelorarbeit werden die möglichen Szenarien dargestellt und auf mögliche Problemfelder hingewiesen, die es bei der vorgesehenen Konkretisierung des § 21g Energiewirtschaftsgesetz durch die Datenkommunikationsverordnung zu berücksichtigen gilt.

Im 3. Fortschrittsbericht der Nationalen Plattform Elektromobilität wurde meine Forderung aufgenommen, Datenschutz und Datensicherheit bereits in der Konzeptionsphase beim Aufbau der neuen Mobilitätskonzepte zu berücksichtigen. Der guten Absicht, dabei den Ansatz eines „privacy by design“ mitzudenken, müssen nun auch die entsprechenden Taten folgen. Bei der Entwicklung der möglichen Geschäftsmodelle rund um die Elektromobilität sollen im Sinne eines „privacy by default“ auch solche Modelle berücksichtigt werden, die eine anonyme Nutzung von Elektromobilitätsangeboten ermöglichen. Eine Abrechnung von Ladevorgängen über den vertraglich gewählten Stromanbieter für den Hausstrom ist zwar komfortabel, es sollte aber immer auch möglich sein, Ladestrom z. B. mit anonym erwerbbaren Prepaid-Karten zu beziehen. Ich werde die Aktivitäten der Nationalen Plattform Elektromobilität weiter begleiten und die Marktentwicklung kritisch verfolgen.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Arbeitkreis Verkehr
Nationale Plattform Elektromobilität.
Runder Tisch Automatisiertes Fahren (BMVI)
Nationale eCall Implementierungsplattform (BMVI)

B. Zudem von besonderem Interesse

Nr. 5.14.5, 8.2, 18.1

15 Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit

15.1 Die Deutsche Umweltstudie zur Gesundheit

Bei einer Kontrolle im Umweltbundesamt stand die für den Zeitraum 2014-2017 vorgesehene Deutsche Umweltstudie zur Gesundheit im Zentrum.

Bei einem Beratungs- und Kontrollbesuch in Berlin habe ich mir einen Überblick über den Umgang des Umweltbundesamts mit personenbezogenen Daten verschafft.

Da das Umweltbundesamt in erster Linie reine Umweltforschung betreibt, benötigt es bei seiner Tätigkeit nur selten personenbezogene Forschungsdaten. Eine Ausnahme bildet die Deutsche Umweltstudie zur Gesundheit, die früher unter der Bezeichnung Umweltsurvey bekannt war. In der für 2014-2017 laufenden nunmehr fünften Welle dieser Studie wird der Einfluss von Umweltfaktoren auf Kinder und Jugendliche untersucht. Die Probanden werden vom Robert-Koch-Institut aus den für die dort durchgeführte Studie zur Gesundheit von Kindern und Jugendlichen (KiGGS) Befragten rekrutiert. Das Umweltbundesamt erhält vom Robert-Koch-Institut die Adressdaten der Familien, die zur Teilnahme bereit sind. Ein Auftragnehmer des Umweltbundesamt führt zur Probenentnahme Hausbesuche bei den Probanden durch. Zudem werden ebenfalls vom Robert-Koch-Institut zur Verfügung gestellte Blut- und Urinproben an das Umweltbundesamt übermittelt. Schriftlich füllen die Probanden noch einen Fragebogen zu ihren Lebensgewohnheiten aus. Alle Erhebungsdaten werden für die Auswertung mit einer nicht-sprechenden Identifikation verbunden. Die datenschutzrechtliche Ausgestaltung des Forschungskonzepts ist insgesamt sehr ausgereift und zeugt von einem gewissenhaften, umsichtigen und professionellen Umgang mit personenbezogenen Forschungsdaten.

Abgesehen von dem konkret betrachteten Forschungsprojekt konnte ich im Umweltbundesamt auch im Übrigen ein hohes Maß an datenschutzrechtlichem und -praktischem Problembewusstsein und Engagement feststellen. Ich habe im Nachgang des Besuchs lediglich ein übergreifendes Datenschutzkonzept angeregt, da bislang die relevanten Informationen auf verschiedene Dokumente verteilt sind. Bei einer einheitlichen Information ist es einfacher, einen raschen Überblick über Datenschutzfragen beim Umweltbundesamt zu erhalten. Auch dies stärkt den Datenschutz.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16 Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

16.1 Auch im Informationszeitalter gilt: Datenschutz für Forschungsdaten

Im Herbst des Jahres 2014 nahm der Rat für Informationsinfrastrukturen seine Arbeit auf.

Der Rat für Informationsinfrastrukturen wurde auf Beschluss der Gemeinsamen Wissenschaftskonferenz (GWK) von Bund und Ländern und auf Empfehlung des Wissenschaftsrats und weiterer Organisationen für eine zunächst vierjährige Projektphase eingerichtet. Im Rat sind die wissenschaftlichen Nutzer, die Einrichtungen der Informationsinfrastrukturen selbst sowie Bund und Länder vertreten. Daneben gehören ihm Vertreterinnen und Vertreter des öffentlichen Lebens an. Der Rat soll beratend und koordinierend für die Selbstorganisation der Wissenschaft sowie für Bund und Länder in der GWK wirken und die Weiterentwicklung der wissenschaftlichen Informationsinfrastrukturen vorantreiben, „indem sich die Akteure des Wissenschaftssystems über die Erarbeitung disziplinen- und institutionenübergreifender Strategien und Standards verständigen“, wie es hierzu im Koalitionsvertrag für die 18. Wahlperiode des Bundestags heißt.

Vom Rat angefragt, habe ich gerne meine Mitarbeit zugesagt. Dabei sehe ich meine Aufgabe vor allem darin, Aspekte des Forschungsdatenschutzes gerade auch im Zusammenhang mit der Veröffentlichung und Weitergabe von Forschungsdaten in die Ratsarbeit einzubringen. Forschungsdaten sind - vor allem in den Sozialwissenschaften - in vielen Fällen personenbezogen. Daher ist es notwendig, stets ein angemessenes Verhältnis zwischen der Wissenschaftsfreiheit des Forschers und dem Recht auf informationelle Selbstbestimmung des Einzelnen zu finden, gerade wenn es um den Zugang zu vorhandenen Forschungsdaten für Dritte geht. Datenschutzrechtliche Standards sind umso dringlicher, als sich die Forschungsdatenlandschaft angesichts der zunehmenden Digitalisierung rasant verändert. Vor diesem Hintergrund begrüße ich die Einrichtung des Rates für Informationsinfrastrukturen, der für die damit zusammenhängenden Fragen Lösungen erarbeiten kann.

16.2 Das Projekt PEREK - Ressortforschung im Bundesinstitut für Berufsbildung

Eine Kontrolle des Bundesinstituts für Berufsbildung (BIBB) galt vor allem einem exemplarischen Forschungsprojekt sowie der Arbeit des Forschungsdatenzentrums.

Mit einem Beratungs- und Kontrollbesuch beim BIBB habe ich mir einen Überblick über den Umgang dieser Ressortforschungseinrichtung mit personenbezogenen Daten verschafft.

Dabei wurde das abgeschlossene Projekt PEREK - Betriebliche Qualifikationsbedarfsdeckung im Fachkräftebereich wachsender Beschäftigungsfelder - vorgestellt. Dieses Projekt ist in methodischer Hinsicht insoweit exemplarisch für die Forschungstätigkeit des BIBB, als es auf Ergebnissen von Betriebsbefragungen basiert. Die Befragungen selbst wurden „technisch“ von Auftragnehmern des BIBB durchgeführt. Die hierfür notwendigen Betriebsdaten erhielten die Auftragnehmer direkt vom Institut für Arbeitsmarkt- und Berufsforschung (IAB) der Bundesagentur für Arbeit. Dieses zog eine Stichprobe aus der IAB-eigenen Betriebsdatenbank. Die gezogenen Adressdaten sowie Angaben zu Betriebsgrößenklasse und Wirtschaftszweig wurden auf einer CD (Einschreiben, Passwort zur Entschlüsselung mit gesondertem Schreiben) auf Grundlage eines Datenlieferungsvertrags mit dem BIBB direkt an den Auftragnehmer gesendet. Das IAB forderte nach Ende der Befragung eine Bestätigung an, dass die übermittelten Daten gelöscht seien.

Die Auftragnehmer lieferten die aus der Umfrage hervorgegangenen Ergebnisdatensätze dann anonymisiert, d. h. ohne Rückschlussmöglichkeit auf einzelne befragte Betriebe, an das BIBB. So gelangen keine Betriebsdaten, die auch personenbezogene bzw. -beziehbare Daten enthalten können, an das BIBB selbst. Außerdem wurden Experteninterviews, teils vom BIBB selbst und teils leitfadengestützt von Auftragnehmern durchgeführt.

Wie sich zusammenfassend festhalten lässt, stellt die Lieferung von sensiblen Betriebsdaten direkt vom IAB an mit dem BIBB verbundene Auftragnehmer - wie bei PEREK - den Regelfall dar; das BIBB hat daher von diesen Daten keine Kenntnis. Der vom IAB vorausgesetzte hohe Sicherheitsstandard für die Bereitstellung von Betriebsdaten strahlt positiv auf das BIBB aus. Durch ein eigenes, mit erfahrenen Mitarbeitern besetztes Forschungsdatenzentrum wird zudem sichergestellt, dass die Weitergabe der im BIBB generierten Forschungsdaten an Wissenschaftler stets datenschutzgerecht erfolgt.

Im BIBB ist ein hohes Maß an datenschutzrechtlichem Problembewusstsein vorhanden und der Dokumentationsstand ist zufriedenstellend. Die laufende Novellierung des IT-Sicherheitskonzeptes begleite ich weiterhin. Im Jahr 2014 führten meine Mitarbeiter außerdem auf Bitte des BIBB eine datenschutzrechtliche Grundschulung durch. Diese Initiative hat mich gefreut, zeigt sie doch, dass Kontrollbesuche meiner Mitarbeiter auch eine vertrauensvolle Zusammenarbeit der kontrollierten Behörde mit meiner Dienststelle fördern können.

16.3 Neues in der Biometrie

Neue Techniken bei der Aufnahme von biometrischen Merkmalen wie auch die Nutzung von Komfortanwendungen bergen so manches datenschutzrechtliche Risiko.

Der Verbreitungsgrad von Produkten, die Biometrie als Zugangsschutz einsetzen, wird durch sogenannte Komfortanwendungen ständig größer. Immer mehr Nutzer verwenden z. B. die vom Hersteller ihres Handys oder des Notebooks ermöglichte Absicherung des Gerätes durch Fingerabdruckscanner. Aber auch in anderen Geschäftsbereichen werden Fingerabdruckanwendungen eingesetzt, z. B. bei Bezahlsystemen. Vor einer entsprechenden Nutzung müssen sich die Bürger zunächst mit ihren Daten inklusive des Fingerabdrucks am System anmelden. Die Daten werden anschließend in einer Datenbank des Systembetreibers, auf einer Smartcard oder auf dem Gerät selbst gespeichert. Bei der Nutzung des Systems werden dann die aktuell aufgenommenen Daten mit den hinterlegten verglichen. Bei einem erfolgreichen Vergleich wird die Nutzung des Gerätes freigegeben. Seitens einer deutschen Bank ist geplant, Handys (derzeit nur das Modell eines bestimmten Herstellers) künftig im Zusammenspiel mit einer Applikation für das Online-Banking nutzbar zu machen. Der Fingerabdrucksensor des Handys dient dabei als Verifikationsinstrument.

Ein grundsätzliches Datenschutz- und Sicherheitsproblem bei der Nutzung von Biometrieverfahren - nicht nur bei Handy oder Notebook - ist dabei die Ungewissheit, wo die Biometriedaten gespeichert werden, wer Zugriff auf diese Daten erhält und an wen die Daten möglicherweise weitergegeben werden. So haben Hersteller bereits bestätigt, dass Fingerabdrücke nicht nur lokal auf dem Handy, sondern für Sicherungszwecke auch in der Datenbank des Herstellers (in der Regel im Ausland) gespeichert werden. Das hohe Datenschutzniveau Deutschlands ist somit dafür nicht mehr garantiert.

Ein weiteres Problem ist die sog. Überwindungssicherheit der Biometriesysteme. Gemeint ist die Sicherheit, dass das System nicht durch nachgeahmte oder auf eine andere Weise gefälschte Daten getäuscht und der Zugangsschutz somit überwunden werden kann. Diese ist häufig nicht garantiert, wie erfolgreiche Überwindungsversuche gezeigt haben. Beispielsweise wurden Bilder des Gesichts, der Iris oder eines Fingers, die mit einer geeigneten Digitalkamera aufgenommen wurden, für die Herstellung von gefälschten Datensätzen, sog. Fakes, genutzt, und das System akzeptierte diese. Besondere Brisanz erfährt das Thema daher bei neuen Verfahren zur Erkennung des Fingerabdrucks, die berührungslos arbeiten. Ähnlich wie bei der Gesichts- oder Iriserkennung wird ein Foto des Fingers mit seinen Merkmalen aufgenommen und mit den gespeicherten Daten abgeglichen. Ein direkter physischer Kontakt ist hierbei nicht mehr notwendig. Die Bilder von den Merkmalen können dabei auch unbeobachtet aufgenommen werden. Biometrieverfahren, die nicht über Sicherheitsfunktionen wie z. B. der Lebenderkennung verfügen, können mit derartigen Techniken möglicherweise überwunden werden. Wie sicher die Systeme sind, werden Tests in der Zukunft zeigen.

Ich rate daher, Biometrie nur dort einzusetzen und zu nutzen, wo Datenschutz und Sicherheit gewährleistet und die Daten vor Missbrauch geschützt werden. Anbieter von biometrischen Verfahren sind aufgefordert, über die Sicherheit des Verfahrens und den Umgang mit den sensiblen biometrischen Daten ihrer Kunden zu informieren. Dies betrifft insbesondere die nichtautorisierte weitere Nutzung der Daten für andere Zwecke oder gar Weitergabe der Daten an Dritte. Nur auf der Grundlage entsprechender Informationen können die Nutzer abwägen, ob sie biometrischen Verfahren vertrauen oder nicht.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit
- Arbeitskreis Wissenschaft,
- Arbeitskreis Datenschutz und Bildung,
- Arbeitskreis Technik

NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA) mit
- NA 043-01-37 AA Arbeitsausschuss Biometrie

Arbeitskreis Identitätsmanagement und Datenschutz-Technologien beim DIN

Teletrust Arbeitsgruppe 3 Biometrie

Rat für Informationsinfrastrukturen (RFII) (gegründet von der Gemeinsamen Wissenschaftskonferenz von Bund und Ländern (GWK))

B. Zudem von besonderem Interesse

Nr. 2.2, 3.1.4, 5.6, 5.14, 5.14.1, 5.14.2, 5.14.3, 5.14.4, 5.14.5, 8.4, 8.5

17 Ausschuss für Kultur und Medien

17.1 Digitales Zwischenarchiv kann datenschutzgerecht betrieben werden

Mit dem Vollzug des E-Government-Gesetzes wird es zu einer flächendeckenden Einführung elektronischer Aktenführungssysteme kommen. Das Bundesarchiv betreibt schon heute ein digitales Zwischenarchiv im Pilotbetrieb mit der Bundesagentur für Arbeit (BA) als Auftragsdatenverarbeiter im Sinne von § 11 BDSG.

Das E-Government-Gesetz gibt den Bundesbehörden vor, ihre Akten elektronisch zu führen. Auch bei elektronischer Aktenführung müssen die Behörden die Grundsätze ordnungsgemäßer Aktenführung genauso einhalten, wie dies bei der Papierakte der Fall ist. Akten, die nicht mehr in Bearbeitung sind, sind noch eine bestimmte Zeit lang aufzubewahren, bevor sie vernichtet oder wegen ihrer besonderen Bedeutung für die Zeitgeschichte dem Bundesarchiv zur dauerhaften Aufbewahrung angeboten werden können. Für diese Zeit gibt es sog. Zwischenarchive. Bislang bietet das Bundesarchiv Bundesbehörden an, ihre nicht mehr für die aktuelle Bearbeitung erforderlichen Akten in einem bzw. mehreren Zwischenarchiven aufzubewahren.

In einem Pilotprojekt prüft das Bundesarchiv, wie ein Digitales Zwischenarchiv beschaffen sein muss, damit bei elektronischer Aktenführung die langfristige Aufbewahrung der Akten genauso sichergestellt werden kann, wie dies derzeit in der Papierwelt der Fall ist. Als technischem Dienstleister, der die entsprechende Ausstattung und Rechenkapazität zur Verfügung stellt, bedient sich das Bundesarchiv der BA. Diese betreibt bereits seit einiger Zeit für sich selbst ein elektronisches Langzeitarchiv und darf bestimmte Dienstleistungen wie die Archivierung von elektronischen Objekten gegen Kostenerstattung auch anderen Bundesbehörden zur Verfügung stellen (§ 368 Abs. 2 SGB III).

Das Pilotprojekt befindet sich noch in der Anfangsphase. Das Bundesarchiv hat mich um datenschutzrechtliche Beratung gebeten, insbesondere um die Verantwortlichkeiten für die Verarbeitung personenbezogener Daten zwischen den Beteiligten herauszuarbeiten. Bei der geplanten Konstruktion handelt es sich um eine Auftragsdatenverarbeitung. Eine Behörde, die ihre Akten an das Bundesarchiv zur Aufbewahrung im Zwischenarchiv abgibt, bleibt sowohl archiv- wie auch datenschutzrechtlich verantwortlich für die Akten und die darin befindlichen personenbezogenen Daten. Die Auslagerung der eigenen aufzubewahrenden Akten erfordert einen Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG. Der Auftragnehmer Bundesarchiv bedient sich insoweit der Unterauftragnehmerin BA. Es steht allerdings noch nicht fest, ob das Bundesarchiv in dieser Konstruktion auch das eigene Ziel verfolgen wird, schon vor Ablauf der Aufbewahrungsfrist auf die Daten zuzugreifen, um mit der Prüfung der Archivwürdigkeit zu beginnen. Nach meiner Auffassung fehlt es hierfür an einer Rechtsgrundlage, die spätestens mit Beginn des Wirkbetriebes vorhanden sein müsste.

Ich habe mir einen Überblick über die verschiedenen Konzepte sowohl des Bundesarchivs als auch der BA verschafft und dazu im Hinblick auf die Datensicherheit keine grundsätzlichen Bedenken. Das von der BA vorgestellte IT-Sicherheitskonzept ist auf den Schutzbedarf „hoch“ ausgelegt und beschreibt hohe Hürden für den unberechtigten Zugriff auf archivierte Daten. Die Administration der Datenträger, Datenbanken und Archivprozesse liegt in den Händen unterschiedlicher Organisationseinheiten bzw. Personen. Insbesondere der Zugang zu den Datenträgern ist ohne Begleitung von Sicherheitspersonal nicht möglich und erfolgt nur zum Auswechseln von Datenträgern, die anschließend unverzüglich der Vernichtung zugeführt werden. Auch wenn die Rekonstruktion eines Archivs aus den gespeicherten Daten alleine möglich ist, wird auf diese Art ausgeschlossen, dass dies durch Diebstahl von Datenträgern geschehen könnte. Aus den Datenbankeinträgen allein lassen sich hingegen weder ein Archiv, noch einzelne Aktenbestände rekonstruieren. Das Benutzer- und Rollenmanagement befindet sich vollständig in den Händen der jeweils nutzenden Behörden. Die im Übrigen vorgesehenen Maßnahmen zur Mandantentrennung, Protokollierung und mindestens logischen Trennung von Netzwerken schließen unberechtigte Manipulationsversuche soweit aus, dass für den Schutzbedarf „hoch“ eine verschlüsselte Datenablage nicht erforderlich scheint. Dies würde im Übrigen auch der Revisionsfähigkeit des Archivs zuwiderlau-

fen. Nach derzeitigem Kenntnisstand erscheint das Projekt daher als ein tragfähiges Konzept zum Betrieb eines datenschutzgerechten Digitalen Archivs.

Ich werde das Bundesarchiv bei der Fortführung des Projektes weiter begleiten.

17.2 Beratungs- und Kontrollbesuche beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

Der datenschutzrechtliche Umgang mit den Stasi-Unterlagen entsprach der nach wie vor hohen Sensibilität dieser Dokumente.

Einen Schwerpunkt meiner Beratung und Kontrolle in zwei Außenstellen des Bundesbeauftragten für die Unterlagen des Staatsicherheitsdienstes der ehemaligen DDR (BStU) bildete die Einhaltung datenschutzrechtlicher Vorschriften bei der Bearbeitung von Anträgen auf Auskunft und Einsicht in die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR gemäß §§ 12 ff. Stasi-Unterlagen-Gesetz (StUG) einschließlich der eingesetzten IT-Unterstützung (sog. datenschutzrechtliche Ablaufkontrolle). Ferner habe ich Aspekte der äußeren und inneren Sicherung der Stasi-Unterlagen gemäß § 40 StUG und des mit diesen im Zusammenhang stehenden behördlichen Schriftverkehrs (sog. Behördenvorgänge) und dessen Nachweis intensiv geprüft und erörtert.

Einen weiteren Schwerpunkt bildeten Fragen der Videoüberwachung der Liegenschaften. Anhand meiner Orientierungshilfe „Datenschutzrechtliche Grundlagen der Videoüberwachung in der öffentlichen Verwaltung des Bundes“ (vgl. 24. TB Anlage 7) habe ich geprüft, ob die Videoüberwachung der jeweiligen Liegenschaften vor dem Hintergrund der in § 40 StUG normierten Vorschriften zur Sicherung der Stasiunterlagen erforderlich war. Hierbei galt es vor allem zwischen Sicherungsaspekten und dem datenschutzrechtlichen Gebot der Datensparsamkeit bei der Videoüberwachung abzuwägen.

Wie bei beiden Beratungs- und Kontrollbesuchen festzustellen war, hatten die jeweiligen Außenstellen den getroffenen organisatorischen Maßnahmen ein hohes Maß an datenschutzrechtlicher Sensibilität zu Grunde gelegt. Gleichwohl habe ich einzelne Verbesserungsvorschläge gemacht. Ich lege Wert darauf, dass diese auch in anderen Außenstellen des BStU, soweit einschlägig, umsetzt werden.

Daneben findet jährlich ein datenschutzbezogener Austausch zwischen meinen Mitarbeitern und der behördlichen Datenschutzbeauftragten des BStU statt. Auf diese Weise können unbürokratisch Lösungen für aktuelle datenschutzbezogene Fragen gefunden und umgesetzt werden.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

18 Ausschuss Digitale Agenda

18.1 Die Digitale Agenda der Bundesregierung 2014-2017 - nicht ohne Datenschutz

Mit dem Regierungsprogramm „Digitale Agenda 2014-2017“ erläutert die Bundesregierung, wie sie den digitalen Wandel unserer Gesellschaft in naher Zukunft fördern und absichern will. Dazu zeigt sie in verschiedenen Politikfeldern wie „Digitale Infrastrukturen“, „Digitale Wirtschaft und digitales Arbeiten“, „Innovativer Staat“ oder „Sicherheit, Schutz und Vertraulichkeit für Gesellschaft und Wirtschaft“ Forderungen und Ziele auf, die innerhalb der nächsten drei Jahre erreicht oder zumindest auf den Weg gebracht werden sollen. Um die Bedeutung dieses Themenfeldes weiß auch der Deutsche Bundestag. Er hat parallel dazu einen eigenen Ausschuss „Digitale Agenda“ eingerichtet, der sich fachübergreifend netzpolitischen Themen widmet. Der Datenschutz muss ein integrativer Bestandteil dieser Überlegungen sein.

Die Bundesregierung hat erkannt, dass mit den Vorteilen einer digitalisierten Welt auch Gefahren für den Einzelnen, die Wirtschaft und das Gemeinwohl einhergehen. Deswegen werden der Datenschutz und das informationelle Selbstbestimmungsrecht in der Digitalen Agenda ausdrücklich genannt. Fehlentwicklungen soll gegengesteuert werden. Dies bedeutet auch, neue Regeln zu schaffen, wo dies erforderlich ist. Die Digitale Agenda spricht von einem „modernen Ordnungsrahmen zur Sicherstellung von Freiheit, Transparenz, Datenschutz und -sicherheit“. Hierzu zählt sicherlich die für das Jahr 2015 angekündigte Verabschiedung der europäischen Datenschutz-Grundverordnung (vgl. dazu Nr. 1), die die Digitale Agenda selbst anspricht. Die Datenschutz-Grundverordnung setzt in einer global-digitalisierten Welt zu Recht einen starken Akzent auf den Aspekt des Datenschutzes durch Technik. Darüber hinaus kann ich mir vorstellen, dass die Instrumente Zertifizierung und Selbstregulierung an Bedeutung gewinnen werden, entweder im Wege freiwilliger Selbstverpflichtungen der Wirtschaftsteilnehmer oder mittels regulierter Selbstregulierung durch förmlich mit den Datenschutzbehörden abgestimmten Verhaltensregeln.

Wie die Bundesregierung zu Recht betont, muss unsere bestehende Werteordnung auch in der digitalen Welt ihre Geltung behalten. Dies schließt insbesondere das Grundrecht auf informationelle Selbstbestimmung ein. Hierzu gehört Transparenz bei Art, Umfang und Dauer der Datenverwendung, damit dieses Grundrecht nicht zur bloßen Worthülse verkommt.

Beeinträchtigungen drohen von staatlicher wie von privater Seite, sowohl aus dem In- als auch aus dem Ausland. „Als Antwort“ auf die globale Vernetzung und die Enthüllungen über den Missbrauch personenbezogener Daten kündigt die Bundesregierung an, Gespräche mit internationalen Partnern aufzunehmen. Deutschland soll eine führende Rolle bei der Entwicklung internationaler Datenschutzprinzipien einnehmen. Beleg für dieses Engagement ist die gemeinsam mit Brasilien initiierte Resolution zum Recht auf Privatheit im digitalen Zeitalter, die am 18. Dezember 2013 in der Generalversammlung der Vereinten Nationen einstimmig angenommen wurde. Die Resolution hat das in Artikel 17 des Internationalen Pakts über Bürgerliche und Politische Rechte (IPBPR) vom 19. Dezember 1966 niedergelegte Recht auf Privatheit unterstrichen (vgl. auch Nr. 4.1). Ich begrüße, dass sich die Bundesregierung auch weiterhin für einen besseren Schutz der Privatsphäre auf internationaler Ebene einsetzt, in dem sie, wiederum mit Brasilien, eine erneute Resolution Ende des Jahres 2014 in die Generalversammlung eingebracht hat, die einen Schwerpunkt auf Datenschutz im Internet legt.

Allerdings machen globale Datenströme auch eine verbesserte globale Datenschutzaufsicht und insoweit eine vertiefte Zusammenarbeit der Aufsichtsbehörden erforderlich. Hierzu gibt es Initiativen der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) sowie der Internationalen Datenschutzkonferenz (vgl. Nr. 4.4 und 4.5). Die Mitgliedsstaaten der OECD sind durch die im Sommer 2013 neu gefassten Richtlinien zum Schutz der Privatsphäre aufgerufen, die Voraussetzungen für eine intensivierte Kontrolle grenzüberschreitender Datenströme zu schaffen. Ferner hat die Internationale Datenschutzkonferenz im Rahmen ihrer 36. Tagung im Jahr 2014 eine Entschließung zur verstärkten globalen Kooperation der Datenschutzaufsichtsbe-

hörden verabschiedet und als Verfahrensgrundlage hierfür ein entsprechendes „Cooperation Arrangement“ akzeptiert. Die Entschließung ist auf meiner Internetseite unter www.datenschutz.bund.de abrufbar.

Nach dem Willen der Bundesregierung soll Deutschland „Verschlüsselungsstandort Nr. 1 auf der Welt“ werden. Die Verschlüsselung privater Kommunikation soll zum Standard werden. Auch soll die Anwendung von Sicherheitstechnologien wie De-Mail weiter ausgebaut werden. Denkbar und begrüßenswert wäre zudem, wenn z. B. Mailprogramme unterschiedlicher Hersteller die Nutzung zueinander kompatibler Verschlüsselungsverfahren unterstützen würden.

Die Sicherheit der IT-Systeme und der Schutz der Daten werden als Querschnittsthemen der Digitalisierung bezeichnet. Um diese zu erreichen, sollen u. a. die BNetzA, das BSI, das BKA und das BfV sachlich und personell verstärkt werden. Eine meiner Kernaufgaben ist es, Bundesbehörden zu beraten und zu kontrollieren und so dafür zu sorgen, dass Bürgerinnen und Bürger nicht von staatlichen Stellen in ihrem Grundrecht auf informationelle Selbstbestimmung verletzt werden. Seit Langem fordere ich daher eine bessere Stellenausstattung auch meiner Dienststelle - bislang vergeblich. Eine Stärkung der Datenschutzaufsicht zum Schutz der Daten und zur Sicherheit der IT-Systeme ist mehr als erforderlich. Dies auch deshalb, weil die Digitalisierung vor den Sicherheitsbehörden nicht Halt macht und auch aus dieser Richtung neue Gefahren für den Datenschutz drohen. Die Nachrichtendienste des Bundes und das BKA werden weiter als Zentralstellen gestärkt. Der Begriff der „Zentralstelle“ wird dabei nicht mehr als Einschränkung angesehen in Abgrenzung zu den im föderalistischen System stärkeren Kompetenzen der Sicherheitsbehörden in den Ländern. Die Zentralstellen ziehen vielmehr bundesweit Datenverarbeitung an sich. Der Trend geht zur zentralen Auswertung und Analyse. Im Bereich des Verfassungsschutzes wird zurzeit sogar diskutiert, den - als Teil des verfassungsrechtlichen Verhältnismäßigkeitsprinzips essentiellen - Grundsatz der Erforderlichkeit in weiten Bereichen durch den Relevanzgrundsatz zu ersetzen. Gespeichert wird dann nicht mehr, was erforderlich ist, um eine konkrete Gefahr abzuwehren oder eine gefährliche Bestrebung zu beobachten. Gegenstand ist vielmehr alles, was für allgemeine Auswerte- und Analysezwecke irgendwie „relevant“ sein könnte. Personenbezogene Daten werden dadurch zunehmend von konkreten Zweckbindungen losgelöst.

Die Bundesregierung hat angekündigt, bei der Umsetzung der Digitalen Agenda die verschiedenen Akteure, insbesondere auch die Beauftragten für den Datenschutz zu beteiligen. Dass dies allein durch die zwei geplanten Kernelemente gelingen kann, nämlich die Ausrichtung des IT-Gipfels auf die Digitale Agenda sowie die Einrichtung eines ressortübergreifenden Steuerungskreises, bezweifle ich allerdings.

Der Staat soll nach der Digitalen Agenda Vorbild für die Digitalisierung in Deutschland sein, und zwar auch durch fortschrittliche IT-Sicherheit und Datenschutz bei seinen Verwaltungsangeboten. Ein Aspekt dabei ist die Digitale Verwaltung 2020 der Bundesregierung, die es sich zum Ziel gesetzt hat, eine effiziente elektronische Verwaltung sowie einfache und schnelle staatliche elektronische Dienstleistungen zu fördern (vgl. dazu auch Nr. 5.1). Ein Aspekt der Optimierung digitaler Verwaltungsangebote ist die IT-Konsolidierung des Bundes, bei der aus datenschutzrechtlicher Sicht allerdings einige organisatorische „Stolpersteine“ zu beachten sind (vgl. Nr. 5.9 und Nr. 5.14.4).

Im Bereich der Wirtschaft - Stichwort „Industrie 4.0“ - will die Bundesregierung u. a. durch die Unterstützung bei der Entwicklung und Verbreitung sicherer und datenschutzfreundlicher Big-Data- und Cloud-Anwendungen neue Geschäftsmodelle und Dienstleistungsinnovationen anstoßen. Außerdem sollen die Rahmenbedingungen des E-Commerce unter Wahrung des Verbraucher- und Datenschutzes fortentwickelt werden. Gleichzeitig soll ein Verbandsklagerecht zur Verbesserung des Datenschutzes eingeführt werden, um den Verbraucherschutz in der digitalen Welt zu stärken (vgl. unter Nr. 6.1). Zudem sollen Datenschutz bei der Konzeption und Entwicklung neuer Technologien (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default) gefördert und eingefordert werden. Weiter sieht die Bundesregierung Handlungsbedarf beim Schutz des geistigen Eigentums. Sie will die rechtlichen Rahmenbedingungen an die fortschreitende Digitalisierung anpassen. Hierbei müssen die verschiedenen Interessen angemessen berücksichtigt und in einen gerechten Ausgleich gebracht werden. Schließlich hat die Bundesregierung den Entwurf eines IT-Sicherheitsgesetzes zum Schutz kriti-

scher Infrastrukturen verabschiedet, mit dem gesetzliche Vorgaben zu Mindeststandards und eine Meldepflicht für erhebliche IT-Sicherheitsvorfälle eingeführt werden. Ich unterstütze diese Initiative und konnte bereits in den Entwurf einige datenschutzrechtliche Verbesserungen einbringen, z. B. eine Klarstellung zur Speicherfrist der von Protokolldaten (vgl. Nr. 5.14.5).

Im Energiebereich will die Bundesregierung den Aufbau intelligenter Netze weiter vorantreiben. Für die dafür notwendigen Kommunikationsinfrastrukturen sind Standards u. a. zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität erarbeitet worden. Noch 2014 soll mit der Schaffung verlässlicher Rahmenbedingungen für den sicheren Einsatz von intelligenten Messsystemen begonnen werden. Diese Ankündigung kommt reichlich spät, denn alle Beteiligten warten schon seit geraumer Zeit darauf, dass die Bundesregierung durch ein Verordnungspaket von der entsprechenden Ermächtigung im Energiewirtschaftsgesetz Gebrauch macht, um dort enthaltene Datenschutzgrundsätze mit Leben zu füllen (vgl. Nr. 8.2).

Insgesamt ist das in der digitalen Agenda an vielen Stellen zum Ausdruck gebrachte datenschutzrechtliche Problembewusstsein ermutigend. Allerdings vermag ich bei der Digitalen Agenda nicht in allen Bereichen zu erkennen, „wo die Reise hingeht“ bzw. was die Bundesregierung konkret plant, um die von ihr gesetzten Ziele zu erreichen.

Ich hoffe sehr, dass sie ihre Ankündigung einhält, die Datenschutzaufsichtsbehörden bei der Umsetzung der Digitalen Agenda einzubeziehen. Die Datenschutzaufsichtsbehörden werden selbstverständlich ihre Erfahrungen und Anregungen für eine datenschutzgerechte digitale Gesellschaft in Deutschland einbringen.

A. Mitarbeit der BfDI in Gremien zu diesem Themenkreis

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Mitarbeit in der Ressort-AG Digitale Verwaltung 2020 (beratendes Mitglied)

B. Zudem von besonderem Interesse

Nr. 2.1, 2.2, 3.1.4, 5.1, 5.14, 5.14.1, 5.14.2, 5.14.3, 8.4, 8.5, 8.6, 16.3

19 Bekämpfung des Dopings im Sport

19.1 Bekämpfung des Dopings im Sport

Der neue WADA-Code und die nationale Initiative für ein Gesetz zur Bekämpfung von Doping im Sport (Anti-Doping-Gesetz) haben dem Antidopingkampf einen neuen Impuls gegeben. Viele datenschutzrechtliche Fragen bleiben indes unberücksichtigt.

Am 1. Januar 2015 ist ein neuer Anti-Doping-Code der Welt-Anti-Doping-Agentur (WADA) in Kraft treten. Zeitgleich wird an einem nationalen Anti-Doping-Gesetz (AntiDopG) gearbeitet. Beide Regelwerke werfen in hohem Maße datenschutzrechtliche Fragen auf. Ich unterstütze den Vorstoß der Bundesregierung, den Kampf gegen Doping zu verbessern. Gleichwohl darf das Grundrecht der Sportlerinnen und Sportler auf informationelle Selbstbestimmung nicht auf der Strecke bleiben.

An der Erarbeitung des neuen WADA-Codes war ich im Rahmen der Artikel-29-Gruppe beteiligt (vgl. Nr. 3.1.3). Die wiederholt gegenüber der WADA ausgesprochenen Empfehlungen wurden im nunmehr verabschiedeten WADA-Code leider im Wesentlichen nicht berücksichtigt. Die Artikel-29-Gruppe wird daher die Umsetzung des WADA-Codes in den Mitgliedstaaten genau beobachten. Im Fokus steht hierbei u. a. das Erheben und Speichern von Aufenthaltsangaben und Gesundheitsdaten der Sportlerinnen und Sportler im ADAMS-Betriebssystem der WADA. Diese sensiblen Angaben werden in großem Umfang und in hoher Detailtiefe seitens der WADA verlangt. Bedenklich ist ebenso, dass die ADAMS-Datenbank in Quebec, Kanada, betrieben wird und ein angemessenes Datenschutzniveau nicht gewährleistet ist (vgl. insgesamt auch 24. TB Nr. 8.14).

Ich begrüße es, dass mit dem Entwurf eines Anti-Doping-Gesetzes nun endlich eine gesetzliche Grundlage für die Erhebung, Verarbeitung und Nutzung von Daten der Athletinnen und Athleten durch die Stiftung Nationale-Anti-Doping-Agentur Deutschland (NADA) geschaffen werden soll. Sie löst die von mir und anderen Datenschützern immer wieder heftig kritisierte „Einwilligungsfiktion“ der betroffenen Sportlerinnen und Sportler ab.

Ich erkenne die Notwendigkeit eines globalen Systems der Dopingbekämpfung bei internationalen Sportveranstaltungen an. Dieses muss aber die Grund- und Menschenrechte auf Privatheit und Wahrung der Intimsphäre sowie auf Schutz der persönlichen Daten angemessen berücksichtigen und im Einklang mit deutschem und europäischem Datenschutzrecht stehen.

Bei der Dopingbekämpfung kommt es zu einer Vielzahl sensibler Eingriffe in das Grundrecht auf informationelle Selbstbestimmung von Athletinnen und Athleten. Solche Eingriffe müssen im Interesse des Grundrechtsschutzes wie auch der Rechtssicherheit aller Beteiligten klar gesetzlich geregelt und auf das unbedingt Verhältnismäßige und Erforderliche begrenzt werden.

Ein Gesetz zur Bekämpfung von Doping im Sport muss daher klaren verfassungsrechtlichen Anforderungen genügen. Es muss, dem verfassungsrechtlichen Wesentlichkeitsgrundsatz folgend, die grundrechtsrelevanten Aspekte der Regelungsmaterie durch eindeutige und bestimmte gesetzliche Vorgaben einer Lösung zuführen. Der Gesetzentwurf offenbart hier Mängel:

Durch die pauschale Bezugnahme des Gesetzestextes auf „das Dopingkontrollsystem der Stiftung Nationale Anti Doping Agentur Deutschland“ (Artikel 1, § 8 Abs. 1, § 9 Satz 1, § 10 Abs. 1 und 2 AntiDopG-E) entledigt sich der Gesetzgeber seiner Aufgabe, selbst einen Ausgleich der widerstreitenden Interessen - dem Interesse an einem fairen und gesundheitlich verantwortbaren Wettkampfsport einerseits und dem Interesse der Athletinnen und Athleten an der freien Ausübung ihres Berufs sowie an der Wahrung ihrer Privat- und Intimsphäre andererseits - zu finden. Durch die dynamisch angelegte Verweisung auf die jeweiligen Regelungen des Dopingkon-

trollsystems der Stiftung Nationale-Anti-Doping-Agentur Deutschland wird der Gesetzgeber seiner verfassungsrechtlichen Verpflichtung nicht gerecht, selbst eine angemessene Problemlösung zu finden.

Klare Vorgaben zur Datenerhebung, zu Auskunfts- und Widerspruchsrechten, zu Löschfristen und zu Fragen der Datensicherheit fehlen.

Das grundlegende datenschutzrechtliche Prinzip der Zweckbindung findet ebenfalls keine ausreichende Berücksichtigung.

Ich habe mich im Rahmen der Ressortabstimmung nachdrücklich für die Berücksichtigung der Datenschutzrechte der Sportlerinnen und Sportler eingesetzt und datenschutzfreundlichere Regelungsalternativen aufgezeigt. Ich werde kritisch beobachten, ob bei der Umsetzung des WADA-Codes und des Anti-Doping-Gesetzes die Datenschutzrechte der Betroffenen ausreichend gewahrt werden.

A Mitarbeit der BfDI in Gremien zu diesem Themenbereich

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

20 Weitere Ausschüsse

Nachfolgend habe ich dargestellt, welche Beiträge meines Berichtes für weitere Ausschüsse des Deutschen Bundestages von besonderem Interesse sein können

Haushaltausschuss	Nr. 2.4 Unabhängige Datenschutzaufsicht – endlich auch im Bund
Petitionsausschuss	Nr. 8.6 Einsatz von RFID-Systemen - eine datenschutzrechtlich unbefriedigende Situation
Ausschuss für Tourismus	Nr. 1 Revision des europäischen Datenschutzrechts Nr. 3.3 „Smart Borders“ vor dem Intelligenztest Nr. 4.7.3 Fluggastdaten - neue Herausforderungen
Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung	Empfehlung zum Rederecht der BfDI
Ausschuss für wirtschaftliche Zusammenarbeit und Entwicklung	Nr. 4.5 OECD - Arbeitsgruppe für Sicherheit und Privatsphäre in der digitalen Wirtschaft Nr. 7.9 OECD Standard für den automatischen Informationsaustausch über Finanzkonten

21 Präsidium des Deutschen Bundestages

21.1 Eingriffsbefugnisse des Polizeivollzugsdiensts beim Deutschen Bundestag

Ich meine, für Maßnahmen des Polizeivollzugsdienstes des Deutschen Bundestages fehlt eine ausreichende formelle Rechtsgrundlage.

Im Oktober 2012 prüften meine Mitarbeiter im Rahmen eines datenschutzrechtlichen Beratungs- und Kontrollbesuchs u. a. die Tätigkeit des Polizei- und Sicherungsdienstes beim Deutschen Bundestag. Das Hausrecht und die Polizeigewalt in dem Gebäude des Deutschen Bundestages obliegen dessen Präsidenten (Art. 40 Abs. 2 Satz 1 GG). Hieraus ergeben sich öffentlich-rechtliche Befugnisse zur Gefahrenabwehr, die andernfalls den Polizeibehörden zustehen würden. Die Ausübung der polizeilichen Befugnisse ist dem Polizeivollzugsdienst beim Deutschen Bundestag durch eine entsprechende Dienstanweisung übertragen (§ 1 Abs. 1 Satz 3 Dienstanweisung für den Polizeivollzugsdienst beim Deutschen Bundestag - DA-PVD), die auch die konkreten Befugnisse und Eingriffsermächtigungen des Polizeivollzugsdienstes umfasst. Eine Reihe von Eingriffsmaßnahmen, zu denen die als Verwaltungsvorschrift einzustufende Dienstanweisung ermächtigt, besitzen datenschutzrechtliche Relevanz und stellen Eingriffe in das Recht auf informationelle Selbstbestimmung der Besucher des Deutschen Bundestages aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG dar. Ein Beispiel hierfür ist die Nutzung des @rtus-Systems (vgl. 21. TB Nr. 5.3.1). Der Polizeivollzugsdienst des Deutschen Bundestages hat auf Grundlage einer Verwaltungsvereinbarung mit der Bundespolizei Zugang zu diesem Vorgangsbearbeitungssystem und damit auch auf eine Vielzahl personenbezogener Daten. Ich halte weder die Geschäftsordnung des Deutschen Bundestages noch die DA-PVD für eine ausreichende formelle Rechtsgrundlage für Maßnahmen des Polizeivollzugsdienstes des Deutschen Bundestages. Ich habe daher beim Präsidenten des Deutschen Bundestages den Erlass einer gesetzlichen Ermächtigungsgrundlage angeregt. Bei einer Normierung sind insbesondere ein differenziertes Berechtigungskonzept, Zugriffsbeschränkungen, angemessene Löschfristen sowie Betroffenenrechte zu regeln. Daneben habe ich angeregt, die aus dem Jahr 1993 stammende Dienstanweisung an die veränderten datenschutzrechtlichen Anforderungen anzupassen. Der Präsident des Deutschen Bundestages hat mir mitgeteilt, die Erforderlichkeit eines Polizeigesetzes für die Arbeit der Polizei beim Deutschen Bundestag werde geprüft. Außerdem sei die Verwaltung beauftragt worden, einen Entwurf zur Änderung der Dienstanweisung der Polizei unter Berücksichtigung meiner Hinweise zu erarbeiten. Ich werde weiterhin auf die Schaffung einer gesetzlichen Ermächtigung hinwirken und diesbezüglich in Kontakt mit dem Deutschen Bundestag bleiben.

22 Aus meiner Dienststelle

22.1 Smarter Internetauftritt - Cleverer Inhalt

Im Berichtszeitraum wurde mein Internetauftritt weiter mit steigendem Interesse genutzt. Um die Leserinnen und Lesern mit Informationen rund um den Datenschutz schnell, komfortabel und überall versorgen zu können, wurde er umfassend überarbeitet.

Der schnelle Zugang zu Auskünften und die Möglichkeit, Nachrichten immer und überall abrufen zu können, bestimmen heutzutage die Nutzung und den Umgang mit den Medien. Die Informationsbeschaffung über das Internet ist dabei gar nicht mehr wegzudenken. Aber es muss einfach, gezielt und direkt geschehen. Aus diesem Grund habe ich meinen Internetauftritt umfassend überarbeitet. Neben der inhaltlichen Änderung, die eine schlankere Navigation und eine übersichtlichere Struktur bietet, wurde die Internetseite für verschiedene Ausgabegeräte wie Smartphones und Tablets optimiert. Und nach nunmehr fast neun Jahren Internetpräsenz hat meine Seite auch ein neues Design bekommen.

In altbewährter Art ist das Datenschutzforum vom Internetauftritt aus zu erreichen, das sich nach wie vor einer stabilen Anzahl an Nutzerinnen und Nutzern sowie Beiträgen erfreut (vgl. Kasten zu Nr. 22.1).

Kasten zu Nr. 22.1

22.2 Erfahrungsaustausch mit den Datenschutzbeauftragten der obersten Bundesbehörden

Der regelmäßige Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden ist auch im Berichtszeitraum fortgesetzt worden.

Die behördlichen Datenschutzbeauftragten haben eine unverzichtbare Funktion bei der Verwirklichung des Datenschutzes. Neben den Datenschutzkontrollbehörden des Bundes und der Länder bilden sie die zweite Säule der deutschen Datenschutzkontrolle. Um dem Bedarf an datenschutzrechtlicher Beratung und Kontrolle der öffentlichen Stellen des Bundes und der Länder gerecht zu werden, ist es eine unabdingbare Strukturvoraussetzung, in den jeweiligen Behörden über kompetente und mit der Datenverarbeitung ihrer Dienststelle bestens vertraute Ansprechpartner zu verfügen. Diese wichtige Brückenfunktion nehmen die behördlichen Datenschutzbeauftragten ein. Mit ihnen steht und fällt die Qualität und Güte eines proaktiven Datenschutzes in der Verwaltung. Auf Bundesebene gilt dies insbesondere für die behördlichen Datenschutzbeauftragten der obersten Bundesbehörden, wirken sie doch auch als Multiplikatoren in die jeweiligen Geschäftsbereichsbehörden hinein.

Angesichts der fortschreitenden Digitalisierung der Gesellschaft wird in Zukunft die Bedeutung der behördlichen Datenschutzbeauftragten noch weiter wachsen. Mir ist es deshalb ein besonderes Anliegen, sie in ihrer wichtigen Arbeit auch weiterhin zu unterstützen und zu fördern. Deswegen führe ich mit ihnen einen jährlichen Erfahrungsaustausch durch. Hiermit biete ich ein Forum an, in dem sich die Datenschutzbeauftragten über konkrete Probleme bei der Erfüllung ihrer Aufgaben austauschen können. Zudem informiere ich über datenschutzpolitische Entwicklungen und gebe vor dem Hintergrund meiner Beratungs- und Kontrollerfahrungen Hinweise zur datenschutzgerechten Gestaltung von Verfahren in der Verwaltung. Zu meiner Freude stößt die Veranstaltung seit Jahren auf großes Interesse.

Beim Erfahrungsaustausch im April 2013 nahmen Themen des technologischen Datenschutzes und der Datensicherheit einen breiten Raum ein. Zudem wurden das Ergebnis meiner bei den öffentlichen Stellen des Bundes durchgeführten Erhebung über den Einsatz von Videoüberwachung (vgl. 24. TB Nr. 3.3.1) sowie die Probleme bei der Ausgestaltung des Verfahrensverzeichnisses erörtert. Letzteres hat mich veranlasst, zu diesem Thema eine Orientierungshilfe zur Verfügung zu stellen (vgl. oben Nr. 2.6).

Bei der Veranstaltung im April 2014 haben sich die Datenschutzbeauftragten über ihre organisatorische Stellung und ihre Arbeitsmöglichkeiten in den jeweiligen Dienststellen sowie die Frage ihrer dienstlichen Beurteilung ausgetauscht. Schon in den vergangenen Jahren hat sich gezeigt, dass hier im Vergleich der obersten Bundesbehörden untereinander große Unterschiede bestehen; angesichts der auslegungsbedürftigen Regelungen zur Funktion und Aufgabe behördlicher Datenschutzbeauftragter in §§ 4f, 4g BDSG ist dies auch nicht weiter verwunderlich. Ich halte es für notwendig und geboten, Mindestanforderungen an Organisationen und Aufgabenbeschreibung für eine einheitliche Ausgestaltung des Amtes in der gesamten Bundesverwaltung zu definieren.

22.3 Besuche ausländischer Delegationen

Datenschutzexperten, insbesondere aus Asien und Osteuropa, haben meine Dienststelle besucht, um aktuelle Fragen des Datenschutzes zu diskutieren und Erfahrungen auszutauschen.

Wie in den Vorjahren habe ich auch im Berichtszeitraum gerne ausländische Delegationen in meiner Dienststelle empfangen. Den Erfahrungsaustausch mit Datenschutzexperten aus Japan konnte ich fortsetzen (vgl. 24. TB Nr. 15.4). Eine Gruppe des japanischen Ministeriums für Wirtschaft, Handel und Industrie habe ich über das Konzept des Datenschutzes in Deutschland und die nationalen Erfahrungen mit dem europäischen Recht informiert.

Zur Unterstützung der Datenschutzbehörden in den Kandidatenländern der EU sowie im Rahmen der Europäischen Nachbarschaftspolitik habe ich - vermittelt durch die Europäische Kommission - Delegationen der Republik Moldau und aus Albanien in meiner Dienststelle in Bonn und in meinem Verbindungsbüro in Berlin empfangen. Gesprächsthemen waren u. a. die gesetzlichen Regelungen und praktischen Erfahrungen mit dem Datenschutz in Deutschland, Fragen der Dienststellenorganisation und des Haushalts sowie aktuelle datenschutzrechtliche Themen, wie z. B. die europäische Datenschutzreform.

Dem Erfahrungsaustausch im Hinblick auf die Ausgestaltung der Unabhängigkeit der Datenschutzbehörden (vgl. oben Nr. 2.4) dienten wechselseitige Besuche von und bei der österreichischen Datenschutzaufsicht.

An dieser Stelle möchte ich den ausländischen Kollegen herzlich danken, die persönlich zur Feier meiner Amtseinführung am 4. Februar 2014 nach Bonn gekommen sind und die ich bei dieser Gelegenheit kennengelernt habe.

Zudem habe ich mich sehr gefreut, kurz nach meinem Amtsantritt die Präsidentin der französischen Datenschutzbehörde (CNIL) in meinem Büro in Berlin empfangen zu können.

22.4 Präsenz in Berlin

Die Einrichtung des Verbindungsbüros hat sich bewährt.

Das seit 2008 in Berlin-Mitte eingerichtete Verbindungsbüro koordiniert weiterhin die Termine meiner Dienststelle in Berlin. Wie in den vergangenen Jahren betrifft dies insbesondere die Ausschusssitzungen des Deutschen Bundestages und Besprechungen bei den Bundesressorts. Im Jahr 2014 war verstärkt meine Anwesenheit im 1. Untersuchungsausschuss („NSA"), erforderlich. Das Verbindungsbüro umfasst derzeit dreizehn Mitarbeiterinnen bzw. Mitarbeitern, wobei jedes Referat meiner Dienststelle mit mindestens einem Mitarbeiter vertreten ist.

Weiterhin gilt, dass sich die Einrichtung des Verbindungsbüros hervorragend bewährt hat. Seit seiner Einrichtung konnte eine Vielzahl der Termine in Berlin von Mitarbeiterinnen und Mitarbeitern des Verbindungsbüros wahrgenommen werden; eine wirkungsvolle und direkte Teilnahme am politischen Geschehen in der Bundeshauptstadt ist damit sichergestellt. Der Dienstreiseaufwand meiner Bonner Dienststelle konnte so deutlich verringert werden.

Inzwischen ist das Verbindungsbüro auch Sitzungsort für Arbeitsgruppen und Unterarbeitsgruppen der Datenschutzkonferenz geworden. Zudem werden, soweit dies möglich ist, auch Besuchergruppen in meinen Diensträumen in Berlin empfangen. Im Berichtszeitraum wurden 42 Besuchergruppen unterschiedlichster Parteien betreut. Im Vergleich zum vorhergehenden Berichtszeitraum ist dies eine Steigerung von 17 Prozent.

22.5 Personelle Ausstattung

Der Aufgaben- und Arbeitsanfall meiner Dienststelle ist weiterhin auf einem hohen Niveau.

Pro Monat haben sich im Berichtszeitraum durchschnittlich 371 Bürgerinnen und Bürger mit ihren Beschwerden und Fragen rund um den Datenschutz an mich gewandt. Gestiegen ist vor allem aber der generelle Aufgaben- und Arbeitsanfall, besonders im Zuständigkeitsbereich der Sicherheitsbehörden. So wurde u. a. am 20. März 2014 durch den Deutschen Bundestag der 1. Untersuchungsausschuss („NSA") eingerichtet, den ich mit einer in meiner Dienststelle eingerichteten Projektgruppe sehr intensiv begleite.

Personellen Zuwachs hat es im Berichtszeitraum nicht gegeben. Vielmehr musste ich im Jahr 2014 durch pauschale Stelleneinsparungen 0,5 Stellen einsparen. Der Stellenhaushalt umfasst derzeit 87 Stellen.

22.6 Forschung braucht Datenschutz, Datenschutz braucht Forschung!

Auch in den Jahren 2013 und 2014 standen meiner Dienststelle jährlich Mittel für Forschungszwecke zur Verfügung.

Hiervon konnte folgender Forschungsauftrag angestoßen werden:

Datenschutzrechtliche Anforderungen zum Cloud Computing

Der strafrechtliche und strafprozessuale Schutz personenbezogener Daten bei der Nutzung von Cloud-Diensten gewinnt auch in der datenschutzrechtlichen Beratungspraxis zunehmend an Bedeutung. Daher sollen bei diesem Forschungsauftrag die rechtlichen und technischen Möglichkeiten und Grenzen des strafrechtlichen und des strafprozessualen Schutzes personenbezogener Daten bei der Nutzung von Cloud Computing untersucht wer-

den. Der Schwerpunkt liegt dabei auf der Reichweite der strafprozessualen Zeugnisverweigerungsrechte (§§ 53, 53a StPO) sowie des strafprozessualen Schutzes vor Zugriffen staatlicher Ermittlungsbehörden auf Cloud-Daten, insbesondere im Rahmen des Beschlagnahmeschutzes (§§ 97, 160a StPO). Dabei spielt auch eine Rolle, ob der Cloud-Dienste-Anbieter seinen Sitz innerhalb der EU/EWR oder in Drittstaaten außerhalb dieses Gebietes hat. Das Forschungsprojekt befindet sich derzeit in der Ausschreibung durch das Beschaffungsamt des BMI. Mit einem Beginn der Arbeiten wird im 2. Quartal 2015 gerechnet.

Das in 2010 angestoßene Forschungsprojekt **„PRIVIDOR - PRIvacy Violation DetectOR“** wird weiterhin in meiner Dienststelle genutzt und wurde in 2014 softwaretechnisch auf den neuesten Stand gebracht.

22.7 BfDI als Ausbildungsbehörde

Referendare, Praktikanten und Anwärter zeigen Interesse am Datenschutz.

Das Interesse an Praktika in meiner Dienststelle ist auch 2013 und 2014 groß geblieben. Insbesondere Studierenden der Rechtswissenschaften und Rechtsreferendaren, die sich für Fragen des Datenschutzes und der Informationsfreiheit interessierten und praktische Kenntnisse erwerben wollten, habe ich einen Einblick in die Aufgaben und Arbeitsweise meiner Behörde gewährt.

Insgesamt haben im Berichtszeitraum 17 Studierende und Referendare Teile ihrer Ausbildung in meinem Hause absolviert. Darüber hinaus konnte ich sechs Anwärtern des gehobenen Verwaltungsdienstes die Möglichkeit bieten, ihr Pflichtpraktikum in meiner Dienststelle abzuleisten.

23 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. 24. TB Nr. 3.3.1 **Versteckte Kamera - auch in der Bundesverwaltung?**

Meine Umfrage zum Einsatz von Videoüberwachungstechnik in der Bundesverwaltung hatte wiederkehrende, geradezu typische datenschutzrechtliche Mängel aufgezeigt. Nachholbedarf bestand unter anderem bei der sehr häufig unterbliebenen Kennzeichnung der Videoüberwachung, den oft überlangen Speicherfristen, der fehlenden Kenntnis der Rechtsgrundlagen und - soweit erforderlich - der unterlassenen Aufnahme in das Verfahrensverzeichnis sowie der versäumten Durchführung einer Vorabkontrolle.

Im Nachgang meiner Erhebung habe ich mich über die Umsetzung meiner Orientierungshilfe zur Videoüberwachung (24. TB Anlage 7) in der Bundesverwaltung unterrichtet. Die Behörden haben mir die deswegen veranlassten Änderungen mitgeteilt und/oder mir versichert, die Kriterien der Orientierungshilfe für einen datenschutzkonformen Einsatz würden (zukünftig) eingehalten. Die Kontrolle der formellen und materiellen Anforderungen an die Videoüberwachung habe ich verstärkt zum Gegenstand meiner Beratungs- und Kontrollbesuche gemacht (vgl. oben Nr. 9.1.6) und werde dies auch weiterhin tun.

2. 24. TB Nr. 8.3 **Fortbildung und Zertifizierung behördlicher Datenschutzbeauftragter**

Der von der Bundesakademie für öffentliche Verwaltung (BAköV) entwickelte und von mir konzeptionell begleitete Fortbildungslehrgang „Behördliche Datenschutzbeauftragte in der Bundesverwaltung“ hat sich etabliert. Nach der erfolgreich durchgeführten Pilotveranstaltung im Sommer 2013 konnte die BAköV das Seminar aufgrund der hohen Nachfrage bislang drei weitere Male anbieten. Von der Möglichkeit zur Zertifizierung, die eine Projektarbeit, die Präsentation der Ergebnisse im Rahmen eines Workshops und die erfolgreiche Teilnahme an der Abschlussprüfung voraussetzt, haben bereits einige Datenschutzbeauftragte Gebrauch gemacht.

Ich begrüße die Initiative und das Engagement der BAköV sehr, gerade weil die Möglichkeit zur Teilnahme an Fort- und Weiterbildungsveranstaltungen für behördliche Datenschutzbeauftragte im Datenschutzrecht gesetzlich ausdrücklich vorgesehen ist.

Darüber hinaus hat die BAköV im Jahr 2014 die „Jahrestagung für behördliche Datenschutzbeauftragte in der Bundesverwaltung“ ins Leben gerufenen. Damit fügt sich ein weiterer Mosaikstein in das Fortbildungs- und Veranstaltungsangebot für die behördlichen Datenschutzbeauftragten der Bundesverwaltung ein. Während das bereit gestellte Fortbildungsangebot in den Bereichen Datenschutz und Datensicherheit der Wissensvermittlung dient, soll die Jahrestagung ganz gezielt den Dialog, den Austausch zwischen Wissenschaft und Praxis, Aufsichtsbehörden und verantwortlichen Stellen fördern. Wie die erfreuliche Resonanz und das außerordentlich große Interesse hoffen lässt, kann die Jahrestagung künftig ein fester Termin für alle Datenschutzinteressierten in der Bundesverwaltung werden.

3. 24. TB Nr. 12.2.4. **Datenübermittlung zu Lehrkräften von Maßnahmeträgern**

Um Träger von Maßnahmen zur Arbeitsförderung im Sinne des SGB III zulassen zu können, darf die BA personenbezogene Daten der Lehrkräfte des Trägers abfragen. Darüber hatte ich berichtet. Nun machte mich ein Maßnahmeträger auf die Praxis der Prüfdienste der BA aufmerksam, im Rahmen der Qualitätsprüfung nach § 183 SGB III Einsicht in die Arbeitsverträge der Lehrkräfte zu nehmen, ohne zuvor die Einwilligung der betroffenen Mitarbeiter einzuholen.

Bei einer solchen Einsichtnahme in Arbeitsverträge von Mitarbeitern der Maßnahmeträger halte ich deren Einwilligung aber für zwingend erforderlich. Ich freue mich, dass die BA diese Einschätzung teilt und inzwischen die Einwilligung der betroffenen Mitarbeiter vorliegen muss, bevor ihr Prüfdienst Einsicht in Arbeitsverträge nehmen darf.

4. 24. TB Nr. 12.2.1 **E-Akte bei der Bundesagentur für Arbeit**

Über meinen Beratungs- und Kontrollbesuch zum Pilotprojekt elektronischen Akte (E-Akte) der BA hatte ich berichtet (24. TB Nr. 12.2.1). Inzwischen wurde die E-Akte bei der BA bundesweit eingeführt. Von der datenschutzgerechten Umsetzung konnten sich meine Mitarbeiter bei weiteren Beratungs- und Kontrollbesuchen in einem Scanzentrum und einer Agentur für Arbeit überzeugen.

In der Vergangenheit hatte ich Zweifel, ob der geplante Umfang der Stichprobenkontrollen ausreichen würde, um bei der Überführung der eingehenden Papierpost in elektronische Dokumente eine geringe Fehlerquote im Scanprozess sicherzustellen. Denn die inhaltliche und bildliche Übereinstimmung der Scanprodukte mit den Originalen wird nur in zwei Prozent der Fälle stichprobenweise geprüft. Inzwischen sind meine Bedenken aber ausgeräumt. Wie eine von mir angeregte Versuchsreihe gezeigt hat, werden auch bei Ausweitung der Stichprobenprüfungen über die zwei Prozent hinaus keine erhöhten Fehlerquoten erkannt. Aus datenschutzrechtlichen Gründen ist es daher nicht erforderlich, die Stichproben auszuweiten.

Neben dem Bereich des SGB III wurde zum Zeitpunkt des Kontrollbesuchs auch bereits für die Familienkassen der BA die E-Akte eingeführt. Im Scanzentrum konnten sich meine Mitarbeiter von einer datenschutzkonformen Trennung des Schriftguts der Familienkasse vom übrigen BA-Schriftgut überzeugen.

5. 23. TB. Nr. 12.3, 5.5 und 24. TB Nr. 13.3 **Entwicklungen bei der elektronischen Personalakte**

Im Berichtszeitraum habe ich mir bei der Deutschen Rentenversicherung Bund (DRV Bund) den Prozess der dort praktizierten Überführung von Papier-Personalakten in digitale Akten vorführen lassen. Die von der DRV Bund gewählte, vom BMAS ausdrücklich genehmigte und aktuell praktizierte Verfahrensweise berücksichtigt die von mir hierzu im 23. und 24. Tätigkeitsbericht dargestellten datenschutzrechtlichen Rahmenbedingungen. Die maßgeblichen gesetzlichen Vorgaben zur Personalaktenführung können also im Praxisbetrieb der DRV Bund umgesetzt werden. Das mir vorgestellte Gesamtkonzept mit den (aufgrund meiner Empfehlungen und Hinweise teilweise neuen) einzelnen, sich ergänzenden Prüf-, Kontroll- und Qualitätssicherungsschritten ist grundsätzlich geeignet, eine hinreichend sichere und vollständige Digitalisierung der Personalakten zu gewährleisten, einschließlich einer qualifizierten elektronischen Signatur nach dem Signaturgesetz. Dies begrüße ich.

Bei der vollständigen Umsetzung der gesetzlichen Vorgaben des Bundesbeamtengesetzes zur Führung elektronischer Personalakten der bei der Deutschen Telekom AG (DTAG) beschäftigten Beamtinnen und Beamten habe ich die DTAG weiter beratend begleitet und ergänzende datenschutzrechtliche Hinweise und Empfehlungen gegeben. Die DTAG hat mir aktuell berichtet, sie habe im Berichtszeitraum nach dem mit mir abgestimmten Konzept die Nachsignatur (entsprechend den Vorgaben des Signaturgesetzes für eine qualifizierte elektronische Signatur) von über 40 Millionen, in den elektronischen Personalakten vorhandenen Dokumenten umgesetzt. Im Rahmen dieser Maßnahme seien u. a. die Dokumente aus den elektronischen Personalakten von ca. 40.000 aktiven Beamtinnen und Beamten und ca. 75.000 beamteten Versorgungsempfängern der DTAG qualifiziert elektronisch signiert worden. Anfang 2015 werde sie die in die elektronischen Personalakten überführten Papier-Personalakten der bei ihr beschäftigten Beamtinnen und Beamten datenschutzgerecht entsorgen. Die Löschung von Dokumenten der elektronischen Personalakten nach Ablauf der gesetzlichen Aufbewahrungsfristen sei nach

dem mit mir abgestimmten Verfahren bereits realisiert. Die sehr konstruktive Zusammenarbeit mit der DTAG, die weiter andauert, begrüße ich ausdrücklich.

6. 20. TB Nr. 17.1.6 und 21. TB Nr. 13.18 **Anforderung von Wunddokumentationen bei der häuslichen Krankenpflege**

Ich hatte zuletzt in meinem 21. Tätigkeitsbericht (Nr. 13.8) über die unzulässige Praxis verschiedener Krankenkassen berichtet, bei der Bewilligung von Leistungen der häuslichen Krankenpflege umfangreiche medizinische Daten wie z. B. Wunddokumentationen oder Arztberichte bei den Leistungserbringern auf der Grundlage von Einwilligungen der Versicherten zu erheben. Meine Rechtsauffassung, nach der dieses Vorgehen in unzulässiger Weise die gesetzlich abschließend normierten Datenerhebungsbefugnisse der Krankenkassen umgeht, halte ich aufrecht. Dies gilt sowohl für die Erst- als auch für die Folgebewilligung.

Wie ich im aktuellen Berichtszeitraum leider feststellen musste, setzen sich verschiedene Krankenkassen weiterhin über die gesetzlichen Vorgaben hinweg. Besonders viele Beschwerden erreichten mich hierzu über die DAK Gesundheit. Ich habe diese fortlaufende rechtswidrige Erhebung von Sozial- und Gesundheitsdaten deshalb nach § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG als Verstoß gegen die Vorschriften §§ 284 Absatz 1, 275 Absatz 1 SGB V beanstandet. Die DAK Gesundheit hat mir daraufhin meine Rechtsauffassung bestätigt und zugesichert, die erforderlichen organisatorischen Maßnahmen zu treffen, um die rechtswidrige Erhebung von Sozial- und Gesundheitsdaten zukünftig zu unterbinden.

7. 24. TB Nr. 11.2 **Das Webportal „eSolution“ der Deutschen Rentenversicherung**

Die DRV Bund hat ihre Zusage, mich bei künftigen Änderungen und Fortentwicklungen zu beteiligen, eingehalten. Eine wichtige Fortentwicklung des Webportals „eSolution“ war im Berichtszeitraum die Entscheidung der DRV Bund, künftig für sämtliche trägerübergreifenden Portalanwendungen, die personenbezogene Daten von Versicherten und Kunden verarbeiten, nur noch eine zentrale Authentifizierungskomponente (E-Login) bei der Datenstelle der Träger der Rentenversicherung zur Anwendung zu bringen und den Service „eSolution“ in diese zentrale Authentifizierungskomponente zu integrieren.

8. 24. TB Nr. 4.2.2 **Bea lebt! Das Projekt „Bescheinigungen elektronisch annehmen“**

Bei Beendigung eines Beschäftigungsverhältnisses muss der Arbeitgeber Arbeitsbescheinigungen ausstellen, die zur Berechnung des Arbeitslosengelds benötigt werden. Mit dem Projekt „Bescheinigungen elektronisch annehmen“ (Bea) sollen diese Bescheinigungen der Arbeitgeber elektronisch an die BA übermittelt werden. Dieses Projekt habe ich von Anfang an begleitet und dafür gesorgt, dass die BA die elektronisch zu meldende Datenmenge an den Umfang der im bisherigen Papierverfahren zu meldenden Daten angeglichen und damit deutlich reduziert hat.

Die für die Einführung von Bea erforderliche gesetzliche Grundlage wurde im Juni 2013 vom Deutschen Bundestag geschaffen (BGBl. I S. 3836), das Verfahren begann zum 1. Januar 2014. Das Fach- und Berechtigungskonzept sowie das Konzept zur Löschung der personenbezogenen Daten, die beim Bea-Verfahren anfallen, hat die BA in enger Abstimmung mit mir erarbeitet. Die BA löscht die Daten derzeit logisch durch zufälliges Überschreiben der Plattenbereiche auf dem Server der BA. Durch die Fortentwicklung der Technik wird es künftig allerdings leichter sein, auch überschriebene Daten zu suchen und zu rekonstruieren. Ich habe die BA daher gebeten, das Löschkonzept an technische Neuerungen anzupassen und zu optimieren. Darüber hinaus werde ich die weitere Entwicklung des Projektes beobachten.

9. 24. TB Nr. 8.1.1 **Der Zensus 2011 als informationstechnische Herausforderung**

Der Zensus 2011 (vgl. Nr. 5.8) war in vielerlei Hinsicht ein Mammutprojekt und stellte insbesondere den Datenschutz vor hohe Herausforderungen. Datenschützer verbinden mit dem Stichwort „Volkszählung“ auch deshalb besondere Assoziationen, weil das so genannte „Volkszählungsurteil“ des Bundesverfassungsgerichts aus dem Jahr 1983 als Geburtsstunde des modernen Datenschutzrechts gilt. Ich habe zum Zensus 2011 in den zurückliegenden Tätigkeitsberichten bereits ausführlich Stellung genommen. Meine Beratung des Statistischen Bundesamts betraf auch Datensicherheitsfragen, die im Bereich des Datenschutzes immer mitgedacht werden müssen. Wie sich bei meinem Kontrollbesuch im Jahr 2011 gezeigt hatte, waren erhebliche Nachbesserungen am IT-Sicherheitskonzept des Statistischen Bundesamtes für den Zensus 2011 notwendig, die ich auch eingefordert habe. Im Herbst 2013 konnten meine Mitarbeiter die noch verbliebenen Fragen mit dem Statistischen Bundesamt klären und sich auch ein Bild über die baulichen Verhältnisse und Veränderungen in den Rechenzentren dieser Behörde am Standort Wiesbaden machen. Die dabei gewonnenen Erfahrungen können für die Arbeiten am IT-Sicherheitskonzept des nächsten Zensus im Jahr 2021 sicherlich hilfreich sein.

10. 24. TB Nr. 7.4.4 **Die Zentraldatei „Politisch motivierte Kriminalität - links“ - noch viel zu tun!**

Zu dem datenschutzrechtlichen Beratungs- und Kontrollbesuch der Datei „PMK-Links-Z“ hatte ich im 24. Tätigkeitsbericht unter Nr. 7.4.4. berichtet. Hierzu hat mir das BMI in der Zwischenzeit folgendes mitgeteilt: Das BKA habe, wie im Gespräch während des Beratungs- und Kontrollbesuch angekündigt, alle sog. Prüffälle in der Datei durchgesehen und gelöscht. Das BKA werde weiterhin Prüffälle auf der Grundlage des § 7 BKAG speichern, allerdings nur solange, bis der Sachverhalt, etwa aufgrund der Informationen anderer Polizeibehörden, abschließend beurteilt werden könne. Ebenso habe das BKA alle Einträge in der Datei gelöscht, die zu „sonstigen Personen“ i. S. d. § 8 Absatz 5 BKAG gespeichert waren. Die Praxis der Speicherung von Beschuldigten nach § 8 Absatz 2 BKAG sei angepasst worden. Zu jedem Fall nehme das BKA orientiert an meinen Anmerkungen eine differenzierte Tatsachenbetrachtung für eine Negativprognose vor.

11. 24. TB Nr. 6.6 **Notrufortung**

In meinem 24. Tätigkeitsbericht habe ich die Erwartung geäußert, bis Ostern 2013 könne die Notrufortung entsprechend den Vorgaben des § 108 TKG, der Notrufverordnung und der Technischen Richtlinie durchgeführt werden. Einige Wochen vor diesem Termin bin ich jedoch gebeten worden, die Duldung der Notrufortung durch die Allianz OrtungsServices GmbH zu verlängern. Nach einer Rückfrage bei den Landesbehörden habe ich einer letztmaligen Verlängerung der Duldung um drei Monate zugestimmt, bevor der Ortungsdienst eingestellt wurde. Bereits bei dieser Rückfrage wurde deutlich, dass die Landesbehörden die Notrufortung gemäß § 108 TKG unterschiedlich schnell umsetzen können. In einem Bundesland wurde wieder eine Initiative ergriffen, Standortdaten der für kommerzielle Zwecke genutzten Schnittstelle für die Notrufortung zu verwenden. Diese Nutzungen sind zwar gut gemeint, werden aber ohne ausreichende Rechtsgrundlage durchgeführt.

12. 24. TB Nr. 6.3 **Neue Regeln für Auskunft über Telekommunikationsbestandsdaten**

Das Bundesverfassungsgericht hatte in seiner Entscheidung vom 24. Januar 2012 (vgl. 24. TB Nr. 6.2) dem Gesetzgeber aufgegeben, die Auskunft über Telekommunikationsbestandsdaten neu zu regeln. Angesichts einer kurzen Übergangsfrist wurde das Gesetzgebungsverfahren (Bundestagsdrucksache 17/12879) zügig eingeleitet und abgeschlossen, so dass das Gesetz bereits am 1. Juli 2013 in Kraft getreten ist. Leider hatte sich das federführende Bundesministerium des Innern im Wesentlichen darauf beschränkt, die verfassungsgerichtlichen Vorgaben umzusetzen. Auch wenn einige meiner Bedenken in der Ressortabstimmung aufgegriffen wurden, wies der vom Kabinett verabschiedete Entwurf daten-

schutzrechtliche Defizite auf. Erfreulicherweise hat der Innenausschuss des Deutschen Bundestages diese Bedenken in einer Sachverständigenanhörung aufgegriffen, in die auch ich eine Stellungnahme eingebracht habe.

Ich habe dabei vor allem den fehlenden Richtervorbehalt und die ebenfalls nicht vorgesehenen Benachrichtigungspflichten bei der IP-Adressen-Auskunft und der Auskunft über Daten zur Zugangssicherung (z. B. PIN/PUK) kritisiert. Zum anderen habe ich bemängelt, dass die IP-Adressen-Auskunft im Bereich der Ordnungswidrigkeiten nicht auf die Verfolgung von besonders gewichtigen Fällen beschränkt war. Eine Vorgabe, die das Bundesverfassungsgericht zwar nicht in der dem Gesetzgebungsverfahren zugrunde liegenden Entscheidung, wohl aber in seinem Urteil zur Vorratsdatenspeicherung im Jahre 2010 ausdrücklich gemacht hatte. Leider blieb gerade dieser Punkt auch im parlamentarischen Verfahren unberücksichtigt. Da aber der Gesetzentwurf im Übrigen in den von mir angesprochenen Kritikpunkten ergänzt wurde, stellen die neuen Vorschriften zur Auskunft über Telekommunikationsbestandsdaten aus datenschutzrechtlicher Sicht immerhin eine deutliche Verbesserung zu dem bisher praktizierten Verfahren dar.

13. 24. TB Nr. 5.8 **Soziale Netzwerke**

Infolge des Audits durch den irischen Datenschutzbeauftragten ist es zwar zu einigen Verbesserungen für die Nutzer von Facebook gekommen, allerdings besteht das soziale Netzwerk weiterhin auf der nach deutscher Rechtslage unzulässigen Klarnamenpflicht, deren Beachtung energisch durchgesetzt wird. Auch datenschutzfreundliche Voreinstellungen werden nach wie vor nicht angeboten. Stattdessen will Facebook mit seinen neuen, ab Ende Januar 2015 geltenden Allgemeinen Geschäftsbedingungen (AGB) seine Mitglieder besser über Datenschutz informieren und dazu in einem neuen Bereich die entsprechenden Grundlagen (Privacy Basics) erläutern. Dies ist allerdings unzureichend, weil erfahrungsgemäß nur wenige Nutzer die von Internetdiensten veröffentlichten, oft detaillierten und verklausulierten Nutzungsbedingungen oder Datenschutzerklärungen lesen und verstehen. Bei den neuen AGB lohnt aber in jedem Fall ein genaues Hinsehen: Zukünftig wird Facebook auch Standortdaten in die Auswertung des Nutzerverhaltens einfließen lassen, um noch genauer auf den jeweiligen Nutzer zugeschnittene, personalisierte Werbung einblenden zu können. Die neu eingeräumte Möglichkeit der Nutzer, der Versendung der Werbung zu widersprechen, entpuppt sich rasch als Mogelpackung, weil der Widerspruch nicht für die Erhebung der Nutzungsdaten gilt. Dass die eigentliche Datenverarbeitung also gar nicht untersagt werden kann, ist ein klarer Verstoß gegen deutsches Datenschutzrecht.

Im Jahr 2014 sorgte die milliardenschwere Übernahme des Messengers WhatsApp durch Facebook auch bei Datenschützern und datenschutzaffinen Nutzern für Furore. Deren Befürchtungen einer Zusammenführung der Daten von Nutzern beider Dienste wurden jedoch von Facebook umgehend in Abrede gestellt. Überprüft wurde das von zuständiger Stelle bisher jedoch nicht.

14. 24. TB Nr. 5.5 **ICANN**

Auch wiederholte Schreiben der Artikel-29-Gruppe und mehrere Gespräche mit ICANN-Vertretern konnten nicht verhindern, dass die neuen Verträge mit den Registraren ohne die nach europäischem Datenschutzrecht erforderlichen Änderungen seit Ende Juni 2013 in Kraft sind. ICANN erklärte sich jedoch bereit, Registrare aus EU-Ländern auf Antrag von denjenigen Vertragspflichten zu entbinden, die aufgrund bestehender Gesetze nicht erfüllt werden können. Hierbei geht es um den Umfang der Daten, die von einem Registranten erhoben werden müssen, und die zweijährige vorsorgliche Speicherung – auch von Verkehrsdaten – für Strafverfolgungszwecke. Die zuständige Datenschutzbehörde oder eine zugelassene Anwaltskanzlei muss dazu den potentiellen Verstoß gegen nationales Recht bestätigen.

Den Vorschlag der Artikel-29-Gruppe, als Repräsentant der europäischen Datenschutzbehörden in deren Namen zu bestätigen, dass die Erhebungs- und Speicherungspflichten in den neuen Verträgen gegen europäisches Recht verstoßen, hat ICANN abgelehnt. Allenfalls ist ICANN bereit, die Bestätigung einer nationalen Datenschutzbehörde oder Kanzlei für alle in ihrem Zuständigkeitsbereich ansässigen Registrare zu akzeptieren. Begründet wird dies mit der unterschiedlichen Auslegung der Datenschutzanforderungen in den einzelnen EU-Ländern. ICANN hat bisher den Anträgen mehrerer Registrare – auch aus Deutschland – stattgegeben.

15. 24. TB Nr. 5.6 **IPv6 - revisited in 2014**

Große Internetfirmen erheben verschiedentlich den Verbreitungsgrad des neuen Internetprotokolls Version sechs (IPv6) mittels Zugriffsstatistiken. Mit einer aktuellen Verbreitungsquote von circa sechs Prozent liegt Deutschland zwar weltweit vorne, dennoch spielt IPv6 für die Nutzer noch keine große Rolle. Jede IPv6-Adresse besteht aus zwei Teilen: Die ersten 64 Bit bilden das Präfix, die letzten 64 Bit den Interface Identifier. Das Präfix wird üblicherweise vom Provider zugewiesen, während der Interface Identifier entweder aus der MAC-Adresse der Netzwerkschnittstellenkarte erstellt oder mittels der so genannten Privacy Extension eindeutig zugewiesen wird. Die komfortable Lösung zum Wechseln des Präfixes, nämlich entweder durch einen Knopf auf der Konfigurationsoberfläche oder auch durch eine automatisierte Funktion in bestimmten Zeitabständen, hat meines Wissens bisher nur ein Anbieter umgesetzt. Mehrere Provider vergeben ein neues Präfix nach dem aktiven Trennen der Verbindung. Es gibt aber auch einen Provider, der eine quasi statische IPv6-Adresse vergibt: Der Kunde kann ein neues Präfix nur erhalten, wenn der Router mindestens zwei Wochen lang ausgeschaltet ist. Zum Wechsel des Interface Identifier wurden die Privacy Extensions eingeführt, die in den aktuellen Betriebssystemen mittlerweile oft voreingestellt sind. Ich werde auch zukünftig die Umsetzung datenschutzfreundlicher Lösungen fördern und die Unternehmen bei deren Entwicklung beraten.

Anlage 1

Übersicht über die durchgeführten Kontrollen, Beratungs- und Informationsbesuche

Deutscher Bundestag
- Verwaltung

Bundeskanzleramt
- Bundesnachrichtendienst

Auswärtiges Amt

Bundesministerium des Innern
- Statistisches Bundesamt
- Bundesamt für Verfassungsschutz (4)
- Bundeskriminalamt (2)

Bundesministerium der Justiz und für Verbraucherschutz
- Bundesamt für Justiz

Bundesministerium für Verkehr und digitale Infrastruktur
- Seeamt Kiel
- Kraftfahrt-Bundesamt
- Bundesamt für Seeschifffahrt und Hydrographie
- 2 Wasser- und Schifffahrtsämter

Bundesministerium für Ernährung und Landwirtschaft
- Bundesanstalt für Landwirtschaft und Ernährung

Bundesministerium für Bildung und Forschung
- Bundesinstitut für Berufsbildung

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit
- Umweltbundesamt

Bundesministerium der Finanzen
- Bundeszentralamt für Steuern (ELStAM, Kontenabrufverfahren, Kirchensteuer auf Kapitalerträge, Steuer-ID)
- Bundesanstalt für Finanzdienstleistungsaufsicht (Beraterregister)
- Bundesanstalt für Immobilienaufgaben
- Bundesfinanzdirektion Nord
- Bundesfinanzdirektion West (Informationsverfahren IMI)

- Familienkasse des Bundeseisenbahnvermögens
- 1 Hauptzollamt (Kfz-Steuer)

Bundesministerium der Verteidigung

- Wehrbereichsverwaltung Nord
- Institut für Wehrmedizinalstatistik und Berichtswesen
- Bataillon Elektronische Kampfführung 931 Daun
- Heeresfliegerausbildungszentrum Le Luc
- Zentrum für Luft- und Raumfahrtmedizin der Luftwaffe

Bundesministerium für Arbeit und Soziales

- 16 Jobcenter (Heilbronn, Neubrandenburg, Kiel, München, Dahme-Spreewald, Oberspreewald-Lausitz, Dresden, Westerwaldkreis, Rhein-Kreis-Neuss, Rhein-Erft, Berlin-Spandau, Berlin Charlottenburg-Wilmersdorf, Berlin Steglitz-Zehlendorf, Bielefeld, Märkischer Kreis, Landkreis Karlsruhe)
- Bundesagentur für Arbeit (Institut für Arbeit und Berufsforschung - IAB)
- 2 Agenturen für Arbeit (Frankfurt am Main, Karlsruhe)
- Deutsche Rentenversicherung Bund, zwei Jobcenter

Bundesministerium für Wirtschaft und Energie

- Abschlussprüferaufsichtskommission (APAK)
- Bundesanstalt für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
- Bundesnetzagentur für Materialforschung und -prüfung

Bundesministerium für Gesundheit

- GKV Spitzenverband
- Bundesversicherungsamt
- Gemeinsamer Bundesausschuss
- Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)
- Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)
- Zentralinstitut für die kassenärztliche Versorgung in Deutschland (ZI)

Bundesgerichtshof

- Der Generalbundesanwalt beim Bundesgerichtshof

Telekommunikationsunternehmen

- Colt Technology Services GmbH
- DE-CIX Management GmbH
- Deutsche Telekom AG
- 1&1 Internet AG
- Kabel Deutschland Vertrieb und Service GmbH
- Level 3 Communications
- E-Plus Mobilfunk GmbH & Co. KG
- mobilcom-debitel GmbH

- mr. net group GmbH & Co. KG
- reventix GmbH
- Syniverse
- Telefónica Germany GmbH & Co. OHG
- Unitymedia KabelBW GmbH
- Vodafone GmbH
- Yahoo Deutschland

Postdienstunternehmen

- arriva gmbh
- AUSTRIAN POST GmbH
- Deutsche Post AG
- General Logistics Systems Germany GmbH & Co. OHG
- PIN Mail AG
- Quick Logistics economail mainz GmbH

Sonstige Behörden

- Bürgel Wirtschaftsinformationen GmbH
- GKV-Spitzenverband
- IKK gesund plus
- KKH
- Knappschaft Bahn See
- IKK - Classic
- Mhplus
- BARMER GEK
- Berufsgenossenschaft Handel und Warendistribution (BGHW)
- Berufsgenossenschaft Rohstoffe und chemische Industrie (BGRCI)
- Berufsgenossenschaft Holz und Metall
- Berufsgenossenschaft der Bauwirtschaft
- Berufsgenossenschaft Nahrungsmittel und Gastgewerbe (BGN)
- Deutsche Rentenversicherung Bund

Anlage 2

Übersicht über Beanstandungen nach § 25 BDSG

Bundesministerium des Innern

- Bei der Migration des Statistischen Bundesamtes in die beim Bundesverwaltungsamt angesiedelte Bundesstelle für Informationstechnik wurden die hierfür erforderlichen Vereinbarungen zur Regelung der datenschutzrechtlichen Vorgaben nicht zeitnah getroffen (vgl. unten Nr. 5.9).

- BMI und das Bundesamt für Verfassungsschutz hatten sich geweigert, von mir angeforderte Informationen zu geben (vgl. Nr. 2.1.1)

Bundesministerium für Arbeit und Soziales

- Mehrere Verstöße eines Jobcenters gegen datenschutzrechtliche Vorschriften der §§ 67a Absätze 1, 2 und 5, 67c Absatz 1 Satz 1, 69 Absatz 1 Nr. 1, 83 Absatz 1 Nr. 1 SGB X und § 93 Absatz 9 Satz 2, Absatz 10 AO und damit gegen das Sozialgeheimnis des § 35 Absatz 1 Satz 1 SGB I wegen der Erhebung, Verarbeitung und Nutzung von Sozialdaten bei der Untersuchung eines Sachverhalts und mangelhafter Dokumentation des Verwaltungshandelns (Beanstandung des Jobcenters Nienburg; vgl. Nr. 9.1.4).

- Verstoß der BA gegen datenschutzrechtliche Vorschriften der §§ 67b Absatz 1 Satz 1, 67d Absatz 1 SGB X und gegen das Sozialgeheimnis des § 35 Absatz 1 Satz 1 SGB I wegen der Übermittlung eines ärztlichen Gutachtens des Ärztlichen Dienstes einer Agentur für Arbeit an einen Arbeitgeber (Übermittlung von Gesundheitsdaten an Arbeitgeber, vgl. Nr. 9.2.2).

- Verstoß der BA gegen datenschutzrechtliche Vorschriften des § 78a SGB X nebst Anlage und gegen das Sozialgeheimnis des § 35 Absatz 1 Satz 1 und 2 SGB I wegen der Verwendung von Echtdaten für Testläufe in den IT-Systemen des Instituts für Arbeitsmarkt- und Berufsforschung (Beratungs- und Kontrollbesuch beim Institut für Arbeitsmarkt- und Berufsforschung; vgl. Nr. 9.2.3).

Bundesministerium der Verteidigung

- Verstoß des BMVg gegen datenschutzrechtliche Vorschriften der §§ 4d Absatz 5, 4e, 4g Absatz 2, 18 BDSG wegen der fehlenden Durchführung einer Vorabkontrolle und der fehlenden Aufnahme eines IT-Verfahrens zur Verarbeitung von Gesundheitsdaten in das Verfahrensverzeichnis des BMVg bei dessen Inbetriebnahme sowie gegen datenschutzrechtliche Vorschriften des § 9 BDSG und der Anlage zu § 9 BDSG wegen der mangelhaften Aufsicht des IT-Betriebes sowie der Gewährleistung der Zugangs- und Zugriffskontrolle (Das Institut-Informationssystem des Zentrums für Luft- und Raumfahrtmedizin der Luftwaffe; vgl. Nr. 11.1.1).

Bundesministerium der Finanzen

- Verstoß des BMF gegen § 9 Satz 1 i. V. m. Anlage zu § 9 Absatz 1 Satz 2 Nr. 2 und 3 BDSG beim Start von ELStAM zu dem gewählten Zeitpunkt, da es noch an ausreichenden technischen und organisatorischen Maßnahmen fehlte, die geeignet sind, die schützenswerten personenbezogenen Daten vor unbefugter Nutzung zu schützen (Beanstandung ELStAM; vgl. Nr. 7.1)

- Verstoß gegen die Regelungen der §§ 106 ff. BBG, insbesondere § 107 Abs. 1 BBG und § 113 Abs. 2 BBG sowie gegen § 12 Abs. 4 i. V. m. § 32 Abs. 1 BDSG (vgl. Nr. 5.7.4)

Bundesministerium für Verkehr, Bau und Stadtentwicklung

Vier Beanstandungen (vgl. Nr. 5.7.4)

- Verstoß gegen die Regelungen der §§ 106 ff. BBG bzw. gegen § 12 Abs. 4 i. v. m. § 32 Abs. 1 BDSG

- Verstoß gegen die Regelungen der §§ 106 ff. BBG bzw. gegen § 12 Abs. 4 i. V. m. § 32 Abs. 1 BDSG

- Verstoß gegen die Regelungen der §§ 106 ff. BBG, insbesondere § 106 Abs. 1 und 2 BBG

- Verstoß gegen die Regelungen des § 12 Abs. 4 i. V. m. § 32 Abs. 1 BDSG und § 7 Abs. 7 und 8 AZV

Telekommunikationsunternehmen

E-Plus Mobilfunk GmbH & Co. KG
Verstoß gegen § 96 TKG wegen Speicherung von Verkehrsdaten (Nr. 8.8.3 Erfahrungen aus Kontrollen)

Vodafone GmbH
Verstoß gegen §§ 96 und 100 TKG wegen Speicherung von Verkehrsdaten (Nr. 8.8.3 Erfahrungen aus Kontrollen)

Telefónica Germany GmbH & Co. OHG
Verstoß gegen §§ 96 und 100 TKG wegen Speicherung von Verkehrsdaten (Nr. 8.8.3 Erfahrungen aus Kontrollen)

Gesetzliche Krankenkassen

Drei Beanstandungen mhplus BKK

- nach § 81 Abs. 2 Satz 1 SGB X i. V. m. § 25 Abs. 1 BDSG wegen Verstoßes gegen § 35 Abs. 1 SGB I und § 284 Abs. 3 Satz 1 SGB V i. V. m. § 67b Abs. 1 SGB X (vgl. Nr. 13.9)

- nach § 81 Abs. 2 Satz 1 SGB X i. V. m. § 25 Abs. 1 BDSG wegen Verstoßes gegen § 35 Abs. 1 SGB I und § 284 Abs. 3 Satz 1 SGB V i. V. m. § 67b Abs. 1 SGB X

- nach § 81 Abs. 2 Satz 1 SGB X i. V. m. § 25 Abs. 1 BDSG wegen erheblichen Verstoßes gegen das Sozialgeheimnis § 35 Abs. 1 SGB I, § 78a nebst Anlage SGB X sowie § 80 Abs. 2 SGB X

Zwei Beanstandungen Siemens BKK

- nach § 81 Abs. 2 Satz 1 SGB X i. V. m. § 25 Abs. 1 BDSG wegen Verstoßes gegen § 24 Abs. 4 BDSG

- nach § 81 Abs. 2 Satz 1 SGB X i. V. m. § 25 Abs. 1 BDSG wegen Verstoßes gegen § 35 Abs. 1 Satz 1 SGB I sowie § 78a nebst Anlage SGB X

Gesetzliche Unfallversicherungsträger

Berufsgenossenschaft für Handel und Warendistribution

- Beanstandung nach § 81 Abs. 2 Satz 1 SGB X in Verbindung mit § 25 Abs. 1 BDSG wegen Verstoßes gegen § 24 Abs. 4 BDSG (vgl. Nr. 9.6)

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13. März 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.

Anlage 4

Erläuterungen der Datenschutzkonferenz zur Entschließung am 13./14. März 2013:

Europa muss den Datenschutz stärken

Jedes personenbeziehbare Datum muss geschützt werden

Nach Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie z. B. IP-Adressen, Kenn-Nummern, Standortdaten
ein.

Es darf keine grundrechtsfreien Räume geben

Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

Einwilligungen müssen ausdrücklich erteilt werden

Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäische Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es - auch mit Blick auf Artikel 8 Absatz 2 der Grundrechtecharta - nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern

Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch - in Anlehnung an Artikel 8 Absatz 2 der Grundrechtecharta - das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

Profilbildung muss beschränkt werden

Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte

Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können

Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission

Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Artikel 8 Absatz 3 der Grundrechtecharta und Artikel 16 Absatz 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

Grundrechtsschutz braucht effektive Kontrollen

Die Sanktionen müssen - wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat - abschreckend und damit geeignet sein, dass die Verantwortlichen und Daten

verarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

Hoher Datenschutzstandard für ganz Europa

Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

Anlage 5

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13. März 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.

Anlage 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5. September 2013:

Keine umfassende und anlasslose Überwachung durch Nachrichtendienste!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u.a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.

- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.

- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.

- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

  Dazu gehört,
  - o zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.
  - o 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.
  - o 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.

Dieses Dokument wurde elektronisch versandt und ist nur im Entwurf gezeichnet.

Anlage 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. März 2014:

Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen. Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.

6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

Anlage 8

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014:

Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke - Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies - ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen - nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131a Abs. 3, § 131b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

- Es ist sicherzustellen, dass
  - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,

  - die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,

  - die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

Anlage 9

Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014:

Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

Anlage 10

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014:

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 - C-131/12 „Google Spain" einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll - nach einer erfolgreichen Beschwerde des Betroffenen - der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.
- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.
- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Anlage 11

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

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

Anlage 12

Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014:

Datenschutz im Kraftfahrzeug - Automobilindustrie ist gefordert

Der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen - etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Anlage 13

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14. November 2014

Keine PKW-Maut auf Kosten des Datenschutzes!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen - beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten - mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monaten währende - Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

Anlage 14

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. Dezember 2014:

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Reha-entlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, - zum Teil mehrfach wöchentlich - von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz - GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI

Das Verfahrensverzeichnis in der Bundesverwaltung

Stand: April 2014

Alle öffentlichen Stellen des Bundes haben - ebenso wie die verantwortlichen Stellen im nicht-öffentlichen Bereich - eine Übersicht über die bei ihnen eingesetzten Verfahren automatisierter Verarbeitungen zu führen (sog. Verfahrensverzeichnis).

Ihre Rechtsgrundlage findet die Pflicht öffentlicher Stellen des Bundes zur Erstellung eines Verfahrensverzeichnisses in § 4g Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) i.V.m. §§ 4e Satz 1, 18 Abs. 2 Sätze 2-4 BDSG.

Die nachfolgenden Erläuterungen stellen die Funktion und den gesetzlichen Inhalt des Verfahrensverzeichnisses in der Verwaltung des Bundes sowie die Rolle des behördlichen Datenschutzbeauftragten bei der Erstellung, Aktualisierung und Zugänglichmachung des Verzeichnisses dar.

I. Zweck und Funktion des Verfahrensverzeichnisses

Gemäß § 4g Abs. 2 Satz 1 BDSG ist dem Datenschutzbeauftragten von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 BDSG genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen. Das Verfahrensverzeichnis soll dem Beauftragten für den Datenschutz einen Überblick über Organisation und Struktur der verantwortlichen Stelle sowie über Art, Umfang, Ablauf und Zweck der in der verantwortlichen Stelle eingesetzten Datenverarbeitungsverfahren vermitteln.

Zugleich bezweckt das Verfahrensverzeichnis die Schaffung von Transparenz für die interessierte Öffentlichkeit. Den öffentlichen Teil des Verfahrensverzeichnisses hat der behördliche Datenschutzbeauftragte gem. § 4g Abs. 2 Satz 2 BDSG jedermann auf Antrag zugänglich zu machen. Hierdurch kann jede Person feststellen, ob und inwieweit sie von einer Datenverarbeitung betroffen ist, und kann entsprechende Auskunftsersuchen nach § 19 BDSG stellen.

Schließlich vermittelt das Verfahrensverzeichnis auch den Mitarbeitern der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eine erste Orientierung bei datenschutzrechtlichen Kontrollen gemäß § 24 BDSG.

II. Adressat der Erstellungspflicht

Adressat der in § 4g Abs. 2 Satz 1 BDSG normierten Verpflichtung zur Erstellung und Führung eines Verfahrensverzeichnisses ist allein die verantwortlichen Stelle. Diese hat dem behördlichen Datenschutzbeauftragten das Verzeichnis „zur Verfügung zu stellen“. Es ist daher nicht Aufgabe des behördlichen Datenschutzbeauftragten, die erforderlichen Angaben selbst zusammenzutragen und in dem Verfahrensverzeichnis zusammenzufassen. Ebenso wenig ist es seine Aufgabe, das Verfahrensverzeichnis zu aktualisieren. Beides, sowohl Erstellung als auch Aktualisierung obliegt der jeweiligen Behörde und kann am besten von den Fachreferaten und Organisationseinheiten geleistet werden, die mit den jeweiligen Datenverarbeitungsverfahren befasst sind.

III. Inhalt des Verfahrensverzeichnisses

Der gesetzliche Inhalt des Verfahrensverzeichnisses ergibt sich aus § 4e Satz 1 Nr. 1 bis 9 BDSG i.V.m. § 18 Abs. 2 Satz 1 BDSG. Die Sätze 2 und 3 des § 18 Abs. 2 BDSG erweitern den Inhalt des Verfahrensverzeichnisses in der Bundesverwaltung um die Nennung der Rechtsgrundlage der Datenverarbeitung, sehen andererseits aber auch Vereinfachungen vor: So sind allgemeinen Verwaltungszwecken dienende automatisierte Verarbeitungen unter bestimmten Voraussetzungen nicht zwingend in das Verzeichnis aufzunehmen.

§ 4e Satz 1 Nr. 1 bis 9 BDSG zählt folgende Pflichtangaben für das Verfahrensverzeichnis auf:

Nr. 1 Name oder Firma der verantwortlichen Stelle,

Nr. 2 Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

Nr. 3 Anschrift der verantwortlichen Stelle,

Nr. 4 Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,

Nr. 5 eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

Nr. 6 Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

Nr. 7 Regelfristen für die Löschung der Daten,

Nr. 8 eine geplante Datenübermittlung in Drittstaaten und

Nr. 9 eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

In Ergänzung hierzu sind gemäß § 4g Abs. 2 Satz 1 BDSG die zugriffsberechtigten Personen zu benennen.

In das Verfahrensverzeichnis aufzunehmen sind auch Verfahren, die von anderen Stellen im Wege der Auftragsdatenverarbeitung durchgeführt werden.

1. Verfahren automatisierter Verarbeitung

Vorbehaltlich der Einschränkungen des § 18 Abs. 2 Satz 3 sind in dem Verfahrensverzeichnis gemäß § 4g Abs. 2 i.V.m. § 4e Satz 1 BDSG sämtliche **Verfahren automatisierter Verarbeitung** aufzuführen.

a) Automatisierte Verarbeitung

Den Begriff der „automatisierten Verarbeitung“ definiert § 3 Abs. 2 BDSG als die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

Entscheidend für das Vorliegen einer automatisierten Verarbeitung ist - neben der durch technische Anlagen erfolgenden Erhebung, Verarbeitung oder Nutzung - die erleichterte Zugänglichkeit und technische Auswertbarkeit der Daten im Datenbestand[1]. Eine automatisierte Verarbeitung ermöglicht, personenbezogene Daten programmgesteuert nach ihrem Informationsgehalt zu selektieren und unterschiedlich zu handhaben. Maßgeblich ist daher, dass die erhobenen oder gespeicherten Daten programmgesteuert („automatisiert“) nach ihrem Informationsgehalt unterscheidbar oder auswertbar sind, die Anlage also über ein Programm verfügt, das in der Lage ist, die dargestellten Inhalte in Abhängigkeit von ihren personenbezogenen Informationsgehalten zu behandeln.

Eine automatisierte Verarbeitung liegt daher nicht vor, wenn lediglich die Wirklichkeit abgebildet wird, ohne dass eine inhaltsbezogene Datenverarbeitung automatisiert stattfindet. Dies betrifft insbesondere die reine Videoübertragung mittels analoger Videotechnik ohne Aufzeichnung[2]. Andere typische Beispiele, wie Kopier- und Faxgeräte, haben sich infolge der technischen Entwicklung überlebt, da solcheGeräte mittlerweile standardmäßig über einen digitalen Speicher verfügen, der eine automatisierte Verarbeitung ermöglicht.

b) Verfahren

In das Verzeichnis aufzunehmen sind gemäß § 4e Satz1 BDSG nur „Verfahren“ automatisierter Verarbeitungen. Aufzunehmen ist daher nicht jeder einzelne automatisierte Datenverarbeitungsvorgang, sondern nur „Verfahren“ automatisierter Verarbeitungen. Etwas anderes ergibt sich auch nicht aus § 18 Abs. 2 Satz 2 BDSG. Soweit sich diese Vorschrift - im Gegensatz zu § 4g Abs. 2 i.V.m. § 4e Satz 1 BDSG - allgemein auf „automatisierte Verarbeitungen“ und nicht auf „Verfahren“ bezieht, ergibt sich daraus keine Erweiterung der Verzeichniserstellungspflicht auf jede einzelne automatisierte Datenverarbeitung. Die Begriffe sind synonym zu verwenden.

Eine Legaldefinition für den Begriff des „Verfahrens“ enthält das BDSG selbst nicht. Abgeleitet aus Art. 18 Abs. 1 der EU-Richtlinie 95/46/EG ist unter einem Verfahren die Gesamtheit von Verarbeitungen „zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen“ zu verstehen.

Durch die Verwendung dieses Begriffs soll sichergestellt werden, dass nicht jeder einzelne Verarbeitungsschritt bzw. -vorgang, d.h. das bloße Erheben oder Übermitteln einzelner Daten, sowie jedes Verarbeitungsergebnis in das Verfahrensverzeichnis aufzunehmen ist, sondern nur einer gemeinsamen Zweckbestimmung dienende „Verarbeitungspakete“ oder Abfolgen von mehreren Verarbeitungsschritten[3].

---

1 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3 Rn. 15a; Dammann in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 79 f.

2 Vgl. zur Videoüberwachung durch öffentliche Stellen des Bundes das Informationspapier der BfDI „Datenschutzrechtliche Grundlagen der Videoüberwachung in der öffentlichen Verwaltung des Bundes“, Anlage 7 zur BT-Drs. 17/13000, abrufbar unter http://dip21.bundestag.de/dip21/btd/17/130/1713000.pdf.

3 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4d Rn. 9a; Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 4d Rn. 2; Thüsing, Arbeitnehmerdatenschutz und Compliance, 1. Aufl. 2010, Rn. 490 ff; Scheja, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4d Rn. 13; a.A. aber Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4d Rn. 6.

Da es somit entscheidend auf die Zweckbestimmung ankommt, ist der Begriff des „Verfahrens automatisierter Verarbeitungen“ von einer Flexibilität und Offenheit geprägt, je nachdem, wie eng oder weit ein spezifischer Zweck definiert wird. Der Daten verarbeitenden Stelle kommt daher bei der Erfassung automatisierter Verfahren ein nicht unerheblicher Gestaltungsspielraum zu. Die Bezeichnung des Verfahrens in dem Verfahrensverzeichnis muss allerdings in jedem Fall so aussagekräftig sein, dass “Jedermann“, der nach § 4g Abs. 2 Satz 2 BDSG Einblick in das Verfahrensverzeichnis nehmen will, anhand der Angaben erkennbar sein muss, um was für eine Art von Datenverarbeitung es sich handelt.

Als Beispiele für hinreichend aussagekräftige, in dem Verfahrensverzeichnis anzugebende automatisierte Datenverarbeitungsverfahren können beispielsweise Personalverwaltungssysteme, Elektronische Akten- und Datenträgervernichtungsverfahren, Zugangskontrollsysteme, Zeiterfassungssysteme, Gehaltsabrechnungssysteme, Buchhaltungssysteme, Reisekosten- und -buchungssysteme, Verfahren zur Abwicklung von Kundenaufträgen, Telekommunikationsanlagen zurTelefondatenerfassung sowie sonstige Systeme oder Arbeitsabläufe, die eine geschlossene Struktur von Verarbeitungen zusammenfassen[4], genannt werden.

Nicht zu den Verfahren automatisierter Verarbeitung zählen

- einzelne elektronische Dokumente oder Dateien,
- einzelne Verarbeitungsschritte bzw. -vorgänge, d.h. das Erheben oder Übermitteln bestimmter Daten[5].

c) Ausnahmen

In das Verfahrensverzeichnis nicht aufzunehmen sind gemäß § 18 Abs. 2 Satz 3 BDSG solche automatisierten Datenverarbeitungen, die allgemeinen Verwaltungszwecken dienen und für die keine Einschränkungen des Auskunftsrechts nach § 19 Abs. 3 und 4 aufgrund eines besonderen Geheimhaltungsinteresses bestehen. „Allgemeinen Verwaltungszwecken“ dienen solche automatisierten Datenverarbeitungen, die grundlegende und allgemein übliche Verarbeitungen betreffen[6]. Dazu zählen insbesondere Standardsoftware (Word, Excel, Outlook) sowie interne Listen und Verteiler (Telefon- und Emailverzeichnisse, Personalbestand, Presseverteiler), sofern die Verfahren nicht zweckbestimmt für eine konkrete programmgesteuerte Auswertung und Selektion nach Informationsgehalten genutzt werden (was z.B. über Filterfunktionen bei Excel möglich ist).

Eine Erleichterung besteht darüber hinaus für Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden. § 18 Abs. 2 Satz 4 BDSG lässt es genügen, dass die diesbezüglichen Festlegungen zusammengefasst werden. Es reicht daher aus, dass die Existenz solcher Verarbeitungen einmal aufgeführt wird[7].

[4] Vgl. Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4d Rn. 26.
[5] Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4d Rn. 9a; Thüsing, Arbeitnehmerdatenschutz und Compliance, 1. Aufl. 2010, Rn. 490 ff.; a.A. Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4d Rn. 6.
[6] Dammann, in: Simitis, BDSG, 7. Aufl. 2011, § 18 Rn. 25.
[7] Gola/Schomerus, BDSG, 11. Aufl. 2012, § 18 Rn. 15.

2. Verantwortliche Stelle

Der Begriff der „verantwortlichen Stelle“ ist in § 3 Abs. 7 BDSG legaldefiniert. Danach ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. „Verantwortliche Stelle“ ist nicht diejenige Organisationseinheit der Behörde, die die Daten tatsächlich speichert (z.B. Rechenzentrum), sondern vielmehr die Behörde, der diese Organisationseinheit angehört, selbst - einschließlich sämtlicher Untergliederungen (Abteilungen, Dezernate, Referate etc.) und unselbstständigen Zweigstellen[8].

Nach § 4e Satz 1 Nr. 1 bis 3 BDSG sollen exakte Angaben zu der verantwortlichen Stelle gemacht werden, die jedermann eine zweifelsfreie Identifizierung und Erreichbarkeit der Stelle sowie der für das Verfahren zuständigen Personen ermöglichen. Es bedarf insoweit der genauen Bezeichnung und Angabe der Anschrift der verantwortlichen Stelle. Die mit der Leitung der verantwortlichen Stelle betrauten natürlichen Personen sind ebenso wie die jeweils mit der Leitung der Datenverarbeitung beauftragten Personen mit Vor- und Zunamen anzugeben.

Eine Angabe von dienstlichen Telekommunikationsverbindungen (Telefon, Telefax, E-Mail etc.) ist zwar ausdrücklich nicht vorgesehen, aber grundsätzlich zulässig. Ebenso ist die Nennung der Person des behördlichen Datenschutzbeauftragten, wenngleich sie gesetzlich nicht vorgeschrieben ist, sinnvoll.

3. Zweckbestimmung

Nach § 4e Satz 1 Nr. 4 BDSG sind die Zwecke mitzuteilen, zu deren Erfüllung die jeweilige automatisierte Datenverarbeitung erfolgt. Anzugeben ist also nicht lediglich ein aus dem Aufgabenbereich und der Tätigkeit der öffentlichen Stelle allgemein abgeleiteter Zweck, sondern der konkrete Zweck des jeweiligen Verfahrens. Ein solcher Verarbeitungszweck kann z.B. die Personalverwaltung sein.

Es sollte eine möglichst eindeutige und aussagekräftige Beschreibung der jeweiligen Zweckbestimmung erfolgen. Insbesondere sind ähnliche oder miteinander verbundene Verfahren durch eine entsprechende inhaltliche Beschreibung voneinander abzugrenzen[9]. Eine spätere Zweckänderung ist unverzüglich im Verfahrensverzeichnis zu dokumentieren.

4. Betroffene Personengruppe und diesbezügliche Daten (-kategorien)

Die betroffenen Personengruppen sind aus den einzelnen Datenverarbeitungsverfahren abzuleiten. Maßgeblich ist, dass die Beschreibung der Personengruppen im Hinblick auf das jeweilige Verfahren zur vorläufigen Rechtmäßigkeitsbeurteilung hinreichend aussagekräftig ist und eine Abgrenzbarkeit schafft[10].

[8] Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3 Rn. 48.
[9] Scheja, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4e Rn. 7.
[10] Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4e Rn. 8; Scheja, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4e Rn. 8.

Es kann u.a. zwischen Mitarbeitern (Tarifbeschäftigte, Beamte), Bewerbern, Antragstellern, Petenten, Anspruchsberechtigten, etc. differenziert werden. Personengruppen können jedoch auch anhand von speziell festgelegten Kriterien definiert werden, die Gegenstand der Datenerhebung oder -verwendung sind (z.B. Einkommens- oder Altersstrukturen)[11].

Jeder Personengruppe sind sodann die sie betreffenden Daten oder Datenkategorien konkret zuzuordnen. Dazu zählen z.B. die für den Verarbeitungszweck erforderlichen Identifikations- und Adressdaten, Geburtsdatum, Familienstand, Beruf, Vertrags-, Abrechnungsdaten, Angehörige, Sozialdaten, Steuerdaten, Einkommen, Kfz-Kennzeichen, Versicherungs- oder Personalnummer etc.

Die Beschreibung der Datenkategorie muss so konkret sein, dass für jede Kategorie deutlich wird, welche personenbezogenen Daten über den Betroffenen bzw. die jeweilige Personengruppe gespeichert wird. Dabei muss insbesondere ersichtlich sein, ob und ggf. welche sensiblen Daten nach § 3 Abs. 9 BDSG erhoben und verwendet werden.

5. Empfänger (-kategorien)

Empfänger ist gemäß § 3 Abs. 8 BDSG jede Person oder Stelle, die Daten erhält. Empfänger ist daher nicht nur eine andere verantwortliche Stelle, sondern auch z.B. Auftragsdatenverarbeiter i.S.d. § 1 BDSG, Zweigstellen oder Nutzer innerhalb derselben verantwortlichen Stelle. Auch Stellen mit Online-Zugriff zählen zu den regelmäßigen Empfängern[12].

Eine namentliche Benennung des konkreten Empfängers ist nicht erforderlich[13]. Bei stelleninternen Empfängern ist zur Klarstellung jedoch die Angabe der Funktionsbezeichnung zweckmäßig[14]. In Betracht kommt auch eine Kategorisierung von gleichartigen Empfängergruppen, soweit die Bezeichnung hinreichend konkret und für Außenstehende verständlich ist und die Tragweite der Übermittlung erkennen lässt.

6. Löschfristen

§ 4e Satz 1 Nr. 7 verlangt eine Angabe über Regelfristen für die Löschung personenbezogener Daten. Gemäß § 20 Abs. 2 BDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig oder ihre weitere Kenntnis für die verantwortliche Stelle nicht mehr erforderlich ist. § 20 Abs. 3 bis 5 BDSG sieht Ausnahmen von der Löschfrist für automatisiert verarbeitete Daten vor.

Sofern Löschfristen nicht spezialgesetzlich vorgegeben sind, lässt sich häufig nicht genau bestimmen, wann die Kenntnis personenbezogener Daten zur Erfüllung der Aufgaben nicht mehr erforderlich ist. In diesem Fall sind möglichst konkrete Löschfristen anhand einer Prognoseentscheidung anzugeben. Der Prognose sind allgemeine Erfahrungswerte für die Erforderlichkeit der weiteren Speicherung zugrunde zu legen und nicht theoretische Ausnahmefälle. Hierbei ist auch zu beachten, dass es sich bei der Angabe um eine „Regel"-Löschfrist handelt, eine längere Speicherdauer im Einzelfall daher zulässig ist.

[11] Scheja, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4e Rn. 8.
[12] Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4e Rn. 8.
[13] Scheja, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4e Rn. 9; Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4e Rn. 8.
[14] Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4e Rn. 8; Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4e Rn. 8.

7. Datenübermittlung in Drittstaaten

§ 4e Satz 1 Nr. 8 BDSG fordert die Angabe der geplanten Übermittlungen in Drittstaaten. Dazu zählen alle Stellen außerhalb der Europäischen Union oder anderer Vertragsstaaten des Europäischen Wirtschaftsraums (EWR). Angaben sind also bereits dann zu machen, wenn es mit einer gewissen Wahrscheinlichkeit zu einer Übermittlung in Drittstaaten kommen wird. Bereits erfolgte Übermittlungen in Drittstaaten sind ebenso anzugeben.

Anzugeben sind die Übermittlungszwecke, die betroffenen Datenkategorien und die Zielländer, um das Vorliegen der Voraussetzungen der §§ 4b und c BDSG nachvollziehbar zu machen[15]. Ein pauschaler Verweis auf eine Übermittlung „in alle Länder der Welt" genügt nicht, da eine Prüfung der Zulässigkeit einer Übermittlung im Einzelfall anhand des im Empfängerland bestehenden Datenschutzniveaus dann nicht möglich ist (§ 4b Abs. 3 und 5 BDSG). Der Zeitpunkt und die näheren Umstände der Datenübermittlung müssen jedoch nicht angegeben werden.

8. Allgemeine Beschreibung mit Blick auf § 9 BDSG

§ 4e Satz 1 Nr. 9 BDSG sieht eine allgemeine Beschreibung der vorgesehenen Datensicherungsmaßnahmen vor, die eine vorläufige Beurteilung ihrer Angemessenheit ermöglichen soll. Ausreichend ist eine stichwortartige Aufzählung anhand der Vorgaben in der Anlage zu § 9 BDSG.

9. Zugriffsberechtigte Personen

§ 4g Abs. 2 Satz 1 fordert für den internen Teil des Verfahrensverzeichnisses zusätzlich Angaben über die zugriffsberechtigten Personen. In Abgrenzung zu „Empfängern" i.S.d. § 4e Satz 1 Nr. 6 BDSG (siehe Punkt IV. 5.) sind zugriffsberechtigte Personen nach § 4g Abs. 2 Satz 1 BDSG in der Regel nur Angehörige der verantwortlichen Stelle, die aufgrund ihrer Position oder Funktion Zugang zu bestimmten dafür relevanten Daten haben[16]. Zu den zugriffsberechtigten Personen zählen aber auch Beschäftigte von Auftragnehmern einer Auftragsdatenverarbeitung nach § 11 BDSG.

Die Angaben zu den zugriffsberechtigten Personen müssen so präzise sein, dass der behördliche Beauftragte für den Datenschutz diese jederzeit hinreichend individualisieren kann.

10. Rechtsgrundlagen

Gemäß § 18 Abs. 2 Satz 2 BDSG ist die Rechtsgrundlage der automatisierten Verarbeitung anzugeben. Dies soll die Prüfung durch die BfDI und den behördlichen Datenschutzbeauftragten erleichtern und trägt dem für Einschränkungen des Rechts auf informationelle Selbstbestimmung bestehenden Gesetzesvorbehalt Rechnung[17].

---

15 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 4e Rn. 8.

16 Simitis, in: Simitis, BDSG, 7. Aufl. 2011, § 4g Rn. 69; a.A. Wolff/Brink, BeckOK BDSG, Stand: 01.05.2013, § 4g Rn.27; Scheja, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4g Rn. 24.

17 Dammann, in: Simitis, BDSG, 7. Aufl. 2011, § 18 Rn. 34.

IV. Aktualisierungspflicht

Das Verfahrensverzeichnis muss stets auf dem neusten Stand und vollständig sein. Es ist daher einer laufenden Überprüfung und Aktualisierung zu unterziehen. Die verantwortliche Stelle hat dabei sicherzustellen, dass neue Verfahren und Verfahrensänderungen unverzüglich zum Verfahrensverzeichnis gemeldet werden. Die Bereitstellung eines Verfahrensverzeichnisses ist daher keine einmalige, sondern vielmehr eine fortlaufende Verpflichtung.

V. Veröffentlichungspflicht

Gemäß § 4g Abs. 2 Satz 2 BDSG hat der behördliche Datenschutzbeauftragte die in dem Verzeichnis enthaltenen Angaben nach § 4e Satz 1 Nr. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar zu machen. Hierdurch soll ein Mindestmaß an öffentlicher Information gewährleistet werden (vgl. Art. 21 der EG-Datenschutzrichtlinie).

Die Angaben sind nur auf Antrag verfügbar zu machen. Ein berechtigtes Interesse an der Einsichtnahme muss jedoch weder erklärt noch nachgewiesen werden.

Die Art und Weise des „Verfügbarmachens“ ist gesetzlich nicht vorgeschrieben und daher dem Datenschutzbeauftragten überlassen. Auch wenn die Gewährung von Einsicht vor Ort grundsätzlich ausreichend ist, darf der in § 4 Abs. 2 Satz 2 BDSG normierte Informationsanspruch nicht durch Auswahl eines ungeeigneten oder unzumutbaren Mittels des „Zugänglichmachens“ unterlaufen werden. Es ist daher empfehlenswert und im Einzelfall auch geboten, die Angaben auf Verlangen postalisch oder elektronisch zu übermitteln oder im Internet zum Abruf bereit zu stellen. Dies trägt dem Prinzip der Bürgernähe Rechnung.

Vom Einsichtsrecht nicht umfasst sind die Angaben zu den technischen und organisatorischen Maßnahmen nach § 4e Satz 1 Nr. 9 BDSG sowie die Angaben über die zugriffsberechtigten Personen.

Die in §§ 6 Abs. 2 Satz 4, 19 Abs. 3 BDSG genannten Stellen (u.a. Sicherheitsbehörden) sind von der Veröffentlichungspflicht ausgenommen, § 4g Abs. 3 Satz 1 BDSG.

VI. Verzeichnis nach § 18 Abs. 2 Satz 1 BDSG

Neben der Erstellung eines Verfahrensverzeichnisses haben öffentliche Stellen des Bundes gemäß § 18 Abs. 2 Satz 1 BDSG ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen zu führen. Sinn und Zweck ist es, v.a. dem behördlichen Datenschutzbeauftragten eine Übersicht darüber zu geben, an welchen Orten in der Dienststelle personenbezogene Daten automatisiert verarbeitet werden können.

Der Begriff der „Datenverarbeitungsanlage“ ist weit auszulegen[18]. Datenverarbeitungsanlagen sind alle Anlagen, mit deren Hilfe personenbezogene Daten verarbeitet werden können[19]. Dazu zählen alle EDV-Anlagen wie z.B. Arbeitsplatzrechner, Aktenerschließungssysteme, mobile Datenverarbeitungsanlagen, Videokamerasysteme, Server, Telefone, Faxgeräte, Kopierer etc.[20] Auf die programmgesteuerte Auswertbarkeit der Daten kommt es im Gegensatz zu der automatisierten Datenverarbeitung i.S.d. § 3 Abs. 2 BDSG nicht an.

[18] Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl. 2013, § 3 Rn. 25; Meltzian, BeckOK BDSG, Stand: 01.05.2013, § 18 Rn. 18.
[19] Meltzian, BeckOK BDSG, Stand: 01.05.2013, § 18 Rn. 18; Dammann, in: Simitis, BDSG, 7. Aufl. 2011, § 18 Rn. 17.
[20] Buchner, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 3 Rn. 22; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 18 Rn. 5.

Das Verzeichnis sollte mindestens folgende Angaben enthalten[21]:

- Angaben zur Identifizierung der Anlagen (z.B. Geräte-, Hersteller- oder Inventarnummer)
- Anzahl und Art der Anlagen (Herstellername, Produktname, Fabrikatsbezeichnung, Typenbezeichnung)
- Einsatzort (Behörde, Organisationseinheit, Gebäude, Raum)
- System- und Sicherheitssoftware sowie Peripheriegeräte

Eine Zusammenfassung mehrerer gleicher, sich innerhalb derselben Organisationseinheit befindlicher Anlagen ist zulässig, soweit eine genaue und verwechslungsfreie Lokalisierung möglich ist.

[21] Dammann, in: Simitis, BDSG, 7. Aufl. 2011, § 18 Rn. 19.

VII. Muster eines Verfahrensverzeichnisses für Bundesbehörden

Hauptblatt

☐ Das Verzeichnis ist nur teilweise zur Einsichtnahme bestimmt (§ 4g Abs. 2 BDSG)

☐ Das Verzeichnis ist nicht zur Einsichtnahme bestimmt (§ 4g Abs. 3 Satz 1 BDSG);
[z.B. Verfassungsschutzbehörden, Bundesnachrichtendienst, Militärischer Abschirmdienst, Behörden aus dem Bereich des Bundesministeriums der Verteidigung, Polizeibehörden, Staatsanwaltschaften etc.]

1. Verantwortliche Stelle

1.1 Name/ Bezeichnung der verantwortlichen Stelle	
1.2 Organisationskennziffer, Ministerium/Amt, Abteilung, ggf. Sachgebiet	
Straße	
PLZ/Ort	
Telefon/Telefax *	
E-Mail-Adresse *	
Internet-Adresse/URL *	

2. Vertretung

2.1 Leitung der verantwortlichen Stelle (einschl. Vertreter)	
2.2 mit der Leitung der Datenverarbeitung beauftragte Person(en):	

3. Angaben zur Person des Datenschutzbeauftragten *

Name(n)	
Straße	
PLZ/Ort	
Telefon/Telefax	
E-Mail-Adresse	
Internet-Adresse/URL	

Anlage Nr.:

(für jedes Verfahren automatisierter Verarbeitung ist eine separate Anlage zum Hauptblatt auszufüllen!)

Name/ Bezeichnung der verantwortl. Stelle (Übernahme der Nr. 1.1 aus Hauptblatt)	

Das Verfahren ist Teil eines gemeinsamen oder verbundenen Verfahrens nach § 10 BDSG	ja ☐ nein ☐ - Zutreffendes ankreuzen -
wenn ja, Bezeichnung der verantwortl. Stelle	

4. Zweckbestimmung, Verfahrensbezeichnung, Rechtsgrundlage

4.1 Zweckbestimmung der Datenerhebung, - verarbeitung oder - nutzung	
4.2 ggf. Bezeichnung des Verfahrens	
4.3 Rechtsgrundlage (ggf. nach Art der Datenverarbeitung unterschieden)	

5. Betroffene Personengruppen und Daten oder Datenkategorien

5.1 Beschreibung der betroffenen Personengruppen	
5.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien	

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können; bei Datentransfers in Drittstaaten siehe Nr. 8

7. Regelfristen für die Löschung der Daten, Zeitraum

8. Geplante Übermittlung in Drittstaaten

8.1 Name des Drittstaates	
8.2 Empfänger oder Kategorien von Empfängern	
8.3 Art der Daten oder Datenkategorien	

Behördeninterner Teil

- nicht zu veröffentlichen (nach § 4g Abs. 2 S. 2 BDSG) -

9. Angaben zur Beurteilung der Angemessenheit getroffener Sicherheitsmaßnahmen

9.1 Art der eingesetzten DV-Anlagen und Software	
9.2 Maßnahmen nach § 9 BDSG i.V.m. der Anlage dazu	

Erläuterungen zu 9.2:

Zutrittskontrolle	
Zugangskontrolle	
Zugriffskontrolle	
Weitergabekontrolle	
Eingabekontrolle	
Auftragskontrolle	
Verfügbarkeitskontrolle	
Trennungsgebot	

(Sind zu einem der vorstehenden Punkte keine Maßnahmen zu treffen, brauchen keine Angaben gemacht zu werden)

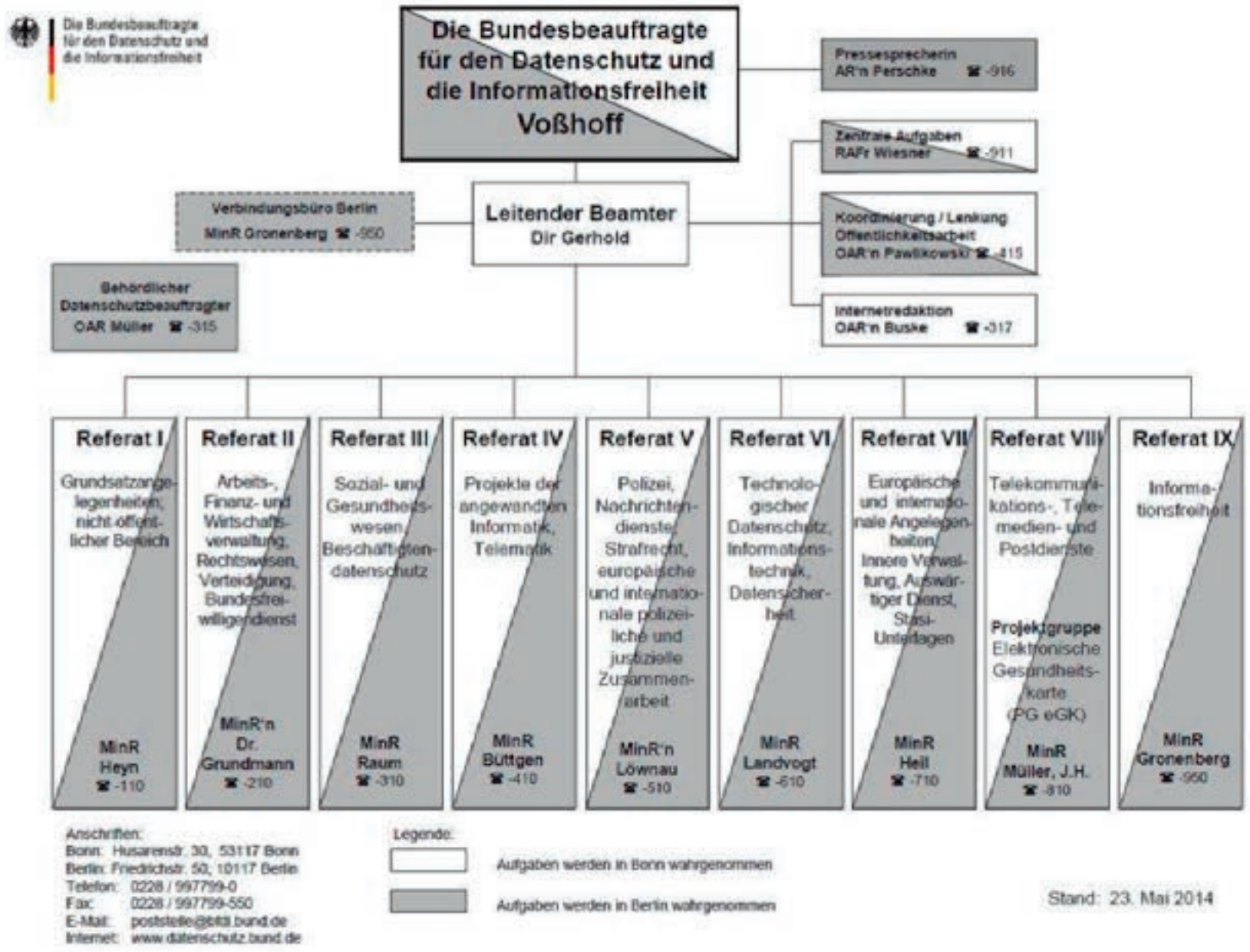
10. Zugriffsberechtigte Personen

Name/ Funktion/ Position	

11. Begründetes Ergebnis der Vorabkontrolle gem. § 4d Abs. 5 BDSG

11. Auftragsdatenverarbeitung * (Angabe freiwillig)

Handelt es sich um eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG ?	ja ☐ nein ☐ - Zutreffendes ankreuzen -


Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Voßhoff
Pressesprecherin
AR'n Perschke ☎ -916
Zentrale Aufgaben
RAFr Wiesner ☎ -911
Verbindungsbüro Berlin
MinR Gronenberg ☎ -950
Leitender Beamter
Dir Gerhold
Koordinierung / Lenkung Öffentlichkeitsarbeit
OAR'n Pawlikowski ☎ -915
Behördlicher Datenschutzbeauftragter
OAR Müller ☎ -315
Internetredaktion
OAR'n Buske ☎ -317
Referat I
Grundsatzangelegenheiten, nicht-öffentlicher Bereich
MinR Heyn ☎ -110
Referat II
Arbeits-, Finanz- und Wirtschaftsverwaltung, Rechtswesen, Verteidigung, Bundesfreiwilligendienst
MinR'n Dr. Grundmann ☎ -210
Referat III
Sozial- und Gesundheitswesen, Beschäftigtendatenschutz
MinR Raum ☎ -310
Referat IV
Projekte der angewandten Informatik, Telematik
MinR Buttgen ☎ -410
Referat V
Polizei, Nachrichtendienste, Strafrecht, europäische und internationale polizeiliche und justizielle Zusammenarbeit
MinR'n Löwnau ☎ -510
Referat VI
Technologischer Datenschutz, Informationstechnik, Datensicherheit
MinR Landvogt ☎ -610
Referat VII
Europäische und internationale Angelegenheiten, Innere Verwaltung, Auswärtiger Dienst, Stasi-Unterlagen
MinR Heil ☎ -710
Referat VIII
Telekommunikations-, Telemedien- und Postdienste
Projektgruppe Elektronische Gesundheitskarte (PG eGK)
MinR Müller, J.H. ☎ -810
Referat IX
Informationsfreiheit
MinR Gronenberg ☎ -950
Anschriften:
Bonn: Husarenstr. 30, 53117 Bonn
Berlin: Friedrichstr. 50, 10117 Berlin
Telefon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de
Legende:
Aufgaben werden in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen
Stand: 23. Mai 2014

Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis/Begriffe

A2LL	**A**lg II-**L**eistungen zum **L**ebensunterhalt
AA	Agenturen für Arbeit
AA	Auswärtiges Amt
a. a. O	am angegebenen Orte
ACTA	Anti-Counterfeiting Trade Agreement
ABl.	Amtsblatt der Europäischen Gemeinschaften
ABG	Automatisierte und biometriegestützte Grenzkontrolle
ABMG	Autobahnmautgesetz
Abs.	Absatz
ADAMS	Anti Doping Administration and Management System
AEO	Authorized Economic Operator
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft, aber auch: Arbeitsgruppe
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
ALG II	Arbeitslosengeld II
ALLEGRO	**Al**g II-**Le**istungsverfahren **Gr**undsicherung **O**nline
Alt.	Alternative
AND	Andere Nachrichtendienste
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
AOS	Allianz Ortungs Services GmbH
APAK	Abschlussprüferaufsichtskommission
APEC	Asia Pacific Economic Cooperation
ARGE	Arbeitsgemeinschaften nach dem Sozialgesetzbuch II
Art.	Artikel

AS	Autorisierte Stelle
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
ATM	Asynchronous Transfer Mode
AufenthG	Aufenthaltsgesetz
AufenthV	Aufenthaltsverordnung
AuslG	Ausländergesetz
AVV	Allgemeine Verwaltungsvorschrift
AWG	Außenwirtschaftsgesetz
Az.	Aktenzeichen
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
BA	Bundesagentur für Arbeit
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesamt für Güterverkehr
BAköV	Bundesakademie für öffentliche Verwaltung
BAMF	Bundesamt für Migration und Flüchtlinge
BArchG	Bundesarchivgesetz
BASt	Bundesanstalt für Straßenwesen
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BBR	Bundesanstalt für Bauwesen und Raumordnung
BBSR	Bundesinstitut für Bau-, Stadt- und Raumforschung
BCR	Binding Corporate Rules; verbindliche unternehmensinterne Datenschutzregelungen

BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
bDSB	behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
Bea	Bescheinigungen elektronisch annehmen
BerCA	Berechtigungszertifikateanbieter
BevStatG	Bevölkerungsstatistikgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BFD	Bundesfinanzdirektion
BFDG	Bundesfreiwilligendienstgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfD/BA	Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BfDBw	behördlicher Datenschutzbeauftragter in der Bundeswehr
BFH	Bundesfinanzhof
BfJ	Bundesamt für Justiz
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BISp	Bundesinstitut für Sportwissenschaft
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
Bluetooth	Standard für die drahtlose Übermitlung von Sprache und Daten im Nahbereich
BMAS	Bundesministerium für Arbeit und Soziales
BMEL	Bundesministerium für Ernährung und Landwirtschaft
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend

BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Energie
BMUB	Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BR	Bundesrat
BR-Drs.	Bundesratsdrucksache
BSG	Bundessozialgericht
BSH	Bundesamt für Seeschifffahrt und Hydrographie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT	Bundestag
BT-Drs.	Bundestagsdrucksache
BVA	Bundesversicherungsamt
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVV	Bundesvermögensverwaltung
BZR	Bundeszentralregister

BZRG	Bundeszentralregistergesetz
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise
ca.	circa
CAA	Competent Authority Agreement
CBPR	Cross Border Privacy Rules
CC	Common Criteria
CD / CD-ROM	Compact Disc - Read Only Memory
CDR	Call Data Records
CIA	Central Intelligence Agency, USA
CRS	Common Reporting Standard
DA-KG	Dienstanweisung zum Kindergeld nach dem Einkommensteuergesetz
DA-PVD	Dienstanweisung für den Polizeivollzugsdienst beim Deutschen Bundestag
DB	Deutsche Bahn
d. h.	das heißt
DDR	Deutsche Demokratische Republik
DECT	Digital Enhanced Cordless Telecommunications
DHR	Deutsches Hämophilieregister
DIBAS	Digitalisierung von Schriftgut der Bundesagentur für Arbeit
DLZ	Dienstleistungszentrum
DMDA	akkreditierte De-Mail-Diensteanbieter
DNS	Domain Name System
DNT	Do not track
Dok.	Dokument
DPAG	Deutsche Post AG
DPI	Deep Packet Inspection
DPIA	Data Protection Impact Assessment

DPMA	Deutsches Patent- und Markenamt
DRM	Digital Rights Management (Digitales Rechte Management)
Drs.	Drucksache
DRV Bund	Deutsche Rentenversicherung Bund
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSL	Digital Subscriber Line
DSRV	Datenstelle der Träger der Rentenversicherung
DTAG	Deutsche Telekom AG
Düsseldorfer Kreis	Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
DV/dv	Datenverarbeitung
DVB-C	Digital Video Broadcasting-Cable
DWH	Data Warehouse
E-Akte	elektronische Akte
eAT	elektronischer Aufenthaltstitel
e. V.	eingetragener Verein
E-Commerce	Elektronic Commerce/Elektronischer Handel
ED	Erkennungsdienst
EDPS	Europäischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EETS / EEMD	Europäischer Elektronischer Mautdienst
EG	Europäische Gemeinschaft(en)
eGK	elektronische Gesundheitskarte
EG-ZIS	Europäisches Zollinformationssystem
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EHUG	Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
EIS	Europäisches Informationssystem
eID	elektronischer Identitätsnachweis, elektronische Identitätsfunktion

EJG	Eurojust-Gesetz
eKA	elektronische Kriminalakte
ELENA	Elektronischer Entgeltnachweis
ELStAM	Elektronische LohnSteuerAbzugsMerkmale
ELSTER	Elektronische Steuererklärung
E-Mail	Electronic Mail
EMF	Elektromagnetische Felder
EnWG	Energiewirtschaftsgesetz
EP	Europäisches Parlament
EPC	Electronic Product Code — Der EPC besteht aus vier Datenblöcken zur Identifizierung der Version, des Herstellers, der Produktkategorie und des individuellen Gegenstands
EPCglobal	EPCglobal Inc. ist ein Joint Venture zwischen EAN International und dem Uniform Code Council (UCC). Die Aufgabe des Nonprofit-Unternehmens liegt in der kommerziellen Vermarktung sowie der Administration des EPC
ERP	Enterprise Resource Planning = Software der Firma SAP
EStA	Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten
EstG	Einkommensteuergesetz
etc.	ecetera
eTIN	Lohnsteuerliches Ordnungsmerkmal
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurodac	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
Europol	Europäisches Polizeiamt
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f.	folgend
FATCA-Abkommen	Foreign Account Tax Compliance Act (US Gesetz zur Erfassung von Vermögenswerten von in den USA steuerpflichtigen Personen und Gesellschaften auf Konten im (US-)Ausland

FATF	Financial Action Task Force, Arbeitskreis Maßnahmen zur Geldwäschebekämpfung
FAQ	Frequently Asked Questions (häufig gestellte Fragen)
FBI	Federal Bureau of Investigation, USA
FDZ	Forschungsdatenzentrum
ff.	folgende
FFI	Foreign Financial Institution (ausländische Finanzinstitute)
FG	Finanzgericht
FGO	Finanzgerichtsordnung
FH Bund	Fachhochschule des Bundes für öffentliche Verwaltung
FIFA	Fédération Internationale de Football Association
Finanzagentur	Bundesrepublik Deutschland Finanzagentur GmbH
FKS	Finanzkontrolle Schwarzarbeit
FTC	Federal Trade Commission
FVG	Finanzverwaltungsgesetz
G10	Artikel-10-Gesetz
GAC	Governmental Advisory Committee
GASIM	Gemeinsames Analyse- und Strategiezentrum Illegale Migration
GBA	Generalbundesanwalt beim Bundesgerichtshof
gem.	gemäß
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GIW	Geoinformationswirtschaft
GIZ	Internetzentrum
GJVollz-E	Gesetzentwurf zur Regelung des Jugendstrafvollzugs

GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GKV-WSG	Gesetz zur Stärkung des Wettbewerbs in der Gesetzlichen Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GMBl	Gemeinsames Ministerialblatt
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GPEN	Global Privacy Enforcement Network
GPS	Global Positioning System
GRCh	EU-Grundrechtecharta
GS1	Global Standards One
GSM	Global System for Mobile Communications
GTAZ	Gemeinsames Terrorismusabwehrzentrum
GwG	Geldwäschegesetz
HEGA	**H**andlungs**e**mpfehlung/**G**eschäfts**a**nweisung der BA
HIS	Hinweis- und Informationssystem
HKP	häusliche Krankenpflege
HPC	Health Professional Card
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
HZA	Hauptzollamt
IAB	Institut für Arbeitsmarkt- und Berufsforschung
IATA	International Air Transport Association
i. d. F.	in der Fassung
i. d. R.	in der Regel
i. S. d.	im Sinne des (der)
i. S. v.	im Sinne von

i. V. m.	in Verbindung mit
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization
ICHEIC	International Commission on Holocaust Era Insurance Claims
ICO	The Information Commissioner's Office
IFG	Informationsfreiheitsgesetz
IFOS-Bund	Interaktives Fortbildungssystem für die Bundesverwaltung
IHK	Industrie- und Handelskammer
IKPO	Internationale Kriminalpolizeiliche Organisation
IKT	Informations- und Kommunikationstechnologie
ILO	International Labour Organization
IMI	Internal Market Information System (Binnenmarktinformationssystem)
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder
IMSI	International Mobile Subscriber Identity
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
IntV	Integrationskursverordnung
IP	Internet Protocol
IPBPR	Internationaler Pakt über Bürgerliche und Politische Rechte
IPR	Internationales Privatrecht
IPv6	Internet Protocol Version 6
IRS	Internal Revenue Service (Bundessteuerbehörde der USA)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISPPI	International Standard for the Protection of Privacy and Personal Information
IT	Informationstechnik
IVBB	Informationsverbund Berlin-Bonn

JI-Rat	Rat der Innen- und Justizminister der Europäischen Union
KBA	Kraftfahrt-Bundesamt
KdU	**K**osten **d**er **U**nterkunft und Heizung
KEV	Kontrolleinheit Verkehrswege
KFU	Krebsfrüherkennungsrichtlinien
Kfz	Kraftfahrzeug
KIWI	Kindergeld-Windows-Implementierung
KOM	Europäische Kommission
KWG	Kreditwesengesetz
LfD	Landesbeauftragter für den Datenschutz
LfV	Landesamt für Verfassungsschutz
LG	Landgericht
lit.	litera (=Buchstabe)
LKA/LKÄ	Landeskriminalamt/Landeskriminalämter
LuftSiG	Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz)
m. E.	meines Erachtens
MAD	Militärischer Abschirmdienst
MAK	Mindestanforderungen an das Kreditgeschäft der Kreditinstitute
MBR	Mitarbeiter- und Beschwerderegister
MDK	Medizinischer Dienst der Krankenversicherung
MfS	Ministerium für Staatssicherheit
MI6	Military Intelligence, Section 6
MRI	Max-Rubner-Institut
MRRG	Melderechtsrahmengesetz
MSISDN	Mobile Subscriber ISDN Number
MSU	Mail Sampling Unit
MVDS	Multifunktionaler Verdienstdatensatz

MVP	zentrale Melde- und Veröffentlichungsplattform der BaFin
m. w. N.	mit weiteren Nachweisen
MZG	Mikrozensusgesetz
NADIS	Nachrichtendienstliches Informationssystem
NADIS-WN	Narichtendienstliches Informationssystem - Wissensnetz
NATO	North Atlantic Treaty Organization
NEMONIT	Nationales Ernährungsmonitoring
NFC	Near Field Communication
NGN	Next Generation Network
NJW	Neue Juristische Wochenschrift
nPA	elektronischer Personalausweis, neuer Personalausweis
Nr.	Nummer
NWR	Nationales Waffenregister
NWRG	Gesetz zur Errichtung eines Nationalen Waffenregisters
o. a.	oben aufgeführt
OCR	Optical Character Recognition (Optische Zeichenerkennung)
o. g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OK	Organisierte Kriminalität
OLAF	Europäisches Amt für Betrugsbekämpfung
OMS	Optimierte Meldeverfahren in der sozialen Sicherung
Opol	Operational Point of Contact
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
P23R	Prozessdatenbeschleuniger
PassG	Passgesetz

PAVOS	Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem (beim BGS)
PbD	Privacy by Design
PC	Personalcomputer
PCAOB	Public Company Accounting Oversight Board (amerikanische Aufsichtsbehörde für Wirtschaftsprüfer)
PCC	Privacy Commissioner of Canada
PDA	Personal Digital Assistant
PEI	Paul-Ehrlich-Institut
PEP	politisch exponierte Personen
PersauswG	Personalausweisgesetz
PIA	Privacy Impact Assessment
PIN	Persönliche Identifikationsnummer
PKGr	Parlamentarisches Kontrollgremium
PMK-Links-Z	Zentraldatei „Politisch motivierte Kriminalität-links“
PNR	Passenger Name Record
Protection Profile	Schutzprofil
Ratsdok.	Ratskokument (EU)
RatSWD	Rat für Sozial- und Wirtschaftsdaten
Rdn.	Randnummer
Reha	Rehabilitation
REHA-Maßnahmen	Rehabilitationsmaßnahme
RFID	Radio Frequency Identification — Transpondertechnik für die berührungslose Erkennung von Objekten
RFID-Chip	Radio Frequency Identification-Chip (Funkchip)
RFV	Registratur Fachverfahren
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RKI	Robert-Koch-Institut
RLTk	Richtlinie Telekommunikation
RSAV	Risikostrukturausgleichsverordnung

RVOrgG	Organisationsreform in der gesetzlichen Rentenversicherung
S.	Seite
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuFV	Schuldnerverzeichnisführungsverordnung
SchwarzArbG	Schwarzarbeitsbekämpfungsgesetz
SDÜ	Schengener Durchführungsübereinkommen
SG	Soldatengesetz
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB II	Sozialgesetzbuch Zweites Buch (Grundsicherung für Arbeitssuchende)
SGB III	Sozialgesetzbuch Drittes Buch (Arbeitsförderung)
SGB IV	Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung)
SGB V	Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung)
SGB VI	Sozialgesetzbuch Sechstes Buch (Gesetzliche Rentenversicherung)
SGB VII	Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung)
SGB VIII	Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe)
SGB IX	Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinderter Menschen)
SGB X	Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozialdatenschutz)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SGB XII	Sozialgesetzbuch Zwölftes Buch (Sozialhilfe)
SigG	Signaturgesetz
SIM	Subscriber Identity Module
SiMKo2	Sichere Mobile Kommunikation
SMS	Short Message Service
SNS	Sichere Netzübergreifende Sprachkommunikation
SOG	Gesetz über öffentliche Sicherheit und Ordnung
sog.	so genannt

SPD	Sozialdemokratische Partei Deutschlands
STADA	Staatsangehörigkeitsdatei
StAG	Staatsangehörigkeitsgesetz
Stasi	Staatssicherheitsdienst der ehemaligen DDR
StDAV	Steuerdaten-Abruf-Verordnung
StDÜV	Steuerdatenübermittlungsverordnung
Steuer-ID	Steuer-Identitätsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVBG	Steuerverkürzungsbekämpfungsgesetz
StVergAbG	Steuervergünstigungsabbaugesetz
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
SDDSG	Suchdienstedatenschutzgesetz
SÜFV	Sicherheitsüberprüfungsfeststellungsverordnung
SÜG	Sicherheitsüberprüfungsgesetz
SUG	Seesicherheits-Untersuchungs-Gesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAB	Büro für Technikfolgenabschätzung beim Deutschen Bundestag
TAL	Teilnehmeranschlussleitung
TAN	Transaktionsnummer
TB	Tätigkeitsbericht
TBG	Terrorismusbekämpfungsgesetz
TFG	Transfusionsgesetz
TFTP	Terrorist Finance Tracking Program
THW	Bundesanstalt Technisches Hilfswerk

TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
TNB	Teilnehmernetzbetreiber
TOP	Tagesordnungspunkt
TR	Technische Richtlinie
TTIP	Transatlantic Trade and Investment Partnership
u. a.	unter anderem
u. ä.	und ähnliches
UAS	Unmanned Aerial Systems
u. U.	unter Umständen
UIG	Umweltinformationsgesetz
UKlaG	Unterlassungsklagengesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
US	United States
USA	United States of America
UStG	Umsatzsteuergesetz
usw.	und so weiter
VAM	Virtueller Arbeitsmarkt
VBM	vorläufiges Bearbeitungsmerkmal
VdAK	Verband der Angestellten-Krankenkassen
VDR	Verband Deutscher Rentenversicherungsträger
VDS	Vorratsdatenspeicherung
VerBIS	Vermittlungs-, Beratungs- und Informationssystem - IT-Fachverfahren der Bundesagentur für Arbeit für die Bereiche Vermittlung und Beratung

VG	Verwaltungsgericht
vgl.	vergleiche
VIS	Europäisches Visa-Informationssystem
VN	Vereinte Nationen
VNB	Verbindungsnetzbetreiber
VOIP	Voice over IP
VPN	Virtual Private Network (dt. virtuelles privates Netz)
vpS	Vorbeugender personeller Sabotageschutz
VS	Verschlusssache
W3C	World Wide Web Consortium
WADA	Welt-Anti-Doping-Agentur
WAP	Wireless Application Protocol
WehrRÄndG	Wehrrechtsänderungsgesetz 2011
WiMax	Wordwide Interoperability for Microwave Access Standard gemäß IEEE 802.16a für lokale Funknetze
WLAN	Wireless Local Area Network
WoGG	Wohngeldgesetz
WP	Working Paper
WPersAV	Personalaktenverordnung Wehrpflichtige
WpHGMaAnzV	WpHG-Mitarbeiteranzeigeverordnung
WPK	Wirtschaftsprüferkammer
WPO	Wirtschaftsprüferordnung
WPPJ	Working Party Police and Justice (Arbeitsgruppe Polizei und Justiz)
WSA	Wasser- und Schifffahrtsamt
www	World wide web
XML	Extensible Markup Language
z. B.	zum Beispiel
z. T.	zum Teil

ZAG	Zentren für Arbeit und Grundsicherung
ZAUBER	Abrufverfahren
ZAV	Zentrale Auslands- und Fachvermittlung der Bundesagentur für Arbeit
ZDG	Zivildienstgesetz
ZensG 2011	Zensusgesetz 2011
ZentrLuRMedLw	Zentrum für Luft- und Raumfahrtmedizin der Luftwaffe
ZFdG	Zollfahndungsdienstgesetz
ZFER	Zentrales Fahrerlaubnisregister
ZIS	Zollinformationssystem
ZIVIT	Zentrum für Informationsverarbeitung und Informationstechnik
ZKA	Zollkriminalamt
ZNwG	Zentrum für Nachwuchsgewinnung
ZORA	Zukunftsorientierte Retailanwendung
ZPO	Zivilprozessordnung
ZSS	Zentrale Speicherstelle
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Tätigkeitsbericht	Berichtszeitraum	Bundestags-Drucksachennummer
1.	1978	8/2460
2.	1979	8/3570
3.	1980	9/93
4.	1981	9/1243
5.	1982	9/2386
6.	1983	10/877
7.	1984	10/2777
8.	1985	10/4690
9.	1986	10/6816
10.	1987	11/1693
11.	1988	11/3932
12.	1989	11/6458
13.	1990	12/553
14.	1991 — 1992	12/4805
15.	1993 — 1994	13/1150
16.	1995 — 1996	13/7500
17.	1997 — 1998	14/850
18.	1999 — 2000	14/5555
19.	2001 — 2002	15/888
20.	2003 — 2004	15/5252
21.	2005 - 2006	16/4950
22.	2007 - 2008	16/12600
23.	2009 - 2010	17/5200
24.	2011 - 2012	17/13000

Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
D-53117 Bonn

Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de

Bonn 2015

Druck:
Silber Druck oHG
Am Waldstrauch 1
34266 Niestetal