Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

26.

Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016

Tätigkeitsbericht 2015-2016

26. Tätigkeitsbericht

Dieser Bericht wurde am 30. Mai 2017 dem Präsidenten des Deutschen Bundestages, Herrn Prof. 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 2015 und 2016 der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - 26. 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

Mit diesem 26. Tätigkeitsbericht lege ich zugleich den ersten Tätigkeitsbericht meines Hauses als eigenständige oberste Bundesbehörde vor. Der Bundesgesetzgeber hat mit der Änderung des BDSG im Jahr 2014 die Weichen für diese Umstrukturierung gestellt und damit auch die Vorgaben des EuGH zur Unabhängigkeit der Datenschutzaufsicht für mein Haus ab dem Jahr 2016 erfüllt.

Der Berichtszeitraum war daher, neben der Erfüllung der mir gesetzlich zugewiesenen Aufgaben, maßgeblich vom Umstrukturierungsprozess im Haus geprägt, um administrativ die Neuaufstellung des Hauses auch mit Leben zu erfüllen.

Mit Beginn des Jahres 2016 ist die BfDI nun eigenständige oberste Bundesbehörde.

Auch im Bereich der Fortentwicklung des Datenschutzrechtes wurden im Berichtszeitraum entscheidende Weichen gestellt. Mit der Verabschiedung der europäischen Datenschutzgrundverordnung wird es ab dem 25. Mai 2018 in der EU unmittelbar geltendes Datenschutzrecht geben. Als Grundsatzthema findet die Darstellung dieser künftigen Rechtslage in diesem Tätigkeitsbericht daher besondere Berücksichtigung. Auch bei den datenschutzrechtlichen Themenstellungen der jeweiligen Ausschüsse des Deutschen Bundestages habe ich erste Fragen zur Auswirkung der DSGVO gestellt und ebenso erste Einschätzungen dazu skizziert.

Im politischen Diskurs zum Datenschutz in der digitalen Welt wird immer wieder die Frage aufgeworfen, ob und in welcher Weise die künftige europäische Grundverordnung das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger sichert und stärkt. Gerade weil der rasante Fortschritt der technologischen Entwicklung immer wieder auch die Grenzen des Datenschutzrechts aufzeigt und das Smartphone mit seiner datenintensiven Nutzung täglicher Begleiter von uns allen geworden ist, wird die DSGVO - so komplex und fordernd der Regelungsbereich bei erster Durchsicht erscheinen mag - mit seiner Grundausrichtung der einheitlichen europäischen Rechtsanwendung zu einer Stärkung des Datenschutzes beitragen.

Um diese Wirkung auch nachhaltig sicher zu stellen, ist der nationale Gesetzgeber in besonderer Weise gefordert, bei der Anpassung an die DSGVO und der Ausgestaltung bestehender nationaler Regelungsspielräume die Stärke der einheitlichen europäischen Rechtsanwendung zu unterstreichen und nicht zu schwächen.

Der nationale Anpassungsprozess wird nicht nur den Gesetzgeber sondern gleichermaßen auch die föderal aufgestellten Datenschutzaufsichtsbehörden fordern. Die durch die DSGVO gewollte Stärkung der Stellung und auch der Befugnisse der Datenschutzaufsicht wird in entscheidender Weise dazu beitragen, dem informationellen Selbstbestimmungsrecht in der digitalen Welt europaweit zu mehr Bedeutung zu verhelfen. Mit dem Haushaltsgesetz für das Jahr 2017 hat der Deutsche Bundestag mit der Ausstattung meines Hauses hierzu erste Weichen gestellt. Dies begrüße ich ausdrücklich.

Neben der künftig europaweit geltenden DSGVO und deren Umsetzung gegenüber öffentlichen und nicht-öffentlichen Stellen kommt aber auch der bis zum 6. Mai 2018 notwendigen Umsetzung der JI-Richtlinie in nationales Recht grundsätzliche Bedeutung zu. Staatliche Datenverarbeitung insbesondere im Polizei- und Sicherheitsbereich steht dabei immer im Spannungsfeld zwischen Sicherheit und Freiheit und in besonderer Weise unter dem Anspruch der Rechtfertigung hinsichtlich der Erforderlichkeit und der Verhältnismäßigkeit. Wegweisende Entscheidungen sowohl des Bundesverfassungsgerichts als auch des europäischen Gerichtshofes haben hierzu klare Vorgaben gesetzt. Von ganz grundsätzlicher Bedeutung ist dabei die Klarstellung durch das Bundesverfassungsgericht, dass zur Kompensation des staatlichen Grundrechtseingriffs in das informationelle Selbstbestimmungsrecht eine effiziente Datenschutzaufsicht erforderlich ist. Hier ist der Gesetzgeber nach wie vor gefordert, die dazu notwendigen Voraussetzungen für mein Haus zu schaffen.

Eine starke Datenschutzaufsicht in der digitalen Welt ist kein Selbstzweck sondern Grundpfeiler zur Wahrung des grundrechtlichen Persönlichkeitsschutzes gegenüber ökonomischen Datenverwertungsinteressen. Eine starke Datenschutzaufsicht ist auch kein Gegensatz zu den wachsenden Aufgaben und neuen Herausforderungen staatlicher Sicherheitsbehörden. Das Gegenteil ist der Fall. Sie stärkt das Vertrauen der Bürger in staatliches Handeln.

Mit der Vorlage dieses Tätigkeitsberichtes darf ich mich gleichzeitig sehr herzlich bei meinen Mitarbeiterinnen und Mitarbeitern für die geleistete Arbeit bedanken. Das Querschnittsthema Datenschutz fordert uns immer wieder und die rasante technologische Entwicklung und deren wachsende Herausforderungen setzen ein hohes Engagement voraus.

Bedanken darf ich mich an dieser Stelle aber auch sowohl bei der Bundesregierung, insbesondere dem BMF, als auch bei den Abgeordneten des Deutschen Bundestages und insbesondere bei den Berichterstattern zu meinem Einzelplan 21 im Haushaltsausschuss, die maßgeblich die Umstrukturierung zur obersten Bundesbehörde begleitet und unterstützt haben.

Gern bedanke ich mich auch bei allen Bürgerinnen und Bürgern, die durch ihre Eingaben und Anfragen immer wieder mit dafür sorgen, dem Datenschutz auch im Alltag zur Durchsetzung zu verhelfen.

Bonn, Mai 2017

Andrea Voßhoff

Die 9-jährige Tochter einer meiner Mitarbeiterinnen ließ sich von mir einmal erläutern, was die Aufgaben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind. Nun ist es gar nicht so einfach, Kindern den Datenschutz zu erklären. Was sie aber verstanden hatte, war, dass ich zur Erledigung meiner Aufgaben noch viele Wünsche habe. Am Ende des Gespräches schenkte sie mir dieses Bild und nannte es „Wunschpunkte“. Sie erläuterte dazu, sobald einer meiner Wünsche erfüllt sei, bräuchte ich ja nur einen Punkt durchstreichen. Das Bild hängt seit diesem Gespräch in meinem Büro.

Zusammenfassung der Empfehlungen

Ich empfehle dem Gesetzgeber in Bund und Ländern, sich bei der Anpassung des nationalen Datenschutzrechts an Geist und Buchstaben der neuen europäischen Datenschutzregeln zu halten, um eine weitgehend einheitliche Anwendung des künftigen europäischen Datenschutzes zu gewährleisten (Nr. 1.1, Nr. 1.2. ff).

Ich empfehle dem Gesetzgeber, von der in der DSGVO eingeräumten Möglichkeit, spezifische nationale Regelungen zum Beschäftigtendatenschutz zu erlassen, zeitnah Gebrauch zu machen (Nr. 3.1, 3.2.1).

Ich empfehle dem Gesetzgeber die Prüfung, bei Regelungen zur Datenverarbeitung besondere Vorschriften zum Schutz von Kindern zu ergreifen (Nr. 7.1).

Ich empfehle dem Gesetzgeber, die nach der DSGVO von Mitgliedsstaaten mit mehr als einer Datenschutzaufsicht einzurichtende zentrale Anlaufstelle personell und sächlich so auszustatten, dass eine Koordinierung der nationalen Mitwirkungsmöglichkeiten im künftigen europäischen Datenschutzausschuss effizient und wirkungsvoll möglich ist (Nr. 1.2.1).

Ich empfehle dem Gesetzgeber, den ihm nach der DSGVO verbleibenden Gestaltungsspielraum im Bereich der gesetzlichen Krankenversicherung zu nutzen, das hier geltende sorgfältig aufeinander abgestimmte Gefüge der bereichsspezifischen datenschutzrechtlichen Vorschriften in seinen Grundfesten zu erhalten (Nr. 9.1).

Ich empfehle dem Gesetzgeber im Rahmen der Umsetzung der Datenschutzrichtlinie für den Bereich Polizei und Justiz, die Untersuchungs-, Anordnungs- und Klagebefugnisse der Datenschutzaufsicht wie in der DSGVO zu regeln (Nr. 1.2.2).

Ich empfehle dem Gesetzgeber im Bereich der Sicherheitsbehörden und der Nachrichtendienste, die notwendigen Voraussetzungen einer effizienten Datenschutzaufsicht entsprechend der vom Bundesverfassungsgericht geforderten Kompensationsfunktion zu schaffen und die begonnene Personalverstärkung der BfDI dringend weiter auszubauen. Effiziente Sicherheitsgewährleistung und wirksame Datenschutzkontrolle sind zwei Seiten derselben Medaille. Der Haushaltsgesetzgeber ist hier weiterhin gefordert (Nr. 1.3).

Ich empfehle dem Gesetzgeber zur Klärung der Zuständigkeitsfragen der beiden Kontrollinstanzen G -10- Kommission und BfDI, die entsprechenden gesetzlichen Klarstellungen sowohl im BDSG als auch im Artikel 10 Gesetz vorzunehmen. Die im Zuge der Umsetzung der DSGVO

anzupassenden Gesetze bieten hierzu eine gute Gelegenheit, die nicht versäumt werden sollte (Nr. 10.2.10.3).

Ich empfehle dem Gesetzgeber, die Rechtsgrundlagen für die Eingriffsbefugnisse der Sicherheitsbehörden und der Nachrichtendienste entsprechend den Vorgaben des Bundesverfassungsgerichtes zum BKAG verfassungskonform auszugestalten, d.h. auch geltende Regelungen entsprechend zu ändern (Nr. 1.3).

Ich empfehle dem Gesetzgeber, den datenschutzrechtlichen Auskunftsanspruch im Besteuerungsverfahren zeitnah gesetzlich zu regeln (Nr. 8.2.3).

Ich empfehle dem Gesetzgeber, gesetzliche Regelungen für das Einführen von Mortalitätsregistern für Forschungszwecke zu schaffen (Nr. 9.2.3).

Ich empfehle dem Gesetzgeber im Bereich der IT-Systeme klare Vorgaben zu schaffen, damit sowohl ein Höchstmaß an Sicherheit und Widerstandsfähigkeit von IT-Systemen als auch das Maximum zum Schutz personenbezogener Daten erreicht werden kann (Nr. 10.2.11.1).

Die Arbeit der BfDI in Zahlen

Die Arbeit der BfDI in Zahlen

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat ein weites Spektrum vielfältiger Aufgaben. Was das für die Dienststelle bedeutet, lässt sich auch mit einigen Zahlen verdeutlichen, die ich im Berichtszeitraum statistisch erfasst habe.

Auch wenn die im Berichtszeitraum erfassten Daten nicht dem Anspruch an eine amtliche Statistik genügen, haben sie dennoch einen aussagefähigen Erkenntniswert und lassen Tendenzen erkennen.

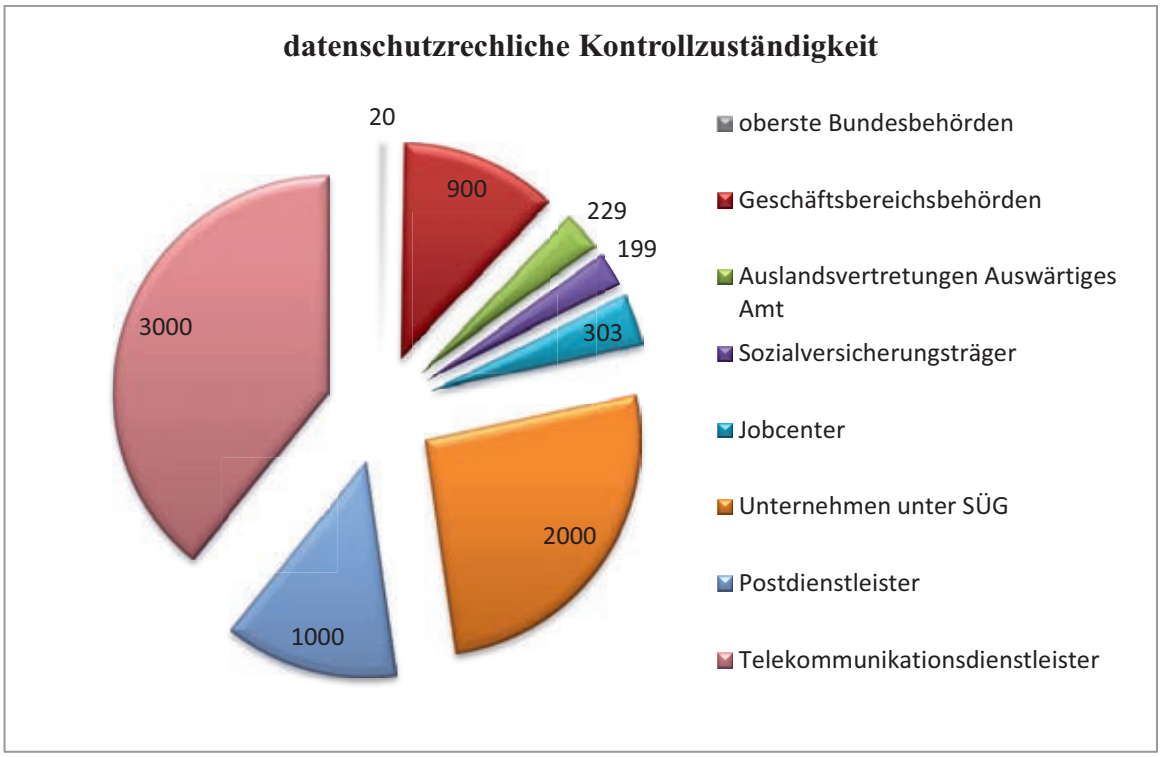
Wen kontrolliert die BfDI?

Zu den Aufgaben der BfDI gehört u. a. die datenschutzrechtliche Kontrolle der öffentlichen Stellen des Bundes. Dazu gehören neben den 20 Obersten Bundesbehörden mit - laut Behördenverzeichnis unter www.bund.de - 900 Geschäftsbereichsbehörden weitere 229 Auslandsvertretungen des Auswärtigen Amtes. Weiter unterstehen meiner Kontrolle u. a auch 199 bundesunmittelbare Sozialversicherungsträger und deren Spitzenverbände sowie 303 „gemeinsame Einrichtungen nach § 50 Absatz 2 SGB II“ (Jobcenter). Zudem unterliegen in den Bereichen Sabotageschutz und Geheimschutz alle öffentlichen Stellen des Bundes und rund 2.000 Unternehmen, die dem Sicherheitsüberprüfungsgesetz unterfallen, meiner Kontrolle.

Die BfDI kontrolliert auch die Einhaltung der datenschutzrechtlichen Bestimmungen bei den Anbietern von Post- und Telekommunikationsunternehmen. Dies umfasst ca. 3.000 Telekommunikations- und ca. 1.000 Postdienstleister (vgl. Kasten a).

Kasten a

datenschutzrechtliche Kontrollzuständigkeit der BfDI	
20	Oberste Bundesbehörden
900	Geschäftsbereichsbehörden
229	Auslandsvertretungen Auswärtiges Amt
199	Sozialversicherungsträger
303	Jobcenter
2.000	Unternehmen nach SÜG
1.000	Postdienstleister
3.000	Telekommunikationsdienstleister



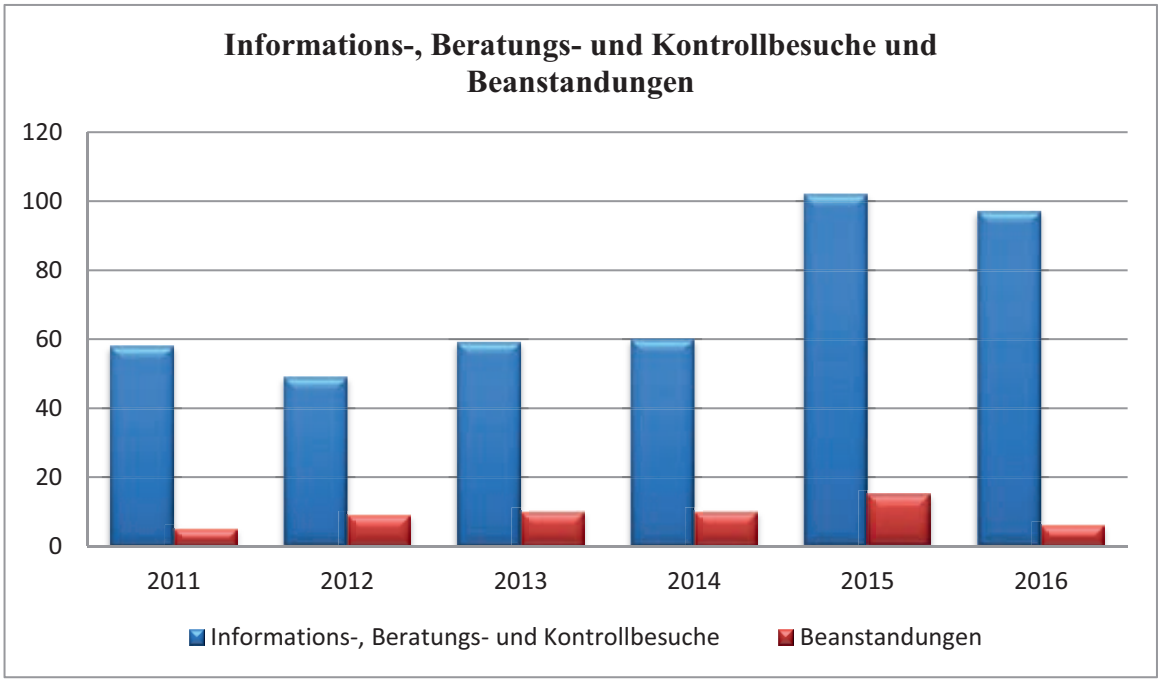
Anzahl der Informations- Beratungs- und Kontrollbesuche

In den letzten beiden Jahren haben meine Mitarbeiterinnen und Mitarbeiter 199 Behörden und Unternehmen in einer oft mehrtägigen Kontrolle umfassend oder in bestimmten Bereichen beraten und geprüft. Dabei habe ich 22-mal erhebliche Mängel festgestellt, die ich förmlich beanstandet habe (vgl. hierzu Kasten b). Bei Kontrollen haben die Mitarbeiterinnen und Mitarbeiter der BfDI das Recht auf Zutritt zu allen Diensträumen der zu kontrollierenden Stellen sowie das Recht auf Auskunft und auf Einsichtnahme in Unterlagen und gespeicherte Daten und Datenverarbeitungsprogramme.

Kasten b

Berichtszeitraum	Informations-, Beratungs- und Kontrollbesuche
2016	97
2015	102
2014	60
2013	59
2012	49
2011	58

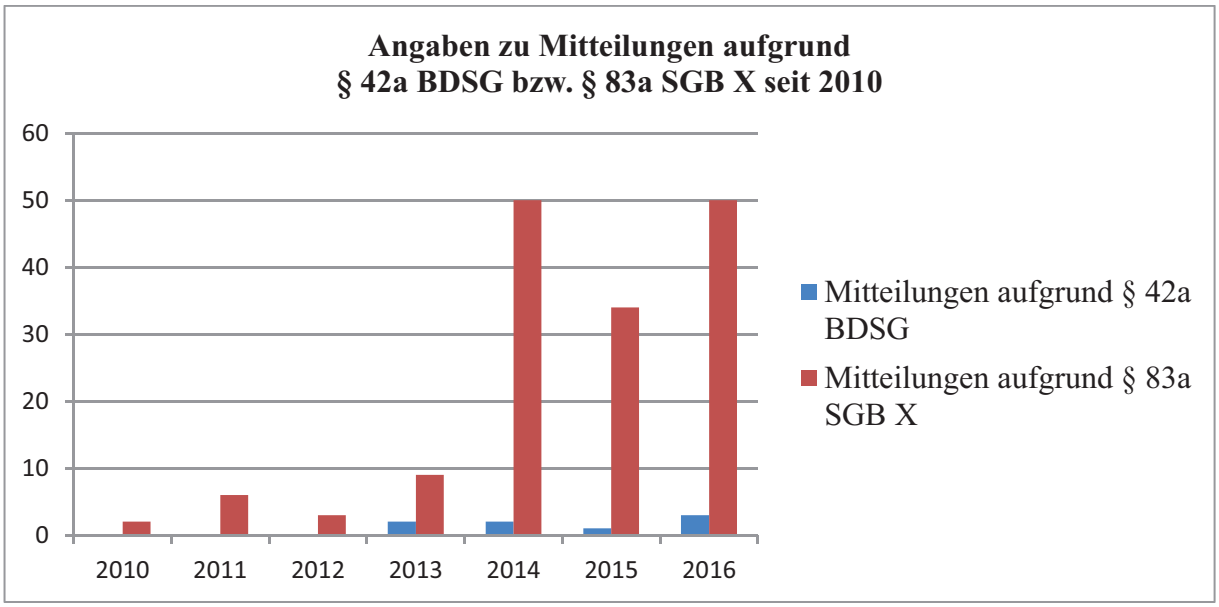
Berichtszeitraum	Beanstandungen
2016	7
2015	15
2014	10
2013	10
2012	9
2011	5



Meldepflichten

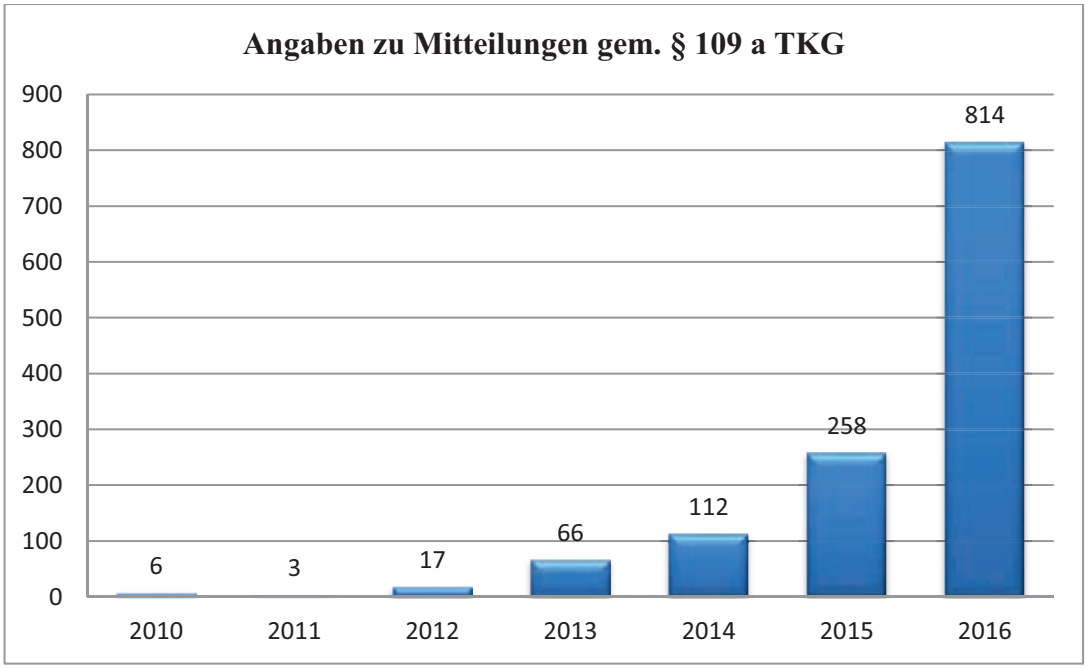
Im Berichtszeitraum sind sowohl Sozialleistungsträger als auch sonstige Stellen ihrer gesetzlichen Verpflichtung nachgekommen, mich über „Datenschutzpannen“ in ihrem Verantwortungsbereich zu informieren. Es ist meine Aufgabe, diese Meldungen zu kontrollieren. Hierzu muss jeder Fall individuell bewertet und gegebenenfalls weitergehende Maßnahmen eingeleitet werden.

Sozialleistungsträger sind nach § 83a SGB X verpflichtet, mir Datenschutzverletzungen innerhalb ihrer Organisationseinheiten mitzuteilen, wenn sie feststellen, dass dort gespeicherte besondere Arten personenbezogener Daten (vgl. § 67 Abs. 12 SGB X) unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Insgesamt haben mich im Berichtszeitraum 84 Meldungen erreicht (vgl. u. Nr. 3.3.1



Darüber hinaus haben mich insgesamt vier weitere Meldungen anderer öffentlicher Stellen erreicht, die nach § 42a BDSG zur Information verpflichtet sind (vgl. u. Nr. 3.3.1).

Weiter wurden mir im Berichtszeitraum 1072 Datenschutzverstöße von Telekommunikationsanbietern gemeldet (vgl. Nr. 17.2.4.6). Durch § 109a Telekommunikationsgesetz werden die Telekommunikationsdiensteanbieter verpflichtet, die Bundesnetzagentur (BNetzA) und mich sowie unter bestimmten Umständen auch die Betroffenen zu benachrichtigen, wenn der Schutz personenbezogener Daten verletzt worden ist.



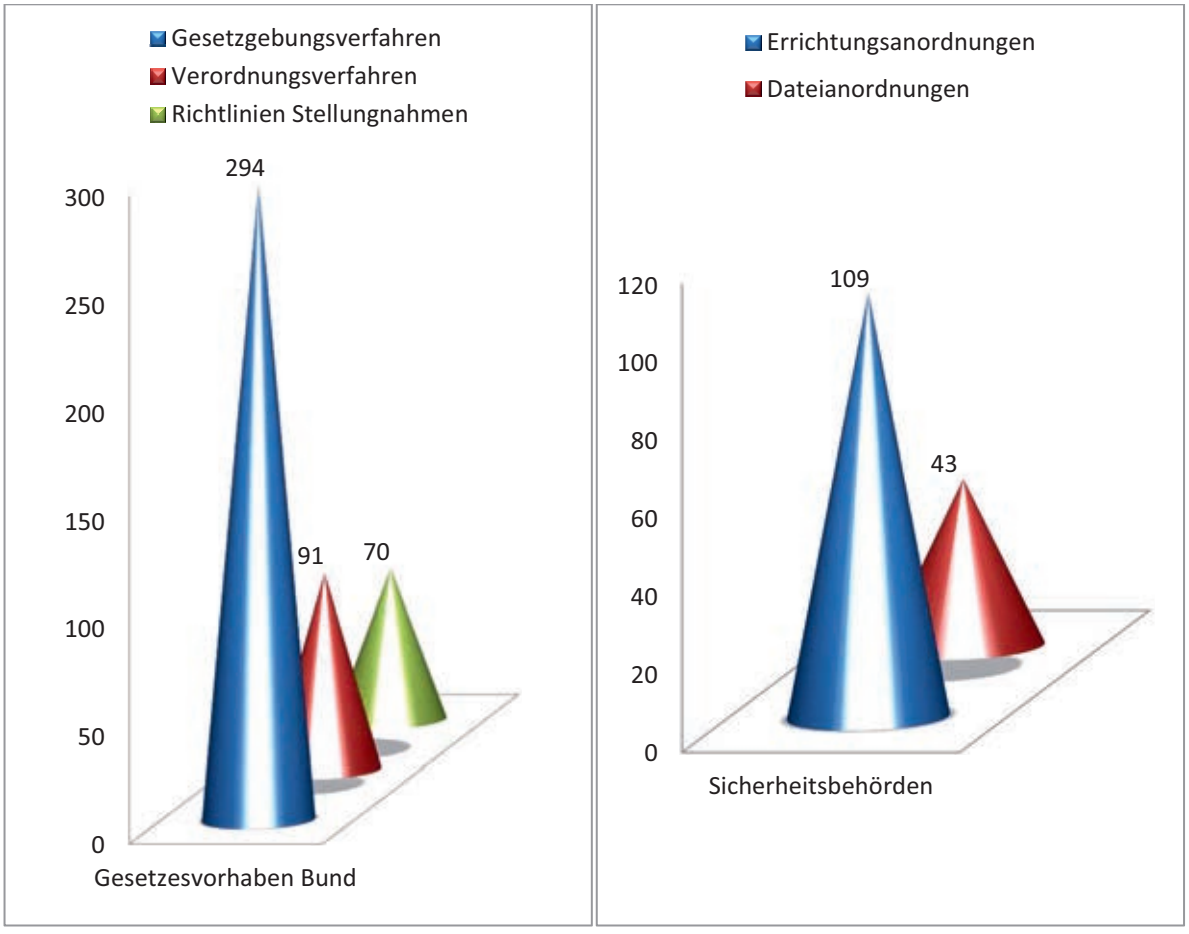
Begleitung von Rechtssetzungsvorhaben

Gemäß der Gemeinsamen Geschäftsordnung der Bundesministerien hat das federführende Bundesministerium - bevor der Entwurf einer Gesetzesvorlage der Bundesregierung zum Beschluss vorgelegt wird - die von dem Gesetzentwurf betroffenen Stellen im Rahmen ihrer gesetzlichen Zuständigkeit frühzeitig bei den Vorarbeiten und der Ausarbeitung einzubeziehen. Im Berichtszeitraum habe ich 294 Gesetzgebungsverfahren, 91 Verordnungsverfahren und 70 Richtlinien Stellungnahmen geprüft und begleitet.

Zudem wurden mir im Bereich der Sicherheitsbehörden 109 Errichtungsanordnungen und 43 Dateianordnungen zur Prüfung vorgelegt (vgl. Kasten c). Das Bundeskriminalamt hat für jede bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten eine Errichtungsanordnung (EAO) zu erlassen. Hier wird unter anderem festgelegt, was die Rechtsgrundlage und der Zweck der Datei ist, von welchen Personen welche Daten in der Datei gespeichert werden sollen, an wen die Daten übermittelt werden dürfen oder wann zu prüfen ist, ob die Daten zu löschen sind. Die BfDI ist vor Erlass der EAO anzuhören. In diesem Verfahren prüft die BfDI die Rechtsmäßigkeit der Datenverarbeitung soweit sie sich aus der EAO ergibt.

Das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der Militärische Nachrichtendienst haben für jede automatisierte Datei, in denen sie personenbezogene Daten verarbeiten, Dateianordnungen (DAO) zu erstellen und in diesen Details zur Datenverarbeitung festzulegen. Auch hier ist die BfDI vor Erlass der DAO anzuhören und prüft im Rahmen der Anhörung die Rechtmäßigkeit der Datenverarbeitung soweit sie sich aus der DAO ergibt.

Kasten c

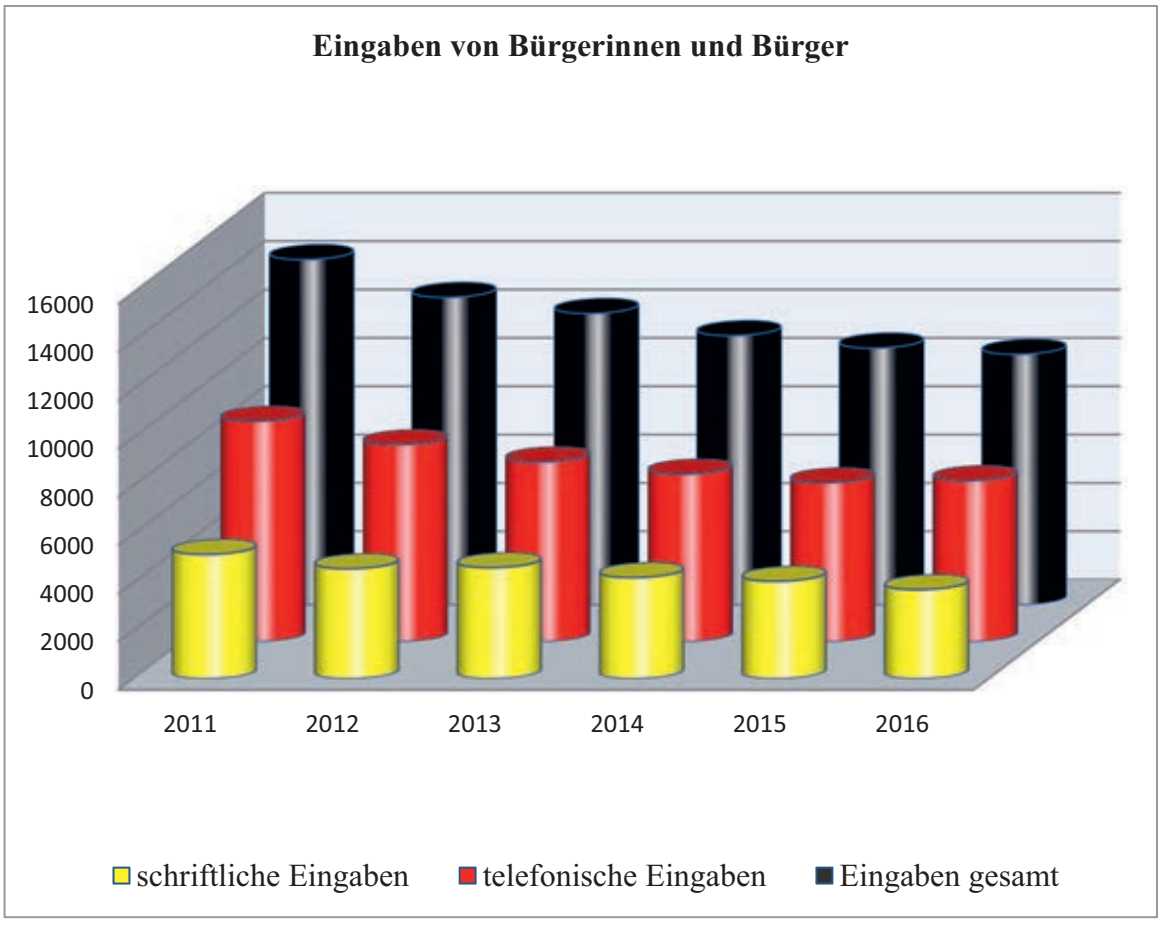


Bearbeitung von Eingaben

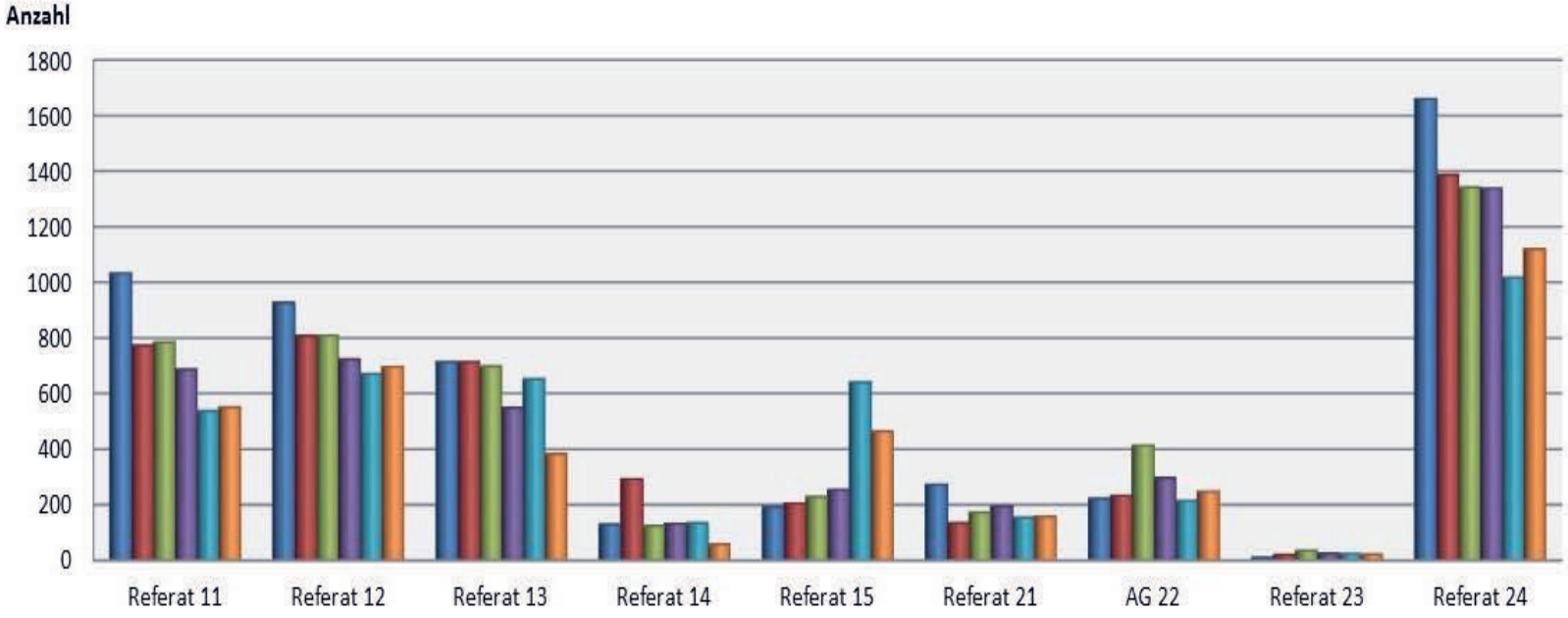
Eine meiner wichtigsten Aufgaben ist die Beratung der Bürgerinnen und Bürger, aber auch der Behörden und Unternehmen. Dazu gehört auch die Bearbeitung von Beschwerden über Datenschutzverstöße. Die Zahl der telefonischen und schriftlichen Eingaben ist schon seit Jahren hoch. Im Berichtszeitraum erreichten mich 21029 telefonische und schriftliche Eingaben (vgl. hierzu Kasten d).

Kasten d

	2011	2012	2013	2014	2015	2016
schriftliche Eingaben	5161	4568	4610	4200	4045	3699
telefonische Eingaben	9143	8173	7464	6958	6598	6687
Gesamt	**14304**	**12741**	**12074**	**11158**	**10643**	**10386**



Eingaben der Bürgerinnen und Bürger nach Referaten* 2011-2016



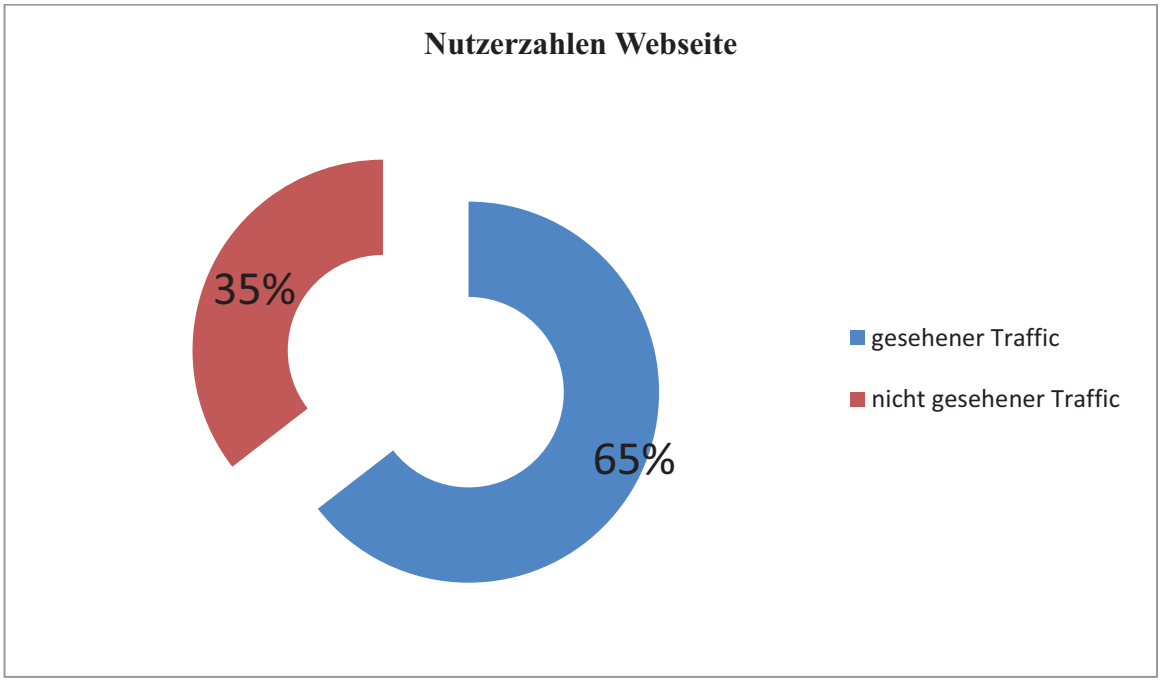
	Referat 11	Referat 12	Referat 13	Referat 14	Referat 15	Referat 21	AG 22	Referat 23	Referat 24
2011	1033	928	713	129	193	273	222	10	1660
2012	773	808	714	293	205	135	233	20	1387
2013	785	809	699	124	229	173	414	35	1342
2014	687	724	549	132	254	194	297	25	1338
2015	537	671	652	134	640	154	215	24	1018
2016	551	696	383	58	464	157	248	22	1120

* Die Aufgabenverteilung der einzelnen Referate entnehmen Sie bitte dem Organigramm im Anhang.

Zugriffs-/Nutzerzahlen der Homepage der BfDI

Internet-Browser	Jahr 2016[1]
Seitenaufrufe (gesehener Traffic)	13.721.078
Seitenaufrufe (nicht gesehener Traffic)*	7.544.451
Seitenaufrufe gesamt	21.265.529

* Nicht gesehener Traffic ist der Seitenzugriff, welcher von Robots, Würmern oder Antworten mit speziellem HTTP-Statuscode verursacht wurde.



Neue Aufgaben für die Bundesbeauftragte

Im Berichtszeitraum wurden mir zahlreiche neue Aufgaben durch Gesetze oder Verordnungen übertragen (vgl. Kasten e, Nr. 21.1).

Kasten e

Gesetz	Neue Aufgabe	Verweis
Kulturgutschutzgesetz (KGSG)	Datenschutzrechtliche Kontrolle des Infoportals www.kulturgutschutz-deutschland.de: Durch § 79 Absatz 3 KGSG ist mir die datenschutzrechtliche Kontrolle des gemeinsamen Verfahrens zum Schutz nationalen Kulturgutes	11.2.2

[1] Die Jahresstatistik für 2015 wurde nicht erstellt, weil die Daten wegen des Relaunchs meines Internetauftrittes nicht zur Verfügung standen.

	übertragen worden.	
Mindestlohngesetz (MiLoG)	Datenschutzrechtliche Kontrolle von Behörden der Zollverwaltung als die gemäß § 14 MiLoG zuständigen Aufsichtsbehörden für die Prüfung der Zahlung der Mindestlöhne durch die Arbeitgeber. Aufgrund § 24 BDSG kontrolliere ich bei der Zollverwaltung die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz auch mit Blick auf diese neue Aufgabe.	
Transplantationsgesetz	Datenschutzrechtliche Kontrolle des Transplantationsregisters mit dem Inkrafttreten des Gesetzes am 1. November 2016 nach Art. 3 des Transplantationsregistergesetzes; Mitwirkung bei der vertraglichen Regelung zwischen dem Spitzenverband Bund der Krankenkassen, der Bundesärztekammer und der Deutsche Krankenhausgesellschaft oder die Bundesverbände der Krankenhausträger zu den Anforderungen an die Erhebung, Verarbeitung und Übermittlung der Daten durch die Transplantationsregisterstelle nach § 15b Abs. 4 Transplantationsgesetz; Mitwirkung bei der vertraglichen Regelung zwischen dem Spitzenverband Bund der Krankenkassen, der Bundesärztekammer und der Deutsche Krankenhausgesellschaft oder die Bundesverbände der Krankenhausträger zum Verfahren der Datenpseudonymisierung und zum Verfahren der Zusammenführung der Daten sowie zur Finanzierung der Vertrauensstelle aus Mitteln der gesetzlichen Krankenversicherung nach § 15c Abs. 3 Transplantationsgesetz; Mitwirkung bei der vertraglichen Regelung zwischen dem Spitzenverband Bund der Krankenkassen, der Bundesärztekammer und der Deutsche Krankenhausgesellschaft oder die Bundesverbände der Krankenhausträger über die Verfahrensordnung für das Verfahren für die Übermittlung der Daten,	9.2.2

	einschließlich der erstmaligen und laufenden Übermittlung nach § 15e Abs. 4 Transplantationsgesetz; Mitwirkung bei der vertraglichen Regelung zwischen dem Spitzenverband Bund der Krankenkassen, der Bundesärztekammer und der Deutsche Krankenhausgesellschaft oder die Bundesverbände der Krankenhausträger über den bundesweit einheitliche Datensatz sowie dessen Fortschreibung nach § 15e Abs. 5 Transplantationsgesetz; Mitwirkung bei der vertraglichen Regelung zwischen dem Spitzenverband Bund der Krankenkassen, der Bundesärztekammer und der Deutsche Krankenhausgesellschaft oder die Bundesverbände der Krankenhausträger über die Verfahrensordnung zu dem Verfahren zur Übermittlung der transplantationsmedizinischen Daten durch die Vertrauensstelle nach § 15e Abs. 8 Transplantationsgesetz; Mitwirkung bei der vertraglichen Regelung zwischen dem Spitzenverband Bund der Krankenkassen, der Bundesärztekammer und der Deutsche Krankenhausgesellschaft oder die Bundesverbände der Krankenhausträger über die Verfahrensordnung zu dem Verfahren zur Übermittlung der transplantationsmedizinischen Daten durch die Registerstelle nach § 15f Abs. 2 Transplantationsgesetz	
E-Health-Gesetz	Mitwirkung bei der Festlegung der erforderlichen Voraussetzungen für die Nutzung der Telematikinfrastruktur im Gesundheitswesen nach § 291b Abs. 1b SGB V; Mitwirkung bei der Festlegung der sicheren Verfahren zur Übermittlung medizinischer Dokumente über die Telematikinfrastruktur durch die Gesellschaft für Telematik nach § 291b Abs. 1e SGB V; Mitwirkung im Beirat der Gesellschaft für Telematik nach § 291b Abs. 2 SGB V; Mitwirkung bei der Prüfung der	9.2.1

	Entscheidung der Schlichtungsstelle der Gesellschaft für Telematik nach § 291c Abs. 9 SGB V; Mitwirkung bei der Empfehlung der Gesellschaft für Telematik zu den im Interoperabilitätsverzeichnis enthaltenen technische und semantische Standards, Profile und Leitfäden als Referenz für informationstechnische Systeme im Gesundheitswesen nach § 291e Abs. 9 SGB V; Mitwirkung bei der Prüfung der Richtlinie der Gesellschaft für Telematik zur Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung nach § 291f Abs. 2 SGB V; Mitwirkung bei der Prüfung der Vereinbarung über das technische Verfahren zur konsiliarischen Befundbeurteilung und zur Videosprechstunde nach § 291g Abs. 1 SGB V.	
Eurodac-Verordnung	Durch Artikel 32 Absatz 2 Eurodac Verordnung wurde die Pflicht zur jährlichen Kontrolle der Verarbeitung personenbezogener Daten eingeführt.	10.3.3
Antiterrordateigesetz (ATDG)	Durch § 10 Absatz 2 ATDG wurde die Pflicht eingeführt, mindestens alle zwei Jahre die Verarbeitung personenbezogener Daten durch die teilnehmenden Behörden in der Antiterrordatei zu kontrollieren.	10.3.5
Rechtsextremismus-Datei-Gesetz (REDG)	Durch § 11 Abs. 2 REDG wurde die Pflicht eingeführt, mindestens alle zwei Jahre die Verarbeitung personenbezogener Daten durch die teilnehmenden Behörden in der Rechtsextremismus Datei zu kontrollieren.	
IT-Sicherheitsgesetz	Mitwirkung bei Meldungen nach dem IT-Sicherheitsgesetz (§ 8b Abs. 7 BSI-Gesetz); Soweit personenbezogene Daten betroffen sein können, wurde mir die Mitwirkung bei Meldungen nach dem IT-Sicherheitsgesetz und die Kontrolle der Datenerhebungs- und -verwendungskonzepte übertragen (§ 5 Abs. 8 BSI-Gesetz).	10.2.11.1

Telekommunikationsgesetz	Kontrollen zur Vorratsspeicherung von Daten: Die neue Aufgabe resultiert aus der Erweiterung der Datenverarbeitungspflichten bei den TK-Providern, die daher auch eine erweiterte Kontrolle der BfDI notwendig machen. Eine eigene Rechtsgrundlage gibt es hierfür nicht, die Zuständigkeit ergibt sich vielmehr - wie bislang auch bei der Aufsichtstätigkeit im TK-Bereich - aus § 115 Abs. 4 TKG; Erstellung des Anforderungskatalogs zur Vorratsspeicherung von Daten: Die Aufgabe bei der Erstellung und Pflege des Anforderungskatalogs mitzuwirken wurde mir nach § 113f Abs. 1 und 2 TKG übertragen	12.2.2
Bewachungsverordnung	Bewachungsverordnung/-register, Kontrollen: Die neuen aufsichtsrechtlichen Aufgaben basieren auf den sich aus der Änderung des § 34a GewO ergebenden Erweiterungen der Datenverarbeitungsprozesse bei Stellen, die nach § 24 BDSG der allgemeinen Zuständigkeit der BfDI unterfallen	17.2.2

1 Schwerpunktthemen - national

1.1 Endspurt zur Europäischen Datenschutzreform und JI-Richtlinie

Nach fast vier Jahre andauernden Verhandlungen haben sich im Dezember 2015 der Rat der Europäischen Union, das Europäische Parlament und die Europäische Kommission auf einen Text für die Datenschutz-Grundverordnung und die Richtlinie für den Datenschutz im Polizei- und Justizbereich geeinigt.

Bereits in meinen letzten beiden Tätigkeitsberichten hatte ich ausführlich über die Reformvorschläge der Europäischen Kommission und über den Fortgang der Verhandlungen berichtet (vgl. 24. TB Nr. 2.1, 25. TB Nr. 1).

Im Jahre 2015 konnten die Verhandlungen nun endlich erfolgreich zu Ende geführt werden. Nachdem sich das Europäische Parlament bereits im März 2014 auf seine Vorschläge verständigt hatte, einigten sich die Justiz- und Innenminister der EU im Juni 2015 auf einen gemeinsamen Standpunkt zur Datenschutz-Grundverordnung (DSGVO).[1] Im Oktober 2015 folgte die Einigung auch für den Vorschlag einer „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ (JI-Richtlinie).[2]

Im Anschluss daran fanden im so genannten informellen Trilog intensive Gespräche zwischen den Vertretern des Rates, des Europäischen Parlaments sowie der Europäischen Kommission mit dem Ziel statt, noch im Jahre 2015 eine Einigung über beide Rechtsakte herbeizuführen. Gemeinsam mit meinen Kolleginnen und Kollegen in der EU und in Deutschland habe ich mich mit konstruktiven Vorschlägen in die Diskussion eingebracht. Sowohl die Artikel-29-Gruppe[3] als auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder[4] hatten in jeweils eigenen - inhaltlich jedoch sehr ähnlichen - Positionspapieren besonders wichtige und kritische Punkte thematisiert, die im Trilog zu beiden Rechtsakten berücksichtigt werden sollten. Gemeinsam mit einigen Landesbeauftragten für den Datenschutz bekam ich dabei die Gelegenheit, die Positionen der deutschen Datenschutzbehörden im Europäischen Parlament, bei der Ratspräsidentschaft und bei der Europäischen Kommission zu erläutern.

Im Dezember 2015 haben sich die Trilogparteien auf einen endgültigen Text beider Rechtsakte geeinigt. Nach den notwendigen redaktionellen und Übersetzungsarbeiten haben Rat und Parlament schließlich beide Rechtsakte im April 2016 angenommen. Diese wurden am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht. Die DSGVO trat daraufhin am 25. Mai 2016, die JI-Richtlinie am 5. Mai 2016 in Kraft. **Die Grundverordnung ist ab dem 25. Mai 2018 verbindlich in allen Mitgliedstaaten anzuwenden, die JI-Richtlinie muss bis zum 6. Mai 2018 in nationales Recht umgesetzt sein.**

Aus meiner Sicht geht von der Einigung über die Europäische Datenschutzreform ein positives Signal aus. Die globale und allgegenwärtige Verarbeitung personenbezogener Daten, die rasante Entwicklung immer neuer Geschäftsmodelle und Big-Data-Anwendungen, aber auch der Überwachung durch staatliche Institutionen verlangen eine globale Antwort. Hierfür ist das neue europäische Recht ein ganz wichtiger Schritt.

---

1 Vgl. Ratsdokument 9565/15, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf

2 Vgl. Ratsdokument 12555/2015, http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/de/pdf

3 Papier vom 17.6.2015 „Zentrale Themen mit Blick auf den Trilog“, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_de.pdf; sowie zur JI Richtlinie WP 233

4 Datenschutzrechtliche Kernpunkte für die Trilog-Verhandlungen zur Datenschutz-Grundverordnung, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20150826_Verbesserung%20DSGrundverordnung.pdf?__blob=publicationFile&v=3; Datenschutzrechtliche Kernpunkte für die Trilog-Verhandlungen der Datenschutzrichtlinie im Bereich von Justiz und Inneres, https://www.bfdi.bund.de/SharedDocs/EU/ModernisierungDSRecht/DSK_Kernpunkte_Trilog_de.pdf?__blob=publicationFile&v=1

Zunächst ist es ein großer Erfolg, dass diese Einigung überhaupt gelungen ist. Angesichts der Vielzahl der sehr unterschiedlichen Interessen von Bürgerinnen und Bürgern, Wirtschaft, Wissenschaft und staatlichen Institutionen ist es nicht selbstverständlich, dass sich alle 28 Mitgliedstaaten und das Europäische Parlament auf einen gemeinsamen Rechtsrahmen für die kommenden Jahre verständigt haben. Dies gilt gerade auch für die JI-Richtlinie, mit der erstmals für die ganze EU ein einheitlicher Mindeststandard auch für die nationale Verarbeitung personenbezogener Daten im Bereich von Polizei und Justiz geschaffen wird.

Für die Menschen und die Unternehmen in Europa ist das neue Datenschutzrecht von großer Bedeutung. Vor allem für die Wirtschaft wird es künftig ein weitgehend einheitliches europäisches Datenschutzrecht geben, das in allen europaweit relevanten Fragen auch einheitlich durchgesetzt wird. Dies erleichtert den Europäerinnen und Europäern die Wahrnehmung ihrer Rechte und ermöglicht den Unternehmen gleiche Rahmenbedingungen auf dem europäischen Markt. Angesichts des Marktortprinzips (vgl. 24 TB Nr. 2.1.1) reicht die Wirkung des europäischen Datenschutzrechts deutlich über Europa hinaus, denn auch außereuropäische Unternehmen werden sich künftig an die hiesigen Regeln halten müssen, wenn sie auf dem europäischen Markt tätig werden wollen.

In den Trilogverhandlungen sind dabei noch einmal deutliche Verbesserungen gegenüber dem Ratsentwurf erreicht und einige zentrale Forderungen der nationalen und europäischen Datenschutzbeauftragten aufgenommen und umgesetzt worden:

So wurde die Datensparsamkeit als wichtiges Grundprinzip in der DSGVO verankert. Dies ist vor allem deshalb wichtig, weil in der öffentlichen Debatte immer wieder das Argument zu hören ist, die Datensparsamkeit sei in Zeiten von Big Data überholt und nicht mehr zeitgemäß. Dabei ist das Gegenteil richtig: Gerade auch die Big-Data-Technologien lassen die vom Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 beschriebenen Gefahren und Bedrohungen Realität werden. Deshalb ist es wichtiger denn je, daran zu erinnern, dass jedes Zusammenführen personenbezogener Daten zu Profilen und deren Auswertung die Selbstbestimmung des Einzelnen beeinträchtigt; deshalb sind solche Eingriffe auf das notwendige Minimum zu reduzieren. Die DSGVO hält an diesem grundrechtsbezogenen Ansatz fest, was ich sehr begrüße.

Darüber hinaus wurde die Zweckbindung im Vergleich zu den Vorschlägen des Rates deutlich gestärkt: Eine Datenverarbeitung zu Zwecken, die nicht mit dem ursprünglichen Erhebungszweck vereinbar sind, wird auch künftig nur bei einer Einwilligung des Betroffenen oder zur Erfüllung wichtiger öffentlicher Interessen erlaubt sein. Hier werde ich sehr genau darauf achten, dass dieser Grundansatz nicht durch nationale Gesetze wieder konterkariert wird (vgl. Nr. 1.2 f.).

Wie weiter positiv hervorzuheben ist, hat sich der Europäische Gesetzgeber vor für klare internationale Regelungen zur Datenübermittlung an Behörden und Gerichte in Staaten außerhalb der EU starkgemacht.

Aus Sicht des deutschen Datenschutzrechts ist es besonders erfreulich, dass ein deutsches Erfolgsmodell europäisch wird: Künftig müssen europaweit alle Behörden und in bestimmten Fällen risikobehafteter Datenverarbeitung auch Unternehmen einen eigenen Datenschutzbeauftragten bestellen. Zudem können die Mitgliedstaaten in zusätzlichen Fällen eine verpflichtende Bestellung von betrieblichen Datenschutzbeauftragten vorsehen.

Ich gehe davon aus, dass der Bundesgesetzgeber von dieser Möglichkeit Gebrauch macht, damit in Deutschland auch künftig das Zwei-Säulen-Modell aus betrieblicher Eigenkontrolle und staatlicher Aufsicht unverändert fortgeführt werden kann.

Das neue Europäische Recht erfüllt aber nicht alle Wünsche der Datenschutzaufsichtsbehörden. So ist die notwendige Modernisierung des Datenschutzrechts nicht durchgängig gelungen.

Um die Selbstbestimmung im digitalen Zeitalter zu stärken, muss die Einwilligung so gestaltet werden, dass der Wille des Einzelnen klar erkennbar ist und er eine echte Wahl hat. Leider muss auch künftig die Einwilligung nicht ausdrücklich erteilt werden. Damit haben gerade global agierende Unternehmen die Möglichkeit, sich durch die Verwendung pauschaler Datenschutzerklärungen weitreichende Möglichkeiten zur Datenverarbeitung

einräumen zu lassen. Zudem wird die Profilbildung als eines der wichtigsten datenschutzrechtlichen Themen nur unzureichend geregelt und damit auch weiterhin sehr umfassend möglich sein.

Ich appelliere an die Gesetzgeber in Bund und Ländern, sich bei der Anpassung des nationalen Datenschutzrechts an Geist und Buchstaben der neuen europäischen Regeln zu halten (vgl. unter Nr. 1.2 f.).

Gern verweise ich an dieser Stelle auf die von mir zur DSGVO herausgegebene Info 6. Sie enthält neben dem Verordnungstext einführende Erläuterungen zum Inhalt der Datenschutz-Grundverordnung.

1.2 Umsetzung der Europäischen Datenschutzreform in nationales Recht

Das deutsche Datenschutzrecht ist bis zum 25. Mai 2018 an die Datenschutz-Grundverordnung anzupassen (vgl. u. Nr. 1.2.1). Bereits bis zum 6. Mai 2018 ist die Richtlinie für den Datenschutz im Polizei- und Justizbereich umzusetzen (vgl. u. Nr. 1.2.2). Das Bundesministerium des Innern hat für beide Vorhaben im Bereich des Bundes den Referentenentwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU) vorgelegt. Die Beratungen innerhalb der Bundesregierung zu dem Gesetzentwurf dauerten bei Redaktionsschluss noch an.

Das DSAnpUG-EU soll noch in der 18. Legislaturperiode vom Deutschen Bundestag verabschiedet werden, um ein rechtzeitiges Inkrafttreten zum 25. Mai 2018 zu gewährleisten. Der Entwurf soll insbesondere die notwendigen Neuregelungen im Bundesdatenschutzgesetz (BDSG) enthalten. Wesentliche bereichsspezifische Folgeänderungen sollen Gegenstand eines gesonderten Gesetzgebungsverfahrens werden. Das DSAnpUG-EU bedarf der Zustimmung des Bundesrates.

1.2.1 Anpassung des nationalen Datenschutzrechts an die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung gilt unmittelbar und zwingend in allen Mitgliedstaaten. Sie soll ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten schaffen (Erwägungsgrund 10). Die Verordnung enthält aber auch eine Reihe von Regelungsspielräumen für den nationalen Gesetzgeber und darüber hinaus gehend auch konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge.

Bei den Beratungen zu dem Entwurf eines Datenschutz-Anpassungs- und Umsetzungsgesetzes EU habe ich mich im Berichtszeitraum insbesondere mit dem Petitum eingebracht, das durch die DSGVO vorgegebene Harmonisierungsziel ernst zu nehmen und bei verbleibendem Spielraum des deutschen Gesetzgebers Regelungen vorzusehen, die ein hohes Datenschutzniveau gewährleisten. Hierzu einige Beispiele:

Zurückhaltung des nationalen Gesetzgebers ist bei Regelungen zur Zulässigkeit zweckändernder Datenverarbeitungsvorgänge angebracht. Der Grundsatz der Zweckbindung ist nicht nur nach deutschem Verständnis essentiell, sondern auch in Artikel 8 der EU-Grundrechtecharta und in Artikel 5 Absatz 1 Buchstabe b DSGVO festgeschrieben.

Artikel 23 DSGVO gestattet nur Einschränkungen der nach der Verordnung vorgesehenen Betroffenenrechte (beispielsweise Recht auf Auskunft oder Widerspruchsrecht), wenn diese zum Schutz bestimmter wichtiger Rechtsgüter erforderlich und verhältnismäßig sind. Nach meiner Auffassung sollten entsprechende Beschränkungen im neuen BDSG äußerst zurückhaltend und nur nach sorgfältiger Prüfung jedes Einzelfalls vorgesehen werden. Auch die nach dem geltenden BDSG bestehenden Einschränkungen dürfen nur dann erhalten bleiben, wenn sie die strengen Voraussetzungen des Artikels 23 DSGVO erfüllen.

In Deutschland wird es auch weiterhin verschiedene Aufsichtsbehörden für die Kontrolle und Beratung in Datenschutzangelegenheiten geben. Nach der Verordnung muss bei mehreren Aufsichtsbehörden in einem Mitgliedsstaat für bestimmte Verfahren und die Vertretung in europäischen Gremien eine innerstaatliche Koordinierung erfolgen. So ist beispielsweise die Errichtung einer „Zentralen Anlaufstelle“ vorgesehen (Erwägungsgrund 119) sowie die Benennung eines „Gemeinsamen Vertreters im Europäischen Datenschutzausschuss“ (Art. 68 Abs. 4 DSGVO). Ich habe mich dafür eingesetzt, diese Aufgaben der BfDI zuzuweisen, um eine einheitliche Vertretung der deutschen Aufsichtsbehörden in Europa zu gewährleisten. Dabei sind die Interessen der Länder in angemessener Weise zu berücksichtigen, denn ihre Datenschutzaufsichtsbehörden sind für die Datenschutzaufsicht im nicht-öffentlichen Bereich zuständig. In das DSAnpUG-EU müssen zudem klare und eindeutige Regelungen zum Verfahren der Kommunikation und Entscheidungsfindung zwischen den verschiedenen Aufsichtsbehörden in Deutschland aufgenommen werden, damit die deutschen Aufsichtsbehörden gemeinsam eine starke Position in Europa einnehmen können.

1.2.2 Umsetzung der JI-Richtlinie: Mindestharmonisierung heißt nicht Vereinheitlichung

Die Datenschutzrichtlinie für den Bereich von Polizei und Justiz (JI-Richtlinie) bildet den zweiten Teil des neuen Datenschutzpaketes der EU und verpflichtet die Mitgliedstaaten, die darin enthaltenen Vorgaben bis zum 6. Mai 2018 in ihr nationales Recht umzusetzen.

Ziel der JI-Richtlinie ist es, erstmalig für den Datenschutz in den Bereichen Polizei und Justiz eine Mindestharmonisierung innerhalb der EU herbeizuführen. Diese Absicht ist uneingeschränkt zu begrüßen. Mindestharmonisierung bedeutet, ein hohes Schutzniveau in der gesamten Union zu gewährleisten. Keinesfalls soll aber in Staaten, die bereits ein höheres Datenschutzniveau haben, eine Angleichung „nach unten“ erfolgen. Dies wird in den Erwägungsgründen der Richtlinie ausdrücklich betont. Die Mitgliedstaaten sollen gerade nicht daran gehindert werden, zum Schutz der Rechte und Freiheiten ihrer Bürgerinnen und Bürger Garantien festzulegen, die strenger sind als die der JI-Richtlinie.

Das bedeutet für die Umsetzung in Deutschland: Dort, wo die JI-Richtlinie strengere Anforderungen stellt als das nationale Recht, muss dieses Recht angepasst werden, und dort, wo das nationale Recht strenger ist, sollte es ausnahmslos erhalten bleiben.

Schon während der Verhandlungen auf europäischer Ebene war der Anwendungsbereich der JI-Richtlinie im Verhältnis zur DSGVO ein besonderer Streitpunkt. Im Ergebnis ist im Richtlinientext nicht abschließend geklärt worden, ob und welche anderen Gefahrenabwehrbehörden bei welchen Tätigkeiten neben Polizeibehörden in den Anwendungsbereich fallen sollen. Um Abgrenzungsschwierigkeiten zu vermeiden, empfehle ich dem Gesetzgeber, weitgehend parallele Regelungen für alle diese Behörden zu treffen.

Ich gehe sogar noch einen Schritt weiter: Auch wenn die Tätigkeit der Nachrichtendienste als Teil der nationalen Sicherheit weder in den Anwendungsbereich der Richtlinie noch in den der Datenschutz-Grundverordnung fällt, sollten hier aus meiner Sicht im Wesentlichen die gleichen Anforderungen gelten.

Von zentraler Bedeutung für meine eigene Tätigkeit und die der anderen Aufsichtsbehörden sind die künftigen Befugnisse der Datenschutzaufsicht. Hier gibt die Richtlinie zwingend eine Erweiterung der bestehenden Möglichkeiten vor. Die Aufsichtsbehörden müssen in die Lage versetzt werden, bei Verstößen wirksam Abhilfe zu schaffen, beispielsweise durch Anordnungen oder Untersagungen.

Außerdem muss für sie die Möglichkeit geschaffen werden, eine gerichtliche Überprüfung einzuleiten. Ich empfehle deswegen dem Gesetzgeber, die Untersuchungs-, Anordnungs- und Klagebefugnisse wie in der DSGVO zu regeln.

Außerdem halte ich insbesondere folgende Regelungen für geboten:

- Der Betroffene muss ein Recht auf Negativauskunft erhalten.

- Datenverarbeitende Stellen müssen zum Aufbau eines Datenschutzmanagements verpflichtet werden, um folgende Ziele zu verfolgen: Datensparsamkeit, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit.

- Verantwortliche Stellen sind zu verpflichten, künftig eine Gesamtübersicht über alle laufenden Datenverarbeitungen (sog. Verfahrensverzeichnisse) zu führen, sinnvollerweise zentral beim behördlichen Datenschutzbeauftragten.

- Bereichsspezifische Anforderungen, nach denen Zweck, Rechtsgrundlage, betroffener Personenkreis, Art der zu speichernden Daten, Eingabe der Daten, Voraussetzungen der Datenübermittlung, Festlegungen zur Speicherdauer sowie notwendige technische und organisatorische Maßnahmen in Verwaltungsvorschriften konkret zu bestimmen sind (z. B. in Errichtungsanordnungen), müssen erhalten bleiben. Das Gleiche gilt für die vorherige Anhörung der Datenschutzaufsicht bei der Einrichtung neuer Dateien oder Verarbeitungen.

- Eine Verpflichtung zur Protokollierung sollte neben den Zugriffen der Nutzerinnen und Nutzer auch für administrative Zugriffe vorgesehen werden.

- Bei der Datenübermittlung an Drittstaaten sind, soweit die EU-Vorgaben nicht entgegenstehen, die Maßgaben des Bundesverfassungsgerichts aus seiner Entscheidung vom 20. April 2016 - 1 BvR 966/09 (Rn. 329 - 341) zum Bundeskriminalamtgesetz zu berücksichtigen. Danach erfordert die Datenübermittlung ins Ausland eine Begrenzung auf hinreichend gewichtige Zwecke, die Vergewisserung über einen rechtsstaatlichen Umgang mit diesen Daten im Empfängerland, der Sicherstellung einer wirksamen inländischen Kontrolle und entsprechende normenklare Grundlagen im deutschen Recht. Eine effektive unabhängige Kontrolle setzt aus meiner Sicht eine Verpflichtung der übermittelnden Stellen zur zentralen Protokollierung von Auslandsübermittlungen voraus (vgl. hierzu auch unter Nr. 1.3).

Die Umsetzung der JI-Richtlinie auf Bundesebene und die künftige Durchführung der ihrer Umsetzung dienenden Rechtsvorschriften werde ich datenschutzrechtlich eng begleiten.

1.3 Grundsatzentscheidungen im Sicherheitsbereich mit weit reichenden Folgen

Das Bundesverfassungsgericht bekräftigt seine bisherige Rechtsprechung und macht weitere Vorgaben für die Tätigkeit der Polizeien und Nachrichtendienste. Dies hat weit reichende Konsequenzen - auch für den Gesetzgeber und die Datenschutzkontrolle. Eine effiziente Kontrolle ist auch bei Datenübermittlungen deutscher Stellen an ausländische Sicherheitsbehörden von herausragender Bedeutung.

A. Vorgaben des Bundesverfassungsgerichts

Am 20. April 2016 hat das BVerfG eine weitere Grundsatzentscheidung getroffen. Anlass war das Gesetz über das Bundeskriminalamt (BKAG) und die dort neu eingefügten Befugnisse zur Terrorismusabwehr. Die Vorgaben des Gerichts gelten nicht nur für die Polizeien, sondern auch für die Nachrichtendienste. Damit führt das Gericht seine bisherige Rechtsprechung im Sicherheitsbereich konsequent fort und baut diese weiter aus.

Im Bereich der Nachrichtendienste besteht nach der Entscheidung des Bundesverfassungsgerichts „eine **besondere Kontrollrelevanz**“ (Beschluss vom 13. Oktober 2016). Die den Kontrollorganen verfassungsgerichtlich zugewiesene **Kompensationsfunktion** zum Schutz der Grundrechte der Betroffenen ist in diesem Bereich aufgrund der regelmäßig heimlich erfolgenden Grundrechtseingriffe von besonderer Bedeutung.

Die Intensivierung der **internationalen Zusammenarbeit** der Sicherheitsbehörden und der kontinuierliche - auch technische - Ausbau der europäischen und internationalen Sicherheitsarchitektur steigert die Bedeutung dieser Kompensationsfunktion und damit die von den Kontrollorganen zwingend zu leistenden Aufgaben.

Das Bundesverfassungsgericht hat den Gesetzgeber wiederholt verpflichtet, den Kontrollbehörden die zur Erfüllung dieser Kompensationsfunktion notwendigen personellen und sachlichen Ressourcen zu gewähren. Insoweit bestehen aber weiterhin noch erhebliche Defizite.

I. Effiziente Datenschutzkontrolle

Ebenso wie im Urteil zum Antiterrordateigesetz vom 24. April 2013 betont das Gericht in seiner Entscheidung zum BKAG wiederum die Bedeutung der externen Kontrolle für verfassungskonforme Sicherheitsgesetze und verpflichtet den Gesetzgeber erneut, dafür Sorge zu tragen, dass die Kontrollbehörden - und damit auch meine Dienststelle - die ihnen verfassungsgerichtlich auferlegte Verpflichtung zur Durchführung effizienter und wirksamer Kontrollen erfüllen können (s. Kasten b zu Nr. 1.3 Punkt B sowie u. Nr. 10.2.10).

1. Pflichtkontrollen

In Bezug auf die Antiterror- und die Rechtsextremismusdatei (vgl. 21. TB Nr. 5.1.1, 24. TB Nr. 7.2 und Nr. 7.3) verlangt das Gericht ausdrücklich, die Datenschutzkontrollen regelmäßig mindestens alle zwei Jahre, d. h. als turnusmäßige Pflichtkontrollen, durchzuführen. Neben diesen Dateien existiert eine Vielzahl weiterer gemeinsamer Dateien, die ebenfalls unter die gerichtlichen Maßgaben fallen. Die Vorgaben haben auch erhebliche Auswirkungen auf den Umfang und die Intensität meiner Kontrollen in diesem Bereich, da sowohl der Kontrollumfang als auch die Kontrolldichte weiter zu intensivieren sind. Diese Vorgabe des Gerichts zur regelmäßigen Kontrolle wurde vom Gesetzgeber für die ATD und die RED bereits umgesetzt. Hierfür stehen mir jedoch bislang keine ausreichenden personellen Ressourcen zur Verfügung.

Die Kontrolle derartiger gemeinsamer Dateien erfordert einen besonderen Aufwand (s. Kasten a zu Nr. 1.3). Es genügt nicht, lediglich die Antiterrordatei (ATD) oder die Rechtsextremismusdatei (RED) einzusehen, um die Rechtmäßigkeit eines dort gespeicherten Datums beurteilen zu können. Dies ist nur möglich, wenn ich auch die Quelldatei(en) derjenigen Stelle kontrolliere, die dieses Datum gespeichert hat, d. h. prüfe, ob das Datum nach den Vorgaben für diese Quelldatei(en) zulässig erhoben und gespeichert worden ist. Dies wiederum macht es notwendig, das Wechselspiel dieser Quelldateien mit anderen Dateien dieser Behörde und damit in Zusammen-

hang stehende vielfältige weitere rechtliche Vorgaben in den Blick zu nehmen (s. Kasten a zu Nr. 1.3). Dafür ist es auch notwendig, auf entsprechende Protokolldatenbanken zurückzugreifen.

Last but not least muss ich - gemäß den Vorgaben des Bundesverfassungsgerichts - zur Bewertung der Rechtmäßigkeit z. B. einer ATD-Speicherung auch prüfen, ob und wenn ja welche sonstigen Maßnahmen gegen den jeweiligen Betroffenen entweder von der speichernden Stelle oder von anderen an der ATD teilnehmenden Behörden getroffen worden sind. Nur so kann ich feststellen, ob eine vom Bundesverfassungsgericht als verfassungswidrig qualifizierte Rund-um-Überwachung oder sogenannte additive Grundrechtseingriffe gegen einen Betroffenen durch eine Behörde oder das Zusammenwirken mehrerer Behörden vorliegen. Kurz gesagt: Um z. B. in der ATD ein einzelnes Datum nach den Vorgaben des Bundesverfassungsgerichts kontrollieren zu können, ist die Prüfung weiterer Datenbanken bei weiteren Stellen unerlässlich - und damit verbunden auch ein immenser zeitlicher und logistischer Aufwand.

2. Kontrolle der Datenübermittlungen an ausländische Sicherheitsbehörden

Das Bundesverfassungsgericht verlangt auch bei der Übermittlung personenbezogener Daten durch deutsche Sicherheitsbehörden an ausländische Sicherheitsbehörden eine effiziente Kontrolle zum Schutz der Grundrechte der Betroffenen. Es betont ausdrücklich, dass die für diese Datenübermittlungen verlangten gerichtlichen Vorgaben wirksam und effizient kontrolliert werden müssen und diese Kontrolle Voraussetzung für die Wirksamkeit dieser Übermittlungen ist. D. h.: **Ohne wirksame Kontrollen** sind diese **Übermittlungen rechtswidrig** und damit unzulässig.

Durch die Veröffentlichungen von Edward Snowden und die Untersuchungen des ersten Untersuchungsausschusses des Deutschen Bundestages in der 18. Wahlperiode zur Tätigkeit der Sicherheitsbehörden der sog. Five-Eyes-Staaten in der Bundesrepublik Deutschland (vgl. u. Nr. 10.3.6) ist die internationale Kooperation der Nachrichtendienste in besonderem Maße in den kritischen Blick der Öffentlichkeit geraten. Die durch diese Kooperationen bekannt gewordenen Defizite und Verstöße geben in besonderer Weise Anlass, die Beachtung der Übermittlungsvorgaben des Gerichts dezidiert zu kontrollieren.

3. Kontrolle der Nachrichtendienste: „Besondere Kontrollrelevanz“

Nachrichtendienste haben besondere Aufgaben und Befugnisse. Sie müssen weit im Vorfeld von konkreten Gefahrenlagen tätig werden und Bedrohungen für unsere freiheitlich demokratische Grundordnung so früh wie möglich erkennen. Dafür hat sie der Gesetzgeber mit besonderen Aufgaben und Befugnissen ausgestattet. Aus diesem Grund dürfen Nachrichtendienste so frühzeitig wie keine andere Behörde und auch weitreichend und heimlich in die Grundrechte der Betroffenen eingreifen. Wegen dieser Sonderstellung ist es unvermeidlich, dass bei bestimmten Anhaltspunkten auch Unbescholtene in den Fokus der Dienste geraten. Daher hat das Bundesverfassungsgericht in seinem Beschluss vom 13. Oktober 2016 eine „**besondere Kontrollrelevanz**“ und die im Bereich der Nachrichtendienste bestehende „**besondere Aufklärungsfunktion**“ der Kontrolle erneut betont.

a) Kompensationsfunktion der Datenschutzkontrolle

Aufgrund dieser Sonderstellung der Nachrichtendienste bedarf es eines besonderen Korrektivs, d. h. einer Kompensation zum Schutz der Grundrechte der Betroffenen (s. Kasten b zu Nr. 1.3, Punkt B). Diese Aufgabe hat das Bundesverfassungsgericht den Kontrollorganen und damit auch mir zugewiesen.

b) Technische und personelle Aufrüstung der Nachrichtendienste; internationale Kooperation

Vor dem Hintergrund der rasanten technischen Entwicklungen werden die Nachrichtendienste weiter und in großem Umfang technisch und personell aufgerüstet.

Terroristen und Kriminelle bedienen sich immer stärker und mit hoher Präzision technischer Mittel, sei es durch den Einsatz mobiler Telekommunikation oder die Nutzung des Internets, insbesondere des sog. Darknets. Aus-

geprägt nutzen sie auch die sozialen Netzwerke und Medien für ihre Propaganda. Daher ist es für die Sicherheitsbehörden unerlässlich, mit diesen Entwicklungen Schritt zu halten und auch die Zusammenarbeit auf internationaler Ebene zu intensivieren.

Die Dienste brauchen die hierfür notwendigen Voraussetzungen sowie verfassungskonforme Rechtsgrundlagen, um diese Aufgabe erfüllen zu können. Erforderlich ist es aber auch, notwendige Gesetzesänderungen verfassungsgemäß und datenschutzkonform auszugestalten - insbesondere hinsichtlich der verfassungsgerichtlich geforderten Kompensation, d. h. der notwendigen effektiven Überprüfbarkeit dieser Maßnahmen durch unabhängige Kontrollinstanzen.

Der Gesetzgeber hat mit unterschiedlichen Ansätzen eine Reihe von Gesetzen - u. a. das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des BND und das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus - ergänzt oder angepasst und den Nachrichtendiensten weitreichende neue Befugnisse eingeräumt, insbesondere im Hinblick auf die Zusammenarbeit und den Informationsaustausch mit ausländischen Sicherheitsbehörden (vgl. o. Nr. 10.2.10.1).

Diese neuen Befugnisse und technischen Möglichkeiten greifen intensiv und weitgehend in die Grundrechte der Bürgerinnen und Bürger ein. Sie haben vielfach eine große Streubreite und erfolgen regelmäßig heimlich und damit ohne Kenntnis der Betroffenen. Aufgrund dessen ist es für deren Grundrechtsschutz unerlässlich, dass unabhängige Kontrollinstanzen, dazu gehört auch meine Dienststelle, die faktisch beschränkten Rechtsschutzmöglichkeiten durch entsprechende **effiziente und wirksame Kontrollen** kompensieren (vgl. o. Nr. 1.3 und Nr. 10.2.10.2).

II. Weitere Vorgaben des Urteils zum BKAG

Die Vorgaben des Bundesverfassungsgerichts „betreffen spezifisch breitenwirksame Grundrechtsgefährdungspotenziale, insbesondere solche der elektronischen Datenverarbeitung (...), ebenso wie einzelfallbezogene Maßnahmen gegen Betroffene, die in den Fokus der handelnden Behörden geraten sind“. Diese Maßstäbe sind also **bei allen eingriffsintensiven Maßnahmen** in das Recht auf informationelle Selbstbestimmung zu beachten. Eingriffe sind nur dann verhältnismäßig, wenn eine effektive Datenschutzkontrolle sichergestellt ist.

Der Gesetzgeber ist nunmehr gefordert, die Rechtsgrundlagen für die Eingriffsbefugnisse der Sicherheitsbehörden und der Nachrichtendienste verfassungskonform auszugestalten, d. h. auch geltende Regelungen entsprechend zu ändern. Dabei sind folgende Vorgaben zu beachten:

- Eingriffsschwellen und Personenkreise
  Fachgesetze erwähnen zum Beispiel die Möglichkeit, Kontakt- und Begleitpersonen in die Beobachtung einzubeziehen oder setzen diese stillschweigend voraus. Diese Vorgaben entsprechen vielfach nicht den Vorstellungen des Bundesverfassungsgerichts, soweit sie nicht den Regelungen des § 20b Absatz 2 Nummer 2 BKAG gleich kommen. Insbesondere im Bereich der Nachrichtendienstgesetze ist der erfasste Personenkreis nur äußerst unzureichend eingegrenzt.

- Zweckbindung und Übermittlungsregelungen
  Das Gericht hat die verfassungsrechtlichen Vorgaben zur Zweckbindung personenbezogener Daten umfassend dargelegt. Daraus folgen sowohl Anforderungen an die innerbehördliche Nutzung der Daten als auch an die Übermittlung an weitere Stellen.
  Eine Übermittlung personenbezogener Daten aus eingriffsintensiven Ermittlungsmaßnahmen hält das Gericht zum einen nur für zulässig, wenn ein gleichgewichtiger Rechtsgüterschutz besteht, darüber hinaus muss sich aus einem hinreichend spezifischen Anlass ein konkreter Ermittlungsansatz ergeben. Ein lediglich potentieller Ermittlungsansatz oder gar eine allgemeine Nützlichkeit reichen nicht aus. Dies macht es erforderlich, die **gesamten Übermittlungsregelungen** im Sicherheitsrecht grundlegend zu **überarbeiten**.
  Im Bereich der Nachrichtendienste ergibt sich dies bereits aus dem Urteil zur Antiterrordatei und dem darin entwickelten informationellen Trennungsprinzip (vgl. 25. TB Nr. 5.2).

- Auslandsübermittlungen
  Besondere Vorgaben gelten für die **Übermittlung ins Ausland**. Hier zeigen sich etwa im geltenden Verfassungsschutzrecht erhebliche Defizite. So fehlt etwa in § 19 Absatz 3 BVerfSchG eine Regelung, die der des BKAG hinsichtlich der Mitteilung des Löschungszeitpunkts der Daten an den Empfänger, der Berücksichtigung schutzwürdiger Interessen der betroffenen Person im Einzelfall sowie zum Vorhandensein eines angemessen Datenschutzniveaus im Empfängerstaat (§ 14 Abs. 7 Satz 6 und Sätze 8, 9 BKAG) entspricht. Auch die Übermittlungsvoraussetzungen des § 14 Absatz 1 Satz 1 Nummer 1 und 3, Satz 2 BKAG sind nicht verfassungskonform. In ähnlicher Weise gilt dies auch für § 19 Absatz 3 BVerfSchG.

- Verfahrenssicherungen
  Richtervorbehalte, Transparenz, Protokollierung und datenschutzrechtliche Kontrolle sollte der Gesetzgeber ebenfalls für das gesamte Sicherheitsrecht überarbeiten.
  Insbesondere im Bereich der heimlichen Datenverarbeitung ist der schwach ausgestaltete Individualrechtsschutz durch effiziente, wirksame und regelmäßige Datenschutzkontrollen zu kompensieren (s. o.). Zunehmend operieren auch Polizeibehörden geheim, obgleich sie Daten grundsätzlich offen erheben müssen. Gerade im Bereich der Zentralstellenfunktion des Bundeskriminalamts kommt es jedoch zu zahlreichen Datenverarbeitungen, die den betroffenen Personen verborgen bleiben und mit denen diese nicht rechnen. Mit neuen polizeilichen Informationsverbünden, die im Hintergrund Zusammenhänge herstellen und Daten abgleichen, ist davon auszugehen, dass derartig verborgene Datenflüsse in Zukunft weiter zunehmen.

Darüber hinaus kann die Kompensationsfunktion nur dann Wirkung entfalten, wenn die betroffenen Behörden auf meine Beanstandungen in derselben Weise reagieren wie auf verwaltungsgerichtliche Urteile. Gerade gegenüber den Verfassungsschutzbehörden habe ich jedoch **keine Weisungsbefugnisse**. Auch ein gerichtliches Verfahren kann ich nach derzeitiger Rechtslage nicht anstoßen. In Bezug auf die Polizeibehörden entspricht dies nicht den Vorgaben der neuen EU Richtlinie zum Datenschutz im Bereich Justiz und Inneres (JI Richtlinie vgl. o. Nr. 1.2.2).

B. Aktuelle Gesetze/Gesetzentwürfe - Defizite hinsichtlich der verfassungsgerichtlichen Vorgaben

Auch aktuelle Gesetze und Gesetzentwürfe weisen erhebliche Defizite im Hinblick auf die Beachtung der verfassungsrechtlichen Vorgaben auf.

Exemplarisch verdeutlicht dies der Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU - Bundestagsdrucksache 18/11325 - vgl. Nr. 1.2). Der Entwurf enthält auch Regelungen zur Änderung des BND-Gesetzes (Art. 4, § 32 BNDG-E und § 32a Abs. 1 Nr. 1 lit. b) BNGG-E). Diese sind aber keine Anpassungen an die Verordnung. Vielmehr sollen - entgegen dem geltenden Recht und den vorgenannten verfassungsgerichtlichen Vorgaben - **meine Befugnisse beschränkt** werden. Ich hoffe, dass der Gesetzgeber meinem Petitum folgend hiervon Abstand nimmt.

C. Konsequenzen für den Haushaltsgesetzgeber

Der Haushaltsgesetzgeber ist aufgrund der Vorgaben des Bundesverfassungsgerichts gefordert, das personelle Defizit in meinem Haus erkennbar in den kommenden Haushaltsjahren abzubauen. Erfreulicherweise sind erste Schritte im Berichtszeitraum erfolgt. Ohne weiteren und kontinuierlichen Personalaufbau sind die Vorgaben des Bundesverfassungsgerichts aber nicht umsetzbar.

Fiktives Beispiel: Kontrolle einer Person (X) in der ATD

- drei Sicherheitsbehörden des Bundes haben Daten zu X in der ATD gespeichert ; diese stammen aus den jeweiligen ATD-Quelldateien dieser Behörden -

Inhalt der ATD zu X

Sicherheitsbehörde 1: Vorname, Name, Wohnort, bes. Fähigkeiten, Gefährder

Sicherheitsbehörde 2: Name, bes. Merkmale, Kontaktperson

Sicherheitsbehörde 3: Name, Wohnort, bes. Fähigkeiten, Gefährder

Sicherheitsbehörde 1 (Nachrichtendienst)

Vorhandene Daten zu X:

ATD- Quelldatei

Person X
- Vor- u. Nachname,
- Wohnort,
- bes. Fähigkeiten, Gefährder

- sonstige Erkenntnisse (die nur in dieser Quelldatei , nicht aber in der ATD gespeichert werden dürfen).

sowie
- andere Dateien/Akten mit Daten des X,
- (aktuelle) Maßnahmen der **Sicherheitsbehörde 1** gegenüber X: Observation, Telekommunikationsüberwachung nach dem G10- Gesetz.

Sicherheitsbehörde 2 (Nachrichtendienst)

Vorhandene Daten zu X:

ATD- Quelldatei

Person X
- Nachname,
- bes. Merkmale, Kontaktperson

- sonstige Erkenntnisse (die nur in dieser Quelldatei , nicht aber in der ATD gespeichert werden dürfen).

sowie
- andere Dateien/Akten mit Daten des X.
- (aktuelle) Maßnahmen der **Sicherheitsbehörde 2** gegenüber X: GPS-Überwachung.

Sicherheitsbehörde 3 (Polizeibehörde)

Vorhandene Daten zu X:

ATD- Quelldatei

Person X
- Nachname,
- Wohnort,
- bes. Fähigkeiten, Gefährder

- sonstige Erkenntnisse (die nur in dieser Quelldatei , nicht aber in der ATD gespeichert werden dürfen).

sowie
- andere Dateien/Akten mit Daten des X.
- (aktuelle) Maßnahmen der **Sicherheitsbehörde 3** gegenüber X: Wohnraumüberwachung und Telekommunikationsüberwachung.

Erläuterungen zum fiktiven Beispiel: Kontrolle einer Person (X) in der ATD

- drei Sicherheitsbehörden des Bundes haben Daten zu X in der ATD gespeichert -

(Verfassungs-)rechtlich vorgegebener Ablauf / Umfang der Kontrolle:

1. **Prüfung der ATD-Speicherung der Sicherheitsbehörde 1 wie folgt:**

   a) Ist die ATD-Speicherung nach den Vorgaben des ATDG zulässig.
   b) Sind die Daten aktuell und identisch in der (den) ATD-Quelldatei (en) gespeichert.
   c) Ist die Speicherung in der Quelldatei rechtlich zulässig (entspricht sie insbesondere den Vorgaben der einschlägigen Dateianordnung; falls nicht, ist die ATD-Speicherung unzulässig).
   d) Wurden die in der Quelldatei gespeicherten Daten rechtlich zulässig erhoben (falls nicht, ist die ATD-Speicherung unzulässig).
   e) Liegen verfassungsrechtlich unzulässige „additive Grundrechtseingriffe“ zu Lasten des X durch diese Sicherheitsbehörde vor, d.h. Ermittlung und Bewertung aller bei dieser Sicherheitsbehörde zu X vorhandenen Daten / Maßnahmen (Vorgabe des Bundesverfassungsgerichts).

2. **Prüfung der ATD-Speicherung der Sicherheitsbehörde 2 wie folgt:**
   Siehe oben 1 a) – e).

3. **Prüfung der ATD-Speicherung der Sicherheitsbehörde 3 wie folgt:**
   Siehe oben 1 a) – e).

4. **Prüfung aller Daten/Maßnahmen aller Sicherheitsbehörden**
   Liegen unzulässige „additive Grundrechtseingriffe“ zu Lasten des X durch das Zusammenwirken der Maßnahmen aller Behörden vor.
   Notwendig ist demnach eine Zusammenschau und Bewertung der zu X bei allen Behörden vorhandenen Daten / Maßnahmen (Vorgabe des Bundesverfassungsgerichts). Konsequenz: Eine bzw. einzelne Maßnahmen könnten - rechtlich isoliert betrachtet - verfassungsrechtlich zulässig sein und sich erst in dieser Zusammenschau als verfassungswidrig erweisen. Die Sicherheitsbehörden sind verpflichtet, dies durch eine entsprechende Kooperation / Abstimmung auszuschließen (Vorgabe des Bundesverfassungsgerichts).

Kasten b zu Nr. 1.3

Zentrale Vorgaben des Bundesverfassungsgerichts aus seinen aktuellen Grundsatzentscheidungen:

A. Übermittlung personenbezogener Daten an ausländische Sicherheitsbehörden (s. Urteil zum BKAG)

- Polizeien und Nachrichtendienste sind an die Grundrechte gebunden.
  Die Grenzen der inländischen Datenerhebung und -verarbeitung des Grundgesetzes dürfen durch einen Austausch **nicht unterlaufen bzw. ausgehöhlt werden**.
  „Keinesfalls darf der Staat seine Hand zu Verletzungen der Menschenwürde reichen".

  Nach den Vorgaben des Gerichts sind Datenübermittlungen demnach nur zulässig, wenn

  - o **ein hinreichender rechtsstaatlicher, d. h. datenschutzrechtlich angemessener und mit elementaren Menschenrechtsgewährleistungen vereinbarer, Umgang mit diesen Daten im Empfängerstaat** zu erwarten ist und

  - • **wirksame Kontrollen auf deutscher Seite durch die zuständigen Kontrollorgane sichergestellt** sind.

- Maßgebend für die Anforderungen an den Übermittlungs- und Nutzungszweck ist das **„Kriterium der hypothetischen Datenneuerhebung".**

  „Die Übermittlung muss damit der Aufdeckung vergleichbar gewichtiger Straftaten oder dem Schutz vergleichbar gewichtiger Rechtsgüter dienen, wie sie für die ursprüngliche Datenerhebung maßgeblich waren".

- Für die Annahme der Gewährleistung des geforderten Schutzniveaus im Empfängerstaat, d. h. z. B. des angemessenen materiellen datenschutzrechtlichen Niveaus im Empfängerstaat, kann eine **„generalisierende tatsächliche Einschätzung der Sach- und Rechtslage"** im Empfängerstaat nur ausreichen, sofern keine entgegenstehenden Tatsachen existieren. Ist dies der Fall bzw. kann die deutsche Stelle keine entsprechende Einschätzung vornehmen, bedarf es **„einer mit Tatschen unterlegten Einzelfallprüfung, aus der sich ergibt, dass die Beachtung jedenfalls der grundlegenden Anforderungen an den Umgang mit Daten hinreichend gewährleistet ist"**. Diese Prüfung muss auf der **Grundlage gehaltvoller und realitätsbezogener Informationen** erfolgen und **regelmäßig aktualisiert** werden. Die Gründe sind **nachvollziehbar** zu **dokumentieren**. Erforderlichenfalls können und müssen verbindliche Zusicherungen bzw. Einzelgarantien der ausländischen Stelle bzw. des Empfängerstaates abgegeben werden. Ist jedoch im Einzelfall zu erwarten, dass die Zusicherung nicht eingehalten wird, darf keine Datenübermittlung erfolgen.

  „Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können".

B. Effektive aufsichtliche Kontrolle (die Gewährleistung der den Kontrollorganen obliegenden „Kompensationsfunktion“) - ständige Rechtsprechung (s. a. Urteil zum BKAG):

Unter Verweis auf seine bisherigen Grundsatzentscheidungen betont das Bundesverfassungsgericht erneut die Bedeutung der wirksamen aufsichtlichen Kontrolle, d. h. der Kompensationsfunktion der Kontrolle zum Schutz der Grundrechte der Betroffenen. Diese ist eine zentrale Voraussetzung für die Wirksamkeit der behördlichen Maßnahmen. Erneut verpflichtet das Gericht den Gesetzgeber, dies zu gewährleisten. D. h. die Aufsichtsinstanzen entsprechend auszustatten, damit sie in der Lage sind, die ihnen obliegende

Kompensationsfunktion überhaupt erfüllen zu können. Von zentraler Bedeutung sind folgende Aussagen des Gerichts:

„Weil die Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung des individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können, kommt der **Gewährleistung** einer **effektiven aufsichtlichen Kontrolle umso größere Bedeutung** zu.

Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an die **wirksame Ausgestaltung** dieser **Kontrolle** sowohl auf der **Ebene des Gesetzes** als **auch** der **Verwaltungspraxis gesteigerte Anforderungen** (…).

Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt zunächst eine mit **wirksamen Befugnissen** ausgestattete Stelle - wie nach geltendem Recht die Bundesdatenschutzbeauftragte - voraus (…). Angesichts der **Kompensationsfunktion der aufsichtlichen Kontrolle** für den schwach ausgestalteten Individualrechtsschutz kommt deren **regelmäßiger Durchführung** besondere Bedeutung zu (…). Dies ist bei der Ausstattung der Aufsichtsinstanz zu berücksichtigen (…). Die **Gewährleistung** der **verfassungsrechtlichen Anforderungen einer wirksamen aufsichtlichen Kontrolle obliegt dem Gesetzgeber und den Behörden gemeinsam“.**

1.4 Das vernetzte und automatisierte Fahrzeug - nicht ohne Datenschutz

Die datenschutzrechtlichen Auswirkungen bei der Entwicklung digitalisierter und vernetzter Kraftfahrzeuge rücken zunehmend in den Fokus.

Das Thema „Datenschutz im Kraftfahrzeug“ wurde im Berichtszeitraum nicht nur von Fachleuten, sondern auch in den Medien breit und kontrovers diskutiert. Begriffe wie „Kfz als rollender PC“ und „Kfz als Datenkrake“ machten die Runde. Seit die Bundesregierung im Rahmen ihrer Strategie zur intelligenten Vernetzung dem automatisierten und vernetzten Fahren besondere Aufmerksamkeit schenkt, hat es noch mehr an Gewicht gewonnen.

Das Auto ist in besonderem Maß Ausdruck persönlicher Freiheit und unabhängiger Mobilität. Die Automatisierung und Vernetzung von Autos wirkt dem tendenziell entgegen. Durch automatisierte und vernetzte Autos soll der Straßenverkehr sicherer und der Fahrkomfort erhöht werden. Allerdings dürfen die persönlichen Rechte und Freiheiten von Haltern, Fahrern und Beifahrern nicht auf der Strecke bleiben. Regulierung und unternehmerische Freiheit müssen dort ihre Grenze finden, wo sie persönliche Rechte und Freiheiten unzulässig einschränken.

Meine Kolleginnen und Kollegen in den Ländern und ich haben in der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wiederholt zur datenschutzgerechten Nutzung von Fahrzeugdaten Stellung genommen und dabei die folgenden zentralen Punkte herausgestellt:

- Alle beim Betrieb von Fahrzeugen anfallenden Daten werden durch den individuellen Gebrauch des Fahrzeugs beeinflusst und sind deshalb personenbezogen. D. h. es gibt keine Daten, die von vornherein datenschutzrechtlich irrelevant sind.

- Die Automobilindustrie trägt die Verantwortung dafür, 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 muss größtmögliche Transparenz über die im Fahrzeug ablaufenden Datenerhebungs- und -verarbeitungsvorgänge geübt werden.
- Durch geeignete technische und organisatorische Maßnahmen nach dem aktuellen Stand der Technik müssen Datensicherheit und Datenintegrität sichergestellt werden. Dies betrifft insbesondere die Datenkommunikation aus dem Fahrzeug heraus.

Dialog mit dem Verband der Automobilindustrie

Der im Dezember 2014 begonnene Dialog der Datenschutzbehörden von Bund und Ländern mit dem Verband der Automobilindustrie (VDA) hat mit einer gemeinsamen Erklärung zu den datenschutzrechtlichen Aspekten bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge Anfang 2016 zu einem ersten positiven Ergebnis geführt (vgl. Anlage 3). Damit bekennen sich die durch den VDA vertretenen Hersteller und Zulieferer zu den Prinzipien des Datenschutzes. Insbesondere erkennen sie an, dass Fahrzeugdaten jedenfalls dann personenbezogen sind, wenn sie mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen verbunden sind. Ein Prüfstein für dieses Bekenntnis wird sein, in welcher Form die Hersteller und Zulieferer ihren datenschutzrechtlichen Transparenzverpflichtungen nachkommen und ob Fahrzeugdaten tatsächlich nur mit Einwilligung der Halter und gegebenenfalls auch der Fahrer und Beifahrer erhoben und verarbeitet werden. Die Hoheit über die Fahrzeugdaten muss vollständig in den Händen der Fahrzeugnutzer verbleiben, über deren Fahrverhalten die Fahrzeugdaten Aufschluss geben können. Dafür werde ich mich im weiteren Verlauf des Dialogs einsetzen.

Runder Tisch Automatisiertes und Vernetztes Fahren

Mit der Digitalisierung im Automobil- und Verkehrssektor werden Cybersicherheit und Datenschutz auch in diesem Bereich zu wichtigen Themen. So berate ich den vom Bundesministerium für Verkehr und digitale Infrastruktur eingerichteten so genannten Runden Tisch Automatisiertes und Vernetztes Fahren, der Industrie, Wissenschaft, Versicherer und Verbraucherschützer an einem Tisch versammelt. Hier werden erste Antworten auf Fragen formuliert, die sich durch technische Entwicklungen ergeben, die automatisierte und vernetzte Fahrsysteme möglich machen sollen. Schon jetzt zeichnet sich ab, dass solche Systeme die Erhebung und Verarbeitung einer noch nicht überschaubaren Anzahl an personenbezogenen Daten notwendig machen werden. Die dafür erforderlichen Vorkehrungen in rechtlicher und technologischer Hinsicht sind frühzeitig zu bedenken, um den datenschutzrechtlichen Grundsatz von Privacy by Design umsetzen zu können. Hier hat die Bundesregierung im Energiebereich mit dem Gesetz zur Digitalisierung der Energiewende Maßstäbe gesetzt, die auch im Automobil- und Verkehrssektor zur Anwendung kommen sollten (vgl. hierzu unter Nr. 17.2.1). Als beispielhaft möchte ich vor allem den Einsatz obligatorisch sicherheitszertifizierter Kommunikationskomponenten erwähnen, mit denen der Stand der Technik zum Schutz vor Cyberangriffen und unkontrolliertem Datenabfluss verbessert wird. Auch vernetzte Fahrzeuge sollten nur über solche Komponenten mit anderen Fahrzeugen, den Backend-Systemen der Hersteller oder Dritten kommunizieren können, die nach dem Vorbild des Smart-Meter-Gateways für die Energiewirtschaft in einer Technischen Richtlinie festgelegte Mindestanforderungen an die Cybersicherheit und den Datenschutz erfüllen.

Car-to-Car-Kommunikation

In diesem Zusammenhang befasse ich mich auch mit der so genannten Car-to-Car-Kommunikation. Es geht hierbei um eine Technologie, die es Fahrzeugen ermöglicht, über spezielle Funkverbindungen Fahr- und Umweltdaten auszutauschen, um sich z. B. gegenseitig vor Gefahrenstellen zu warnen oder selbstständig Kollisionen in Kreuzungsbereichen zu vermeiden. Die mir vorliegenden Informationen lassen die Sorge wachsen, dass bei der Entwicklung der Kommunikationsstandards und der Festlegung von Art und Umfang der zu übermittelnden Datenkategorien der Grundsatz von Datensparsamkeit und Datenvermeidung nicht ausreichend beachtet wird. Insbesondere scheinen nur unzureichende Vorkehrungen dafür getroffen zu werden, dass im Car-to-Car-Netz befindliche Fahrzeuge nicht verfolgbar sind und dass auf Basis der ausgetauschten Fahrdaten keine personenbezogenen Bewegungsprofile erstellt werden können. Auch bei dieser Form der Online-Kommunikation von Fahrzeugen lassen sich Datenschutz- von Datensicherheitserwägungen nicht trennen. Da die Sicherheit der Verkehrsinfrastruktur von überragender Bedeutung ist, müssen Bedrohungspotentiale analysiert und technische Vorkehrungen darauf abgestimmt werden. Ich werde die Entwicklung weiter beobachten und ausreichende Datenschutz- und Datensicherheitsstandards einfordern.

Ausblick

Mir sind die positiven Wirkungen des technologischen Fortschritts im Automobilbau durchaus bewusst. Neuartige Systeme, für deren Funktionalität eine Vielzahl der beim Fahrbetrieb entstehenden Daten verarbeitet werden müssen, sind etwa im Hinblick auf ein Mehr an Verkehrssicherheit von Vorteil für die auf Mobilität angewiesene Gesellschaft. Das erlaubt es der Industrie aber nicht, ihre datenschutzrechtliche Verantwortlichkeit für die von ihr verbauten Systeme zu vernachlässigen. Wichtig sind Transparenz, Datensparsamkeit und weitestgehende Erhaltung der Datenherrschaft beim Betroffenen.

Es wird ein großer Wettbewerbsvorteil für die deutsche Automobilindustrie sein, wenn sie ihre Marktposition im globalen Kontext durch eine datenschutzfreundliche Gestaltung ihrer Produkte zu sichern bzw. auszubauen sucht. Solche Technologien könnten sich dann nicht nur durch die eigene Produktpalette hindurch, sondern auch herstellerübergreifend durchsetzen. Kunden werden nach meiner Überzeugung künftig zunehmend datenschutzfreundliche Technologien nachfragen und den Grad ihres Vertrauens in die Hersteller daran messen.

1.5 Gesundheits-Apps und Wearables - mit Datenschutz gesünder

Gesundheits-Apps erfreuen sich einer steigenden Beliebtheit. Die Nutzer sind sich der datenschutzrechtlichen Risiken oft nicht bewusst. Es fehlen nicht nur ausführliche und verständliche Datenschutzerklärungen, auch im Übrigen mangelt es an der erforderlichen Transparenz.

Das Angebot von Apps im Gesundheitsbereich wächst zusehends und wird immer unüberschaubarer. Fitness-, Gesundheits-, Lifestyle-, Sport- und „medizinische" Apps haben alle einen gesundheitlichen Bezug und werden gemeinhin in Ermangelung einer einheitlichen Definition mit Gesundheits-App bezeichnet, wobei die wenigsten eine medizinische Relevanz besitzen. Gemeinsames Merkmal dieser Apps ist, dass sie die Körperdaten ihrer Nutzer in einem großen Umfang elektronisch erfassen. Nur in wenigen Fällen werden diese Daten lediglich im Gerät selbst (z. B. Smartphone, Tablet, Smartwatch, Tracker) gespeichert. Überwiegend werden sie per App an Dritte übermittelt. Dabei ist oft unklar, wo, ob im Inland oder Ausland, durch wen und unter welchen Sicherheitsbedingungen diese Daten erhoben, verarbeitet und gespeichert werden. Es mangelt hier an ausführlichen und verständlichen Datenschutzerklärungen. Die Nutzer wissen nicht, was mit ihren Körper- bzw. Gesundheitsdaten geschieht, die zu den sensibelsten aller personenbezogenen Daten zählen und besonders schützenswert sind. Die Gesundheits-Apps bergen somit erhebliche datenschutzrechtliche Risiken.

Zudem ermöglichen oft Mängel in der technischen Datensicherheit Unbefugten den Zugriff auf die sensiblen Daten. Ein weiteres erhebliches Risiko für die Nutzer ist die unberechtigte und unkontrollierte Zusammenführung sowie Auswertung der Daten. Selbst wenn personenbezogene Daten aus Apps anonymisiert verwendet würden, können die erfassten Körperdaten mit Daten kombiniert werden, die an anderer Stelle über die Nutzer frei verfügbar sind, und so zu ihrer Re-Identifizierung führen. Dadurch ließen sich umfassende Gesundheitsprofile einzelner Menschen erstellen und im Geschäftsverkehr, im Versicherungswesen oder in anderen Zusammenhängen ohne Wissen der Nutzer gegen diese verwenden.

Eine Vielzahl von Apps zu diversen Themenfeldern (u. a. Ernährung, Bewegung, Stressbewältigung, Impfungen, Gesundheitswissen, ärztliche Versorgung, Marketing, Service) werden mittlerweile auch durch die gesetzlichen Krankenkassen und privaten Krankenversicherungen angeboten. Soweit gesetzliche Krankenkassen Apps zur Verfügung stellen, mit denen Gesundheitsdaten und somit Sozialdaten erhoben werden, sind die spezialgesetzlichen Regelungen des Sozialgesetzbuches zu beachten, die abschließend regeln, welche Sozialdaten sie zu welchem Zweck erheben und verarbeiten dürfen. Darüber hinausgehende Verarbeitungen von Sozialdaten sind unzulässig, auch wenn die Betroffenen hierin eingewilligt haben (falls nicht im Einzelfall vom Gesetzgeber die Einwilligung vorgesehen ist). Daher ist in jedem Fall zu prüfen, ob die mit Hilfe von Apps gewonnenen Daten von den Erlaubnistatbeständen des Sozialgesetzbuches erfasst sind. In der Regel ist dies nicht der Fall.

Der Einsatz von Apps in der privaten Krankenversicherung unterliegt dagegen den Vorgaben des Versicherungsvertrags- und des allgemeinen Zivilrechts. Die Nutzung von Apps muss individuell vertraglich geregelt werden. Datenschutzrechtlich gelten hier nicht die Vorschriften des Sozialgesetzbuches, sondern das Versicherungsvertrags- und das Bundesdatenschutzgesetz. Aber auch hier sind die Anforderungen an eine datenschutzkonforme Einwilligung und an die technisch-organisatorische Ausgestaltung der Datenerhebung, -verarbeitung und -nutzung einzuhalten. Besonders wichtig sind u. a. Transparenz und Aufklärung der Nutzer. Der Gesetzgeber sollte erwägen, den Schutz, den er über das Sozialrecht den gesetzlich Versicherten bietet, hier auch den Versicherten privater Kassen zu gewähren und die Erhebung von Gesundheitsdaten über entsprechende Apps für private Krankenversicherer nur dann erlauben, wenn es hierfür eine spezifische Rechtsgrundlage gibt.

In 2016 haben Datenschutzaufsichtsbehörden aus Bund und den Ländern stichprobenartig Geräte und Apps von verschiedenen Anbietern überprüft. Dabei zeigte sich, dass Hersteller, Betreiber und Verkäufer der getesteten Geräte und Apps die Nutzer nicht ausreichend darüber informieren, was mit ihren Daten geschieht. Die meisten der untersuchten Datenschutzerklärungen erfüllten nicht die gesetzlichen Anforderungen, waren zu pauschal oder lagen nicht einmal in deutscher Sprache vor. Viele Geräte, und die damit verbundenen Nutzerkonten, boten keine Möglichkeit, Daten selbst vollständig zu löschen. Außerdem gaben viele der Geräte und Apps Daten ohne

Kenntnis der Nutzer an Dritte weiter, beispielsweise zu Forschungs- oder Marketingzwecken. Viele Hersteller sind in Deutschland nur mit Serviceniederlassungen präsent, während ihr Hauptsitz in anderen EU- oder gar in Drittstaaten liegt, in denen europäisches Verbraucher- und Datenschutzrecht nicht gilt. Dies wird sich erst nach Inkrafttreten der Europäischen Datenschutz-Grundverordnung im Mai 2018 ändern (vgl. o. Nr. 1.1).

In einer Entschließung hat sich die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder für einen effektiven Schutz der sensiblen Gesundheitsdaten der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps eingesetzt (Anlage 4).

Auf europäischer Ebene existieren verschiedene Initiativen zu diesem Thema. Im April 2014 veröffentlichte die Europäische Kommission ein Grünbuch über Mobile-Health-Dienste. In der Folge erarbeitet die „mHealth assessment guidelines working group", die sich aus Vertretern verschiedener öffentlicher und privater Institutionen aus einigen EU-Mitgliedstaaten zusammensetzt, Qualitätskriterien für die Bewertung von Gesundheits-Apps. Der „Code of Conduct on privacy for mHealth", der ein System der freiwilligen Selbstverpflichtung etabliert und vordringlich Entwickler sowie Hersteller mobiler Anwendungen anspricht, wurde der Artikel-29-Gruppe im Juni 2016 mit der Bitte um datenschutzrechtliche Bewertung vorgelegt. Eine Arbeitsgruppe der Artikel-29-Gruppe ist derzeit mit den Verfassern des Code of Conduct im Gespräch, um auf Verbesserungen des Datenschutzniveaus hinzuwirken. Im Rahmen der Prüfung des Codes of Conduct on privacy for mHealth werden die wesentlichen datenschutzrechtlichen Vorgaben für mobile Anwendungen auf europäischer Ebene abgestimmt (vgl. u. Nr. 2.4).

Gesundheits-Apps müssen den Datenschutz sowohl in technischer als auch in rechtlicher Hinsicht gewährleisten. Dies umfasst u. a., bereits bei der Entwicklung von Gesundheits-Apps und den entsprechenden Geräten die datenschutzrechtlichen Vorgaben hierfür zu beachten. Zudem sind die Nutzer umfassend und verständlich über bestehende Risiken zu informieren, z. B. die Übermittlung ihrer Daten an Dritte. Neben Selbstverpflichtungen der Hersteller und einer Sensibilisierung der Nutzer für Risiken und Gefahren bei der App-Anwendung halte ich gesetzliche Rahmenbedingungen für notwendig. Der Gesetzgeber sollte durch regulatorische Vorgaben für die Nutzung von Apps und dadurch erhobene Daten die Rechte der Verbraucher schützen, beispielsweise in der privaten Krankenversicherung. Dazu gehört auch das Verbot der unberechtigten Zusammenführung, Re-Identifizierung und Auswertung der Daten durch Dritte.

Zu diesem Thema verweise ich ergänzend auf eine Ausgabe meiner Publikationsreihe „Datenschutz kompakt", die auf meiner Internetseite unter www.datenschutz.bund.de abrufbar ist.

1.6 Die betrieblichen und behördlichen Datenschutzbeauftragten

Die Datenschutzbeauftragten in Behörden und Unternehmen spielen eine außerordentlich wichtige Rolle bei der Anwendung und Umsetzung des Datenschutzrechts. Das seit Jahrzehnten etablierte Zwei-Säulen-Modell aus innerbetrieblicher bzw. innerbehördlicher Kontrolle und der staatlichen Aufsicht durch die unabhängigen Datenschutzbehörden ist ein entscheidender Faktor für die vergleichsweise hohe Akzeptanz und das hohe Datenschutzniveau in Deutschland. Die Datenschutzbeauftragten stehen in ihren Behörden und Betrieben allen Mitarbeitern mit Rat und Hilfe zur Verfügung, beraten die Verantwortungsträger und kontrollieren die Einhaltung der datenschutzrechtlichen Bestimmungen.

Die zugrundeliegenden gesetzlichen Bestimmungen in Europa und in der Folge auch in Deutschland haben sich im Berichtszeitraum in eine erfreuliche Richtung weiterentwickelt.

Zudem habe ich im Berichtszeitraum einen Schwerpunkt meiner Arbeit auf die Beratung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung und die Kontrolle der öffentlichen Stellen des Bundes im Hinblick auf die Rechtsstellung der Datenschutzbeauftragten und den Umgang mit ihnen gelegt.

Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung

Mit der Datenschutz-Grundverordnung (DSGVO) ist es erstmals gelungen, das Zwei-Säulen-Modell europaweit zu verankern. Erfreulicherweise besteht in Deutschland weitgehend Konsens, die Regelungsspielräume der DSGVO mit dem Ziel einer weiteren Beibehaltung der nahezu flächendeckenden Ausstattung mit betrieblichen Datenschutzbeauftragten zu nutzen.

Nach langen Diskussionen hat sich der Europäische Gesetzgeber darauf verständigt, zumindest in bestimmten Fällen die Bestellung eines internen Datenschutzbeauftragten europaweit verbindlich vorzuschreiben (vgl. o. Nr. 1). Danach müssen Behörden immer einen Datenschutzbeauftragten bestellen; Ausnahmen gelten hier nur für die Gerichte im Rahmen ihrer rechtsprechenden Tätigkeit.

Darüber hinaus müssen Unternehmen immer dann einen Datenschutzbeauftragten bestellen, wenn

- die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer sensibler Daten im Sinne der Artikel 9 und 10 DSGVO besteht.

Die Rechtsstellung und die Aufgaben des Datenschutzbeauftragten sind in den Artikel 37 bis 39 DSGVO ähnlich denen nach dem geltenden BDSG ausgestaltet.

Die Artikel-29-Gruppe hat hierzu inzwischen Leitlinien beschlossen, in denen wertvolle Hinweise zur Bestellung, Rechtsstellung und den Aufgaben der Datenschutzbeauftragten gegeben werden (Leitlinien in Bezug auf Datenschutzbeauftragte vom 13. Dezember 2016, WP 243 – abrufbar über meine Internetseite unter www.datenschutz.bund.de). An der Ausarbeitung dieses Papiers habe ich mich intensiv beteiligt und auf diese Weise meine Erfahrungen aus dem seit langem bestehenden deutschen System einbringen können. In den Leitlinien wird konkretisiert, in welchen Fällen ein Datenschutzbeauftragter bestellt werden muss, wie dieser in die Organisation von Unternehmen und Betrieben eingebunden und welche Stellung er dort haben sollte, wann Interessenkonflikte mit anderen Aufgaben entstehen können und welche konkreten Aufgaben der Datenschutzbeauftragte hat.

Für die Behörden und Unternehmen in Deutschland wird sich voraussichtlich gar nicht so viel ändern, was in diesem Falle eine gute Nachricht ist. Behörden werden bereits unmittelbar durch die DSGVO verpflichtet, Datenschutzbeauftragte zu bestellen. Artikel 37 Absatz 4 DSGVO erlaubt es den Mitgliedstaaten darüber hinaus, nationale Regelungen zu schaffen, in denen Unternehmen über die entsprechenden Regelungen der DSGVO hinaus zur Bestellung von Datenschutzbeauftragten verpflichtet werden. Die Bundesregierung hat in ihrem Gesetzentwurf zur Anpassung des Datenschutzrechts von dieser Möglichkeit Gebrauch gemacht und will die Pflicht zur Bestellung von Datenschutzbeauftragten im bisherigen Umfang aufrechterhalten (vgl. o. Nr. 1.2.1). Erfreulicherweise besteht bislang ein Konsens zwischen Politik, Wirtschaft und Aufsichtsbehörden, dass Deutschland daran festhalten sollte.

Die behördlichen Datenschutzbeauftragten in der Bundesverwaltung

Im Rahmen meiner Beratung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung tauchen bei der praktischen Umsetzung der Anforderungen des BDSG viele Fragen auf. Zudem stelle ich bei Kontrollen von Bundesbehörden immer wieder Defizite beim Umgang mit den behördlichen Datenschutzbeauftragten fest.

Erfahrungsaustausch der Datenschutzbeauftragten der obersten Bundesbehörden fortgeführt - Neue Orientierungshilfe für die behördlichen Datenschutzbeauftragten

Auch im Berichtszeitraum habe ich den Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden fortgeführt. Die Erörterung gemeinsamer Probleme und die Diskussion offener Rechtsfragen bilden eine gute Basis für die Arbeit der Datenschutzbeauftragten (vgl. a. u. Nr. 12.2.4).

Die bei diesen Konsultationen wiederkehrenden Fragestellungen haben mich dazu veranlasst, das Konzeptpapier „*Mindestanforderungen an die Organisation und Aufgabenbeschreibung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung"* herauszugeben (vgl. Anhang 10 meiner Informationsbroschüre „Info 4").

Diese Mindestanforderungen konkretisieren die Funktion und die unabhängige Stellung der Datenschutzbeauftragten sowie die Unterstützungspflicht der verantwortlichen Stelle und enthalten viele wertvolle Hinweise, um die Position der Datenschutzbeauftragten zu stärken und damit die Wahrnehmung ihrer wichtigen Aufgabe zu unterstützen.

Um mir über die praktischen Auswirkungen der Mindestanforderungen ein Bild zu machen, habe ich im Berichtszeitraum ihre Umsetzung und die Einhaltung der gesetzlichen Vorgaben der §§ 4f und 4g BDSG schwerpunktmäßig in einer Reihe von Bundesbehörden geprüft. Dabei habe ich sehr unterschiedliche Erfahrungen gemacht.

Die Unterstützungspflicht der verantwortlichen Stelle

Für die Tätigkeit des Datenschutzbeauftragten gilt als oberster Grundsatz, dass er bei der Wahrnehmung seiner Aufgaben keinen Weisungen unterliegen darf (§ 4f Abs. 3 Satz 2 BDSG). In seiner Funktion ist er nach § 4f Absatz 3 Satz 1 BDSG dem Leiter der öffentlichen oder nicht-öffentlichen Stelle daher unmittelbar zu unterstellen um sicherzustellen, dass keine der von ihm zu kontrollierenden Organisationseinheiten Einfluss auf seine Tätigkeit nehmen kann. Dadurch wird einerseits seine unabhängige Stellung abgesichert und andererseits organisatorisch gewährleistet, dass er jederzeit sein direktes Vortragsrecht gegenüber der Leitung wahrnehmen kann.

Hieraus folgt auch die Pflicht zu einer angemessenen Freistellung des Beauftragten für den Datenschutz von anderen dienstlichen Tätigkeiten. Entsprechend seiner herausgehobenen Stellung muss die Tätigkeit als Datenschutzbeauftragter bei zeitlichen Konflikten mit anderen Aufgaben grundsätzlich Vorrang haben (vgl. § 4f Abs. 3 BDSG).

Wie die Praxis in den Bundesbehörden gezeigt hat, erfolgt oft keine Freistellung von anderen behördlichen/betrieblichen Aufgaben oder diese wird nur in einem zu geringem Umfang vorgenommen. Hier besteht bei vielen Stellen Nachbesserungsbedarf.

So befürworte ich bei einer Anzahl von mehr als 1.000 Beschäftigten in der Regel die vollständige Freistellung allein aufgrund des Umfangs der im Zusammenhang mit dem Beschäftigtendatenschutz bestehenden Aufgaben des Datenschutzbeauftragten. In Abhängigkeit vom Umfang oder der Komplexität der Verarbeitung personenbezogener Daten oder von deren Sensibilität kann auch bei einer geringeren Beschäftigtenzahl eine vollständige Freistellung erforderlich sein.

Bei meiner Tätigkeit hat sich sowohl im Zusammenhang mit Kontrollbesuchen bei Behörden als auch in Konsultationen mit den Datenschutzbeauftragten der obersten Bundesbehörden gezeigt, dass in der Praxis die besondere Rechtstellung der behördlichen Datenschutzbeauftragten nicht immer beachtet wird und oftmals in einem Spannungsverhältnis zu den tatsächlichen Gegebenheiten steht.

Bei der Umsetzung der notwendigen Freistellung hat die öffentliche Stelle einen organisatorischen Spielraum, der von den Gegebenheiten vor Ort und den konkreten Bedürfnissen des Datenschutzbeauftragten und seines Hilfspersonals abhängt. So kann es beispielsweise hingenommen werden, wenn der Datenschutzbeauftragte selbst zu 50 Prozent freigestellt ist und er einen Mitarbeiter hat, der ebenfalls von seinen sonstigen Aufgaben zu 50 Prozent freigestellt ist, was zusammengenommen einer vollständigen Freistellung entspricht. Maßstab muss dabei immer sein, insgesamt die notwendige Freistellung von sonstigen Aufgaben und eine effektive Aufgabenwahrnehmung zu gewährleisten (vgl. u. Nr. 14.1).

Vertretung des Datenschutzbeauftragten

Das BDSG sieht die Bestellung eines Vertreters nicht vor, schließt diese Möglichkeit jedoch auch nicht aus. Dieser ist als „Hilfspersonal“ im Sinne von § 4f Absatz 5 BDSG anzusehen, die Bestellung mehrerer Datenschutzbeauftragten wäre mit der Unabhängigkeit des Amtes aber nicht vereinbar. Die Bestellung eines Vertreters muss sich daher auf Fälle von Abwesenheit oder sonstiger Verhinderung des Beauftragten für den Datenschutz beschränken. Die nach dem BDSG dem Datenschutzbeauftragten eingeräumten besonderen Rechte wie der besondere Kündigungsschutz und das Zeugnisverweigerungsrecht gelten nicht für das Hilfspersonal und damit auch nicht für den Stellvertreter des Datenschutzbeauftragten.

Datenschutzbeauftragter als IT-Sicherheitsbeauftragter? Zwei Seelen sollten nicht in einer Brust schlagen

Bei meiner Beratungstätigkeit hatte ich zu prüfen, ob der Datenschutzbeauftragte zugleich auch die Funktion des IT-Sicherbeauftragten innehaben kann. Beide Aufgaben haben insbesondere in stark IT-basierten Unternehmen, wie Telekommunikations- oder Postdienstleistungsunternehmen, hohe synergetische Effekte, da sich beide das faktische Wissen zur Datenerhebung, Verarbeitung und Speicherung erarbeiten müssen. Insofern ist gerade bei Unternehmen mit einer schmalen Personaldecke eine Personalunion von Datenschutzbeauftragten und IT-Sicherheitsbeauftragten verlockend.

Allerdings stehen beide Rollen potentiell in Konflikt, z. B. wenn es um die Speicherfristen personenbezogener Daten geht. Während der Datenschutzbeauftragte eines Telekommunikationsunternehmens gemäß den Vorgaben des Telekommunikationsgesetzes (TKG) für eine restriktive Speicherung eintreten muss, strebt der IT-Sicherheitsbeauftragte zu Zwecken der Störungserkennung und -analyse eine möglichst langfristige Speicherung der Daten an. Hier besteht ein handfester Interessenskonflikt. Belegt wird dies beispielsweise durch Telekommunikationsunternehmen, die immer wieder die Speicherfrist für Verkehrsdaten, wie sie im gemeinsamen Leitfaden der BfDI und der Bundesnetzagentur für eine datenschutzgerechte Speicherung von Verkehrsdaten 2012 festgelegt wurde, mit verschiedensten Argumenten hinterfragen. Schließlich ist auch eine objektive Prüfung z. B. des IT-Sicherheitskonzeptes durch den Datenschutzbeauftragten in Frage zu stellen, wenn er selbst das Konzept zuvor in seiner Funktion als IT-Sicherheitsbeauftragter erstellt hat.

Um eine Interessenskollision zu verhindern, rate ich daher grundsätzlich dazu, die Rollen des Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten personell zu trennen.

Der Beauftragte für den Datenschutz - auch extern immer eine natürliche Person

Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden (§ 4f Abs. 2 Satz 3 erster Halbsatz BDSG). Dabei kann es sich nur um eine natürliche Person, nicht aber eine juristische Person oder eine Partnerschaftsgesellschaft handeln.

Die an den Beauftragten für den Datenschutz zu stellenden Anforderungen an „Fachkunde“ und „Zuverlässigkeit (§ 4f Abs. 2 Satz 1 BDSG), sowie die in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes bestehende Weisungsfreiheit (§ 4f Abs. 3 Satz 2 BDSG) sind von Gesetzes wegen - was auf der Hand liegt - auf natürliche Personen hin formuliert und gelten ebenso für Beauftragte für den Datenschutz außerhalb der verantwortlichen Stelle. Betroffene, die sich vertraulich an die Person des Beauftragten für den Datenschutz wenden möchten, könnten bei einer juristischen Person oder einer Partnergesellschaft als externem Datenschutzbeauftragten zudem nicht sicher sein, dass die Person, der das Anliegen vorgetragen wird, sie tatsächlich vertritt und auch weiterhin als Organ der juristischen Person tätig sein wird, zumal sich die Zusammensetzung der natürlichen Personen als Organe einer juristischen Person ändern kann. Zuletzt ist eine juristische Person nicht in der Lage, verschwiegen zu sein (§ 4f Abs. 4 BDSG); dies können nur natürliche Personen.

Auch die DSGVO geht grundsätzlich von dem Verständnis aus, dass nur natürliche Personen die Anforderungen an Fachkunde und Eignung erfüllen können. In den Leitlinien der Artikel-29-Gruppe (s. oben Nr. 1.6) wird zwar akzeptiert, dass externer Datenschutzbeauftragter auch eine juristische Person sein könne. Allerdings müsse dann jede (natürliche) Person, die innerhalb dieser Organisation Funktionen des Datenschutzbeauftragten wahrnimmt, sämtliche Voraussetzungen für die Benennung eines Datenschutzbeauftragten erfüllen. Dabei sollten in einem Team klare Verantwortlichkeiten festgelegt und eine Person als primärer Ansprechpartner festgelegt werden.

Amtszeit des Beauftragten für den Datenschutz

Die Bestellung des Beauftragten für den Datenschutz erfolgt grundsätzlich ohne zeitliche Einschränkung auf unbestimmte Zeit. Insbesondere enthält § 4f BDSG keine besonderen Regelungen für eine feste Amtszeit oder die Möglichkeit zur befristeten Bestellung des Datenschutzbeauftragten.

Allerdings ist nach überwiegender Ansicht, die ich teile, eine befristete Bestellung trotzdem möglich. Dem gleichen Rechtsgedanken folgend enthalten beispielsweise die Landesdatenschutzgesetze Mecklenburg-Vorpommerns und Thüringens bereits ausdrückliche Regelungen zur Befristung bzw. zu einer festen Amtszeit.

Eine Befristung ist allerdings dann rechtswidrig, wenn sie den Datenschutzbeauftragten an der ordnungsgemäßen Erfüllung seiner Aufgaben hindert oder mit den Schutzvorschriften des § 4f Absatz 3 BDSG kollidiert, was insbesondere bei zu kurzen Befristungen der Fall wäre.

Eine zu knapp bemessene Befristung hindert den Datenschutzbeauftragten beispielsweise daran, intensive Prüfungen besonders schwieriger Sachverhalte durchzuführen und könnte gegebenenfalls auch zur Umgehung des Abberufungsschutzes missbraucht werden. In der Regel kann daher erst eine Befristungsdauer von mindestens vier Jahren als rechtmäßig anerkannt werden. Kürzere Befristungen müssten dagegen besonders begründet werden oder aufgrund der Eigenart der jeweiligen Dienststelle notwendig sein.

Die Befristung ist dabei stets frei von weiteren Bedingungen außerhalb des Zeitablaufs zu halten, da der Sinn und Zweck der besonderen Schutzvorschriften nicht vereinbar mit auflösenden Bedingungen ist.

Beendigung der Bestellung des Beauftragten für den Datenschutz

Neben dem Ablauf einer zeitlichen Befristung kann die Bestellung des Beauftragten für den Datenschutz nur einvernehmlich, durch einseitigen Rücktritt oder durch die besonderen Vorschriften zum Widerruf gemäß § 4f Absatz 3 Satz 4 BDSG beendet werden.

Nach dieser Regelung ist ein Widerruf der Bestellung zum Beauftragten für den Datenschutz nur zulässig, wenn die Voraussetzungen für eine fristlose Kündigung aus wichtigem Grund gemäß § 626 BGB entsprechend vorliegen. Hierfür müssen wiederum Tatsachen gegeben sein, auf Grund derer dem Widerrufenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der gegenseitigen Interessen eine weitere Fortsetzung der Bestellung nicht zugemutet werden kann.

Die Zielrichtung des § 4f Absatz 3 Satz 4 BDSG unterscheidet sich jedoch von der des § 626 BGB, da sie nicht dem Schutz eines Arbeitnehmers, sondern dem Schutz der Funktion des Datenschutzbeauftragten dient. Daher sind auch Sachverhalte möglich, bei denen lediglich die Bestellung des Datenschutzbeauftragten widerrufen werden kann, nicht jedoch das zu Grunde liegende Rechtsverhältnis. Umgekehrt ist die Lösung des zu Grunde liegenden Arbeits- oder Dienstverhältnisses allerdings stets ein wichtiger Grund zum Widerruf der Bestellung.

Wichtige Gründe im Sinne des § 4f Absatz 3 Satz 4 BDSG sind daneben nur solche, die sich auf die Funktion des Datenschutzbeauftragten beziehen und eine weitere Ausübung unmöglich machen. Hierzu gehören unter anderem eine dauerhafte Verletzung der Kontrollpflichten, schwerwiegende Verstöße gegen das Datenschutzrecht hinsichtlich der eigenen Tätigkeit oder eine schwerwiegende Interessenkollision.

2 Schwerpunktthemen - europäisch und international

2.1 Von Safe Harbor zum Privacy Shield - alter Wein in neuen Schläuchen oder berechtigte Hoffnung für einen rechtssicheren transatlantischen Datenverkehr?

Durch die Aufhebung der Safe-Harbor-Entscheidung der Europäischen Kommission rückt der EuGH die umfassenden und anlasslosen Überwachungsaktivitäten der US-Nachrichtendienste erneut in den Fokus datenschutzrechtlicher Betrachtungen. Ob das Nachfolgeregelwerk „EU-US Privacy Shield" dauerhafte Rechtssicherheit für den transatlantischen Datenverkehr schaffen kann, bleibt abzuwarten.

Die Aufhebung des Adäquanzbeschlusses der Europäischen Kommission zum Safe-Harbor-Arrangement (2000/520/EG) vom 26. Juli 2000 durch das sog. Schrems-Urteil des Europäischen Gerichtshofs (EuGH) vom 6. Oktober 2015 (Az. C-362/14) war ein Paukenschlag, der noch lange Zeit nachhallen wird. Die von einem österreichischen Staatsbürger initiierte Beschwerde bei der irischen Datenschutzbehörde wegen der Übermittlung seiner Daten in die USA durch Facebook führte zu einem Urteil, das in vielerlei Hinsicht wegweisend ist.

So stellt der EuGH fest, die Safe-Harbor-Entscheidung der Kommission hindere die nationalen Kontrollstellen nicht daran, in völliger Unabhängigkeit zu prüfen, ob bei der Datenübermittlung die in der Datenschutzrichtlinie 95/46/EG aufgestellten Anforderungen zum Schutz des Grundrechts auf Datenschutz aus Artikel 8 der EU-Grundrechtecharta (Charta) gewahrt sind. Diese erhebliche Aufwertung der europäischen Datenschutzbehörden verband der EuGH mit der Forderung nach einem Klagerecht für Datenschutzbehörden gegen Unionsrechtsakte. Die für das Jahr 2017 vorgesehene Umsetzung dieser richterlichen Vorgabe in deutsches Recht erwarte ich mit großer Spannung.

Darüber hinaus erklärt der EuGH die Safe-Harbor-Entscheidung selbst für nichtig, weil die Kommission darin nicht hinreichend begründet festgestellt habe, ob die USA aufgrund innerstaatlicher Rechtsvorschriften oder internationaler Verpflichtungen ein Schutzniveau gewährleisten, das dem in der Europäischen Union garantierten Niveau der Sache nach gleichwertig sei.

Zusätzlich zu diesem formalen Argument gibt das Gericht Hinweise zur Rechtslage und Rechtspraxis in den USA, welche Regelungen bezüglich der Überwachungsbefugnisse staatlicher Stellen und der Rechtsschutzmöglichkeiten des Betroffenen als besonders schwerwiegende Verletzungen europäischer Grundrechte angesehen werden müssen.

So verletze beispielsweise eine Regelung, die den Behörden einen generellen Zugriff auf den Inhalt elektronischer Kommunikation gestatte, den Wesensgehalt des durch Artikel 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.

Ebenso verletze eine Regelung das in Artikel 47 der Charta verankerte Grundrecht auf wirksamen gerichtlichen Rechtsschutz, wenn sie keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken.

An diesen Vorgaben und Rechtsgedanken des Urteils werden sich sämtliche Angemessenheitsentscheidungen der Kommission sowie die alternativen Instrumente für Datenübermittlungen in Staaten ohne angemessenes Datenschutzniveau, wie Standardvertragsklauseln und verbindliche Unternehmensregelungen (Binding Corporate Rules - BCR), messen lassen müssen.

Dies gilt zuvorderst für die Nachfolgeregelung zu Safe Harbor. Mit der Entscheidung der Kommission (2016/1250) vom 12. Juli 2016 steht nach intensiven Verhandlungen zwischen Kommission und US-Regierung

mit dem „EU-US Privacy Shield“ eine neue Rechtsgrundlage für Datenübermittlungen in die USA in Form eines Angemessenheitsbeschlusses nach Artikel 25 Absatz 6 Datenschutzrichtlinie 95/46/EG zur Verfügung.

Die intensive Begleitung des Verhandlungsprozesses durch die Artikel-29-Gruppe der europäischen Datenschutzaufsichtsbehörden hat dabei zu zahlreichen Verbesserungen geführt. So wurden insbesondere die Regelungen für Übermittlungen an Dritte datenschutzfreundlicher gestaltet und der im europäischen Datenschutzrecht zentrale Begriff der Zweckbindung im EU-US Privacy Shield verankert. An der Erarbeitung der Stellungnahmen der Artikel-29-Gruppe habe ich maßgeblich mitgewirkt.

Der EU-US Privacy Shield enthält in seiner jetzt verabschiedeten Fassung weitere - teils erhebliche - Verbesserungen im Vergleich zur Vorgängerregelung Safe Harbor. So wurde u. a. die Funktion einer Ombudsperson im US-Außenministerium eingerichtet, über die Beschwerden zu möglichen Überwachungstätigkeiten US-amerikanischer Geheimdienst- und Sicherheitsbehörden eingereicht werden können.

Ferner sind die - den Vorgaben des EuGH-Urteils folgend - im EU-US-Privacy Shield nicht mehr enthaltenen Beschränkungen der Befugnisse der völlig unabhängigen europäischen Datenschutzbehörden hervorzuheben.

Aus datenschutzrechtlicher Sicht bleiben dennoch gewichtige Kritikpunkte am EU-US Privacy Shield bestehen. Hervorzuheben sind insbesondere der Mangel an konkreten Zusagen der US-Regierung im Hinblick auf die Einschränkung der Massenüberwachung und die Frage, ob die Ombudsperson tatsächlich einen wirksamen Rechtsschutz im Sinne von Artikel 47 der Charta gewährleisten kann. Hierfür müsste sie von den zu kontrollierenden Stellen unabhängig sein, die Möglichkeit haben, sich aufgrund von eigenständiger Inaugenscheinnahme von Unterlagen ein eigenes Urteil zu bilden, und über die Fähigkeit verfügen, Abhilfe zu schaffen.

Trotz der fortbestehenden Vorbehalte hat die Artikel-29-Gruppe beschlossen, die Ergebnisse der ersten, jährlich durchzuführenden Überprüfung des EU-US Privacy Shield durch die Kommission und die US-Regierung im Jahre 2017 abzuwarten. Die europäischen Datenschutzbehörden streben bei dieser Überprüfung eine aktive Beteiligung an. Auch ich werde mich dabei in gestaltender Weise einbringen.

Ob die bereits jetzt sichtbaren Maßnahmen auf US-Seite ausreichen, die Bedenken der europäischen Datenschutzbehörden, insbesondere mit Blick auf die Überwachungsmaßnahmen und Rechtsschutzmöglichkeiten, zu zerstreuen, bleibt also abzuwarten.

Bereits wenige Monate nach Inkrafttreten des EU-US Privacy Shield liegen mehrere Klageverfahren beim Gericht der Europäischen Union (EuG) gegen diese Kommissionsentscheidung vor. Die Verwendung von Standardvertragsklauseln für Datenübermittlung aus der EU in die USA ist gleichfalls Gegenstand gerichtlicher Überprüfung. Auch diese Verfahren werden weiteren Aufschluss über die Rahmenbedingungen für den transatlantischen Datenverkehr und Datenübermittlungen in andere Drittstaaten geben.

2.2 Umbrella Agreement: Der Schirm ist aufgespannt. Hat er Löcher?

Das sog. Umbrella Agreement ist in Kraft. Die Praxis wird nun zeigen, ob sich die Rechtschutzmöglichkeiten von EU-Bürgern in den USA im Sicherheitsbereich tatsächlich verbessern.

Nach Jahren der Verhandlungen ist das sog. Umbrella Agreement abgeschlossen worden. Das Abkommen schafft keine neuen Rechtsgrundlagen, um personenbezogene Daten an Sicherheitsbehörden in den USA zu übermitteln, sondern verpflichtet die Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union und der USA dazu, die mit dem Abkommen gesetzten datenschutzrechtlichen Standards im Falle einer Übermittlung einzuhalten. Unabhängig davon ist für die Übermittlung jeweils eine eigenständige Rechtsgrundlage erforderlich. Mit anderen Worten schafft das Abkommen Rechte für Betroffene und Pflichten für Sicherheitsbehörden, die fortan stets gelten und nicht mehr zur Diskussion stehen, soweit das Abkommen Anwendung findet. Diese

Einschränkung hat Bedeutung, denn die Standards gelten nicht, wenn Nachrichtendienste personenbezogene Daten austauschen oder wenn US-Sicherheitsbehörden personenbezogene Daten europäischer Bürgerinnen und Bürger anderweitig erheben, sei es in den USA oder in anderen Teilen der Welt.

Dieses Übereinkommen wird aus datenschutzrechtlicher Sicht aber nur ein Erfolg, wenn sich der Rechtsschutz in den USA für europäische Bürgerinnen und Bürger tatsächlich verbessert. Denn dieser Mangel an Rechtsschutzmöglichkeiten hat die transatlantischen Sicherheitsdiskussionen seit Jahren belastet, und auch der EuGH hat dieser Frage im sog. Schrems-Urteil erhebliche Bedeutung beigemessen (Urteil vom 06.10.2015, Az. C-362/14; vgl. o. Nr. 2.1).

In meinem letzten Tätigkeitsbericht stand noch die Ankündigung des damaligen US-Justizministers im Raum, die US-Regierung wolle sich für einen verbesserten Rechtsschutz für europäische Bürgerinnen und Bürger in den USA einsetzen. Dieser Ankündigung sind Taten gefolgt. Der US-Kongress hat den sog. Judicial Redress Act angenommen und damit den Rechtschutz der europäischen Bürgerinnen und Bürger dem von US-amerikanischen Staatsangehörigen zumindest angenähert. Also: Fortschritt ja, aber was bedeuten die neuen Regelungen konkret im Sicherheitsbereich? Um das zu beantworten, ist es noch zu früh. Die Regelungen in den USA sind komplex, und in welchem Maße der verbesserte Rechtsschutz auch gegenüber den Sicherheitsbehörden in den USA gilt, wird die Praxis erst noch zeigen müssen.

So wie auch die anderen Abkommen mit den USA im Sicherheitsbereich sieht das Umbrella Agreement eine gemeinsame Überprüfung („joint review“) vor, ob die Vereinbarungen in den USA eingehalten bzw. wie sie umgesetzt werden. Die Artikel-29-Gruppe wird sich hieran aktiv beteiligen. Ich messe der Überprüfung des Abkommens in der Praxis große Bedeutung bei und werde die weiteren Entwicklungen genau verfolgen.

Ich sehe in dem Abkommen einen wichtigen Schritt, um verbindlich möglichst hohe Standards für den Datenaustausch mit den USA im Sicherheitsbereich zu setzen. Auch wenn mit dem Abkommen nicht alle umstrittenen Fragen ausgeräumt sind, unterstütze ich den eingeschlagenen Weg. Es ist langwierig und mühsam, sich transatlantisch verbindlich auf Verbesserungen beim Schutz der Betroffenen im sensiblen Sicherheitsbereich zu einigen. Sollte dies aber gelingen, kann das Abkommen Vorbildcharakter für weitere Vereinbarungen mit anderen Staaten haben.

2.3 Sicherheit, Grenzmanagement und datenschutzrechtliche Herausforderungen

Die Außengrenzen müssen nach Auffassung der Europäischen Kommission sicherer werden. Hierin sind sich die EU-Kommission und die Sicherheitsbehörden der Mitgliedstaaten einig. Eine Modernisierung des Grenzmanagements steht daher ganz oben auf der politischen Agenda; die Persönlichkeitsrechte dürfen dabei aber nicht auf der Strecke bleiben.

Mit ihrer Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom April 2016 hat die Europäische Kommission den strategischen Überbau für verschiedene Vorhaben vorgelegt. Dazu gehören die Einrichtung eines Ein- und Ausreiseregisters (EES), die Einrichtung eines Reiseinformations- und -genehmigungssystems (ETIAS - vgl. beides u. Nr. 2.3.1), Anpassungen der Eurodac-Verordnung (vgl. Nr. 10.3.3) und die Umsetzung der Richtlinie zur Nutzung von so genannten Passenger Name Records (PNR, vgl. u. Nr. 2.3.2).

Das Gesamtpaket ist gekennzeichnet durch das Bestreben, vorhandene Informationssysteme aus den Bereichen Grenzkontrolle, Asyl und Migration mit Daten anzureichern, die Systeme jeweils gegenseitig und zusätzlich für Zwecke der Gefahrenabwehr, Strafverfolgung und Terrorismusbekämpfung lückenlos nutzbar zu machen und ggf. noch bestehende Erkenntnislücken durch zusätzliche Systeme gezielt zu schließen.

Die zunehmende Vernetzung der Systeme ist mit erheblichen Eingriffen in die Rechte der Betroffenen verbunden und stellt datenschutzrechtliche Grundsätze in Frage. Wesentliche Schutzmechanismen für das Persönlichkeitsrecht des Einzelnen müssen aber erhalten bleiben. Hierzu gehören Zweckbindung, Datensparsamkeit, Löschfristen, Zugriffsbeschränkungen und Kontrollierbarkeit der Datenverarbeitung. Ich werde daher die geplanten Regelungen weiterhin kritisch begleiten.

2.3.1 Smart borders und Interoperabilität - Mit EES und ETIAS auf dem Weg zu vernetzten Grenzen

Hinter diesen Abkürzungen verbergen sich Vorhaben, mit denen umfassend Personen erfasst werden sollen, die Schengen-Grenzen übertreten. Datenbanken sollen verknüpft, die Daten über Jahre hinweg aus allgemeinen Sicherheitserwägungen gespeichert bleiben. Grundlegende Prinzipien des Datenschutzes sind gefährdet.

Die unter dem Schlagwort „smart borders" verfolgten Projekte habe ich schon in vorangegangenen Tätigkeitsberichten kritisch betrachtet (24. TB Nr. 2.5.3.4., 25. TB Nr. 3.3). Der Vorschlag der Kommission für die Errichtung eines Ein- und Ausreiseregisters (Entry-Exit-System, kurz EES) sieht vor, künftig alle Grenzübertritte von Drittstaatsangehörigen im Zusammenhang mit Kurzaufenthalten zentral zu erfassen. Dabei sollen biographische Daten, Fingerabdrücke und biometrische Gesichtsbilder sowie Einträge zu Grenzübertritten und Zurückweisungen (sog. entry-exit-records) verarbeitet werden. Das System soll mit dem Visainformationssystem (VIS) gekoppelt werden, so dass Grenzbehörden aus dem EES unmittelbar auf VIS zugreifen können und alle Daten nur einmal gespeichert werden. Visum- und Asylbehörden sollen auf das EES für laufende Verfahren zugreifen können, Polizeibehörden sowie Nachrichtendienste für die Abwehr und Verfolgung terroristischer und sonstiger schwerer Straftaten.

Die umfangreichen Zugriffsmöglichkeiten, einschließlich solcher für die Nachrichtendienste, stellen den Grundsatz der Zweckbindung ebenso in Frage wie die Verknüpfung des Zugangs zu verschiedenen Datenbanken. Hiermit wird ein System geschaffen, das umfangreich Drittstaatsangehörige erfasst, die Schengen-Grenzen übertreten, und das diese Daten über Jahre hinweg aus allgemeinen Sicherheitserwägungen speichert. Denn ob die Datenbank ihren Primärzweck, die Erleichterung der Grenzkontrollen, tatsächlich erreichen kann, erscheint angesichts der komplexen Prozesse innerhalb des EES eher fraglich. Die Einrichtung einer Großdatenbank mit biometrischen Daten zur Verfahrenserleichterung begegnet außerdem erheblichen Bedenken bei der Verhältnismäßigkeit.

Nach dem Vorschlag zur Einrichtung eines Reiseinformations- und -genehmigungssystems (European Travel Information and Authorisation System, kurz ETIAS) sollen künftig alle visabefreit einreisenden Drittstaatsangehörigen vor einer Einreise in den Schengen-Raum über ETIAS eine Reisegenehmigung beantragen müssen. Dieses Verfahren soll insbesondere eine vorgezogene Bewertung von Sicherheitsrisiken, Migrationsrisiken und Gesundheitsgefahren ermöglichen. Dazu sollen biographische Daten bis hin zum Ausbildungsstand und der aktuellen Beschäftigung erfasst werden sowie Antworten auf verschiedene Hintergrundfragen und die IP-Adresse, von der aus der Antrag gestellt wurde. Im weitgehend automatisierten Genehmigungsverfahren erfolgt anschließend ein Datenabgleich mit allen relevanten EU-weiten Reise-, Asyl- und Polizeiinformationssystemen sowie bestimmten Risikoindikatoren und einer Kontrollliste. Bei Treffern erfolgt eine manuelle Entscheidung über den Antrag. Neben den Genehmigungs- und Grenzkontrollbehörden erhalten insbesondere Sicherheitsbehörden Zugriff zur Abwehr und Verfolgung terroristischer und anderer schwerer Straftaten.

Das vorgeschlagene System mag einen Beitrag dazu leisten, Zurückweisungen an der Außengrenze zu vermeiden und insoweit die Grenzkontrollen zu entlasten. Im Übrigen bestehen jedoch Zweifel, ob das System überhaupt geeignet ist, Personen mit Sicherheits-, Migrations- und Gesundheitsrisiken vorab herauszufiltern. Überzeugende Beispiele sind bislang nicht vorgetragen. Der pauschale Verweis auf gute Erfahrungen in anderen Staaten überzeugt an dieser Stelle nicht. Das gilt insbesondere, soweit die erhobenen Daten noch über die im Visumverfahren erhobenen Daten hinausgehen. Hier stellt sich die Frage, mit welcher Berechtigung von visumbefreit Reisenden mehr Daten verlangt werden können als von denen, die ein Visum beantragen. Auch ein Be-

darf für die vorgesehenen Zugriffsmöglichkeiten der Sicherheitsbehörden ist bisher nicht überzeugend dargelegt. Ähnlich wie beim EES-Vorschlag soll eher rein vorsorglich eine mehrjährige Vorratsspeicherung über Daten von Einreisewilligen eingerichtet werden. Die vorgesehene Abgleichfunktion über IP-Adressen bietet zahlreiche Verknüpfungsmöglichkeiten.

Weitere Vernetzungsmöglichkeiten verfolgt die Kommission unter der Zielvorgabe der Interoperabilität. In deren Langzeitvision sollen die relevanten Informationssysteme aus den Bereichen Grenzmanagement, Migration und Strafverfolgung zu einem neuen Gesamtsystem mit einer zentralen Identitätsdatenbank (Kernmodul) und damit verknüpften Fachmodulen verschmelzen.

Die Pläne für ein solches Kernmodul sehe ich mit großer Besorgnis. Der Schritt zu einer EU-weiten Bevölkerungsdatenbank ist nicht mehr weit entfernt. Ein solches System ist mit europäischem Datenschutzrecht kaum zu vereinbaren. Elementare Grundsätze wie die Zweckbindung, das Recht auf Löschung/Vergessen, die Kontrollierbarkeit, die Datenminimierung und die Datensparsamkeit („need to know“) sind erheblich gefährdet.

Auch die Artikel-29-Gruppe hat sich in einem Brief an Rat, Kommission und Europäisches Parlament zu EES, ETIAS und Interoperabilität kritisch geäußert.

2.3.2 Fluggastdaten: Das nächste Kapitel

Der europäische Gesetzgeber hat nach Jahren eine Richtlinie zur Erfassung und Speicherung von Fluggastdaten (PNR-Daten) für Sicherheitszwecke verabschiedet. Während die Regierungen der Mitgliedstaaten bereits die Umsetzung vorbereiten, richtet sich der Blick auf den Europäischen Gerichtshof in Luxemburg.

Bereits in meinem 22. Tätigkeitsbericht (Nr. 13.5.3) habe ich von ersten Vorschlägen berichtet, so genannte passenger name records (PNR-Daten) für Sicherheitszwecke zu nutzen und auf Jahre zu speichern. Es handelt sich hierbei um einen Datensatz, den die Fluggesellschaften erstellen, um die Passagiere zu befördern. Die PNR-Richtlinie verpflichtet nun die Fluggesellschaften, diese Daten schon vor Abflug einer Sicherheitsbehörde zu übermitteln.

Insbesondere das Europäische Parlament stand dem Vorhaben lange skeptisch gegenüber, doch unter dem Eindruck der schrecklichen Terroranschläge von Brüssel und Paris hat der europäische Gesetzgeber schließlich im April 2016 die Richtlinie verabschiedet. Danach haben alle Mitgliedstaaten bis zum Mai 2018 Zeit, bei einer Sicherheitsbehörde eine Fluggastzentrale einzurichten, die PNR-Daten erfasst und für fünf Jahre speichert, und zwar nach den Vorstellungen der Innenminister bei allen Flügen, die nicht rein nationale Flüge sind.

Das PNR-System verfolgt im Wesentlichen zwei Zwecke. Zunächst dient es dem Abgleich aller Flugpassagiere mit abstrakten Gefährdungsmustern. Ein Flugpassagier gerät in das Visier für eine Kontrolle an der Grenze, wenn er verschiedene Kriterien erfüllt, die bei zuvor gefassten Straftätern vorlagen (z. B. Art der Buchung, gewählte Flugroute etc.). Ausdrückliches Ziel ist es also, bestimmte Passagiere in den Fokus zu nehmen, gegen die bislang gerade kein Verdacht bestand, deren PNR-Datensatz aber einem Gefährdungsmuster entspricht. Nach der Richtlinie muss die Entscheidung über die konkrete Kontrolle an der Grenze immer ein Mensch treffen, doch folgt die Vorauswahl zukünftig der Programmierung der Muster.

Der andere wesentliche Zweck ist die Nutzung der gespeicherten Daten für die Zwecke der Verhütung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Einer Vorratsdatenspeicherung entsprechend werden die Fluggastdaten für fünf Jahre verdachtsunabhängig gespeichert, allerdings nach sechs Monaten „depersonalisiert“. Der Zugriff auf einen vollständigen Datensatz ist hiernach nur noch zulässig, wenn ein Richter die Überzeugung gewonnen hat, dass die Daten im Einzelfall für die Verfolgung schwerer Kriminalität erforderlich sind.

Um das Ausmaß der zu erwartenden Speicherungen in Deutschland zu verstehen, ist ein Blick auf die folgenden Zahlen hilfreich. Nach den Angaben der europäischen Statistikbehörde Eurostat wären in Deutschland im Jahr 2014 PNR-Daten zu etwa 164 Millionen Fluggästen analysiert und gespeichert worden. Dass die Zahl so hoch ist, liegt wesentlich an dem erklärten Willen der europäischen Innenminister, auch Flüge zu erfassen, deren Abflug- und Landeort innerhalb der Europäischen Union liegen. Die Erfassung dieser Flüge ist nach der Richtlinie nicht verbindlich. Für Deutschland bedeutet dies, dass PNR-Daten zu fast 100 Millionen Flugpassagieren mehr erhoben werden, als wenn man die Erfassung auf die Flüge in oder aus Drittstaaten begrenzen würde.

An meiner von Anfang an bestehenden Skepsis hat sich nichts geändert: Mit der Richtlinie schaffen die Mitgliedstaaten riesige Datenbanken, für deren Erforderlichkeit in diesem Umfang wenig Konkretes vorgetragen worden ist. Ich erkenne an, dass während der jahrelangen Verhandlungen verschiedene zusätzliche Verfahrenssicherungen eingebaut worden sind, um die Verhältnismäßigkeit zu wahren. Hierzu zählen etwa die Depersonalisierung der Daten nach sechs Monaten, ein besonderer Genehmigungsvorbehalt für den Zugriff danach oder das Verbot, bestimmte sensible Daten zur Grundlage für den Abgleich mit Gefährdungsmustern zu machen.

Bei der Umsetzung der Richtlinie in deutsches Recht werde ich mich dafür einsetzen, die vorhandenen Spielräume datenschutzfreundlich zu nutzen. Dabei wird der Blick auch auf den EuGH in Luxemburg gerichtet bleiben. Zum Thema PNR habe ich bereits in meinem letzten Tätigkeitsbericht auf die Rechtsprechung des EuGH zu grundrechtssensiblen Eingriffen hingewiesen, die mehr und mehr der des Bundesverfassungsgerichts entspricht. Das letzte Wort darüber, ob und wie die europäischen Fluggastzentralen personenbezogene Daten verdachtslos analysieren und speichern dürfen, wird der EuGH haben. Nachdem der EuGH die Richtlinie zur Vorratsdatenspeicherung von Telekommunikationsdaten aufgehoben hatte, hat das Europäische Parlament den EuGH um ein Gutachten gebeten, mit dem die Rechtmäßigkeit eines Abkommens überprüft werden soll, auf dessen Grundlage PNR-Daten in ähnlicher Art und Weise an die kanadischen Sicherheitsbehörden übermittelt werden dürfen.

2.3.3 Schengen-Evaluierung in Deutschland

Die Expertengruppe zur Prüfung der Umsetzung des Schengener Besitzstandes hat auch meine Arbeit unter die Lupe genommen.

Bereits im Sommer 2015 hat eine Expertengruppe die Umsetzung des sog. Schengener Besitzstandes in Deutschland geprüft. Die Gruppe bestand aus Vertretern der Europäischen Kommission und Mitarbeitern der Datenschutzbeauftragten der Mitgliedstaaten. Hierbei wurde untersucht, inwieweit die jeweiligen Institutionen in Deutschland zur effizienten Umsetzung des Schengen-Raumes und der dazu erlassenen Rechtsakte beitragen (Verordnung (EU) Nr. 1053/2013 des Rates vom 07.10.2013, Artikel 2). Dies betraf neben meiner Tätigkeit und der der Datenschutzbeauftragten der Länder u. a. auch die der Bundespolizei, des Bundeskriminalamts und des Auswärtigen Amts.

In meinem Zuständigkeitsbereich wurde u. a. meine Kontroll- und Beratungstätigkeit beim Schengener Informationssystem, dem Visainformationssystem sowie Projekten im Bereich des Grenzschutzes geprüft. Hierzu zählt auch meine Hilfestellung bei Ersuchen von betroffenen Bürgern und von mir zur Verfügung gestelltes Informationsmaterial zu diesen Themen.

Ein weiterer sehr wichtiger Prüfpunkt war meine Unabhängigkeit, hinsichtlich derer bei der vorherigen Schengen-Evaluierung Bedenken bestanden. Da ich seit dem 1. Januar 2016 vollkommen unabhängig bin, ist diese wichtige Voraussetzung jetzt endlich erfüllt.

Dem vorläufigen Prüfbericht der Expertengruppe zufolge sehe ich alle an mich gestellten Anforderungen erfüllt. Zu erwähnen ist jedoch, dass für die Erledigung der an mich gestellten Anforderungen immer auch eine ausreichende Personalstärke hinterlegt sein sollte. Dies auch, um Kontrollen in den vorgegebenen Intervallen und in

der gebotenen Sorgfalt durchführen und Auskunftsersuchen Betroffener in einem angemessenen Zeitrahmen beantworten zu können.

2.4 Datenschutz auf EU-Ebene: die Artikel-29-Gruppe und ihre Untergruppen sind der Motor

Die Artikel-29-Gruppe setzt sich aktiv für einen einheitlichen und effektiven Datenschutz in der Europäischen Union ein.

In den Jahren 2015 und 2016 hat sich die Artikel-29-Gruppe wieder mit einer breiten Palette unterschiedlicher Themen befasst. Sie verabschiedete sechs offizielle Stellungnahmen („Opinion"), Standpunkte („Statements") und weitere Arbeitspapiere zu aktuellen datenschutzrechtlichen Fragestellungen. Die behandelten Themen betrafen insbesondere die Reform des europäischen Datenschutzrechts (vgl. o. Nr. 1) und die Neuregelung des datenschutzrechtlichen Rahmens im transatlantischen Verhältnis der EU zu den USA (vgl. o. Nr. 2.1, Nr. 2.2).

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

Aktionsplan zur Umsetzung der Datenschutz-Grundverordnung

Nachdem sich das Europäische Parlament und der Rat der EU Ende 2015 auf die Neuregelung des EU-Datenschutzrechts geeinigt hatten (vgl. o. Nr. 1.1), begann die Artikel-29-Gruppe mit den Vorbereitungen zu deren praktischer Umsetzung. Hierzu hat sie in ihrem 104. Plenum im Februar 2016 einen Aktionsplan zur Umsetzung der Datenschutz-Grundverordnung (DSGVO) angenommen. In diesem Rahmen haben sich die Subgroups Future of Privacy, Key Provisions und Cooperation vor allem mit strukturellen Fragen des künftigen Europäischen Datenschutzausschusses - dem Nachfolgegremium der Artikel-29-Gruppe - und mit den neuen Verfahren zur Zusammenarbeit und Kooperation der Aufsichtsbehörden in grenzüberschreitenden Fällen befasst. Die Artikel-29-Gruppe hat dabei Leitlinien und Arbeitspapiere zu folgenden Themen erarbeitet:

- Durchführung des sog. One-Stop-Shop- und des Kohärenzverfahrens, einschließlich der Auslegung wichtiger Rechtsbegriffe der DSGVO in diesem Zusammenhang (wie z. B. des Begriffs der Hauptniederlassung);

- gegenseitige Amtshilfe, gemeinsame Maßnahmen und Behördenkooperation in grenzüberschreitenden Fällen;

- Bestimmung der federführenden Aufsichtsbehörde in „One-Stop-Shop"-Fällen;

- betriebliche und behördliche Datenschutzbeauftragte;

- Recht auf Datenübertragbarkeit.

Diese Arbeiten der Artikel-29-Gruppe wurden von mir intensiv begleitet. Dies gilt insbesondere für die Leitlinien zu den Themen „federführende Behörde" und „Datenschutzbeauftragter", für die ich als Ko-Berichterstatter in der Subgroup Key Provisions tätig war. Darüber hinaus habe ich ebenfalls in der Funktion des Ko-Berichterstatters an den Entwurfsarbeiten für eine Geschäftsordnung des Europäischen Datenschutzausschusses mitgewirkt, die 2017 fortgesetzt werden. Die Artikel-29-Gruppe hat für das Jahr 2017 einen weiteren Aktionsplan zur Umsetzung der DSGVO und zur Vorbereitung der Tätigkeit des künftigen Europäischen Datenschutzausschusses beschlossen.

Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit und der Grenzkontrolle

Neben der Umsetzung der EU-Datenschutzreform hat sich die Artikel-29-Gruppe intensiv mit datenschutzrechtlichen Fragen im Sicherheitsbereich befasst. Die Arbeiten der Gruppe standen ganz im Zeichen der Verhandlungen zwischen der EU und den USA zum Privacy Shield (vgl. o. Nr. 2.1). In Wahrnehmung ihrer Beratungsfunktion hat die Border, Travel, Law Enforcement (BTLE)-Subgroup, bei der ein Mitarbeiter meines Hauses die Funktion eines Koordinators wahrnimmt, die wesentlichen grundrechtlichen und datenschutzrechtlichen Standards bei der Durchführung von Überwachungsmaßnahmen aus der Rechtsprechung des Europäischen Gerichtshofes und des Europäischen Gerichtshofes für Menschenrechte herausgearbeitet und auf dieser Grundlage die US-amerikanische Rechtspraxis analysiert. Diese Auswertung der europäischen Rechtsprechung ist im Arbeitspapier 1/2016 „European Essential Guarantees“ der Artikel-29-Gruppe zusammengefasst. Die Analyse des US-Rechts nimmt wesentlichen Raum in den Stellungnahmen der Artikel-29-Gruppe zum EU-US Privacy Shield ein (Stellungnahme 1/2016 zur EU-US Privacy Shield Adäquanzentscheidung, vgl. o. Nr. 2.1).

Darüber hinaus hat die BTLE-Subgroup eine Vielzahl von Stellungnahmen der Artikel-29-Gruppe zu anderen Gesetzgebungsvorhaben vorbereitet. Dazu zählen unter anderem die EU-PNR-Richtlinie (vgl. u. Nr. 2.3.2), das Smart Borders-Programm (vgl. u. Nr. 2.3.1), das Umbrella Agreement (vgl. o. Nr. 2.2) und die Datenschutzrichtlinie für den Bereich von Polizei und Justiz (vgl. o. Nr. 1.1, Nr. 1.2.2.).

Die Artikel-29-Gruppe hat sich im Berichtszeitraum weiter mit der Frage befasst, ob und unter welchen Voraussetzungen Sicherheitsbehörden Zugriff auf Daten nehmen dürfen, die nicht auf inländischen Servern gespeichert sind. Diese Problematik stellt sich in Zeiten der Globalisierung, des Internets und der Speicherung von Daten in „Clouds“ in besonderem Maße. Große Beachtung hat in diesem Zusammenhang ein Gerichtsverfahren erlangt, auf das ich schon in meinem letzten Tätigkeitsbericht hingewiesen hatte (vgl. 25. TB Nr. 4.7.1). Es wurde durch die Firma Microsoft angestoßen, die in den USA auf Antrag einer US-Sicherheitsbehörde verpflichtet worden war, Daten zu einem Kunden-E-Mail-Konto herauszugeben, die auf Servern in Irland gespeichert sind. Inzwischen hat ein US-Berufungsgericht hierüber entschieden und die US-Regierung auf den Weg der Rechtshilfe verwiesen, um auf die in Irland gespeicherten Daten zugreifen zu können. Nach Auffassung des Berufungsgerichts erlaubt das geltende US-Recht keinen unmittelbaren Zugriff. Der endgültige Ausgang dieses Verfahrens ist noch offen, ebenso wie die grundsätzliche Fragestellung des behördlichen Zugriffs auf im Ausland gespeicherte personenbezogene Daten, die von allen Rechtsordnungen beantwortet werden muss.

Internationaler Steuerdatenaustausch und Geldwäsche

Ein weiteres Themengebiet der Artikel-29-Gruppe betraf den internationalen automatischen Steuerdatenaustausch (vgl. u. Nr. 8.2.4) und die Anpassung der geldwäscherechtlichen Regelungen durch die Vierte und Fünfte EU-Geldwäscherichtlinie (vgl. u. Nr. 8.2.2). Im Mittelpunkt der geldwäscherechtlichen Diskussion stehen der transparente Geldfluss und die Frage, wie und in welchem Umfang Bargeldzahlungen beibehalten werden sollen. Hierzu habe ich an einer Konsultation zu einer von der Europäischen Kommission in Auftrag gegebenen Studie teilgenommen, deren Ergebnisse in die Vorschläge für eine zukünftige EU-Gesetzgebung eingebracht werden sollen.

Datenschutz beim E-Government

Schließlich prüft die Artikel-29-Gruppe den „Code of Conduct on privacy for mHealth“, der ein System der freiwilligen Selbstverpflichtung etabliert und vordringlich Entwickler sowie Hersteller mobiler Gesundheitsanwendungen anspricht. Er wurde der Artikel-29-Gruppe im Juni 2016 vorgelegt. Die Subgroup E-Government ist derzeit mit den Verfassern des Code of Conduct im Gespräch, um auf Verbesserungen des Datenschutzniveaus hinzuwirken. Anhand dieses Dokumentes werden die wesentlichen datenschutzrechtlichen Vorgaben für mobile Anwendungen auf europäischer Ebene abgestimmt (vgl. u. Nr. 1.5).

Datenschutz bei neuen Technologien

Aus der Arbeit der Technology Subgroup der Artikel-29-Gruppe ist insbesondere eine Empfehlung zur Nutzung von Drohnen (vgl. u. Nr. 10.2.6) zu nennen sowie eine Stellungnahme zur Überarbeitung der ePrivacy-Richtlinie (EU-Datenschutzrichtlinie für elektronische Kommunikation) (vgl. u. Nr. 17.2.4.1).

Koordinierung nationaler Durchsetzungsmaßnahmen

Die Ende 2016 wieder aktivierte Subgroup Enforcement soll sich künftig damit beschäftigen, die anderen Subgroups bei den erforderlichen nationalen Durchsetzungsmaßnahmen zu koordinieren und entsprechende Verfahrensweisen zu harmonisieren. Die erste Aktivität dieser Subgroup galt dem Messenger-Dienst WhatsApp. Nach dessen Übernahme durch Facebook hat die Artikel-29-Gruppe WhatsApp schriftlich aufgefordert, die Datenübermittlung von personenbezogenen Daten an Facebook für EU-Bürger zu unterlassen. WhatsApp hat entsprechend reagiert und die Datenübermittlung vorrübergehend bis zur endgültigen Klärung der rechtlichen Fragen gestoppt (vgl. u Nr. 17.3.1).

2.5 Europarat

Fortschritte bei der Revision der Datenschutz-Konvention 108

Die Globalisierung des Datenverkehrs hat nicht nur eine Modernisierung des Datenschutzrechts der Europäischen Union erforderlich gemacht, auch der Europarat befasst sich seit dem Jahre 2009 mit der Revision des „Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" (Konvention 108) aus dem Jahre 1981. Im Berichtszeitraum wurden in den Verhandlungen über ein Änderungsprotokoll erhebliche Fortschritte erzielt, eine vollständige Einigung steht indes noch aus.

Nach Abschluss der Beratungen der EU zur Datenschutz-Grundverordnung (vgl. Nr. 1.1) konnten die Arbeiten an der Überarbeitung der Konvention 108 im Berichtszeitraum erheblich voran gebracht werden (vgl. 24. TB Nr. 2.4.3). Im Juni 2016 hat das für die Reform der Konvention Nr. 108 des Europarates eingerichtete „Ad-hoc Committee on Data Protection" (CAHDATA) einen weitgehend konsentierten Protokollentwurf zur Änderung der Konvention an die Berichterstattergruppe „Justizielle Zusammenarbeit" (GR-J) des Europarats weitergeleitet. Dort sollen die wenigen verbliebenen offenen Punkte abschließend verhandelt werden, um die Annahme durch das Ministerkomitee zu ermöglichen. Trotz intensiver Arbeiten der Berichterstattergruppe konnte bis Ende 2016 kein vollständiger Konsens über das Änderungsprotokoll erzielt werden. Die Gründe hierfür lagen unter anderem an der Forderung der Russischen Föderation nach erweiterten Ausnahmeregelungen für Datenverarbeitungen zu Zwecken der nationalen Sicherheit. Zudem bestanden zwischen den EU-Mitgliedstaaten unterschiedliche Auffassungen zur Frage der künftigen Stimmrechtsausübung im Beratenden Konventionsausschuss „T-PD" durch die Europäische Union und die Modalitäten des Inkrafttretens des Änderungsprotokolls. Trotz dieser noch offenen Punkte begrüße ich die erheblichen Fortschritte, die bei der Überarbeitung der Konvention erzielt wurden. Dies gilt zunächst für deren Anwendungsbereich, der sich auf den gesamten öffentlichen und nicht-öffentlichen Bereich erstreckt. Positiv ist herauszustellen, dass die Bundesregierung die Forderung der Russischen Föderation zur vollständigen Ausnahme von Datenverarbeitungen durch Nachrichtendienste aus dem Geltungsbereich der Konvention im Ergebnis nicht mitgetragen hat. Positiv ist zudem, dass der materielle Gehalt des Änderungsprotokolls mit den datenschutzrechtlichen Grundprinzipien, den Betroffenenrechten und Pflichten der verantwortlichen Stelle nunmehr weitgehend mit den Grundsätzen der EU-Datenschutzgrundverordnung und der EU-Datenschutzrichtlinie übereinstimmt, so dass die notwendige Kohärenz zwischen der Konvention und dem neuen EU-Rechtsrahmen erreicht werden konnte. Ein bedeutender Fortschritt für den Datenschutz stellt ferner die in dem Änderungsprotokoll vorgesehene Verpflichtung der Vertragsparteien dar, auf nationaler Ebene unabhängige Aufsichtsbehörden vorzusehen, die über Kontroll- und Sanktionsbefugnisse bei Datenschutzverstößen verfügen und zu Zwecken der Umsetzung der Konvention miteinander kooperieren und gegenseitige Amtshilfe leisten sollen.

Das federführende BMI ist im Jahr 2016 meinem langjährigen Petitum nachgekommen und hat meiner Teilnahme an den datenschutzrelevanten Sitzungen des Europarates zugestimmt. Ich kann jetzt an den Sitzungen des mit der Reform der Datenschutz-Konvention 108 befassten Ad-hoc Datenschutzausschusses des Ministerrates (CAHDATA) und an den Sitzungen des Beratenden Ausschusses nach Artikel 18 der Konvention 108 (Consultative Committee/T-PD) als Beobachterin teilnehmen. Im T-PD wurde mir vom BMI zudem eingeräumt, mich als Vertreterin der unabhängigen Datenschutzaufsicht in Deutschland frei zu äußern. Dies begrüße ich und nehme die neuen Beteiligungsmöglichkeiten aktiv wahr. Dies gilt für die Ressortabstimmungen sowie für die Arbeit im T-PD-Plenum zur Verbesserung der im Jahre 2016 vom T-PD erörterten Leitlinien für Datenschutz im Zusammenhang mit Big Data und Empfehlungen zum Datenschutz im Zusammenhang mit Gesundheitsdaten.

2.6 Internationale Datenschutzkonferenz

Im Berichtszeitraum befassten sich zwei Internationale Datenschutzkonferenzen mit wichtigen Zukunftsthemen und Initiativen zur Verbesserung der globalen Zusammenarbeit.

Die 37. Internationale Datenschutzkonferenz in Amsterdam (26. - 29. Oktober 2015) stand im Zeichen der „Privacy Bridges“. Der mit diesem Motto thematisierte datenschutzrechtliche Brückenbau zwischen der EU und den USA hatte kurz vor Beginn der Konferenz durch die Aufhebung der Safe-Harbor-Entscheidung im sog. Schrems-Urteil des EuGH (vgl. Nr. 2.1) eine noch höhere Bedeutung erlangt.

Zudem standen die datenschutzrechtlichen Herausforderungen der Verarbeitung von Gesundheits- und genetischen Daten sowie Fragen zur Rolle der Datenschutzaufsichtsbehörden im Kontext geheimdienstlicher Überwachungsmaßnahmen im Fokus. Auf der Konferenz wurden drei Resolutionen verabschiedet. Neben den Entschließungen über „Transparenz durch Berichterstattung“ und „Datenschutz und internationale humanitäre Maßnahmen“ ist die Entschließung über die „Zusammenarbeit mit dem Sonderberichterstatter der Vereinten Nationen zum Recht auf Privatheit“ hervorzuheben. Diese von mir eingebrachte Resolution greift eine deutsch-brasilianische Initiative zum Recht auf Privatheit im digitalen Zeitalter bei den Vereinten Nationen auf. Auf die Initiative hin verabschiedete die Generalversammlung der Vereinten Nationen zwei Resolutionen (68/167 vom 18.12.2013 und 69/166 vom 18.12.2014). Sie bildeten die Grundlage für den Beschluss des Menschenrechtsrates der Vereinten Nationen vom 26. März 2015, einen Sonderberichterstatter für das Recht auf Privatheit einzusetzen. Seine Aufgabe ist es, jährlich über Verstöße gegen das Recht auf Privatheit zu berichten, das in der Allgemeinen Erklärung der Menschenrechte und im Internationalen Pakt über bürgerliche und politische Rechte der Vereinten Nationen (UN-Zivilpakt) verbrieft ist. Außerdem soll der Sonderberichterstatter die internationale Debatte zu Fragen des Rechts auf Privatsphäre begleiten. Im Sommer 2015 wurde Professor Joseph Cannataci von der Universität Malta für den Zeitraum von drei Jahren zum Sonderberichterstatter ernannt.

Die 38. Internationale Datenschutzkonferenz in Marrakesch (17. - 20. Oktober 2016) trug das Motto „Opening New Territories for Privacy“. Im Zentrum der Diskussionen standen dementsprechend die Herausforderungen, die die aktuellen Entwicklungen bei Robotertechnik, künstlicher Intelligenz und maschinellem Lernen für die informationelle Selbstbestimmung des Einzelnen und die Fortentwicklung des Datenschutzes mit sich bringen. Die Konferenz diskutierte auch über die Verschlüsselung als ein - angesichts der zunehmenden internationalen Datenströme - immer wichtiger werdendes Instrument zum Schutz personenbezogener Daten. Zudem wurden Entschließungen zu Rahmenbedingungen für Datenschutzerziehung in Schulen, zur Entwicklung neuer Messgrößen für die Datenschutzregulierung, zum Schutz von Menschenrechtsverteidigern und zur Weiterentwicklung der internationalen Zusammenarbeit der Datenschutzaufsichtsbehörden verabschiedet.

Zur Überprüfung der Strategie, Größe und Effektivität der Internationalen Konferenz wurde eine neue Arbeitsgruppe eingesetzt, an der ich mich aktiv beteiligen werde. Dies gilt auch für eine Expertengruppe zur Stärkung der grenzüberschreitenden Kooperation der Aufsichtsbehörden.

Die Entschließungen der Internationalen Datenschutzkonferenzen stehen in englischer Sprache auf meiner Internetseite (www.datenschutz.bund.de) zum Abruf bereit.

Die 39. Internationale Datenschutzkonferenz wird vom 25. - 29. September 2017 in Hongkong stattfinden.

2.7 Europäische Datenschutzkonferenz

Die jährliche Frühjahrskonferenz („Spring Conference") der europäischen Datenschutzbeauftragten befasste sich in den Jahren 2015 und 2016 vor allem mit der praktischen Durchführung des Datenschutzes in Europa und der Umsetzung der neuen Europäischen Datenschutz-Grundverordnung.

Die europäische Datenschutzkonferenz findet in der Regel 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. o. Nr. 2.6). Das Forum dient dem Gedanken- und Erfahrungsaustausch aller europäischen Datenschutzbeauftragten sowie von Vertretern der Europäischen Kommission, des Europarats und der OECD und ist insofern weiter gefasst als die Datenschutzgremien der Europäischen Union. Es schließt insbesondere die Datenschutzbeauftragten aus den Ländern Südosteuropas mit ein.

Die von der britischen Datenschutzbehörde ICO vom 18. - 20. Mai 2015 in Manchester ausgerichtete Frühjahrskonferenz mit dem Titel „Navigating the Digital Future - let's get practical" konzentrierte sich auf die praktische Durchführung des Datenschutzes. Die Diskussionen in verschiedenen Foren befassten sich u. a. mit den Erwartungen der Bürger bei der Durchsetzung ihrer Rechte sowie den Möglichkeiten, die Organisationen und Datenschutzbehörden dabei zur Unterstützung der Bürger haben.

Bei der Frühjahrskonferenz am 26. und 27. Mai 2016 in Budapest wurden vor allem die Umsetzung der Europäischen Datenschutz-Grundverordnung (DSGVO) auf europäischer und nationaler Ebene sowie das Verhältnis der DSGVO zur Konvention 108 des Europarats (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) thematisiert. Etliche Teilnehmer sprachen sich für die Harmonisierung nationaler Vorschriften, gesamteuropäische Ansätze und eine verstärkte Zusammenarbeit aus. Der Nutzen europäischer Leitlinien sowie Standards für die Umsetzung der DSGVO wurde betont und für die Harmonisierung nationaler Vorschriften und die Vereinbarung gesamteuropäischer Herangehensweisen geworben.

Die Entschließungstexte der Frühjahrskonferenzen 2015 und 2016 sind auf meiner Internet-Seite abrufbar unter www.datenschutz.bund.de. Die nächste Frühjahrskonferenz wird auf Einladung der zypriotischen Datenschutzbehörde am 27. und 28. April 2017 in Limassol stattfinden.

3 Ausschuss für Arbeit und Soziales

3.1 Auswirkungen der DSGVO auf diesen Themenbereich

Die DSGVO muss ab dem 25. Mai 2018 angewendet werden. Als europarechtliche Verordnung hat sie allgemeine Gültigkeit, ist in allen ihren Teilen verbindlich und gilt unmittelbar in Deutschland und den anderen EU-Mitgliedsstaaten. Die DSGVO ermöglicht den Mitgliedstaaten in begrenztem Umfang Regelungsspielräume, national spezifischeres Recht zu schaffen oder zu erhalten. Entsprechende Regelungen dürfen das Datenschutzniveau der DSGVO aber weder über- noch unterschreiten.

In Deutschland unterliegen bisher sowohl die Arbeitsverwaltung in den Sozialgesetzbüchern als auch der Beschäftigtendatenschutz sowie die gesetzliche Unfall- und Rentenversicherung bereichsspezifischem nationalem Recht. Wie der deutsche Gesetzgeber hier seinen Gestaltungsspielraum nutzen wird, steht noch nicht endgültig fest.

Der nationale Gesetzgeber ist insoweit insbesondere gefordert die Regelungsspielräume des Artikels 88 DSGVO zu nutzen, in deren Rahmen er den Beschäftigtendatenschutz spezifisch regeln kann. Hierzu soll im Datenschutz-Anpassungs- und Umsetzungsgesetz EU zunächst eine dem bisherigen § 32 BDSG entsprechende Bestimmung aufgenommen werden. Ob und inwieweit darüber hinaus bereits in diesem Gesetz weitere spezifische beschäftigungsdatenschutzrechtliche Regelungen getroffen werden, ist noch offen (vgl. u. Nr. 3.2.1).

3.2 Einzelthemen

3.2.1 Beschäftigtendatenschutz

Beim Beschäftigtendatenschutz gab es auf nationaler Ebene kaum Bewegung.

Beschäftigtendatenschutzgesetz - jetzt aber!

Die Bundesregierung wollte beim Beschäftigtendatenschutz in der laufenden Legislaturperiode die Reform des europäischen Datenschutzrechts abwarten. Jetzt ist die DSGVO beschlossen und ermöglicht den Mitgliedstaaten, spezifischere nationale Regelungen zum Schutz der Beschäftigtendaten zu erlassen. Dies sollte jetzt aber auch dringend genutzt werden!

Der Beschäftigtendatenschutz ist bisher gesetzlich nur unzureichend in § 32 BDSG geregelt. Viele Fragen zu einem angemessenen Ausgleich zwischen berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers sind umstritten. Eine Streitklärung für die Betroffenen bleibt daher der Datenschutzaufsicht und den Gerichten überlassen. Seit Jahren fordern meine Länderkollegen und ich daher ein Beschäftigtendatenschutzgesetz. So hat die Konferenz der Datenschutzbeauftragten hierzu mehrere Entschließungen gefasst, zuletzt im März 2014 (vgl. 25. TB Nr. 9.3.1).

Dieser unbefriedigende Rechtszustand wird auch mit der DSGVO zunächst erhalten bleiben. Der hier einschlägige Artikel 88 DSGVO verzichtet auf detaillierte Regelungen und legt lediglich fest, der Beschäftigtendatenschutz habe sich an der Wahrung der Menschenwürde, den berechtigten Interessen und Grundrechten der betroffenen Personen sowie dem Transparenzgedanken auszurichten. Nicht ohne Grund sieht die DSGVO auch Regelungsspielräume für die Mitgliedstaaten vor. Sie können spezifischere und damit an die jeweiligen nationalen Gegebenheiten angepasste beschäftigungsdatenschutzrechtliche Vorschriften erlassen, deren Regelungsniveau sich im Rahmen der DSGVO bewegen muss.

Zu dem Ergebnis, es bedürfe eines national geregelten Beschäftigungsdatenschutzes, ist auch das federführende BMAS im Rahmen seines Konsultationsprozesses zum Thema „Arbeiten 4.0“ gekommen. Im abschließenden Weißbuch kündigt das Ministerium an, zeitnah einen interdisziplinär besetzten Beirat einzurichten, der den Auftrag erhält, bereichsspezifische Regelungen für den Beschäftigtendatenschutz im Rahmen eines verbindlichen Zeitplans vorzubereiten. Ich bin gerne bereit, hier meine datenschutzrechtliche Expertise einzubringen.

Regelungsbedarf für ein neues Beschäftigtendatenschutzrecht sehe ich insbesondere in folgenden Bereichen:

- Datenschutz im Bewerbungsverfahren,
- Gestaltung des Arbeitsverhältnisses und Compliance-Fragen,
- Personalentwicklung und Persönlichkeitsprofile,
- Umgang mit Gesundheitsdaten
- Überwachungssysteme am Arbeitsplatz,
- Einsatz von biometrischen Verfahren und Big Data Anwendungen,
- Private Nutzung dienstlicher Kommunikationsmittel
- Dienstliche Nutzung privater Kommunikationsmittel,
- Transparenz der Datenverarbeitung,
- Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben und
- Whistleblowing.

Ich werde mich weiterhin für die zeitnahe Verabschiedung eines Beschäftigtendatenschutzgesetzes einsetzen.

3.2.2 ... aus dem Bereich der Arbeitsverwaltung

Bei den Jobcentern konnte in den letzten zwei Jahren das Niveau in den Bereichen Sozial- und Personaldatenschutz durch gemeinsame Anstrengungen und eine gute Zusammenarbeit mit meiner Dienststelle weiterhin verbessert werden.

Im Bereich der Arbeitsförderung war die Prüfung zentraler IT-Verfahren der Bundesagentur für Arbeit (BA) im Berichtszeitraum Gegenstand meiner Beratungs- und Kontrolltätigkeit. Im Juli 2015 hat die BA ihre IT-Strategie 2020 beschlossen. Darin ist vorgesehen, dass Geschäftsprozesse digitalisiert und neue Online-Angebote für die Kunden entwickelt werden sollen. Hintergrund ist die Neuausrichtung der BA in der „Entwicklungsperspektive BA 2020“.

3.2.2.1 Übermittlung von Sozialdaten der Jobcenter an Polizei und Staatsanwaltschaften

Der Sozialdatenschutz muss auch dann beachtet werden, wenn Polizeibehörden oder Staatsanwaltschaften um die Übermittlung von Sozialdaten bitten.

Aus Eingaben von Petenten wurde mir bekannt, dass Polizeibehörden oder Staatsanwaltschaften in Einzelfällen Jobcenter bitten, Sozialdaten zu übermitteln. Einzelne Jobcenter haben sich von mir daraufhin beraten lassen, unter welchen Voraussetzungen und in welchem Umfang sie die erbetenen Sozialdaten datenschutzkonform übermitteln können. Zwar sind auch Jobcenter nach der Strafprozessordnung verpflichtet, Auskunft zu erteilen. Die datenschutzrechtlichen Vorschriften im Zweiten Kapitel des SGB X gehen der Strafprozessordnung jedoch als spezialgesetzliche Regelungen vor. Deshalb ist eine Übermittlung nur dann zulässig, wenn eine Übermittlungsbefugnis nach dem Sozialgesetzbuch vorliegt. Infrage kommen hier insbesondere die §§ 68, 69 und 73

SGB X. Grundvoraussetzung ist dabei, dass die Polizeibehörden oder Staatsanwaltschaften ihre Übermittlungsersuchen nachvollziehbar schriftlich begründen. Ist für das Jobcenter anhand des vorliegenden Sachverhaltes nicht ersichtlich, ob eine Übermittlungsgrundlage besteht, kann es versuchen, den Sachverhalt aufzuklären oder muss das Ersuchen ablehnen. Hierzu ist es nach § 35 Absatz 3 SGB I ausdrücklich berechtigt, da ohne eine Übermittlungsbefugnis die Auskunftspflicht gegenüber der Staatsanwaltschaft oder Polizeibehörde nicht besteht.

Die Jobcenter (und nicht die anfragende Stelle) tragen die Verantwortung für eine datenschutzkonforme Übermittlung der Sozialdaten (§ 67d Abs. 2 Satz 1 SGB X) und zwar auch dann, wenn eine Polizeibehörde oder Staatsanwaltschaft um Sozialdatenübermittlung ersucht. Denn diese sind nur für die Richtigkeit ihrer Angaben im Übermittlungsersuchen verantwortlich.

Es lässt sich festhalten, dass die Übermittlung von Sozialdaten an die Staatsanwaltschaft und Polizeibehörden unter Beachtung der dafür vorgegebenen Voraussetzungen grundsätzlich möglich ist. Allerdings sind die Polizeibehörden und Staatsanwaltschaften angesichts des besonderen Sozialdatenschutzrechts gehalten, den Jobcentern ein ausreichend begründetes und am erforderlichen Umfang (Datensparsamkeitsgrundsatz) ausgerichtetes Übermittlungsersuchen vorzulegen. Andernfalls dürfen die Jobcenter keine Sozialdaten übermitteln.

3.2.2.2 Plakativer Werbeaufdruck „JOBBÖRSE“ auf Briefen der Bundesagentur für Arbeit wurde rechtzeitig gestoppt

Briefe mit deutlich sichtbarem Logo der Jobcenter verstoßen gegen den Datenschutz. Gleiches gilt für einen plakativen Werbeaufdruck „JOBBÖRSE“ auf zentralen Briefumschlägen der Bundesagentur für Arbeit im Bereich der Grundsicherung für Arbeitssuchende (SGB II).

Die Bundesagentur für Arbeit (BA) hat mich frühzeitig in ihre Überlegungen eingebunden, einen Werbeaufdruck „JOBBÖRSE“ auf Briefumschlägen im Bereich des SGB II zu verwenden. Ein entsprechendes Muster mit den Originalmaßen des Aufdrucks von 7 x 5,5 Zentimeter in den Farben Rot, Grau und Schwarz war beigefügt. Hintergrund war meine bisher vertretene Rechtsauffassung: Die Verwendung eines solchen Logos, das entweder das Jobcenter oder die BA erkennen lässt, halte ich für datenschutzwidrig, da Dritte bereits bei flüchtiger Betrachtung erkennen können, dass der Empfänger der Briefsendung ein potentieller Leistungsempfänger ist (vgl. 25. TB Nr. 9.1.7).

Die BA und die Jobcenter sind nach § 78a SGB X bei einem zentralen oder dezentralen Postversand aber gesetzlich verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, um den Anspruch des Sozialgeheimnisses nach § 35 SGB I zu gewährleisten. So konnte durch die frühzeitige Einbindung meiner Behörde die Umsetzung einer weiteren datenschutzwidrigen Werbung der BA rechtzeitig vermieden werden.

3.2.2.3 Einsatz privater Sicherheitsdienste in den Jobcentern

In ihrem Arbeitsumfeld verzeichnen die Jobcenter in letzter Zeit eine gestiegene Aggressionsbereitschaft bei Besuchern. Deshalb werden dort immer häufiger private Sicherheitskräfte eingesetzt.

Beschäftigte und Besucher der Jobcenter sehen sich zunehmend Übergriffen und Bedrohungen durch aggressives verbales oder physisches Verhalten ausgesetzt. Das Spektrum dieser Gewalt umfasst sowohl Angriffe der Besucher untereinander als auch gegenüber Mitarbeiterinnen und Mitarbeitern bis hin zu Gewaltdelikten. Immer wieder wird darüber auch in den Medien berichtet.

Viele Jobcenter beauftragen deshalb zunehmend private Sicherheitsdienste, um die Sicherheit aller sich im Jobcenter aufhaltenden Personen sowie den Gebäudeschutz zu erhöhen. Damit kommen sie ihrer Verpflichtung nach, einen geordneten Dienstbetrieb aufrecht zu erhalten. Die Jobcenter verfügen in den jeweiligen Liegen-

schaften über das Hausrecht und sind deshalb berechtigt, private Sicherheitsdienste zu beauftragen, um die ungestörte Wahrnehmung ihrer Verwaltungsaufgaben sicherzustellen.

Datenschutzrechtlich relevant ist diese Einbindung privater Sicherheitsdienste, weil deren Mitarbeiter Kenntnis von Sozialdaten nehmen können. In vielen Fällen sind nämlich gerade diese mit der Zutrittskontrolle beauftragt. Dabei sehen sie entweder das Einladungsschreiben und/oder Ausweisdokumente des Besuchers und nehmen insoweit Sozialdaten zur Kenntnis. Darüber hinaus werden Mitarbeiter des Sicherheitsdienstes auch dann hinzugezogen, wenn ein aggressives Verhalten während der Vorsprache zu erwarten ist. Auch in diesen Fällen ist nicht ausgeschlossen, dass sie Kenntnis von Sozialdaten nehmen. Sie halten sich dann räumlich in der Nähe des geführten Kundengesprächs auf, so dass unter Umständen entsprechende Informationen mitgehört werden können. Zwar handelt es sich bei den Sicherheitsdienstmitarbeitern nicht um Beschäftigte der Jobcenter, sie werden aber vertraglich zur Wahrung des Datenschutzes verpflichtet. Aus diesen Gründen habe ich keine beanstandungswürdige Verletzung des Datenschutzes erkennen können, wenn private Sicherheitsdienste von Jobcentern beauftragt wurden.

Gleichwohl halte ich es für geboten, diese Aufgabenwahrnehmung über die Befugnisse aus dem Hausrecht hinaus auch auf eine vertragliche Rechtsgrundlage zu stellen. Ich habe daher das Bundesministerium für Arbeit und Soziales (BMAS) gebeten, die Muster- und Rahmenverträge so überarbeiten zu lassen, dass der Einsatz privater Sicherheitsdienste im Rahmen der Auftragsdatenverarbeitung vertraglich geregelt wird. Die vom BMAS damit beauftragte BA hat zwischenzeitlich die Rahmenverträge entsprechend angepasst und wird sie nach der Schlussabstimmung mit dem BMAS allen Jobcentern zur Verfügung stellen. Damit wird hier zukünftig datenschutzrechtlichen Belangen deutlich besser Rechnung getragen.

3.2.2.4 Weiterentwicklung der E-Akte

Nach der von mir begleiteten Einführung der E-Akte bei der BA (vgl. 24. TB Nr. 12.2.1, 25. TB Nr. 23.4) muss diese jetzt in der Anwendung auch datenschutzkonform genutzt werden.

Seit der Einführung der E-Akte hat die BA ihre Arbeitsabläufe neu strukturiert. So wurde den Service-Centern der BA im Bereich des SGB III zentral die Aufgabe übertragen, Kundenanliegen zu bearbeiten, die telefonisch oder per E-Mail an die BA herangetragen werden. Nur wenn die Anfragen spezifisches Fachwissen erfordern, werden sie an die zuständigen Bearbeiter in den Arbeitsagenturen weitergeleitet. Die Beschäftigten in den Service-Centern haben daher inzwischen deutlich erweiterte Zugriffe auf die in der E-Akte gespeicherten Daten.

Ich habe mich bei einem Besuch in einem Service-Center hierüber näher informiert und im Anschluss das Ausmaß der Zugriffsmöglichkeiten gegenüber der BA kritisiert. Leider hat die BA mir bis heute nicht erklärt, warum alle Beschäftigten in den Service-Centern einen bundesweiten und zeitlich nicht eingeschränkten Zugriff auf die E-Akte der BA-Kunden im Bereich des SGB III haben müssen. Daher habe ich sie aufgefordert, den bundesweiten Zugriff auf wenige Beschäftigte zu beschränken. Außerdem müssen die Zugriffsmöglichkeiten aller Beschäftigten in den Service-Centern zeitlich begrenzt werden. Ich halte es für ausreichend, wenn nur noch auf die Daten der zwei vorangegangenen Jahre in der E-Akte zugegriffen werden kann. Darüber hinausgehende Zugriffsmöglichkeiten sind aus meiner Sicht nicht erforderlich.

Auch zu anderen Fragestellungen des aktuellen fachlichen Berechtigungskonzepts zur E-Akte befinde ich mich zurzeit in Abstimmung mit der BA und hoffe, hier zeitnah ein datenschutzkonformes Ergebnis zu erreichen.

3.2.2.5 Das neue IT-Verfahren für Stammdatenerfassung STEP

*Seit dem 20. April 2015 ist das **St**ammdaten**e**rfassungssystem und Stammdaten**p**flegesystem STEP das zentrale Stammdatensystem der BA. Es integriert die bisherigen Basisdienste in einer webbasierten Anwendung.*

Die BA hat 2015 die neue webbasierte IT-Anwendung STEP zur Erfassung der Stammdaten aufgesetzt. Dieses IT-Fachverfahren ersetzt die bisherigen Stammdatenverfahren zPDV und zBTR, die aufgrund ihrer veralteten Programmstruktur nicht mehr gepflegt werden konnten. Die beiden bisherigen Verfahren waren mit einer zentralen Datenbank verknüpft, über die sie auf die dort abgelegten Stammdaten zugreifen konnten. Die verknüpfte, zentrale Datenbank ist bestehen geblieben und wurde in STEP integriert, so dass eine Datenmigration von zPDV und zBTR in STEP entbehrlich gewesen ist. Mit STEP ist es der BA möglich, alle Stammdaten der BA (Personendaten und Betriebedaten) in einem einzigen IT-Fachverfahren zu vereinen. Damit ist STEP das zentrale Stammdaten-IT-Fachverfahren der BA sowohl für den Bereich des SGB II und des SGB III als auch für die Familienkassen der BA.

Den von mir während der Pilotierungsphase festgestellten Verbesserungsbedarf hat die BA aufgegriffen und überwiegend umgesetzt. Ein Punkt ist allerdings noch offen geblieben. In der Sache geht es um das Protokollierungskonzept zu STEP, wonach Protokolldaten für mindestens 90 Tage aufbewahrt werden sollen. Zu den Protokolldaten gehören sowohl personenbezogene Beschäftigtendaten als auch Daten zu zahlungsbegründenden Unterlagen. Insgesamt halte ich eine Aufbewahrungsfrist der Protokolldaten von höchstens 90 Tagen für angemessen und ausreichend, zumal in begründeten Ausnahmefällen die Löschung der Protokolldaten ausgesetzt werden kann. Ich habe die BA daher gebeten, in Hinblick auf zahlungsbegründende Unterlagen mit dem Bundesministerium der Finanzen abzustimmen, welche kassenrechtlichen Gründe zwingend für eine längere Speicherdauer der Protokolldaten als 90 Tage sprechen.

3.2.3 ... aus dem Bereich der Gesetzlichen Unfall- und Rentenversicherung

Im Bereich der gesetzlichen Unfall- und Rentenversicherung haben mich im Berichtszeitraum sowohl Themen, die seit Jahren auf der Agenda stehen, als auch ganz neue Themen beschäftigt.

Bei der gesetzlichen Unfallversicherung ist die Auslegung der Gutachterregelung in § 200 Absatz 2 SGB VII noch immer ein virulentes Thema. Die Eingabezahlen zu diesen Fragen haben sich erhöht (vgl. u. Nr. 3.2.3.2).

Die Zusammenarbeit in datenschutzrechtlichen Fragen mit der gesetzlichen Rentenversicherung ist seit vielen Jahren gut. Umso ärgerlicher war deswegen meine Feststellung, dass die meisten von der DRV Bund betriebenen Rechner noch mit einem veralteten Betriebssystem ausgestattet waren, was eine Gefahr für die unter dem besonderen Schutz des Sozialrechts stehenden Daten der Versicherten bedeutete. Gerade in der heutigen Zeit muss nicht nur, aber gerade auch bei den Sozialversicherungsträgern deutlich mehr im Bereich der IT-Sicherheit getan werden. Diese sind aufgefordert, proaktiv für mehr Sicherheit bei den ihnen anvertrauten Sozialdaten zu sorgen (vgl. u. Nr. 3.2.3.4).

3.2.3.1 Umfang und Einschränkungen bei Akteneinsicht und Auskunft nach dem Sozialgesetzbuch

Ein Versicherter kann seine Rechte in allen Bereichen der Sozialversicherung nur dann geltend machen, wenn er sich umfassend über die zu seiner Person gespeicherten Sozialdaten informieren kann. Daher die große Bedeutung von Akteneinsichts- und Auskunftsrechten.

Einer der Kernsätze des sog. Volkszählungsurteils des Bundesverfassungsgerichtes vom 15. Dezember 1983 (1 BvR 209/83) ist die Feststellung, mit dem Recht auf informationelle Selbstbestimmung sei eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Unmittelbar im Zusammenhang mit dieser Feststellung stehen die Akteneinsichts- und Auskunftsrechte des Zehntes Buches Sozialgesetzbuch (SGB X). Gleichwohl haben sich Betroffene auch in diesem Berichtszeitraum immer wieder bei mir beschwert, weil ihnen diese Rechte nicht oder nicht in ausreichendem Ausmaße gewährt würden.

So war ich mit der Frage befasst, wie weit das Akteneinsichtsrecht nach § 25 SGB X reicht. Dieses Recht steht grundsätzlich allen an einem Verfahren Beteiligten zu. Es gilt aber vor Abschluss des Verfahrens nicht für Entwürfe der Entscheidungen und für Vorbereitungsarbeiten (§ 25 Absatz 1 Satz 2 SGB X).

Die Unfallversicherungsträger vertreten unter Berufung auf diese Ausnahmeregelung die Auffassung, eine Behörde habe das Recht, Überlegungen, die für den Betroffenen letztendlich irrelevant seien, nicht offen zu legen. Ich halte dies für problematisch, da keine klaren Kriterien dafür bestehen, welche Daten noch zu den bloßen Entwürfen einer Entscheidung und welche Daten zu den Grundlagen der Entscheidung zählen. Im Sinne der Verfahrenstransparenz fordere ich daher, grundsätzlich alle Aktenbestandteile für eine Akteneinsicht zur Verfügung zu stellen. Sollte ein Unfallversicherungsträger in ganz seltenen Ausnahmefällen von seiner o. a. Ausnahmeregelung Gebrauch machen wollen, ist dies konkret zu begründen. Die Entwürfe wären dann zu sperren und für eine mögliche spätere Überprüfung aufzubewahren. Für diese Handhabung des § 25 Absatz 1 Satz 2 SGB X werde ich mich weiterhin einsetzen.

Die Deutsche Gesetzliche Unfallversicherung (DGUV) hatte in einem anderen Fall die Auffassung vertreten, der Versicherte habe lediglich gegenüber dem zuständigen Unfallversicherungsträger, nicht aber gegenüber dem Gutachter selbst ein Akteneinsichtsrecht oder ein Auskunftsrecht bezüglich des vom ihm erstellten Gutachtens. Der Unfallversicherungsträger schließe mit dem Gutachter einen Werkvertrag ab, sodass das geschuldete Werk Teil der Verwaltungsakte werde. Der Versicherte habe daher lediglich ein Akteneinsichtsrecht nach § 25 SGB X gegenüber dem Unfallversicherungsträger.

Ich habe die DGUV überzeugen können, diese Auffassung aufzugeben. Denn durch einen mit dem Gutachter abgeschlossenen Vertrag können gesetzlich normierte Rechte grundsätzlich nicht abbedungen werden. Für den Anwendungsbereich des Bundesdatenschutzgesetzes legt § 6 BDSG ausdrücklich fest, dass Rechte eines Betroffenen auf Auskunft nach § 19 BDSG und § 34 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können. Darüber hinaus ist zu beachten, dass durch den geschlossenen Werkvertrag auch Patientenrechte nach § 630g BGB ausgeschlossen würden, nach denen der Begutachtete das Gutachten auch direkt von dem Arzt herausverlangen könnte.

In den mit Gutachtern geschlossenen Verträgen wird nunmehr ausdrücklich festgelegt, dass eigene Rechte des Versicherten gegen den Gutachter auf Auskunft unberührt bleiben.

3.2.3.2 Weitere Einschränkung der Gutachterregelung im SGB VII

Seit der Einfügung des § 200 Absatz 2 SGB VII in das Sozialgesetzbuch habe ich eine gesetzliche Klarstellung dieser Gutachterregelung gefordert.

Am 1. Januar 1997 war die Gutachterregelung in Kraft getreten, nach der die Versicherten unter drei Vorschlägen einen Gutachter auswählen können und auf das Recht hinzuweisen sind, der Übermittlung ihrer Daten an einen Gutachter zu widersprechen. Seitdem haben die Unfallversicherungsträger versucht, den Anwendungsbereich und die Bedeutung der ungeliebten Vorschrift einzuschränken. Obwohl der Wortlaut des § 200 Absatz 2 SGB VII die Gewährung dieser Rechte anordnet, wird dies aber immer wieder durch juristische Spitzfindigkeiten unterlaufen. Deswegen habe ich wiederholt eine gesetzliche Klarstellung des § 200 Absatz 2 SGB VII angemahnt, damit die Versicherten nicht hilflos intransparenten Verfahren in der gesetzlichen Unfallversicherung ausgeliefert sind (vgl. 25. TB Nr. 9.6). Auch zwanzig Jahre nach Einführung der Gutachterregelung führt diese Norm noch zu vielen Eingaben Betroffener. Dabei konnte ich innerhalb des Berichtszeitraumes eine deutliche Steigerung der Eingabezahlen zur Gutachterregelung feststellen.

Zu meinem Bedauern sieht das zuständige BMAS seit Jahren, zuletzt im Rahmen eines Verfahrens vor dem Petitionsausschuss des Deutschen Bundestages, nicht nur keinen Handlungsbedarf für eine Klarstellung des § 200 Absatz 2 SGB VII, sondern lobt die Vorschrift sogar als gelungenen Ausgleich zwischen den Interessen der Unfallversicherungsträger und den Interessen der Versicherten.

Auch die Sozialgerichtsbarkeit hat leider die Tendenz, den Anwendungsbereich und auch die Bedeutung des § 200 Absatz 2 SGB VII zunehmend einzuschränken. So haben die Unfallversicherungsträger im Berichtszeitraum unter Berufung auf die ständige Rechtsprechung der Sozialgerichte den Einwand der Rügepflichtverletzung erhoben, wenn ein Versicherter von seinem Widerspruchsrecht im Verwaltungsverfahren keinen Gebrauch gemacht bzw. bis zum Schluss der gerichtlichen Verhandlung in der Vorinstanz die Nichtverwertbarkeit des Gutachtens nicht gerügt hat. Die Verletzung der Rügepflicht führe nach ihrer Auffassung dazu, dass ein etwaiger Verstoß gegen die Gutachterregelung nicht mehr geltend gemacht werden könne.

Als Konsequenz verlieren die Versicherten ihre Rechte nach § 200 Absatz 2 SGB VII, wenn sie nicht in der Instanz, in der ein Gutachten eingeführt wurde, die Verwertbarkeit gerügt haben, auch wenn sie auf ihre entsprechenden Rechte zuvor gar nicht hingewiesen worden waren.

Es wird der Bedeutung der Gutachterregelung des § 200 Absatz 2 SGB VII und des grundlegenden Ranges des Widerspruchsrechtsrechts, mit dem der Schutz des informationellen Selbstbestimmungsrechts der Versicherten beabsichtigt war, nicht gerecht, wenn diese Rechte durch die Einrede der Rügepflichtverletzung, das letztlich auf dem Gedanken der Verfahrensbeschleunigung beruht, eingeschränkt werden.

Deswegen sehe ich auch weiterhin den Gesetzgeber in der Pflicht, für die bereits überfällige Klarstellung des § 200 Absatz 2 SGB VII zu sorgen.

3.2.3.3 Einwilligungserklärungen trotz gesetzlicher Erhebungs- und Übermittlungsbefugnis im Sozialrecht

Die Informationsschreiben der Unfallversicherungsträger an die Versicherten zu den geltenden gesetzlichen Regelungen über die Erhebung und Verarbeitung personenbezogener Daten müssen verbessert werden. Dies dient der Transparenz und Vertrauensbildung.

Für Verwirrung sorgt die Praxis der Unfallversicherungsträger, zu Beginn eines Verfahrens mit „Einwilligungserklärung“ überschriebene Formulare zu versenden, mit denen sich die Versicherten mit verschiedenen Datenerhebungen einverstanden erklären sollen.

Für Datenerhebungen bei den gesetzlichen Krankenkassen und bei behandelnden Ärzten gibt es bereits gesetzliche Vorschriften (§ 188 SGB VII bzw. § 203 SGB VII), die den Unfallversicherungsträgern die Befugnis zu dieser Datenerhebung einräumen. Das zusätzliche Einholen einer Einwilligung führt nicht zu transparenten Verfahren. Denn es wäre für einen Versicherten völlig unverständlich, wenn er seine Einwilligung zu diesen Datenerhebungen verweigert, die Unfallversicherungsträger aber - zulässigerweise - aufgrund ihrer gesetzlichen Erhebungsbefugnis die Daten von den Krankenkassen und Ärzten gleichwohl anfordert.

Die Deutsche Gesetzliche Unfallversicherung (DGUV) und die Unfallversicherungsträger haben erkannt, dass die „Einwilligungsformulare“ überarbeitet werden müssen.

Im Hinblick auf eine neue Formulargestaltung bin ich bereits mit der DGUV im Gespräch. Ich bin zuversichtlich, dass es gelingen wird, die erforderlichen Informationen und Befugnisse zur Datenerhebung durch eine transparent gehaltene Formulargestaltung zu verbessern.

3.2.3.4 Probleme bei der Umstellung auf sichere Betriebssysteme in der Rentenversicherung

Auf den Rechnern der DRV Bund waren Betriebssysteme mit datenschutzrechtlichen Risiken installiert. Die Umstellung auf eine aktuelle Software erfolgte nur schleppend.

Obwohl die Firma Microsoft seit April 2014 keinerlei technischen Support inklusive Sicherheitsaktualisierungen für das Betriebssystem Windows XP mehr anbietet, sind noch immer nicht alle PC der DRV Bund auf ein

aktuelles Betriebssystem umgestellt. Bereits im September 2014 hatte ich anlässlich eines Kontroll- und Beratungsbesuchs im Rehabilitationszentrum Bad Kissingen die DRV Bund auf die datenschutzrechtlich bedenkliche Nutzung veralteter Betriebssysteme hingewiesen. Da die DRV Bund auch besondere Arten personenbezogener Daten, insbesondere Gesundheitsdaten, erhebt, nutzt und verarbeitet, besteht aufgrund mangelnder Sicherheit in der Informationstechnik eine erhöhte Bedrohungslage.

Nach den Vorgaben u. a. im IT-Grundschutzhandbuch und Empfehlungen des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) ist eine schnelle Migration auf ein modernes Betriebssystem angezeigt. Nachdem ich dieses Problem regelmäßig und mit Nachdruck angesprochen hatte, teilte mir die DRV Bund mit, bis Mitte Oktober 2016 seien über 22.000 PC auf Windows 7 umgestellt worden, was ca. 90 Prozent des Gesamtbestandes der Standardarbeitsplätze der DRV Bund entspräche. In den Leistungsabteilungen Versicherung, Rente, Rehabilitation und der Zentralen Zulagenstelle für Altersvermögen sowie in den Kliniken der DRV Bund würden nunmehr alle Standardarbeitsplätze über eine aktuelle Software verfügen. Dies begrüße ich ausdrücklich. Leider wurde jedoch bis Ende 2016 noch immer nicht mit der Umstellung in kleineren Außenstandorten, beispielsweise den Auskunfts- und Beratungsstellen aber auch der mobilen IT-Systeme mit Anbindung an das Datennetz der DRV-Bund begonnen.

Wie die DRV Bund angekündigt hat, soll die vollständige Überleitung zu Windows 7 bis zum Ende des ersten Halbjahres 2017 abgeschlossen sein. Dies betrachte ich als allerletzte, nicht mehr verschiebbare Frist. Sollte ich bei Kontrollen nach diesem Zeitpunkt feststellen, dass von der DRV Bund noch immer Windows XP eingesetzt wird, werde ich dies wegen Verstoßes gegen § 9 BDSG förmlich beanstanden.

Die schleppende Migration eines modernen Betriebssystems auf den Rechnern der DRV Bund sehe ich sehr kritisch. Bereits seit Anfang dieses Jahrzehnts stand fest und wurde auch in der Fachpresse kommuniziert, dass der technische Support inklusive Sicherheitsaktualisierungen für das Betriebssystem Windows XP im April 2014 enden werde. Gleichwohl hat die DRV Bund erst reagiert, als die Datenschutzaufsichtsbehörden die unsicheren Betriebssysteme bei ihr kritisiert haben. Sie hätte aber bereits mehrere Jahre vor dem angekündigten Ende des Supports mit den Planungen für die Migration ihrer Rechner auf ein sicheres Betriebssystem beginnen müssen, damit bei Ende des Supports bereits alle Rechner umgerüstet gewesen wären.

3.3 Aus Beratung und Kontrolle

3.3.1 Informationspflichten bei Datenschutzverstößen

Im Berichtszeitraum sind sowohl Sozialleistungsträger als auch sonstige Stellen ihrer gesetzlichen Verpflichtung nachgekommen, mich über „Datenschutzpannen“ in ihrem Verantwortungsbereich zu informieren.

Sozialleistungsträger sind nach § 83a SGB X verpflichtet, mir Datenschutzverletzungen innerhalb ihrer Organisationseinheiten mitzuteilen, wenn sie feststellen, dass dort gespeicherte besondere Arten personenbezogener Daten (vgl. § 67 Absatz 12 SGB X) unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

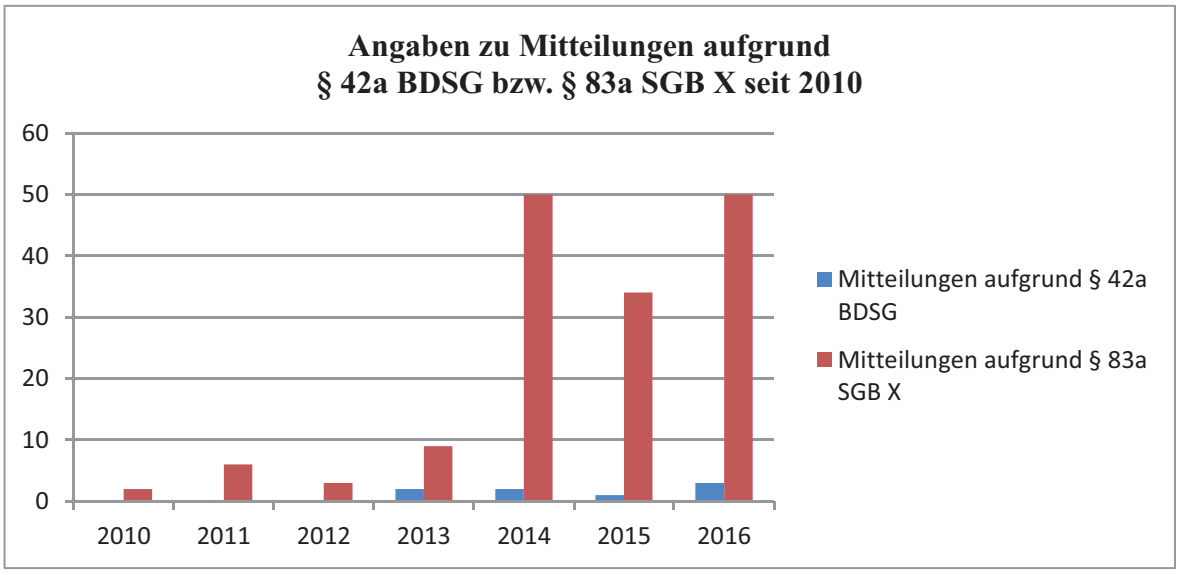
Insgesamt haben mich im Berichtszeitraum 84 Meldungen erreicht. Häufig hat es sich dabei um Datenschutzverstöße gehandelt, die auf ein einmaliges Fehlverhalten einzelner Mitarbeiter zurückzuführen sind. Auffällig waren die Verluste von Sozialdaten im Rahmen von Postversendungen oder Diebstählen sensibler Unterlagen einschließlich Laptops aus dienstlich genutzten Kraftfahrzeugen. Hier habe ich bei gravierenden Mängeln betroffene Dienststellen zu verbesserten Sicherungsmaßnahmen verpflichtet. Darüber hinaus haben mich insgesamt vier weitere Meldungen anderer öffentlicher Stellen erreicht, die nach § 42a BDSG zur Information verpflichtet sind. Es handelte sich um Einzelfälle, in denen versandte Post nicht beim richtigen Empfänger angekommen ist oder in einem Fall nach einem Einbruch nicht ausgeschlossen werden konnte, dass unberechtigte Dritte Zugang zu schützenswerten personenbezogenen Daten erhalten haben.

Sowohl für die Sozialleistungsträger als auch sonstige Stellen wird ab dem 25. Mai 2018 Artikel 33 DSGVO gelten, so dass derartige Datenschutzverstöße künftig „unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde“, mir gemeldet werden müssen, soweit diese Stellen meiner datenschutzrechtlichen Aufsicht unterliegen.

Kasten zu Nr. 3.3.1

Angaben zu Mitteilungen aufgrund § 42a BDSG bzw. § 83a SGB X seit 2010

	§ 42a BDSG	§ 83a SGB X
2010	0	2
2011	0	6
2012	0	3
2013	2	9
2014	2	50
2015	1	34
2016	3	50



3.3.2 Kontrollen von Jobcentern

Aufgrund von Kundenbeschwerden und bei bundesweiten Beratungs- und Kontrollbesuchen musste ich im Berichtszeitraum erneut datenschutzwidrige Verfahrensweisen feststellen.

Das Sozialgeheimnis (§ 35 SGB I) erfordert, innerhalb des Jobcenters sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Darunter fallen auch angemessene technische und organisatorische Maßnahmen (vgl. § 78a SGB X). Eine solche organisatorische Maßnahme besteht darin, eingehende Post zwingend vor Zugriffen Dritter zu schützen und dazu auch geeignete Außen- und Innenbriefkästen zu verwenden. Ich habe alle in meiner Zuständigkeit liegenden Jobcenter über die Einzelheiten solcher zu treffenden organisatorischen Maßnahmen unterrichtet.

Zudem musste ich ein Jobcenter wegen datenschutzwidriger Erhebung und Speicherung von Kontendaten bei Weiterbewilligungsanträgen beanstanden. So wurden grundsätzlich die vollständigen Auszüge sämtlicher Konten einer Bedarfsgemeinschaft für den vergangenen Bewilligungszeitraum von sechs Monaten angefordert, obschon das Bundessozialgericht höchstrichterlich entschieden hat, dass die Anforderung von Kontoauszügen bei der Beantragung von Leistungen nach dem SGB II grundsätzlich nur für einen zurückliegenden Zeitraum von drei Monaten bei Erst- und Folgeanträgen sowie einmaligen Leistungen erfolgen darf (vgl. 24. TB Nr. 12.1.3.6 und die Urteile des BSG vom 19.09.2008, Az. B 14 AS 45/07 R und 19.02.2009, Az. B 4 AS 10/09 R). Ein längerer Zeitraum kann bei selbstständig tätigen Leistungsberechtigten erforderlich sein, oder es liegen plausible Gründe vor, die eine Bedürftigkeitsprüfung nur dann ermöglichen, wenn im Einzelfall länger zurückliegende Kontoauszüge vorgelegt werden. Anlasslose Vorlagepflicht von Kontendaten über mehr als drei zurückliegenden Monaten halte ich weder für geeignet noch verhältnismäßig, vielmehr liegt in solchen Fällen häufig ein datenschutzrechtliche Verstoß gegen den Grundsatz der Datenvermeidung und Datensparsamkeit nach § 78b SGB X vor.

3.3.3 Online-Portal APOLLO

Ein zentraler Baustein zur Umsetzung der IT-Strategie 2020 der BA ist APOLLO (Antragsportal Leistungen Online). Dieses Portal ist über die Internetseite der BA erreichbar. Es ermöglicht sowohl Arbeitsuchenden als auch Arbeitgebern, bestimmte Leistungen der BA nach dem Dritten Buch Sozialgesetzbuch (SGB III) online zu beantragen. Zudem stehen dem Nutzer des Portals Basisdienste zur Verfügung, z. B. eine Dokumentenablage. Auch bestimmte Mitteilungen an die BA, wie die Arbeitsuchend-Meldung oder Veränderungsmitteilungen, können über das Portal gesendet werden. Zukünftig will die BA ihre Leistungen komplett über das Portal online abwickeln.

Eine Kontrolle von APOLLO zeigte noch Schwachpunkte des Portals in Hinblick auf die Authentifizierung der Nutzer, die Integrität und Authentizität der über APOLLO übermittelten Dokumente sowie die mangelhafte Trennung zwischen Bereichen, die reine Information durch die BA darstellen und solchen, die der Aufgabenerfüllung der BA nach dem Sozialgesetzbuch dienen.

APOLLO steht grundsätzlich jedem Internetnutzer offen. Zur Nutzung der im Portal angebotenen „eServices“ bedarf es einer Registrierung über den „Single Sign On“ der BA. Hierbei kann der Nutzer zwischen fünf Sicherheitsstufen wählen: von „keine Überprüfung“, über die Bestätigung der Identität des Nutzers, über E-Mail oder PIN-Brief, bis zur Nutzung der Identifizierungsfunktion von Personalausweis oder Aufenthaltstitel bzw. der Vorlage des Ausweises in einer Arbeitsagentur. Grundlage für die Nutzung der bisher freigeschalteten E-Services sind aber nur Sicherheitsstufen bis zur Identitätsbestätigung über PIN-Brief. Das sehe ich kritisch. Die Authentifizierung der Nutzer von Online-Portalen ist die zentrale Grundlage für dessen datenschutzgerechten Betrieb. Für die Übermittlung von Sozialdaten und die Auszahlung von Leistungen reichen die bisher gewählten Sicherheitsstufen nicht aus. Zur Behebung dieser eingeräumten Mängel hat mir die BA Vorschläge für ein verbessertes Authentifizierungsverfahren unterbreitet. Ich erwarte eine zeitnahe Umsetzung dieser Vorschläge und empfehle dringend, für weitere Ausbaustufen von APOLLO höhere Sicherheitsstufen zu wählen.

Ist der Nutzer mit der entsprechenden Sicherheitsstufe in APOLLO registriert, kann er online seine Anträge ausfüllen, speichern und bearbeiten, die notwendigen Anlagen in die Dokumentenablage hochladen und alles an die BA übersenden. Die Antragsformulare und die hochgeladenen Dokumente werden dabei über eine Schnittstelle direkt in der elektronischen Akte der BA abgelegt. Diese Dokumente sind weder unterschrieben noch elektronisch signiert und damit nicht manipulationssicher.

Neben der Feststellung, dass der Nutzer die Person ist, auf die sich die im Portal angegebenen Daten beziehen, muss im Online-Portal auch sichergestellt werden, dass Daten, die auf diesem Weg in Anträgen oder Dokumenten übermittelt werden, mit den ursprünglich eingegebenen Daten übereinstimmen. Manipulationen durch Dritte sind während der gesamten Verarbeitungsdauer auszuschließen. Der bisher in APOLLO vorgesehene, rein technisch über eine Schnittstelle ausgestaltete Schutz vor Manipulation reicht hierzu nicht aus. Ich habe die BA gebeten, zu prüfen, wie die Integrität der Dokumente besser sichergestellt werden kann. Langfristig habe ich empfohlen, qualifizierte elektronische Signaturen und De-Mail in APOLLO zu integrieren.

Schließlich wird in APOLLO und in dem seit 1. Dezember 2016 auf der Internetseite der BA vorgeschalteten **A**nwender**p**ortal **O**nline**k**anal (APOK) nicht transparent genug zwischen Bereichen, die reine Information durch die BA darstellen, und solchen Bereichen, die der Aufgabenerfüllung nach dem Sozialgesetzbuch dienen, getrennt. Die Datenerhebung, -verarbeitung und -nutzung unterliegt aber jeweils eigenen Rechtsgrundlagen mit unterschiedlicher Reichweite. Personen, die sich lediglich als Nutzer registrieren, um sich die Informationsangebote der BA z. B. mit Merklisten zu strukturieren, unterfallen den Regelungen des Telemediengesetzes. Stellt ein Nutzer hingegen einen Antrag auf Arbeitslosengeld, sind seine personenbezogenen Daten durch das Sozialgeheimnis geschützt. Die Vorschriften nach dem Sozialgesetzbuch erlauben hier allerdings eine deutlich weitergehende Datenerhebung, -verarbeitung und -nutzung, um der BA die Aufgabenerfüllung zu ermöglichen. Der Nutzer muss also wissen, wann er in Bereiche wechselt, die der Aufgabenerfüllung der BA dienen und was das für seine personenbezogenen Daten bedeutet.

Ich habe die BA aufgefordert, die entsprechenden Bereiche klarer voneinander zu trennen und die Nutzungsbedingungen und die Datenschutzerklärung anzupassen.

3.3.4 Kontrolle einer Leistungsabteilung der Deutschen Rentenversicherung Bund

Ein weiterer Kontroll- und Beratungsbesuch in einer Leistungsabteilung der DRV Bund offenbarte Handlungsbedarf bei der datenschutzkonformen Vernichtung von Unterlagen.

Erneut habe ich in einer großen Leistungsabteilung der DRV Bund in verschiedenen Organisationseinheiten den Umgang mit personenbezogenen Daten der Versicherten geprüft. Insbesondere habe ich dabei darauf geachtet, wie die bei meinem dortigen Beratungs- und Kontrollbesuch im Jahr 2010 (vgl. 23. TB Nr. 11.1.9) von mir empfohlenen technischen und organisatorischen Maßnahmen im aktuellen Praxisbetrieb umgesetzt worden waren.

Wie der Besuch gezeigt hat, sind zahlreiche meiner damaligen datenschutzrechtlichen Empfehlungen von der DRV Bund umgesetzt worden. Leider musste ich aber datenschutzrechtliche Mängel bei der Vernichtung von Unterlagen mit sensiblen Sozialdaten feststellen. So hatte sich z. B. in einigen Dezernaten - entgegen der damaligen Zusage der DRV Bund - eine Verfahrensweise ausgebildet, die auch unberechtigten Dritte (externes Reinigungspersonal) Zugang zu Sozialdaten der Versicherten ermöglichte. Die DRV Bund hat sofort reagiert, diese Praxis umgehend noch während meines Besuches abgestellt und eine datenschutzgerechte Verfahrensweise eingeführt, von deren Umsetzung ich mich bei einem weiteren Beratungsbesuch überzeugen konnte. Von einer förmlichen Beanstandung des Datenschutzverstoßes gemäß § 81 Absatz 2 SGB X in Verbindung mit § 25 Absatz 2 BDSG habe ich deshalb abgesehen.

A. Zudem von besonderem Interesse

Nr. 1,1; 1.2 f., 1.6; 10.2.11.3; 21.1; 21.5; 28.5; 28.6 , 28.7; 28.9

4 Auswärtiger Ausschuss, Ausschuss für die Angelegenheiten der Europäischen Union

4.1 Auswirkungen der DSGVO auf diesen Themenbereich

Die Zunahme grenzüberschreitender Datenübertragungen im globalen Internetzeitalter erfordert eine effektive Zusammenarbeit der Datenschutzbehörden innerhalb der EU. Diesem Umstand trägt die EU-Datenschutz-Grundverordnung Rechnung, indem sie mit dem sogenannten „One-Stop-Shop“ sowie dem Kooperations- und Kohärenzverfahren neue Verfahren der Zusammenarbeit und Abstimmung zwischen den Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten einführt. Diese müssen künftig miteinander kooperieren, wenn ein datenverarbeitendes Unternehmen über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt oder durch eine Datenverarbeitung Personen in mehreren Mitgliedstaaten betroffen sind. Für diesen Abstimmungsprozess schafft die Datenschutzgrundverordnung eine neue, mit eigener Rechtspersönlichkeit ausgestattete Einrichtung der EU, den Europäischen Datenschutzausschuss. In diesem Gremium sind - entsprechend bisheriger Praxis in der sogenannten Artikel-29-Gruppe - die Datenschutzbehörden aller 28 EU-Mitgliedstaaten und der Europäische Datenschutzbeauftragte vertreten. Der Ausschuss kann in bestimmten Fällen verbindliche Entscheidungen treffen, die von den Aufsichtsbehörden in den Mitgliedstaaten umgesetzt werden müssen.

Die EU-Datenschutz-Grundverordnung übernimmt weitgehend die bereits in der EU-Datenschutzrichtlinie 95/46/EG angelegte Systematik der Datenübermittlungen in Drittstaaten. Übermittlungen sind danach weiterhin auf Grundlage entsprechender Angemessenheitsbeschlüsse der EU-Kommission, Standardvertragsklauseln und Binding Corporate Rules (BCR) möglich. Zusätzlich werden mit der Zertifizierung und genehmigten Verhaltensregeln neue Rechtsgrundlagen eingeführt. Die europäischen Datenschutzbehörden müssen künftig dafür sorgen, dass diese neuen Rechtsgrundlagen das gleiche hohe Datenschutzniveau wie die bisherigen Instrumente garantieren.

4.2 Aus Beratung und Kontrolle

Kontrolle des Auswärtigen Amtes

Beratungs- und Kontrollbesuche in der Zentrale des Auswärtigen Amts (AA) und Auslandsvertretungen in den Vereinigten Arabischen Emiraten deckten erheblichen Verbesserungsbedarf auf, zum Teil auch beim Personaldatenschutz.

Ein Schwerpunkt meiner Kontrolltätigkeit war die Ausstattung der behördlichen Datenschutzbeauftragten (bDSB) mit Personal- und Sachmitteln. Bereits im Vorfeld war mir bekannt, dass die in meinen Leitlinien empfohlenen „Mindestanforderungen an die Organisation und Aufgabenbeschreibung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung“ vom April 2015 (vgl. o Nr. 1.6) im AA nicht erfüllt waren. Erste Abhilfe wurde geschaffen, indem anlässlich meines Informationsbesuches in der AA-Zentrale im Juli 2015 der behördliche Datenschutzbeauftragte vollständig für diese Aufgabe freigestellt wurde. Die von mir als notwendig erachtete und vom AA angekündigte Bestellung eines teilweise freigestellten Vertreters wurde bis Redaktionsschluss nicht umgesetzt.

Bei den im Mai 2015 kontrollierten Auslandsvertretungen war zudem festzustellen, dass die behördlichen Datenschutzbeauftragten keine Schulung oder Vorbereitung auf ihre Aufgabe erhalten hatten und ihnen daher die erforderliche Fachkunde nach § 4f Absatz 2 Satz 1 BDSG am Anfang ihrer Tätigkeit fehlte.

Ein weiterer erheblicher Mangel betraf das Verzeichnis der Verfahren automatisierter Datenverarbeitungen, das nach den Vorschriften des BDSG in jeder öffentlichen Behörde vorhanden sein muss: Weder in der Zentrale noch in den Auslandsvertretungen wurden Verfahrensverzeichnisse geführt, die den Anforderungen der §§ 4d und 4e BDSG entsprechen. Angesichts der Schwere des Verstoßes gegen §§ 4d und 4e BDSG war hier eine

Beanstandung gemäß § 25 Absatz 1 Nummer 1 BDSG auszusprechen. Zu begrüßen ist, dass das Verzeichnis in der AA-Zentrale nunmehr nachträglich erstellt worden ist.

Der Umgang mit Personaldaten im Generalkonsulat in Dubai und in der Botschaft in Abu Dhabi ließ gleichfalls Verbesserungsbedarf erkennen. So führte die nicht abgeschlossene Einführung eines einheitlichen Personalmanagementsystems zur Missachtung vorgegebener Löschungsvorschriften von Beschäftigtendaten. Darüber hinaus waren Personalnebenakten entgegen § 106 Absatz 1 Satz 2 Bundesbeamtengesetz nicht ausreichend durch technische und organisatorische Maßnahmen, wie z. B. abschließbare Aktenschränke, geschützt. Des Weiteren waren auf einigen Arbeitsplatzrechnern in den Auslandsvertretungen zahlreiche veraltete Dateien mit - teils sensiblen - personenbezogenen Daten vorzufinden.

Ich werde aufgrund der erwähnten Erkenntnisse auch künftig durch Beratungs- und Kontrollbesuche auf die Wahrnehmung des Themas Datenschutz als wichtige Leitungsaufgabe hinwirken.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.6; 2 ff.; 21.1; 21.5; 21.6; 22.11; 22.12

5 Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

5.1 Auswirkungen der DSGVO auf diesen Themenbereich

Bei der Umsetzung der Datenschutz-Grundverordnung (DSGVO) in nationales Recht muss eine ausgewogene Balance zwischen den Grundrechtsgütern Datenschutz und Forschungsfreiheit gefunden werden.

In der DSGVO ist die Intention des Verordnungsgebers erkennbar, einerseits die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher und historischer Forschung zu erleichtern und andererseits den Schutz des Einzelnen auf einen selbstbestimmten Umgang mit seinen Daten nicht abzusenken. Einen allseits zufriedenstellenden Ansatz zur Lösung des grundsätzlichen Widerstreits zwischen dem Interesse freier Forschung und dem individuellen Recht auf informationelle Selbstbestimmung kann die DSGVO aber allein nicht bieten, so dass der deutsche Gesetzgeber im Rahmen der Umsetzung der europäischen Vorgaben in nationales Recht gefordert ist (vgl. Nr. 1.1, Nr. 1.2.1).

Bei der Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken verlangt Artikel 89 Absatz 1 DSGVO von den Mitgliedsstaaten, „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person“ zu gewähren. Dazu zählen „technische und organisatorische Maßnahmen“, mit denen vor allem der Grundsatz der Datenminimierung zu gewährleisten ist; dabei werden ausdrücklich Pseudonymisierungsverfahren benannt.. Die Verarbeitung besonderer Kategorien personenbezogener Daten für Forschungszwecke muss nach dem Ausnahmekatalog des Artikel 9 Absatz 2 DSGVO darüber hinaus besondere Anforderungen erfüllen. Sie muss für den Forschungszweck erforderlich sein sowie auf einer gesetzlichen Grundlage beruhen, die in einem angemessenen Verhältnis zu dem verfolgten Zweck steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene Schutzmaßnahmen vorsieht.

Diese Vorgaben geben nach meiner Auffassung im Wesentlichen das Datenschutzniveau des geltenden nationalen Rechts wieder. Ich hoffe daher, dass die Umsetzung der DSGVO in deutsches Recht dieses Schutzniveau widerspiegelt. Im Fall der Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen Zwecken muss das wissenschaftliche bzw. öffentliche Interesse an dem Forschungsprojekt das Interesse des Einzelnen an dem Ausschluss der Verarbeitung seiner individuellen Daten erheblich überwiegen.

5.2 Einzelthemen

5.2.1 Gesetzgebung im Bildungsbereich

Im Bildungsbereich wurde ich vom Bundesministerium für Bildung und Forschung an Ressortabstimmungen entsprechender Rechtsetzungsvorhaben beteiligt. So konnten im Fall der Novellierung des Gesetzes über die Feststellung der Gleichwertigkeit von Berufsqualifikationen datenschutzgerechte Regelungen im Hinblick auf die Übermittlung von Daten an das Bundesinstitut für Berufsbildung erreicht werden. Mit der Novellierung des Hochschulstatistikgesetzes wurde eine Verlaufsstatistik zu den Studienverläufen eingeführt, für die mit meiner Hilfe eine datenschutzkonforme Regelung gefunden werden konnte. Maßgeblich dafür waren eine Reduzierung der Erhebungsmerkmale für die Studienverlaufsstatistik sowie die Ausgestaltung des dabei angewandten Pseudonymisierungsverfahrens.

5.2.2 Datenschutz und Forschungsdaten

Gerade im Zeitalter der Digitalisierung braucht es angemessene Datenschutzstandards auch für Forschung und Wissenschaft.

Wie ich im letzten Tätigkeitsbericht bereits berichtet habe, hat der Rat für Informationsinfrastrukturen seine Arbeit im Herbst 2014 aufgenommen (vgl. 25. TB Nr. 16.1). Der Rat ist von der Gemeinsamen Wissenschaftskonferenz für vier Jahre berufen worden und soll Vorschläge für die Gestaltung zukunftsfähiger Informationsinfrastrukturen für die Wissenschaft erarbeiten. Informationsinfrastrukturen sind technisch und organisatorisch vernetzte Dienste und Angebote zur Arbeit mit wissenschaftlich relevanten Daten, Informationen und Wissensbeständen. Von Bedeutung für die Arbeit des Rates ist insbesondere die zunehmende digitale Transformation in der Wissenschaft, die bei der Konzeption künftiger Informationsinfrastrukturen zu berücksichtigen ist.

Wissenschaftler greifen auf Daten zu, verarbeiten diese und produzieren Daten. Ohne die Arbeit auch mit personenbezogenen Daten sind Forschung und wissenschaftlicher Fortschritt in vielen Bereichen nicht möglich. Dabei muss Forschung aber auch Datenschutzstandards beachten und das Recht der Beforschten auf informationelle Selbstbestimmung gewährleisten. Gleich zu Beginn der Arbeit des Rates zeigte sich die Bedeutung des Datenschutzes für seinen Arbeitsauftrag, als der Rat im Frühjahr 2015 zur Bearbeitung des Themas „Schutz persönlicher Daten in der Forschung“ einen von mir moderierten Fachausschuss eingesetzt hat.

Mit der DSGVO ist auf europäischer Ebene ein neuer rechtlicher Rahmen für die Mitgliedsstaaten entstanden, der bis Mai 2018 auch eine Anpassung deutscher Datenschutzbestimmungen erfordert. Die für den Wissenschaftsbereich maßgebliche Vorschrift ist Artikel 89 DSGVO, der die Verarbeitung personenbezogener Daten zu im öffentlichen Interessen liegenden Archivzwecken, zu wissenschaftlichen oder historischen Zwecken und zu statistischen Zwecken regelt (vgl. Nr. 5.1).

Der Rat beabsichtigt, ein Positionspapier zum Thema Datenschutz und Forschungsdaten zu veröffentlichen und dieses in den politischen Diskurs über die Umsetzung der DSGVO in Deutschland einzubringen. Dieses Positionspapier wird vom Ausschuss Datenschutz erarbeitet, der mehrere interne Sitzungen, zwei Expertenanhörungen und einen Workshop durchgeführt hat. Zu den identifizierten Fragestellungen zählt insbesondere das Spannungsfeld zwischen dem individuellen Grundrecht auf informationelle Selbstbestimmung und der verfassungsrechtlich garantierten Forschungsfreiheit. Ein weiteres Spannungsfeld besteht zwischen der Möglichkeit bzw. Notwendigkeit einer rechtlichen Rahmensetzung einerseits und ethischen Orientierungshilfen andererseits. In diesem Zusammenhang ist zudem zu klären, inwiefern fachliche Standards und gute wissenschaftliche Praxis dem Bereich der ergänzenden ethischen Regelungen zugeordnet werden können. Schließlich konkurrieren individuelle Maßnahmen (z. B. Selbstdatenschutz) mit organisatorisch-institutionellen Lösungen (z. B. Forschungsdatenzentren, Treuhandstellen). Das Positionspapier war bis zum Redaktionsschluss noch nicht verabschiedet.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2.1; 1.6; 21.1; 21.5; 22.10

6 Ausschuss für Ernährung und Landwirtschaft

6.1 Aus Beratung und Kontrolle

Beratungs- und Kontrollbesuch beim Bundesinstitut für Risikobewertung

Beim Bundesinstitut für Risikobewertung musste ich feststellen, dass die Sicherheitsarchitektur des IT-Bereichs verbesserungsbedürftig ist.

Im Herbst 2015 habe ich mir beim Bundesinstitut für Risikobewertung (BfR), einer Behörde im Geschäftsbereich des Bundesministeriums für Ernährung und Landwirtschaft, einen Überblick über den Umgang mit personenbezogenen Daten im Rahmen der Aufgaben des Instituts verschafft. Neben der Funktion und Stellung der behördlichen Datenschutzbeauftragten (bDSB) waren für mich dabei die vom Institut selbst durchgeführten bzw. in Auftrag gegebenen Forschungsvorhaben von besonderem Interesse, ebenso wie die IT-Sicherheitsarchitektur.

Die organisatorische Einbindung der bDSB unmittelbar unterhalb der Behördenleitung entspricht den gesetzlichen Vorgaben. Datenschutzkritische Punkte wurden vom BfR im Nachgang des Besuches aufgegriffen. Ein neues Datenschutzkonzept befindet sich derzeit in der Abstimmung mit dem zuständigen Ministerium. Ich gehe davon aus, das Konzept in Kürze zur Prüfung zu erhalten.

Nach den Vor-Ort-Feststellungen meiner Mitarbeiter erhebt das BfR im Rahmen seiner Forschungstätigkeit nur in begrenztem Umfang personenbezogene Daten. Die stichprobenhafte Betrachtung eines Projekts erfüllte die datenschutzrechtlichen Erfordernisse und gab keinen Anlass zu kritischen Anmerkungen.

Bei der Einrichtung und Umsetzung von IT-Sicherheitsvorgaben habe ich allerdings Mängel feststellen müssen. Das BfR verfügte nicht über ein Informations-Sicherheits-Management-System, wie es die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik vorsehen. Obwohl zwischenzeitlich eine Vollzeitstelle für die Aufgaben des IT-Sicherheitsbeauftragten geschaffen wurde, konnte diese Funktion innerhalb des Berichtszeitraums nicht besetzt werden. Die zum Zeitpunkt meines Besuchs noch ausstehende Erstellung und Umsetzung eines umfassenden Informationssicherheitskonzepts soll nach Aussage des BfR vordringlichste Aufgabe des neuen IT-Sicherheitsbeauftragten sein. Das BfR hat mir zwischenzeitlich versichert, das personelle Defizit bei der Realisierung der Sicherheitsanforderungen des Instituts übergangsweise durch eine interne Stellenumsetzung gelöst werde. Ich gehe daher davon aus, das IT-Sicherheitskonzept in Kürze vorgelegt zu bekommen.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2.1; 1.6; 21.1; 21.5

7 Ausschuss für Familie, Senioren, Frauen und Jugend

7.1 Auswirkungen der DSGVO auf diesen Themenbereich

Die besondere Schutzbedürftigkeit personenbezogener Daten von Kindern wird in der europäischen Datenschutz-Grundverordnung (DSGVO) an mehreren Stellen ausdrücklich hervorgehoben.

Die DSGVO, die ab dem 25. Mai 2018 gelten wird, unterstreicht den besonderen Schutz personenbezogener Daten von Kindern und Minderjährigen. Wörtlich heißt es in Erwägungsgrund 38: „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind." Auch im eigentlichen Verordnungstext wird immer wieder hervorgehoben, dass die Datenschutzrechte von Kindern besonders schutzwürdig sind (vgl. Art. 6 Abs. 1 Buchstabe f) DSGVO). Die Einwilligung eines Minderjährigen ist nach Artikel 8 Absatz 1 DSGVO erst ab Vollendung des sechzehnten Lebensjahres zulässige Voraussetzung dafür, personenbezogene Daten rechtmäßig verarbeiten zu können. Der Gesetzgeber wird künftig prüfen müssen, ob er bei Regelungen zur Datenverarbeitung besondere Regelungen zum Schutz von Kindern ergreifen muss. Ich werde hierauf mein Augenmerk richten.

Auch die Aufsichtsbehörden werden nach Artikel 57 Absatz 1 Buchstabe b) DSGVO verpflichtet, insbesondere bei ihrer Aufgabe zur Sensibilisierung der Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Datenverarbeitung spezifische Maßnahmen für Kinder vorzusehen. Gemeinsam mit meinen Kolleginnen und Kollegen aus den Ländern werde ich prüfen, welche Möglichkeiten es gibt, spezifische Maßnahmen für Kinder zu ergreifen.

7.2 Aus Beratung und Kontrolle

7.2.1 Datenschutzfragen bei der Conterganstiftung

Ein Beratungs- und Kontrollbesuch deckte Probleme und Schwachstellen auf.

Die Conterganstiftung für behinderte Menschen ist eine öffentlich-rechtliche Stiftung des Bundes. Sie erbringt Leistungen an behinderte Menschen, deren Fehlbildungen mit der Einnahme thalidomidhaltiger Präparate der Stolberger Firma Chemie Grünenthal GmbH durch die Mutter während der Schwangerschaft in Verbindung gebracht werden können. Es handelt sich daher bei den dort zu verarbeitenden Daten um sehr sensible Gesundheitsdaten.

Bei einem Besuch der Conterganstiftung zeigten sich verschiedene datenschutzrechtliche Probleme, von denen einige ungewöhnlich, andere aber symptomatisch für viele öffentliche und nicht-öffentliche Stellen waren. Bei der Anbindung der Geschäftsstelle der Conterganstiftung beim damaligen Bundesamt für den Zivildienst (BAZ - heute: Bundesamt für Familie und zivilgesellschaftliche Aufgaben - BAFzA) im Jahr 2010 war die Datenschutzbeauftragte des BAZ auch mit den Aufgaben der Datenschutzbeauftragten der Conterganstiftung betraut worden. Dies ist nach § 4f Absatz 2 Satz 4 BDSG grundsätzlich bei öffentlichen Stellen des Bundes zulässig. Ungewöhnlich war allerdings, dass diese Bestellung sich nicht auf die ganze Conterganstiftung erstreckte, sondern ausschließlich auf ihre Geschäftsstelle. Für andere Organe der Conterganstiftung, wie etwa den Vorstand oder die ärztlichen Kommissionen war die Datenschutzbeauftragte ausdrücklich nicht zuständig. Ich habe die Conterganstiftung deswegen darauf hingewiesen, dass sie als öffentliche Stelle des Bundes nicht nur für einen Teil, sondern für alle ihre Organe und Bereiche nach § 4f BDSG einen internen Datenschutzbeauftragten bestellen muss. Zu meinem Bedauern war am Ende des Berichtszeit ein behördlicher Datenschutzbeauftragter nach § 4f BDSG für die gesamte Conterganstiftung noch nicht bestellt.

7.2.2 Datenschutz beim Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs

Beim Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs (UBSKM) wurde eine unabhängige Kommission eingerichtet, die den Missbrauch in Institutionen und im familiären Kontext in Deutschland untersuchen soll. Der UBSKM bindet mich in die Verarbeitung der sehr sensiblen Daten vorbildlich ein.

Die Unabhängige Kommission zur Aufarbeitung sexuellen Kindesmissbrauchs soll Strukturen aufdecken, die sexuelle Gewalt gegen Kinder und Jugendliche in der Vergangenheit ermöglicht und ihre Aufarbeitung verhindert haben. Im Wesentlichen soll sie dabei bundesweit Betroffene anhören. Dabei fallen naturgemäß sehr viele und sehr sensible Daten an. Mittlerweile bindet mich der UBSKM bei datenschutzrechtlichen Fragen in das Projekt ein. Das ist besonders wichtig, da sich das Projekt noch in der Aufbauphase befindet und datenschutzrechtliche Probleme bei der Berücksichtigung meiner Anregungen erst gar nicht entstehen.

Bei einem Besuch des UBSKM, der der Datenschutzorganisation der Dienstelle galt, konnte ich zudem erfreulicherweise feststellen, dass bei den dortigen Beschäftigten eine große Sensibilität für das Thema und vor allem für die besondere Art der dort anfallenden Daten vorhanden ist.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.6; 21.1; 21.5; 22.3

8 Finanzausschuss

8.1 Auswirkungen der DSGVO auf diesen Themenbereich

Die Datenschutz-Grundverordnung (DSGVO) ist ab dem 25. Mai 2018 auch im Bereich der Finanzen in Deutschland unmittelbar geltendes Recht.

Grundsätzlich gilt die DSGVO auch im Bereich der Finanzen und der Steuerverwaltung. Allerdings eröffnet die DSGVO vielfältige Regelungsspielräume für diesen Bereich. Für die Verarbeitung personenbezogener Daten durch die Steuer- und Finanzverwaltung ist dieser Spielraum am größten, denn hier lässt Artikel 6 Absatz 2 und 3 DSGVO zum einen spezifische materiell-rechtliche Regelungen zu bzw. erfordert solche. Zudem können die Betroffenenrechte (z. B. auf Information, Auskunft oder Widerspruch) zur Wahrung der finanziellen Interessen eines Mitgliedstaats nach Artikel 23 Absatz 1 lit. e DSGVO eingeschränkt werden.

Für die Verarbeitung personenbezogener Daten durch Unternehmen der Finanzbranche (z. B. Banken oder Versicherungen) wird die DSGVO hingegen weitgehend unmittelbar gelten. Der nationale Gesetzgeber hat nur sehr punktuelle Regelungsspielräume, die sich wiederum meist auf die Datenverarbeitung im öffentlichen Interesse beziehen, wie z. B. bei Meldepflichten zur Geldwäscheprävention.

8.2 Einzelthemen

In den vergangenen zwei Jahren habe ich eine Reihe wichtiger Gesetzgebungsvorhaben im Finanzbereich begleitet. Auch wenn nicht in jedem Einzelfall meinen datenschutzrechtlichen Empfehlungen gefolgt wurde, so erkenne ich doch eine deutlich stärkere Einbindung meiner Behörde.

8.2.1 AnaCredit oder der Weg zum allgemeinen Kreditregister

Die Europäische Zentralbank (EZB) verfolgt mit dem Projekt AnaCredit (Analytical Credit Datasets) den Aufbau eines granularen und damit passgenauen Kreditmeldewesens. Im Gegensatz zu einigen Staaten der Eurozone, verfügt Deutschland derzeit über kein Kreditregister. Datenschutzrechtlich relevant wird dieses Vorhaben, wenn dort Daten natürlicher Personen verarbeitet werden sollen.

Mit der Verordnung (EU) 2016/867 der EZB vom 18. Mai 2016 über die Erhebung granularer Kreditdaten und Kreditrisikodaten (EZB/2016/13) verpflichtet die EZB ab September 2018 alle Banken, ihr detaillierte Kreditnehmerdaten vorzulegen. Diese sog. AnaCredit-Verordnung ist zu unterscheiden von der Wohnimmobilienkreditrichtlinie 2014/17/EU der Europäischen Kommission, die bereits in nationales Recht umgesetzt wurde und die Pflicht zur Kreditwürdigkeitsprüfung bei Verbraucherdarlehensverträgen regelt (§§ 505a und 505b BGB).

Die EZB will das EU-weite zentrale Kreditregister in zwei Schritten einführen, hat bisher aber nur die erste Phase definiert. In der „Phase 1“ müssen Kreditdaten natürlicher Personen noch nicht gemeldet werden, sondern nur solche juristischer Personen. Gleichwohl zeichnet sich schon jetzt eine Ausweitung des Anwendungsbereiches von AnaCredit auf natürliche Personen in der zweiten Umsetzungsphase ab. Aus diesem Grund begleite ich bereits heute dieses Vorhaben.

Für die zu meldenden Kredite werden zahlreiche Merkmale der Kategorien Betrag, Laufzeit, Zins, Währung u. ä. abgefragt. Für den zu meldenden Kreditnehmer sind bis zu 26 Attribute anzugeben, darunter Name, Sitz, Rechtsform, Größe, Sektor und Wirtschaftszweig und weitere Identifikatoren. Kreditinstitute mit Sitz in der Eurozone sowie Niederlassungen ausländischer Banken in der Eurozone müssen die Kennziffern monatlich an

die jeweiligen Nationalbanken melden, die dann an die EZB weiterzuleiten sind. Die Meldungen werden für Deutschland von der Deutschen Bundesbank entgegengenommen und an die EZB übermittelt.

Die EZB will mit der AnaCredit-Verordnung nicht nur eine einheitliche Erhebungsmethode für Kredite im Euroraum vorgeben, sondern auch den Kreis der Meldepflichtigen deutlich erweitern, um die Daten für das geldpolitische Risikomanagement und die Finanzstabilitätsüberwachung zu nutzen. So werden in Deutschland bislang nur große Kreditvolumina an die Bankenaufsicht gemeldet, wohingegen beispielsweise in Portugal die Meldeschwelle im Bagatellbereich angesiedelt ist. Die Deutsche Bundesbank hat allerdings die ihr eingeräumte Möglichkeit genutzt und für kleinere Institute die Meldeerfordernisse erleichtert.

Ergänzt wird die Datenerhebung durch AnaCredit durch das vom BMF geplante Aufsichtsrechtsergänzungsgesetz. Dieses Gesetzgebungsvorhaben beruht auf einer Empfehlung des Ausschusses für Finanzstabilität vom 30. Juni 2015. Danach erhält die Bundesanstalt für Finanzdienstleistungsaufsicht die Befugnis, mittels Allgemeinverfügung Beschränkungen bei der Vergabe von Darlehen zum Bau oder Erwerb von im Inland belegenen Wohnimmobilien festzulegen, wenn dies zur Verhinderung einer Störung unseres Finanzsystems oder der Finanzstabilität erforderlich sein sollte.

Ich werde dieses Vorhaben auch weiterhin sowohl in der Artikel-29-Gruppe als auch auf nationaler Ebene begleiten und mich für eine datenschutzkonforme Ausgestaltung der Phase 2 einsetzen, bei der es dann auch um die Datenerfassungen natürlicher Personen gehen wird.

8.2.2 Umsetzung der Geldwäscherichtlinie wird zu einer Daueraufgabe

Am 20. Mai 2016 wurde die so genannte Vierte Geldwäscherichtlinie vom Europäischen Parlament und Rat verabschiedet.

Die Vierte Geldwäscherichtlinie soll den Rechtsrahmen für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung vereinheitlichen. Durch sie wird erstmals auch ein Transparenzregister geschaffen. In dieses öffentliche Register werden künftig die wirtschaftlich Berechtigten einer Gesellschaft eingetragen. Darüber hinaus wird erstmals der gesamte Glückspielsektor (nicht nur die Kasinos) ab einem Transaktionsbetrag von 2.000 Euro erfasst. Der geldwäscherechtlich relevante Schwellenwert für gewerblich gehandelte Waren wird herabgesetzt und der Kreis der Verpflichteten ausgeweitet.

Der bisherige Schwellenwert für meldepflichtige Barzahlungen liegt bei 15.000 Euro und soll im Zuge der Umsetzung der Vierten Geldwäscherichtlinie EU-weit auf höchstens 10.000 Euro begrenzt werden, wobei der nationale Gesetzgeber diese Obergrenze noch weiter herabsetzen darf. Die nationale Festlegung eines Schwellenwertes darf aus meiner Sicht aber nicht dazu führen, dass Barzahlungen von größeren Alltagsbeschaffungen wie z. B. Tablets, Computern oder Fernsehern bei der Geldwäschebekämpfung in den Fokus rücken und mit Datenerhebungen, -übermittlungen, -speicherung und -auswertung verbunden sind. Alltagsausgaben sollten nicht unter einen generellen Geldwäsche- oder Terrorismusfinanzierungsverdacht gestellt werden. Den Bürgerinnen und Bürgern muss auch weiterhin die Möglichkeit eingeräumt bleiben, alltägliche Ausgaben ohne Datenerfassung tätigen zu können.

Noch vor der Umsetzung der Vierten Geldwäscherichtlinie in nationales Recht hat die EU-Kommission am 5. Juli 2016 bereits einen weiteren Vorschlag für eine Fünfte Geldwäscherichtlinie unterbreitet. Mit der Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung von Richtlinie 2009/101/EG, soll künftig die Finanzierung terroristischer Aktivitäten verhindert werden. Um dieses Ziel erreichen zu können, werden die zentralen geldwäscherechtlichen Meldestellen Zugriff auf Informationen in zentralen Registern für Bank- und Zahlungskonten sowie elektronischen Datenabrufsystemen erhalten. Erstmals werden künftig auch Stellen, an denen virtuelle Währungen umgetauscht werden können, in die Bekämpfung von Geldwäsche und Terrorismusfinanzierung eingebunden. Zudem wird der Schwellenwert des

anonymen Bezahlens, z. B. durch Guthabenkarten, von 250 Euro auf 150 Euro abgesenkt und es gelten strengere Anforderungen an die Kundenüberprüfung, wenn mit Guthabenkarten bezahlt wird. Zudem wird der öffentliche Zugang zum neu eingeführten Transparenzregister erweitert.

Die künftig beim Zollkriminalamt angesiedelte zentrale Meldestelle für Verdachtsmeldungen (Financial Intelligence Unit, FIU) wird erweiterte Befugnisse erhalten. Die weit im Vorfeld eines Gefahrenverdachts bzw. eines strafrechtlichen Anfangsverdachts übermittelten Meldungen sollen künftig ausgewertet und auch nach Anreicherung mit weiteren Daten analysiert werden dürfen. Mit welchen konkreten Mitteln und in welchem Umfang, ist nach dem aktuell vorliegenden Entwurf gesetzlich nicht begrenzt. Wenig begrenzt sind auch die Auskunftspflichten von anderen Behörden gegenüber der FIU. Diese erstrecken sich sogar darauf, automatisierte Datenaustauschverfahren einzurichten. Dies kann mit umfassenden Zweckänderungen verbunden sein. In der Regel sind die Daten ohne Kenntnis der Betroffenen erhoben worden. Das Gesetz regelt sogar ausdrücklich das Verbot, den Betroffenen zu informieren. Damit gelten prinzipiell die vom Bundesverfassungsgericht festgelegten verfassungsrechtlichen Anforderungen für die Verwendung von Daten aus heimlichen Informationseingriffen (vgl. Nr. 1.3). Die Verknüpfung mit den Änderungsvorschlägen zum Zollfahndungsdienstgesetz wirkt sich zusätzlich auf die Grundrechtsrelevanz des Entwurfs aus (vgl. Nr. 10.2.9.1).

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 weiterhin konstruktiv, aber kritisch begleiten.

8.2.3 Modernisierung des Besteuerungsverfahrens; weiterhin kein datenschutzrechtlicher Auskunftsanspruch

Auch mit dem Gesetz zur Modernisierung des Besteuerungsverfahrens hat das BMF eine weitere Chance vergeben, die damit fortschreitende Automatisierung im Besteuerungsverfahren durch einen bundeseinheitlichen Auskunftsanspruch in der Abgabenordnung zu flankieren, so dass ab dem 25. Mai 2018 der in Artikel 15 DSGVO geregelte Auskunftsanspruch unmittelbar gelten wird, wenn nicht zuvor bereichsspezifische Regelungen getroffen werden.

Mit dem vom BMF vorgelegten Gesetz zur Modernisierung des Besteuerungsverfahrens sollen insbesondere die Arbeitsabläufe durch den Einsatz moderner Informationstechnologie optimiert werden. Das Ziel ist klar zu erkennen, nämlich Steuererklärungen künftig online abwickeln und von den Finanzämtern möglichst ausschließlich IT-gestützt bearbeiten zu können. Ich bin in diesen Prozess von Beginn an eingebunden gewesen und musste zu meinem Erstaunen feststellen, dass das BMF seinen noch im Diskussionsentwurf von 2014 enthaltenen Vorschlag, den datenschutzrechtlichen Auskunftsanspruch endlich auch bundeseinheitlich in der Abgabenordnung zu verankern, im Gesetzgebungsverfahren wieder zurückgenommen hat. Dies bedaure ich sehr, zumal mein Haus seit Jahrzehnten einen solchen datenschutzrechtlichen Auskunftsanspruch fordert (vgl. zuletzt 23. TB Nr. 9.4). Daten, die im Besteuerungsverfahren erhoben, gespeichert und verarbeitet werden, zeichnen sich durch eine besondere Sensibilität aus, da sie Einblick in die finanziellen Verhältnisse der Betroffenen eröffnen und dadurch Rückschlüsse auf deren private Lebensumstände und wirtschaftliche Leistungskraft ermöglichen. Bereits 2008 hat das Bundesverfassungsgericht die Rahmenbedingungen für einen datenschutzrechtlichen Auskunftsanspruch im Besteuerungsverfahren definiert (Urteil vom 10.03.2008, Az. 1 BvR 2388/03). Danach gilt grundsätzlich auch im Besteuerungsverfahren das Grundrecht auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG, flankiert durch die Rechtsschutzgarantie des Artikel 19 Absatz 4 GG.

Ich halte es deswegen für rechtswidrig, wenn Auskunftsersuchen im Besteuerungsverfahren nach wie vor ausschließlich über die Vorgaben des BMF-Anwendungserlasses aus dem Jahr 2008 beschieden werden. Die Entscheidung darüber, ob Auskunft zu gewähren ist, darf nicht in das Ermessen der Auskunft gewährenden Finanzbehörde gestellt werden. In der Praxis beobachte ich immer wieder eine bundesuneinheitliche Handhabung dieses Anwendungserlasses. Finanzbehörden verlangen von Steuerpflichtigen z. B. in unterschiedlicher Weise den Nachweis eines berechtigten Interesses. Das BDSG, das allerdings nur für Bundesbehörden gilt, regelt daten-

schutzrechtliche Auskunftsansprüche demgegenüber voraussetzungslos und als gebundene Entscheidung, bei der nur ausnahmsweise Ausschlussgründe eingreifen.

Die mit dem Gesetz zur Modernisierung des Besteuerungsverfahrens einhergehende Automatisierung birgt die konkrete Gefahr, dass Daten nicht korrekt eingegeben, übernommen oder übermittelt werden. Datenfehler, die der Steuerpflichtige möglicherweise nicht zu verantworten hat, können zu schwerwiegenden Fehleinschätzungen der Finanzbehörden führen, ohne dass der Steuerpflichtige ohne weiteres erkennen kann, wo die Ursachen dafür liegen. Auch Personenverwechslungen, die ich bei jedem bisher eingeführten Automatisierungsprozess beobachten musste, könnte mit Transparenz- und Auskunftsrechten effizienter entgegengesteuert werden. Die hohe Fehlerquote zeigte sich zuletzt, als die Steuer-Identifikationsnummer eingeführt wurde und es weit über 100.000 Fälle von Datenvermischungen oder Mehrfacherfassungen gab.

Das BMF hat jedenfalls eine Chance vergeben, bereits heute den datenschutzrechtlichen Auskunftsanspruch gesetzlich auszugestalten und in ein ausgewogenes Verhältnis zu den Belangen des Besteuerungsverfahrens zu setzen.

8.2.4 Internationaler Steuerdatenaustausch: Datenverarbeitung muss innerhalb der EU stattfinden

Auch der zweifellos notwendige internationale Steuerdatenaustausch muss die datenschutzrechtlichen Standards bewahren. Mit Blick auf den US-patriot act muss er auf europäischen Servern abgewickelt werden, um einen Zugriff der US-Behörden auf steuerliche Daten auch zu anderen Zwecken zu vermeiden.

Die „Panama Papers“ von April 2016 haben wieder einmal gezeigt, wie globalisiert Steuerhinterziehung funktioniert. Dies unterstreicht gleichzeitig auch die Aktualität des OECD-Standards für den automatischen Informationsaustausch über Finanzkonten. Die zunehmende Globalisierung von Finanzanlagen und die damit verbundene Folge unversteuerter Einnahmen, macht eine internationale Zusammenarbeit der Steuerverwaltungen zweifellos zwingend notwendig. Allerdings muss auch dieser internationale Steuerdatenaustausch die datenschutzrechtlichen Standards bewahren. Bei der nationalen Umsetzung des OECD-Standards durch das Gesetz zum automatischen Austausch von Informationen über Finanzkonten in Steuersachen und zur Änderung weiterer Gesetze vom 21. Dezember 2015 (BGBl. I Nr. 55, S. 2531) konnte ich mich nicht mit meiner Forderung durchsetzen, die übermittelten Daten statt für einen Zeitraum von 15 Jahren nur für einen Zeitraum von zehn Jahren beim Bundeszentralamt für Steuern zu speichern Die Erläuterungen des BMF zur Erforderlichkeit dieser langen Speicherfrist haben mich nicht überzeugt. Zudem hat mein Vorschlag, die nach § 6 Absatz 1 vorgesehene Datenerhebung durch die Finanzinstitute an den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und Datensparsamkeit auszurichten, keine ausdrückliche Berücksichtigung im Gesetz gefunden. Allerdings wurde meinen Forderungen insoweit Rechnung getragen, dass der datenschutzrechtliche Grundsatz der Zweckbindung, nach dem Daten nur für steuerliche Zwecke verwendet werden dürfen, in den Regelungen verankert wurde.

Derzeit läuft die Vorbereitungsphase für den ersten internationalen Steuerdatenaustausch, der für September 2017 geplant ist. Im Rahmen der Artikel-29-Gruppe habe ich in den vergangenen Monaten daran mitgewirkt, sog. Guidelines insbesondere für den Steuerdatenaustausch mit Drittländern zu entwickeln. Ferner habe ich mich dafür eingesetzt, den Steuerdatenaustausch über einen europäischen Server abzuwickeln. In diesem Zusammenhang wurde zunächst auch diskutiert, den bereits aktiven Server, der für den bilateralen Steuerdatenaustausch zwischen den USA und Deutschland im Rahmen von FATCA (Foreign Account Tax Compliance Act, vgl. 25. TB Nr. 7.5) genutzt wird, gleichermaßen für den internationalen OECD Steuerdatenaustausch zu verwenden. Hier habe ich große datenschutzrechtliche Bedenken, da der US-patriot act US-Behörden einen unbegrenzten Zugriff auf diese Daten auch zu anderen Zwecken erlaubt. Ich setze mich daher weiterhin dafür ein, dass der internationale Steuerdatenaustausch auf europäischem Boden stattfindet.

8.2.5 Erfassung von Flugpassagierdaten für zollspezifische Aufgaben

Der Entwurf eines Gesetzes zur Änderung des Zollverwaltungsgesetzes sah die Erfassung von Flugpassagierdaten für zollspezifische Aufgaben vor. Nachdem ich dazu gegenüber dem BMF meine erheblichen datenschutzrechtlichen Bedenken zum Ausdruck gebracht hatte, wurde das Gesetz letztlich vom Bundeskabinett ohne die von mir kritisierte Regelung verabschiedet.

Als mir der Entwurf eines Gesetzes zur Änderung des Zollverwaltungsgesetzes zur datenschutzrechtlichen Stellungnahme vorgelegt wurde, musste ich feststellen, dass damit auch ein IT-basiertes System zur Übermittlung von Flugpassagierdaten an den Zoll eingeführt werden sollte. Die vorgeschlagene Regelung griff Überlegungen des BMF aus den vergangenen Jahren auf, zu denen ich mich bereits kritisch geäußert hatte. Das Ziel der neuen Regelung sollte die risikoorientierte zollrechtliche Kontrolle sein. Es handelte sich ausweislich der Gesetzesbegründung jedoch gerade nicht um die Umsetzung der Richtlinie 2016/681 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (sog. EU-PNR-Richtlinie).

Die vom BMF vorgeschlagene neue Regelung (der ursprüngliche § 10a ZollVG E) war inhaltlich eng an die Vorschrift des § 31a Bundespolizeigesetz (BPolG) angelehnt, die bereits eine Übermittlung von Fluggastdaten an die Bundespolizei zum Zwecke der Grenzkontrollen ermöglicht und der Umsetzung der Richtlinie 2004/82/EG (API-Richtlinie) dient. Gleichwohl verstieß die vorgelegte Regelung gegen nahezu alle datenschutzrechtlichen Grundsätze und wurde von mir als nicht datenschutzkonform bewertet: Die datenschutzrechtliche Zweckbindung bei der Übermittlung der freiwilligen und nicht überprüfbaren Angaben der Flugpassgiere wurde nicht beachtet. Die Datenerhebung und Datenübermittlung orientierte sich weder am Datensparsamkeitsgrundsatz noch wurde deren Notwendigkeit plausibel und überzeugend begründet. Obwohl offensichtlich eine IT-basierte Datenverarbeitung geplant war, wurde nicht bedacht, dass belastende Entscheidungen nicht ausschließlich auf automatisierte Verarbeitungen gestützt werden dürfen (§ 6a BDSG). Zudem sollten die gespeicherten Daten aus steuerlichen Gründen länger als 24 Stunden gespeichert werden, ebenfalls ohne hierfür überzeugende Gründe benennen zu können. Schließlich blieb die Regelung lückenhaft, da sie keine Information der Flugpassagiere über diese Datenverarbeitung vorsah.

Ich habe meine erheblichen datenschutzrechtlichen Bedenken gegenüber dem BMF zum Ausdruck gebracht. Der vom Bundeskabinett letztlich verabschiedete Entwurf zur Änderung des Zollverwaltungsgesetzes verzichtete auf diese von mir kritisierte Regelung.

8.2.6 Zweites Finanzmarktnovellierungsgesetz sieht Telefonaufzeichnungspflichten vor

Im Rahmen meiner Einbindung in das Gesetzgebungsverfahren zum zweiten Finanzmarktnovellierungsgesetz konnte ich Verbesserungen bei den in das Wertpapierhandelsgesetz aufgenommenen Telefonaufzeichnungspflichten erreichen. Im Zusammenhang mit den auch im Rahmen dieses Gesetzgebungsvorhaben vorgesehenen Internetbekanntmachungen, setze ich mich - soweit dies möglich ist – für deren Anonymisierung ein und weise auf ein „Recht auf Vergessen“ im Netz hin, dass Artikel 17 DSGVO als Konsequenz des sog. Google-Spain-Urteils regelt.

Das BMF hat mich frühzeitig in die Gesetzgebung für ein zweites Finanzmarktnovellierungsgesetz eingebunden. Mit diesem Gesetz sollen u. a. die Anlageberatung, Aufsichtsrechte und der Hochfrequenzhandel geregelt und die EU-Richtlinie über Märkte für Finanzinstrumente (MiFID II, 2014/65/EU) in nationales Recht umgesetzt werden. Die Änderungen betreffen insbesondere den Wertpapierhandel, das Kreditwesen und die Börse. Datenschutzrechtlich relevant sind insbesondere die Telefonaufzeichnungspflichten, die in das Wertpapierhandelsgesetz (WpHG) aufgenommen werden. Wertpapierdienstleistungsunternehmen, die nach dem WpHG der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Auskunft verpflichtet sind, sollen zur Beweissicherung Telefongespräche und elektronische Kommunikation aufzeichnen müssen. Ich konnte erreichen, dass vorab auf die Aufzeichnung des Telefongespräches hingewiesen wird und die Zweckbindung dieser Datenaufzeichnung konturiert wurde. Zudem habe ich dafür plädiert, entsprechend den europarechtlichen Vorgaben nur eine fünfjährige Speicherdauer vorzusehen.

Im Zusammenhang mit diesem Gesetzgebungsvorhaben konnte ich wieder einmal beobachten, dass der Gesetzgeber zunehmend auf bekanntmachende Veröffentlichungen im Internet setzt. Ich werbe in diesen Fällen dafür, Internetbekanntmachungen - soweit dies möglich ist - zu anonymisieren. Werden personenbezogene Daten im Internet veröffentlicht, handelt es sich um Eingriffe in das Recht auf informationelle Selbstbestimmung, die nur im Allgemeininteresse gestattet sind. Im Übrigen sehe ich hier auch Missbrauchsrisiken: Internetveröffentlichungen werden immer häufiger von anderen Portaldienstanbietern durch sog. Crawling-Verfahren vollständig kopiert und auf eigene Internetseiten eingestellt. In vielen Fällen werden damit personenbezogene Informationen dauerhaft über den eigentlich vom Gesetzgeber vorgesehenen Veröffentlichungsgrad hinaus zur Verfügung gestellt. Ich halte es in diesem Zusammenhang für geboten, geeignete technische Maßnahmen vorzusehen, um ein Abgreifen der personenbezogenen Daten einer vom Gesetzgeber vorgegebenen Internetveröffentlichung zu verhindern. Diese technischen Maßnahmen werden an Bedeutung gewinnen, wenn die Datenschutz-Grundverordnung anzuwenden ist. Als Konsequenz des sog. Google-Spain-Urteils regelt Artikel 17 DSGVO ein „Recht auf Vergessen“ im Netz, das Verantwortliche, die personenbezogene Daten öffentlich gemacht haben, dazu verpflichtet, anderen Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen davon zu löschen (vgl. Kasten zu Nr. 8.2.6).

Kasten zu Nr. 8.2.6

Das **„Recht auf Vergessenwerden“** wird in Erwägungsgrund 66 folgendermaßen beschrieben:

„Um dem „Recht auf Vergessen werden“ im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen - auch technischer Art - treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.“

8.2.7 Investmentsteuerreformgesetz betrifft auch natürliche Personen

Im Rahmen meiner Einbindung in das Gesetzgebungsverfahren zum Investmentsteuerreformgesetzes konnte ich eine Klarstellung in der Gesetzesbegründung erreichen.

Das Gesetz zur Reform der Investmentbesteuerung richtet sich hauptsächlich an juristische Personen. Es betrifft aber dann natürliche Personen, wenn die Normadressaten Personengesellschaften sind. Meine Anregung, in der Gesetzesbegründung klarzustellen, dass es sich bei dem nach diesem Gesetz zu führenden Anteilsregister um ein intern von der jeweiligen Gesellschaft zu führendes Register handelt, wurde übernommen.

8.2.8 Rentenmitteilungen per Kontoauszug ohne rechtliche Grundlage

Die Versorgungsanstalt des Bundes und der Länder hatte die in 2016 zeitweise eingeführte Information ihrer Versicherten über Rentenerhöhungen und über Beiträge zur gesetzlichen Kranken- und Pflegeversicherung per Bankkontoauszug wegen fehlender rechtlicher Grundlage wieder zurücknehmen müssen.

Jährlich zum 1. Juli erhalten die Versicherten der Versorgungsanstalt des Bundes und der Länder (VBL) eine Anpassung ihrer Betriebsrente um ein Prozent des Rentenbetrages. Sowohl für den Antrag auf Betriebsrente als auch für die Berechnung der Leistungen oder die Gründe der Ablehnung gilt laut Satzung der VBL die Schriftform. Wobei die VBL satzungsgemäß zwischen dem Postweg oder - soweit der Versicherte der Nutzung des

Kundenportals „Meine VBL“ widerruflich zugestimmt hat - einer Kommunikation über das Kundenportal wählen kann.

Anfang 2016 hatte die VBL ihre Versicherten über die Einführung einer veränderten Rentenanpassungsmitteilung informiert. Ab Juli 2016 sollte über die jährlichen Rentenerhöhungen und über gegebenenfalls abzuführende Beiträge zur gesetzlichen Kranken- und Pflegeversicherung nicht mehr mit der Post, sondern fortan nur noch per Mitteilung auf dem Bankkontoauszug oder online über das Kundenportal „Meine VBL“ informiert werden.

Zu diesem dann zeitweise eingeführten Verfahren „Mitteilung über den Kontoauszug“ haben mich mehrere Eingaben erreicht. Darin wurde ich gebeten zu klären, ob es datenschutzkonform sein könne, Kreditinstitute in diesen Informationsprozess über den Rentenbezug einzubinden, da diesen dabei personenbezogene Daten bekanntgemacht würden. Wie meine Prüfung ergeben hat, war diese Verfahrensänderung nicht datenschutzkonform. Meines Erachtens fehlte es an einer Rechtsgrundlage, um über eine Mitteilung im Kontoauszug der jeweiligen Bank auch gleichzeitig über das personenbezogene Datum der Rentenerhöhung informieren zu dürfen. Es lagen weder eine satzungsmäßige Erlaubnis (vgl. §§ 39, 46, 46a der Satzung der VBL) noch wirksame Einwilligungen der Versicherten für diesen neuen Kommunikationsweg vor. Die VBL hat daraufhin das im Juli 2016 eingeführte Kontoauszugsmitteilungsverfahren für die Zeit ab September 2016 ausgesetzt und plant 2017 ein mit mir abgestimmtes neues Verfahren.

Ich habe der VBL empfohlen, zunächst eine Satzungsänderung zu prüfen. Sollte sich die VBL jedoch entscheiden, statt einer Satzungsänderung auf Einwilligungen der Versicherten zurückzugreifen, habe ich gebeten, diesen Weg bereits heute im Hinblick auf die ab Mai 2018 geltenden Anforderungen der Datenschutz-Grundverordnung zu klären.

8.2.9 Kontenabrufverfahren

Das Kontenabrufverfahren wird weiter ausgeweitet.

Die Zahl der Kontenabrufe ist durch die 2013 hinzugekommene Abrufmöglichkeit für Gerichtsvollzieher stark angestiegen (vgl. 25. TB Nr. 7.2). Dieser Trend hielt auch in den letzten zwei Jahren an. 2015 stieg die Zahl der Kontenabrufe von ca. 237.000 auf über 300.000 Abrufe. Im Jahr 2016 nahmen die Abrufe noch weiter auf über 417.000 zu.

Dieser Trend wird durch zwei neue Gesetzesänderungen weiter verstärkt. Dies betrifft das Gesetz zur Durchführung der Verordnung (EU) Nr. 655/2014 sowie zur Änderung sonstiger zivilprozessualer, grundbuchrechtlicher und vermögensrechtlicher Vorschriften und zur Änderung der Justizbeitreibungsordnung, das bereits am 22. November 2016 in Kraft getreten ist. Hierdurch ist die 500 Euro-Wertgrenze aufgehoben worden, für die ich mich im Gesetzgebungsverfahren zur Reform der Sachaufklärung in der Zwangsvollstreckung eingesetzt hatte. Gerichtsvollzieher dürfen künftig Kontenabrufe unabhängig von der Höhe der zu vollstreckenden Forderung durchführen.

Die zweite Ausweitung wird voraussichtlich durch das Gesetz zur Reform der Sachaufklärung in der Verwaltungsvollstreckung erfolgen. Ziel dieses Gesetzgebungsvorhabens ist es, auch für die Verwaltungsvollstreckungsbehörden des Bundes und der Länder Ermittlungsbefugnisse zu schaffen, die denen entsprechen, die Gerichtsvollziehern gegenüber Dritten gesetzlich eingeräumt sind (§§ 755 und 802l ZPO). Der Gesetzentwurf befand sich bei Redaktionsschluss in der parlamentarischen Bewertung.

Ein Ende des Anstiegs der Kontenabrufe ist damit noch lange nicht in Sicht!

8.3 Aus Beratung und Kontrolle

Ein Ergebnis meiner Beratungs- und Kontrollbesuche ist ein deutlicher Verbesserungsbedarf in der Unterstützung der behördlichen Datenschutzbeauftragten. Diese werden trotz ihrer umfangreichen internen Beratungs-, Kontroll-, Multiplikator- und Ombudsfunktion vielfach nur unzureichend personell ausgestattet und unterstützt.

Beratungs- und Kontrollbesuch bei der Deutschen Bundesbank

Die Deutsche Bundesbank (BBk) ist als Zentralbank der Bundesrepublik Deutschland integraler Bestandteil des Europäischen Systems der Zentralbanken. Bei einem Beratungs- und Kontrollbesuch habe ich mich von einer weitgehend den Ansprüchen genügenden Organisation des Datenschutzes überzeugen können. Optimierungsbedarf sehe ich allerdings noch hinsichtlich der organisatorischen Anbindung und der personellen Ausstattung des behördlichen Datenschutzbeauftragten (bDSB) sowie bei einzelnen IT-Verfahren hinsichtlich fehlender Verfahrensbeschreibungen und verfahrensspezifischer Löschkonzepte. Die BBk will meine Anregungen aufgreifen.

Ich begrüße es zudem sehr, dass die BBk Möglichkeiten der Ausgestaltung nationaler Spielräume bei der Umsetzung europäischer Verordnungen weiterhin eng mit mir abstimmen will.

Beratungs- und Kontrollbesuch bei der Bundesanstalt für Immobilienaufgaben

Die Bundesanstalt für Immobilienaufgaben (BImA) ist nach eigenen Angaben eine der größten Immobilieneigentümerinnen Deutschlands. Wie ich bei einem Beratungs- und Kontrollbesuch feststellen musste, hat die BImA für ihre zahlreichen und umfangreichen IT-Verfahren weder ein Gesamtlöschkonzept noch zu jedem Einzelverfahren ein verfahrensspezifisches Löschkonzept. Auch als Konsequenz aus meinen Feststellungen und Empfehlungen will die BImA zunächst ein Gesamtlöschkonzept ausarbeiten und umsetzen. Dieses soll Teil einer geplanten Datenschutzrichtlinie der BImA werden. Anschließend sollen verfahrensspezifische Löschkonzepte entwickelt bzw. angepasst werden. Ich werde die Entwicklung datenschutzrechtlicher Standards bei der BImA weiterhin aufmerksam verfolgen.

Beratungs- und Kontrollbesuch beim Bundesamt für zentrale Dienste und offene Vermögensfragen

Das Bundesamt für zentrale Dienste und offene Vermögensfragen (BADV) war zum Prüfungszeitpunkt Betreiber des SAP-basierten einheitlichen Personalverwaltungssystems der Bundesfinanzverwaltung (PVS). Seit Januar 2015 stellt es die von ihm für ca. 300.000 Bezügeempfänger geleistete Bezügeabrechnung schrittweise auf die Bearbeitung mit der PVS-Komponente Payment (PY) um. Zum 1. Januar 2017 wurde das für den Betrieb von PVS zuständige Kompetenzzentrum KPVS in das 2016 etablierte Informationstechnikzentrum Bund (ITZBund) verlagert. Die zentralen Dienstleistungsbereiche des BADV sollen zum 1. Juni 2017 in das Bundesverwaltungsamt (BVA) integriert werden.

Meine Kontrolle ergab, dass der bDSB des BADV bei der Einführung neuer Projekte im Allgemeinen und bei der Einführung von PVS im Besonderen nur unzureichend eingebunden worden ist. Aufgrund seiner unzureichenden Einbindung und Schulung konnte der bDSB in diesem Fall seinen Aufgaben nicht angemessen nachkommen. So konnte er z. B. nicht abschließend beurteilen, ob die bei den verschiedenen PVS-Komponenten zur Durchführung von Sperrungen und Löschungen eingesetzte Software SAP-ILM für PVS datenschutzgerecht konzipiert ist und angewendet wird. Dies halte ich für einen unhaltbaren Zustand. Gemäß § 4f Absatz 5 BDSG ist das BADV gesetzlich verpflichtet, seinen bDSB bei der Aufgabenwahrnehmung zu unterstützen. Hier sehe ich noch einen deutlichen Verbesserungsbedarf.

Dem bDSB ist von seiner Behörde die für die Aufgabenstellung erforderliche Sach- und Personalausstattung zur Verfügung zu stellen. Zumindest ab einer Beschäftigtenzahl von 1.000 Beschäftigten ist der bDSB regelmäßig von anderen dienstlichen Tätigkeiten freizustellen und abhängig vom Umfang der Verarbeitung personenbezo-

gener Daten, der Zahl und Komplexität der Verarbeitungen sowie der Innovationsgeschwindigkeit durch die Bereitstellung weiteren Personals zu unterstützen. Trotz der zum Prüfungszeitpunkt ca. 1.900 Mitarbeiter an 14 Standorten und eine Vielzahl verschiedener, auch datenschutzrelevanter Aufgabenstellungen ist beim BADV nur eine Person für die Aufgabe bDSB bestellt und freigestellt. Zwar wurde dem bDSB eine Mitarbeiterin für Vertretungsfälle zugeordnet. Diese wurde jedoch dafür nicht anteilig von ihren sonstigen Aufgaben entbunden. Diese personelle Unterstützung des bDSB halte ich angesichts der oben beschriebenen Aufgaben des BADV für nicht ausreichend.

Als problematisch sehe ich es auch an, dass die Vertreterin des bDSB zudem Leiterin der für administrativen Datenschutz, IT-Sicherheit, Korruptionsprävention, Notfall- und Krisenmanagement, Ideenmanagement, Stiftungsprüfung und externen Datenschutz zuständigen Stabsstelle ist. Diese Aufgabe halte ich für nicht vereinbar mit der eines bDSB. Die weitgehend weisungsfreie Aufgabenerfüllung durch den bDSB ist dadurch gefährdet. Ich empfehle, auch bei der Auswahl eines stellvertretenden bDSB auf mögliche Unvereinbarkeiten übertragener Funktionen zu achten (vgl. Info 4 der BfDI „Datenschutzbeauftragte in Behörde und Betrieb“, abrufbar auf meiner Internetseite unter www.datenschutz.bund.de).

Ich werde die Anwendungsbetreuung von und die Arbeit mit PVS auch nach der veränderten organisatorischen Anbindung der betroffenen Stellen weiterhin begleiten.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.6; 2.3.2; 2.4; 21.1; 21.5; 22.1

9 Ausschuss für Gesundheit

9.1 Auswirkungen der DSGVO auf diesen Themenbereich

auf die gesetzliche Krankenversicherung

Öffnungsklauseln in der Datenschutz-Grundverordnung ermöglichen dem nationalen Gesetzgeber das sorgfältig aufeinander abgestimmte Gefüge der datenschutzrechtlichen Vorschriften im Recht der gesetzlichen Krankenversicherung in seinen Grundzügen zu erhalten.

Gemäß Artikel 6 Absatz 2 der Datenschutz-Grundverordnung (DSGVO) können die Mitgliedstaaten „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung“ von personenbezogenen Daten „beibehalten oder einführen“, soweit dies u. a. für die Erfüllung einer Aufgabe erforderlich ist, „die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde“ (Artikel 6 Absatz 1 Buchstabe e)).

Die Voraussetzungen des Artikel 6 Absatz 1 Buchstabe e) liegen für das deutsche Recht der gesetzlichen Krankenversicherung vor, so dass Artikel 6 Absatz 2 anwendbar ist und dem nationalen Gesetzgeber einen Spielraum eröffnet, spezifischere Rechtsgrundlagen zu schaffen oder beizubehalten (vgl. 25. TB Nr. 1.2.1).

Dieser Spielraum für die öffentliche Verwaltung erlaubt aber nur Konkretisierungen und Präzisierungen, keine grundsätzlichen Abweichungen vom Datenschutzniveau der DSGVO. Dies wirft Fragen auf, die in Zukunft zu beantworten sein werden.

Wie groß der Anpassungs- oder Bereinigungsbedarf tatsächlich sein wird, kann derzeit noch nicht abschließend beurteilt werden. Hierzu gilt es den Umsetzungsprozess, die ersten Anwendungserfahrungen sowie sich daraus ergebende Einzelprobleme und deren - gegebenenfalls gerichtliche - Klärung aufmerksam zu beobachten.

Da die Krankenversicherungsträger auch besonders sensible Daten - hier vor allem Gesundheitsdaten - zur Erfüllung ihrer Aufgaben verarbeiten, ist auch Artikel 9 Absatz 1 DSGVO bei der Anpassung des nationalen Rechts von Bedeutung, der die Verarbeitung von bestimmten, besonders schützenswerten Daten (u. a. Gesundheitsdaten, genetische Daten oder Daten über das Sexualleben) verbietet. Artikel 9 Absatz 2 DSGVO legt wiederum Ausnahmen für das Verbot aus Absatz 1 fest: Besondere Datenkategorien dürfen danach unter anderem verarbeitet werden, wenn dies für Zwecke der Gesundheitsvorsorge, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten der Gesundheits- oder Sozialfürsorge erforderlich ist.

auf die Forschung mit Gesundheitsdaten und anderen besonders sensiblen Daten

Die Digitalisierung des Gesundheitswesens und die raschen technologischen Entwicklungen versprechen neue Chancen für die Forschung mit Gesundheits- und genetischen Daten. Die Datenschutz-Grundverordnung setzt hierfür Rahmenbedingungen. Dabei genießen Gesundheits- und genetische Daten besonderen Schutz.

Die DSGVO will der digitalen Revolution durch ein hohes Datenschutzniveau und mit einem soliden und kohärenten Datenschutzrechtsrahmen begegnen. Dies gilt insbesondere auch für den Umgang mit den sensiblen „besonderen Kategorien personenbezogener Daten“, wie Gesundheitsdaten oder genetischen Daten. Für die Forschung grundlegend ist Artikel 89 DSGVO. Danach sind bei der Datenverarbeitung zu wissenschaftlichen Forschungszwecken angemessene Garantien für die Rechte und Freiheiten der betroffenen Person zu treffen, zum Beispiel sind die Rechte auf Auskunft oder Datenlöschung zu gewährleisten, wobei Einschränkungen möglich sind. Es müssen technische und organisatorische Maßnahmen ergriffen werden, wie Anonymisierung und Pseudonymisierung, durch die insbesondere auch der Grundsatz der Datenminimierung beachtet wird. Für die Wei-

terverarbeitung zu Forschungszwecken sind die Daten möglichst zu anonymisieren. Big Data-Ansätze, die dem Grundsatz der Datensparsamkeit widersprechen, können für die Forschung mit Gesundheitsdaten oder genetischen Daten daher grundsätzlich nicht nutzbar gemacht werden.

Die Begriffe „Gesundheitsdaten“ (Art. 4 Nr. 15) und „genetische Daten“ (Art. 4 Nr. 13) definiert die DSGVO präziser als das BDSG. Die besonders sensiblen Daten unterliegen einem Verarbeitungsverbot nach Artikel 9 Absatz 1 DSGVO. Artikel 9 Absatz 2 Buchstabe j) DSGVO erlaubt für Zwecke der wissenschaftlichen Forschung eine Ausnahme, wenn die Datenverarbeitung auf der Grundlage europäischen oder nationalen Rechts erfolgt. Gemäß Artikel 9 Absatz 4 DSGVO können die Mitgliedstaaten zusätzliche Regelungen treffen, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. Inwieweit das deutsche Datenschutzanpassungsgesetz derartige Regelungen enthalten wird, bleibt abzuwarten (vgl. u. Nr. 1.2 f.). Da in den meisten Forschungsprojekten Einwilligungen der Teilnehmer eingeholt werden, ist für die Forschung mit Gesundheitsdaten Artikel 9 Absatz 2 Buchstabe a) DSGVO wesentlich. Danach ist die Einwilligung bei besonderen Kategorien personenbezogener Daten ausdrücklich für einen oder mehrere festgelegte Zwecke zu erteilen. Der in Erwägungsgrund 33 beschriebene, hinsichtlich der Zweckbestimmung weitere sog. „broad consent“ bezieht sich nur auf Einwilligungen bei einfachen personenbezogenen Daten nach Artikel 6 Absatz 1 a) DSGVO. Es ist daher sehr zweifelhaft, ob dieses Modell für die Forschung mit Gesundheitsdaten oder genetischen Daten anwendbar ist. Eine Weiterverarbeitung sensibler Daten durch dieselbe datenschutzrechtlich verantwortliche Stelle zu einem anderen Zweck als dem Erhebungszweck, darf ohne neuen Ausnahmetatbestand i. S. v. Artikel 9 Absatz 2 DSGVO nur erfolgen, wenn der Erhebungszweck und der Weiterverarbeitungszweck kompatibel sind. Werden Register geschaffen und verknüpft, die Gesundheitsdaten enthalten, birgt dies die Gefahr der Erstellung umfassender Persönlichkeitsprofile. Solche verknüpften Datensätze mit Gesundheitsdaten dürften insgesamt unter das strenge Regelungsregime für besondere Kategorien personenbezogener Daten fallen.

9.2 Einzelthemen

9.2.1 Das „E-Health-Gesetz“

Das E-Health-Gesetz etabliert die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitswesen. Dies bedeutet einen weiteren Schritt zur Digitalisierung des Gesundheitswesens.

Das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen („E-Health-Gesetz“) wurde im Dezember 2015 verkündet und ist in weiten Teilen Anfang 2016 in Kraft getreten. Es regelt einen Zeitplan für die bundesweite Einführung der Telematikinfrastruktur, der zum flächendeckenden Anschluss von Arztpraxen und Krankenhäusern im Jahr 2018 führen soll (vgl. auch unter Nr. 9.2.7). Im Gesetzgebungsverfahren habe ich gegenüber dem BMG sowie dem Ausschuss für Gesundheit des Deutschen Bundestages mehrfach Stellung genommen. In einer Entschließung vom 18./19. März 2016 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Nachbesserungen beim E-Health-Gesetz gefordert (vgl. Anlage 5).

Einige meiner Anregungen wurden zwar aufgenommen. Im Kernpunkt zielt meine Kritik jedoch darauf, dass das E-Health-Gesetz noch immer kaum konkrete Datenschutzregelungen enthält. Beispielsweise werden bei telemedizinischen Anwendungen nach § 291g SGB V Datenschutzanforderungen nicht explizit berücksichtigt. Bedenklich ist auch die in § 291b Absatz 1 Satz 13 SGB V angesprochene Prüfung der Einbeziehung mobiler Endgeräte der Versicherten ohne Festlegung der entsprechenden datenschutzrechtlichen Voraussetzungen.

Für weitere geplante Gesetzgebungsvorhaben im E-Health-Bereich empfehle ich, konkrete Datenschutzanforderungen im Gesetz selbst zu verankern. Insbesondere halte ich es für wesentlich, vor einer Einbeziehung neuer Anwendungen in die Gesundheitsversorgung einen hohen Datenschutzstandard sicherzustellen, der mindestens den Anforderungen der Datenschutz-Grundverordnung genügt. Soweit mobile Anwendungen in die Regelversorgung und in das E-Health-System integriert werden sollen, muss zunächst ihre Qualität sowie ihre daten-

schutz- und datensicherheitsgerechte Ausgestaltung sichergestellt und Transparenz für die Nutzer hergestellt sein. Dies ist bislang nicht der Fall (vgl. o. Nr. 1.5).

Insgesamt bietet die Digitalisierung des Gesundheitswesens große Chancen, doch dürfen damit einhergehend nicht die Privatheit abgeschafft und der Schutz sensibler Gesundheitsdaten verringert werden. So müssen die Vertraulichkeit und der besondere Schutz des Arzt-Patienten-Verhältnisses gewährleistet bleiben, ebenso wie das Selbstbestimmungsrecht der Patienten und Versicherten hinsichtlich ihrer medizinischen Daten. Ich werde mich daher auch in Zukunft für ein hohes, gesetzlich abgesichertes Datenschutzniveau im Gesundheitswesen einsetzen.

9.2.2 Das neue Transplantationsregister

Am 1. November 2016 ist das Gesetz zur Errichtung eines Transplantationsregisters in Kraft getreten, bei dem ich das BMG umfassend beraten habe. Erfreulicherweise wird in diesem Gesetz dem Recht auf informationelle Selbstbestimmung ein hoher Stellenwert beigemessen.

Mit dem Gesetz zur Errichtung eines Transplantationsregisters und zur Änderung weiterer Gesetze vom 11. Oktober 2016 (BGBl. I, S. 2233) ging eine sehr intensive Begleitung einer entsprechenden Änderung des Transplantationsgesetzes (TPG) zu Ende. Bereits in der Vorbereitung des Gesetzgebungsverfahrens hatte mich das BMG im Beirat zu einem „Fachgutachten zu einem nationalen Transplantationsregister“ frühzeitig beteiligt. Eine derartig frühe Beteiligung halte ich für beispielhaft.

Ziel des Transplantationsregistergesetzes ist die Errichtung eines bundesweiten Registers, in dem die bislang nur dezentral vorliegenden transplantationsmedizinischen Daten zusammengeführt werden. Man verspricht sich hiervon wesentliche Erkenntnisse, die zu einer Verbesserung und Weiterentwicklung der transplantationsmedizinischen Versorgung und zur Erhöhung der Transparenz führen. Mit dem Transplantationsregister sollen die Grundlagen geschaffen werden für

- eine Datenharmonisierung und Effizienzsteigerung bei der Dokumentation,
- die Datenintegration, Datenvalidität und Datenverfügbarkeit,
- die Weiterentwicklung der Wartelistenkriterien und Allokationsregeln,
- die Qualitätssicherung in der transplantationsmedizinischen Versorgung sowie
- die Transparenz in der Organspende und Transplantation.

Zudem soll - ausdrücklich unter Wahrung des Datenschutzes - der Zugang zu den Daten für die wissenschaftliche Forschung ermöglicht werden.

Der hohen Bedeutung der Vollständigkeit der Daten für die Weiterentwicklung der Transplantationsmedizin kann nur dann Rechnung getragen werden, wenn Patienten und Gesellschaft Vertrauen in den rechtmäßigen Umgang mit den hochsensiblen transplantationsmedizinischen Gesundheitsdaten haben. Unabdingbare Voraussetzung für dieses Vertrauen ist der Schutz der Persönlichkeitsrechte der Betroffenen.

Mit dem Inkrafttreten des Gesetzes kommen allerdings auch auf mich zusätzliche Aufgaben zu. Da sowohl das Transplantationsregister als auch die Vertrauensstelle öffentliche Stellen des Bundes sind, ist auch aufgrund der Sensibilität der Daten eine regelmäßige datenschutzrechtliche Kontrolle und Beratung erforderlich. Zudem bin ich unter anderem an der Festlegung des bundeseinheitlichen Datensatzes sowie den Regelungen zum Datenaustausch mit anderen Registern beteiligt. Ich bin dem Gesetzgeber dankbar, dass er es mir durch die Bereitstellung der erforderlichen personellen Ressourcen ermöglicht, diese zusätzlichen Aufgaben effektiv wahrnehmen zu können.

Bedauerlicherweise ist der Gesetzgeber nicht dem Vorschlag gefolgt, meine Beteiligung auch beim Bereitstellungsverfahren der Daten an Dritte zu Forschungszwecken vorzusehen. Bei der Entscheidung, ob und in welchem Umfang die wissenschaftliche Forschung Zugang zu personenbezogenen Registerdaten erhält, fehlt daher die Datenschutzexpertise.

Bei den Beratungen zur Änderung des TPG habe ich gegenüber den Mitgliedern des Gesundheitsausschusses des Deutschen Bundestages zudem den Schutz des postmortalen Persönlichkeitsrechts der verstorbenen Spender und Organempfänger für deutlich verbesserungsfähig bezeichnet und meine Hoffnung ausgedrückt, dass dies bei der nächsten Novellierung des Transplantationsgesetzes berücksichtigt wird. Neben dem Schutz der Menschenwürde, der einen Missbrauch von Daten Verstorbener verhindern soll, gebietet es auch das allgemeine Persönlichkeitsrecht der betroffenen Personen zu Lebzeiten, dass sie frei und selbstbestimmt über ihre transplantationsmedizinischen Daten im Todesfalle verfügen können. Diese auch praktisch ohne weiteres realisierbare Möglichkeit sollte im Gesetz besser abgebildet werden.

9.2.3 Die „NAKO-Gesundheitsstudie“ entwickelt sich

Epidemiologische Langzeitstudien wie die Nationale Kohorte (NAKO) erfordern eine kontinuierliche datenschutzrechtliche Begleitung. Viele datenschutzrechtliche und technische Fragen entstehen erst im Laufe der Zeit.

Über die NAKO habe ich bereits berichtet (25. TB Nr. 13.2). Es handelt es sich um eine epidemiologische Langzeitstudie von Wissenschaftlern der Helmholtz-Gemeinschaft, der Leibniz-Gemeinschaft sowie von Universitäten und anderen Forschungseinrichtungen in Deutschland. 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. Die Zahl der vorgesehenen 200.000 Studienteilnehmer soll Anfang 2019 erreicht werden.

Aktuell habe ich mit der NAKO die regelmäßig vorgesehene Zusammenführung der in den Studienzentren gewonnenen Befragungs- und Gesundheitsdaten mit aktualisierten Sekundärdaten diskutiert. So sollen die in den Studienzentren gewonnenen Daten mit Daten der gesetzlichen Krankenkassen, der privaten Krankenversicherungen, der Deutschen Rentenversicherungen, der Bundesagentur für Arbeit, der epidemiologischen und klinischen Krebsregister sowie mit ärztlichen Behandlungsdaten zusammengeführt werden. Die Anschrift der Teilnehmer soll über Abfragen bei den Meldeämtern aktualisiert werden. In diesem Zusammenhang wurde auch die Einführung eines Mortalitätsregisters angesprochen. Derartige Mortalitätsregister gibt es bereits in einigen wenigen Bundesländern, allerdings in ganz unterschiedlichen Ausprägungen. Grundsätzlich stehe ich der Schaffung von Mortalitätsregistern für Forschungszwecke nicht entgegen, sehe allerdings zunächst den Gesetzgeber in der Pflicht, hierfür gesetzliche Regelungen zu schaffen.

Einzigartig bei der NAKO ist nicht nur die Größe der Kohorte (d. h. der Teilnehmerzahl) und die Dauer der Datenspeicherung, die bis über den Tod der Studienteilnehmer hinausgehen soll, sondern auch der Umfang und die Detailtiefe der gesammelten Daten. Zusätzlich wurde im Rahmen der „NAKO-Gesundheitsstudie“ die bislang größte Biobank Deutschlands angelegt, in der Proben von Körperflüssigkeiten der Probanden sowie Gewebeproben eingelagert werden. Sowohl dieses „Biorepository“ als auch das beim Helmholtz-Institut in Augsburg eingerichtete Studienzentrum habe ich im Rahmen meiner Kontrollzuständigkeit im August 2016 besucht. Weitere Studienzentren, die bei Landesstellen eingerichtet wurden, haben im Berichtszeitraum meine Kollegen von den Landesbeauftragten für den Datenschutz kontrolliert.

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 gesammelten Daten gelöscht. Die bei den Studienteilnehmern erhobenen Daten sowie die Daten aus Sekundärquellen

stehen Wissenschaftlern auf Antrag nur pseudonymisiert zur Auswertung zur Verfügung, sodass eine Identifizierung des Einzelnen wenig wahrscheinlich ist.

Meine Anregungen zu ihrem Datenschutzkonzept hat die Nationale Kohorte e. V. in konstruktiver Zusammenarbeit aufgenommen. Das Datenschutzkonzept entwickelt sich mit der Studie kontinuierlich weiter. Wesentlich ist, dass ich die Teile des Datenschutzkonzeptes geprüft habe, die für den derzeitigen Stand des Projekts relevant sind. Angesichts der langen Laufzeit und der komplexen datenschutzrechtlichen Herausforderungen, die diese Studie bietet, werde ich sie auf Dauer begleiten.

9.2.4 Mobile Gesundheitsanwendungen - Gesundheits-Apps und Wearables

Die Entwicklung von sogenannten Apps für Smartphones und Tablets haben auch den Gesundheitsbereich erfasst. Die Möglichkeit, mit Hilfe von „Wearables“, d. h. (sehr) kleinen tragbaren Computern etwa zur Erfassung von Körperfunktionen (Puls, Blutzuckerspiegel, Blutdruck etc.) seinen Gesundheitszustand zu überwachen, bietet sowohl Chancen als auch Gefahren. Mehrere Millionen Bürgerinnen und Bürger nutzen bereits Gesundheits-Apps. Im Berichtszeitraum hat sich das Thema „Mobile Gesundheitsanwendungen“ mehr und mehr in den Vordergrund geschoben und sich zu einem Schwerpunktthema entwickelt (vgl. o. Nr. 1.5).

9.2.5 Krankengeld- und andere Formen des Fallmanagements bei den Gesetzlichen Krankenkassen - Status Quo und Ausblick

Für das von vielen Krankenkassen betriebene Krankengeldfallmanagement wurde eine gesetzliche Grundlage geschaffen, die praktische Umsetzung entspricht jedoch nicht immer den gesetzlichen Vorgaben. Das Bestreben der Krankenkassen, den Versicherten auch in anderen Bereichen ein Versorgungsmanagement anzubieten, ist ungebrochen.

In meinem letzten Tätigkeitsbericht habe ich über die Pläne des Gesetzgebers berichtet, eine Rechtsgrundlage für das Krankengeldfallmanagement zu schaffen (vgl. 25. TB Nr. 13.7.1). Trotz meiner erheblichen datenschutzrechtlichen Bedenken ist mit § 44 Absatz 4 SGB V durch das Gesetz zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz, BGBl. I, S. 1211) am 23. Juli 2015 eine gesetzliche Grundlage in Kraft getreten. Danach haben Versicherte Anspruch auf individuelle Beratung und Hilfestellung durch die Krankenkassen, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind. Die hierfür erforderliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf nur mit schriftlicher Einwilligung und nach vorheriger schriftlicher Information des Versicherten erfolgen. Im Zuge des Gesetzgebungsverfahrens konnte ich erreichen, dass die Krankenkassen die Durchführung des Krankengeldfallmanagements nicht auf private Stellen übertragen dürfen. Außerdem sieht § 44 Absatz 4 SGB V eine Verpflichtung des BMG vor, dem Deutschen Bundestag bis zum 31. Dezember 2018 einen Bericht über die Umsetzung des Anspruchs auf individuelle Beratung und Hilfestellung durch die Krankenkassen vorzulegen.

Im Rahmen von Kontrollen der in meinen Zuständigkeitsbereich fallenden gesetzlichen Krankenkassen musste ich feststellen, dass die gesetzlichen Vorgaben von den Krankenkassen nur teilweise berücksichtigt wurden. So fehlte in der schriftlichen Information, die der Einwilligung vorangehen muss, etwa ein Hinweis auf die Freiwilligkeit der Teilnahme und der Preisgabe sensibler personenbezogener Daten, oder der Einstieg in das Krankengeldfallmanagement erfolgte über einen telefonischen Kontakt, bei dem bereits Sozialdaten erhoben wurden, ohne dass die gesetzlich geforderte schriftliche Einwilligung des Versicherten vorlag. Auch bei künftigen Kontrollen werde ich mein besonderes Augenmerk auf die Einhaltung der gesetzlichen Vorgaben zum Krankengeldfallmanagement richten.

Neben dem Bereich des Krankengeldes wurden auch für zwei weitere Bereiche vergleichbare Rechtsgrundlagen geschaffen: Zum einen führte das GKV-Versorgungsstärkungsgesetz ein sog. Entlassmanagement zur Unterstützung einer sektorenübergreifenden Versorgung der Versicherten nach einer Krankenhausbehandlung (§ 39

Abs. 1a SGB V) ein, zum anderen wurde mit dem Gesetz zur Verbesserung der Hospiz- und Palliativversorgung in Deutschland (Hospiz- und Palliativgesetz, BGBl I, S. 2114) eine gesetzliche Grundlage für die individuelle Beratung und Hilfestellung durch die Krankenkasse zu den Leistungen der Hospiz- und Palliativversorgung (§ 39b Abs. 1 SGB V) geschaffen. Meine Kritik an den gesetzlichen Regelungen erhalte ich aufrecht. Zum einen weichen sie den Grundsatz auf, nach dem im Regelungsbereich der gesetzlichen Krankenversicherung personenbezogen Daten nur aufgrund einer konkreten Rechtsgrundlage erhoben werden dürfen, darüber hinausgehende Datenerhebungen sich also nicht durch eine Einwilligung des Versicherten legitimieren lassen. Zum anderen lassen sie die Grenzen zwischen den sonst strikt getrennten Erhebungsbefugnissen von Krankenkassen und dem Medizinischen Dienst der Krankenkassen verschwimmen. Wird auf der einen Seite ein Versorgungsmanagement in bestimmten Bereichen legitimiert, ergibt sich daraus im Umkehrschluss, dass in anderen Bereichen, in denen eine solche gesetzliche Grundlage fehlt, ein umfassendes Fallmanagement nicht zu den Aufgaben der Krankenkassen zählt und eine damit verbundene Datenerhebung, -verarbeitung oder -nutzung unzulässig ist.

Über eine große Krankenkasse, die ein Fallmanagement ohne gesetzliche Grundlage durchführte, habe ich in meinem letzten Tätigkeitsbericht (25. TB Nr. 13.7.2) berichtet. Die Krankenkasse bot Programme an, die sich an psychisch erkrankte Versicherte richteten, sowie an solche, die an schwerwiegenden Erkrankungen, wie Herzinfarkt, Schlaganfall oder Diabetes litten und eine umfassende Versorgung (Organisation von Therapien, Betreuungsgespräche mit privaten Dienstleistern, etc.) angeboten bekommen wollten. Meiner Aufforderung, diese Programme einschließlich der damit einhergehenden Erhebung, Verarbeitung und Nutzung personenbezogener Daten einzustellen, kam die Krankenkasse nicht nach. Ich habe deshalb eine förmliche Beanstandung gemäß § 81 Absatz 2 SGB X i. V. mit § 25 Absatz 1 BDSG wegen Verstoßes gegen § 284 Absatz 1 SGB V ausgesprochen. Daneben hat das Bundesversicherungsamt als allgemeine Aufsichtsbehörde einen Verpflichtungsbescheid erlassen, gerichtet auf die Kündigung der Verträge mit den privaten Dienstleistern, welche die Programme im Auftrag der Krankenkasse durchführten. Die Krankenkasse hat hiergegen Klage erhoben. Das Klageverfahren ist derzeit noch nicht zum Abschluss gekommen. Ich werde die Angelegenheit weiterhin aufmerksam beobachten.

9.2.6 Das Umschlagsverfahren - was lange währt, wird (hoffentlich) endlich gut

Zum 1. Januar 2017 wurde das Verfahren zur Beteiligung des Medizinischen Dienstes (MDK) durch die gesetzlichen Krankenkassen auf ein elektronisches Benachrichtigungssystem umgestellt. Datenschutzverstöße sollen damit ausgeschlossen werden.

In meinem letzten Tätigkeitsbericht hatte ich über die bereits seit einiger Zeit beobachteten Fehlentwicklungen bei der Durchführung des sog. Umschlagsverfahrens berichtet und angekündigt, dieses Verfahren zukünftig nicht mehr zu tolerieren (vgl. 25. TB Nr. 13.11). Der Gesetzgeber hat inzwischen meine Rechtsauffassung, medizinische Unterlagen, die bei den Leistungserbringern (Ärzte, Krankenhäuser) zur Erstellung von medizinischen Gutachten durch den MDK im Auftrag der Krankenkassen angefordert werden, seien unmittelbar dem MDK zu übermitteln, und dürften nicht - sei es auch in einem verschlossenen Umschlag - den Umweg über die Krankenkassen nehmen, durch eine klarstellende Änderung des § 276 Absatz 2 Satz 2 SGB V bestätigt. Der seit dem 1. Januar 2016 geltende neue Wortlaut dieser Regelung lässt nun keinen Interpretationsspielraum mehr zu: In Fällen, in denen Krankenkassen oder der MDK für eine gutachtliche Stellungnahme oder Prüfung nach § 275 Absatz 1 bis 3 SGB V erforderliche versichertenbezogene Daten bei den Leistungserbringern angefordert haben, sind diese jetzt verpflichtet, „diese Daten unmittelbar an den Medizinischen Dienst zu übermitteln“.

Gemeinsam mit allen Beteiligten sollte ein Verfahren erarbeitet werden, das neben den erforderlichen datenschutzrechtlichen Anforderungen auch Aspekte der Wirtschaftlichkeit sowie die Sicherstellung möglichst kurzfristiger Leistungsentscheidungen der Krankenkassen berücksichtigt. Dabei sollte ein maschineller Datenaustausch zwischen den Krankenkassen und den MDK vorgesehen werden, der eine kassenseitige Meldung an den MDK über die Anforderung von Unterlagen, eine maschinelle Fallanlage beim MDK sowie eine Rückmeldung an die Krankenkasse im Falle des Eingangs der Unterlagen beinhaltet. Außerdem wurde der Aufbau eines elekt-

ronischen Archivs bei allen MDK in Aussicht gestellt, auf das Gutachter in einer Fallberatung extern zugreifen könnten.

Dieses angestrebte digitalisierte Verfahren halte ich für die Umsetzung meiner Forderung und der gesetzlichen Vorgaben für zielführend. Natürlich werden die mit der Verfahrensumstellung verbundenen IT-technischen, organisatorischen und haushälterischen Erfordernisse eine gewisse Vorlaufzeit benötigen. Deswegen wurde von allen Beteiligten das Ziel einer flächendeckenden Umstellung des Verfahrens zum 1. Januar 2017 als realistisch eingeschätzt. Ich habe deshalb zunächst von einer förmlichen Beanstandung der meiner Aufsicht unterstehenden gesetzlichen Krankenkassen abgesehen, die das Umschlagsverfahren bis zu diesem Zeitpunkt weiterhin durchführen. Aufgrund der Rückmeldungen der Verfahrensbeteiligten gehe ich zum jetzigen Zeitpunkt von einer vollständigen Finalisierung der Verfahrensumstellung zum geplanten Termin aus.

9.2.7 Elektronische Gesundheitskarte - alles wie immer oder gibt es Fortschritte?

Die Erprobung der elektronischen Gesundheitskarte in der Praxis hat zwar endlich begonnen, aber auf die ersten medizinischen Anwendungen müssen Patientinnen und Patienten weiter warten.

In meinem 25. Tätigkeitsbericht (Nr. 13.2) habe ich über die bereits für das Jahr 2015 geplanten Erprobungsmaßnahmen in den Testregionen Nordwest und Südost berichtet. Aber es dauerte bis zum November 2016, ehe wenigstens ca. 20 Arztpraxen und ein Klinikum in der Testregion Nordwest den Startschuss zur Erprobung des Online-Rollouts gegeben haben. In der Region Südost ist mit dem Start der Erprobung erst im April 2017 zu rechnen.

Eine spürbare Belebung des Projekts der elektronischen Gesundheitskarte ist durch das im Januar 2016 in Kraft getretene „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz; vgl. o. Nr. 9.2.1) erfolgt. Der Gesetzgeber hat zahlreiche Fristen zur Einführung medizinischer Anwendungen gesetzt und dies teilweise mit finanziellen Sanktionen verbunden, falls diese Fristen nicht eingehalten werden. So müssen z. B. bis zum 31. Dezember 2017 die Maßnahmen zur Einführung des Notfalldatenmanagements abgeschlossen sein. Nach derzeitigem Stand ist davon auszugehen, dass die Speicherung der Notfalldaten auf der elektronischen Gesundheitskarte die erste verfügbare medizinische Anwendung sein wird. Bereits seit Ende 2016 werden hierzu in dem Pilotprojekt „Notfalldatenmanagement-Sprint“ in der Region Münster umfangreiche Tests auf freiwilliger Basis durchgeführt.

Bis zum 31. Dezember 2018 müssen die Voraussetzungen für die Nutzung des Patientenfachs vorliegen. In dieses gemäß § 291a Absatz 3 Satz 1 Nummer 5 SGB V vorgesehene Patientenfach können Versicherte nicht nur eigene Daten einstellen, sondern auch Kopien sämtlicher anderer medizinischer Daten, die mittels der elektronischen Gesundheitskarte gespeichert sind, einfügen lassen (vgl. 25. TB Nr. 13.2). Die bisher schon geltenden erleichterten Zugriffsmöglichkeiten (keine Nutzung des Heilberufsausweises des Arztes, sondern Authentifizierung durch die Signaturkarte der Versicherten), hat der Gesetzgeber durch das E-Health-Gesetz nochmals verbessert. Da sich die Nutzung einer Signaturkarte in Deutschland entgegen der damaligen Erwartung nicht flächendeckend durchgesetzt hat, reichen künftig sonstige geeignete technische Verfahren zur Authentifizierung aus.

Ich werde auch weiterhin die Entwicklung der elektronischen Gesundheitskarte aufmerksam und kritisch begleiten. Dabei warte ich voller Spannung auf einen Bericht der Gesellschaft für Telematik, den diese bis zum 31. März 2017 dem Deutschen Bundestag vorzulegen hat und in dem die Nutzung mobiler und stationärer Endgeräte der Versicherten zur Wahrnehmung ihrer Zugriffsrechte auf ihre eigenen Daten untersucht werden soll.

9.3 Aus Beratung und Kontrolle

9.3.1 Mitgliedergewinnung einer Krankenkasse durch unzulässige Datenerhebung

Bemerkenswert, wie kreativ Krankenkassen bei der Mitgliedergewinnung sein können.

Wie ich durch die Eingabe eines Petenten erfahren habe, hat eine Geschäftsstelle der BARMER GEK Ausbildungsbetrieben Unterstützung bei der Suche nach geeigneten Auszubildenden angeboten. Gleichzeitig wurden die Sozialdaten bereits eingestellter Auszubildender abgefragt. Diese Daten wurden zur Mitgliedergewinnung erhoben.

Zum Zweck von Mitgliedergewinnung ist eine Datenerhebung jedoch nur erlaubt, wenn die Daten allgemein zugänglich sind. Allgemein zugänglich sind Daten, wenn der Zugang bzw. die Kenntnisnahme nicht in besonderer Weise beschränkt sind. Das ist z. B. bei nicht besonders geschützten Daten im Internet (Homepage des Betroffenen) der Fall. Die hier infrage stehenden Daten waren nicht allgemein zugänglich. Somit war eine Datenerhebung nicht zulässig. Nachdem ich an die BARMER GEK herangetreten war, wurde das Verfahren unverzüglich eingestellt.

9.3.2 Das Forderungsmanagement - aber wie?

Nach Presseberichten arbeiteten gesetzliche Krankenkassen mit der Schufa zusammen. Zur Aufklärung des Sachverhalts habe ich eine Umfrage an alle Krankenkassen gerichtet. Das Ergebnis forderte mein sofortiges Handeln.

Im Berichtszeitraum machte eine Meldung über die Zusammenarbeit der gesetzlichen Krankenversicherungen mit der Schufa Schlagzeilen. Eine Abfrage bei den meiner Datenschutzaufsicht unterstehenden Kassen ergab, dass einige von ihnen tatsächlich private Auskunfteien für die Ermittlung von Adress- oder in manchen Fällen auch Vermögensdaten zur Prüfung der Solvenz einschalteten. Diese Zusammenarbeit ist datenschutzrechtlich problematisch: Mit der Anfrage der gesetzlichen Krankenkassen bei Auskunfteien geht sowohl eine Datenübermittlung, -erhebung als auch -verarbeitung einher. Dies sind Eingriffe in das Recht auf informationelle Selbstbestimmung der Versicherten, die nur mit einer gesetzlichen Grundlage zulässig sind. Zwar dürfen die Krankenkassen nach § 284 Absatz 1 Nr. 3 SGB V Sozialdaten erheben und speichern, um die Beitragspflicht und die Höhe der zu leistenden Beiträge zu ermitteln. Eine großzügige Auslegung dieser Rechtsvorschrift dahingehend, eine Adress- oder gar Solvenzdatenermittlung sei also zulässig, scheitert aber an der tatsächlichen Erforderlichkeit. Denn Krankenkassen können weniger einschneidende Alternativen nutzen, beispielsweise Anfragen an die Meldeämter richten oder die öffentlichen Vollstreckungsportale der Länder in Anspruch nehmen. Entsprechend hat ein großer Teil der gesetzlichen Krankenkassen diese Möglichkeiten auch als ausreichend bewertet und auf die Einschaltung privater Auskunfteien verzichtet. Alle anderen habe ich dazu aufgefordert, eine Zusammenarbeit einzustellen. Das Bundesversicherungsamt teilt insoweit meine Auffassung.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.5; 1.6; 2.4; 21.1; 21.5; 22.7; 22.8; 22.10

10 Innenausschuss

10.1 Auswirkungen der DSGVO auf diesen Themenbereich

Im Zuständigkeitsbereich des Innenausschusses wird die EU-Datenschutz-Grundverordnung (DSGVO) nachhaltige Auswirkungen haben. Der Bereich der polizeilichen Tätigkeit (vgl. unter Nr. 10.2.9 f.) fällt jedoch unter den Geltungsbereich der Richtlinie für den Datenschutz im Polizei- und Justizbereich, die ebenfalls bis Mai 2018 umgesetzt werden muss. Beide sind Gegenstand des Entwurfs des Anpassungs- und -Umsetzungsgesetzes EU (vgl. o. unter Nr. 1.2 f.), das als Kern das neue Bundesdatenschutzgesetz (BDSG-neu) enthält.

Wie im gesamten öffentlichen Bereich gilt auch für den Bereich Inneres, dass die DSGVO weitgehende Öffnungsklauseln enthält. Insbesondere wird die konkrete Rechtsgrundlage für die Datenverarbeitung durch Behörden weiterhin häufig im nationalen Recht zu finden sein, beispielsweise für die Meldebehörden im Bundesmeldegesetz und den Meldegesetzen der Länder. Für die Tätigkeit der Nachrichtendienste findet die DSGVO keine Anwendung, weil es für diesen Bereich keine Zuständigkeit im Gemeinschaftsrecht gibt.

Die Datenschutz-Grundverordnung hat auch Auswirkungen auf das nationale Ausländer- und Asylrecht (vgl. hierzu unter Nr. 10.2.3) . Insbesondere mit Blick auf die weitreichenden Transparenz- und Informationsvorschriften in der DSGVO könnte sich hier ein Anpassungsbedarf ergeben. Durch die Aufnahme biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person in den Katalog der besonderen Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO ist deren Verarbeitung künftig an diesen gesonderten Regelungen zu messen.

Bei der Datenverarbeitung zu in öffentlichem Interesse liegenden Archivzwecken, zu Forschungszwecken und zu statistischen Zwecken (vgl. unter Nr. 10.2.2) sind gemäß Artikel 89 Absatz 1 DSGVO geeignete Garantien für die Rechte und Freiheiten der betroffenen Person vorzusehen. Nach Artikel 89 Absatz 2 DSGVO können einige Betroffenenrechte (beispielsweise das Auskunftsrecht und das Recht auf Widerspruch) unter bestimmten Voraussetzungen durch Gesetze der Mitgliedstaaten eingeschränkt werden.

Auch auf den Bereich des technologischen Datenschutzes (vgl. unter Nr. 10.2.11) wirkt sich die Datenschutz-Grundverordnung aus. Zukünftig werden Verfahren der Datenschutzfolgeabschätzung, der Zertifizierung, der Implementierung von Gütesiegeln eine neue Rolle spielen. Neu ist auch das Prinzip der Datenübertragbarkeit. Das in der DSGVO festgelegte Gebot der Datenminimierung und die Vorgaben eines Datenschutzes durch „privacy by design“ bzw. „privacy by default“ sind technologisch zu gestalten. Die detaillierte Ausgestaltung entsprechender technischer und organisatorischer Maßnahmen ist aktuell auf EU-Ebene in vollem Gange. Mit der Konkretisierung entsprechender Regelungen, wie z. B. der Erstellung von Richtlinien in den Bereichen Zertifizierung und Akkreditierung, ist insbesondere die Technology Subgroup (TS) als Unterarbeitsgruppe der Artikel-29-Gruppe befasst.

Darüber hinaus befasst sich die Artikel-29-Gruppe mit einer ganzen Reihe von Querschnittsthemen im Zusammenhang mit der praktischen Umsetzung und Anwendung der Datenschutz-Grundverordnung. Diese Aktivitäten sind unter Nr. 2.4 im Einzelnen dargestellt.

10.2 Einzelthemen

10.2.1 Novelle des Personalausweisgesetzes

Die von der Bundesregierung geplante Novelle für ein neues Personalausweisgesetz würde datenschutzrechtliche Standards verschlechtern.

Seit November 2010 wird der sog. neue bzw. elektronische Personalausweis sowie korrespondierend der elektronische Aufenthaltstitel ausgegeben (vgl. 23 TB Nr. 3.2). Auf einem Chip sind das biometrische Foto und, sofern gewünscht, auch die Fingerabdrücke gespeichert. Außerdem kann mit der sog. elektronischen Identitätsfunktion (eID-Funktion) die eigene Identität sicher auf elektronischem Wege gegenüber Behörden und Unternehmen bestätigt werden.

Die Nutzung der eID-Funktion ist bislang freiwillig. Wird ein neuer Ausweis ausgestellt, kann der Ausweisinhaber selbst entscheiden, ob diese Funktion aktiviert oder deaktiviert werden soll. Diese Wahlmöglichkeit soll nach dem Willen der Bundesregierung bald der Vergangenheit angehören, um damit die Verbreitung der eID-Funktion in der Bevölkerung zu fördern. Ich habe die Einführung der eID-Funktion immer unterstützt und halte sie weiterhin für ein sehr zuverlässiges Mittel, sich medienbruchfrei auf elektronischem Wege gegenüber anderen zu identifizieren. Die nunmehr obligatorische Aktivierung der eID-Funktion ist aus meiner Sicht hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion resultiert. Die Nutzung dieser Funktion sollte weiterhin freiwillig bleiben, damit das Selbstbestimmungsrecht der Bürgerinnen und Bürger weiterhin gewahrt bleibt.

Weitere Änderungen sind für das Verfahren zum Erhalt eines sog. Berechtigungszertifikates vorgesehen. Solche Zertifikate benötigen Behörden und Unternehmen, die die eID-Funktion in ihren Verfahren nutzen und so Bürger bzw. Kunden auf elektronischem Weg identifizieren möchten. Bislang prüft die sog. Vergabestelle für Berechtigungszertifikate (VfB) beim Bundesverwaltungsamt (BVA) vorab die Erforderlichkeit der Speicherung bzw. Übermittlung jedes einzelnen Datums aus dem Ausweis entsprechend dem vom Anbieter angegebenen Zweck. Dieses Verfahren ist zwar aufwändig, hat sich aber als sehr sinnvoll erwiesen, weil so von vorneherein Datenschutzverstöße verhindert werden konnten (vgl. auch Nr. 12.3.2). Künftig sollen Behörden und Unternehmen die Nutzung der eID-Funktion faktisch der VfB nur noch vorab anzeigen müssen. Eine Genehmigung ist nicht mehr erforderlich. Die Begrenzung des Zertifikates auf einen bestimmten Zweck ist ebenfalls nicht mehr vorgesehen. Hierdurch werden nach meiner Einschätzung Datenschutzverstöße zunehmen.

Außerdem sollen künftig mehrere Stellen einfacher ein einziges Zertifikat nutzen können. Dies mag für diese Stellen zwar praktisch und vor allem kostengünstig sein. Alle Beteiligten müssen sich dann allerdings bewusst sein, dass diejenige Stelle, die das Zertifikat verwaltet, verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften ist. Verstöße einzelner Zertifikatsnutzer gehen zur ihren Lasten.

Schließlich soll mit der Gesetzesnovelle geregelt werden, in welchem Umfang Ablichtungen von Ausweisen erlaubt sind. Eine solche gesetzliche Klarstellung hatte ich in der Vergangenheit erbeten, nachdem dieses Thema immer wieder an mich herangetragen worden war. Der Gesetzentwurf stellt insoweit auf die Einwilligung des Betroffenen ab. Zudem verweist er auf die „Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verarbeitung personenbezogener Daten“. Ich hätte mir gewünscht, dass insbesondere das datenschutzrechtliche Prinzip der Erforderlichkeit festgeschrieben worden wäre. Es dürfte nämlich fraglich sein, ob die Betroffenen tatsächlich stets ausreichend informiert werden und freiwillig in die Ablichtung ihres Personalausweises einwilligen.

In dem Gesetzentwurf vermisse ich zudem eine Klarstellung, inwieweit eine Hinterlegung des Personalausweises erlaubt ist. Die geltende Vorschrift ist in der Vergangenheit immer wieder unterschiedlich ausgelegt worden und hat zu datenschutzrechtlichen Problemen bei der Anwendung des Gesetzes geführt.

Ausdrücklich begrüße ich die Vorschläge der Bundesregierung zur Aufnahme neuer Bußgeldtatbestände für die unzulässige Nutzung der eID-Funktion bzw. das unerlaubte Kopieren bzw. Scannen von Ausweisen. Ich habe die Hoffnung, dass durch konsequentes Ahnden das rechtswidrige Kopieren von Ausweispapieren eingedämmt werden kann.

Das Gesetzgebungsverfahren war zum Ende des Berichtszeitraums noch nicht abgeschlossen. Zudem wird auch noch die Personalausweisverordnung novelliert. Ich werde beides weiter begleiten.

10.2.2 Zensus 2021

Aufgrund europarechtlicher Vorgaben müssen die Mitgliedsstaaten der Europäischen Union alle zehn Jahre eine Volkszählung durchzuführen. Nach 2011 steht damit der nächste Zensus in Deutschland im Jahr 2021 an.

Das BMI hat hierzu im Juli 2016 den Entwurf eines Gesetzes zur Vorbereitung eines registergestützten Zensus einschließlich Gebäude- und Wohnungszählung 2021 (Zensusvorbereitungsgesetz 2021- ZensVorbG2021) vorgelegt, der im November 2016 vom Bundeskabinett beschlossen (Bundestagsdrucksache 18/10458) und kurz nach Ende des Berichtszeitraums mit der zuletzt vom Innenausschuss empfohlenen Änderung (Bundestagsdrucksache 18/10880) vom Deutschen Bundestag angenommen worden ist.

Auch wenn das Gesetz den Zensus 2021 in rechtlicher, organisatorischer und technischer Hinsicht lediglich vorbereiten soll, enthält es eine Reihe von Regelungen mit datenschutzrechtlicher Relevanz. Im Rahmen der Ressortabstimmung konnte ich mich mit Erfolg dafür einsetzen, dass die Löschungspflicht nach § 16 ZensVorbG2021-E auch auf die im Rahmen der Durchführung dieses Gesetzes bei den Statistischen Landesämtern vorgehaltenen Datenbestände ausgedehnt wird. Allerdings ist die Verpflichtung zur Löschung an zwei alternativ anwendbare Voraussetzungen („frühestmöglich“ - „spätestens“) gebunden. Dies führt zu einer datenschutzrechtlich unbefriedigenden Handhabung der Regelung. Mein Einsatz für eine noch stärkere Beachtung der Grundsätze der Normenklarheit und -bestimmtheit in einzelnen Regelungen war leider nur zum Teil erfolgreich. So ist mein Hinweis, den Aufbau eines Steuerungsregisters nach diesem Gesetzentwurf von dem bereits bestehenden und dauerhaft vorgesehenen Anschriftenregister nach dem Bundesstatistikgesetz eindeutig und plausibel abzugrenzen, bedauerlicherweise nicht aufgegriffen worden. Die weitere Entwicklung werde ich intensiv begleiten.

10.2.3 Entwicklungen im Ausländer- und Asylrecht

Trotz des dringenden Handlungsbedarfs bei der Durchführung von Asylverfahren darf der Datenschutz im Ausländer- und Asylrecht nicht auf der Strecke bleiben.

Wie der Anstieg der Flüchtlingszahlen im Jahr 2015 gezeigt hat, waren die bisherigen Verfahren und Systeme zur Bewältigung eines solchen Ansturms nicht geeignet. Der Gesetzgeber hat daher im Berichtszeitraum in mehreren sog. Asylpaketen zahlreiche gesetzliche Änderungen vorgenommen. Der zweifellos bestehende Handlungsdruck führte dazu, dass die in der Gemeinsamen Geschäftsordnung der Bundesministerien für Gesetzgebungsverfahren vorgesehenen Fristen regelmäßig deutlich unterschritten wurden. Auch wenn die Zusammenarbeit mit den beteiligten Stellen stets konstruktiv war, die kurze Frist ist zu kritisieren, da eine sachgerechte Prüfung deshalb nicht immer möglich war.

Ausländerzentralregister

Zu den aus datenschutzrechtlicher Sicht wesentlichsten Neuerungen gehörte die Weiterentwicklung des Ausländerzentralregisters (AZR) zu einer zentralen Datenplattform für das Asylverfahren durch das Datenaustauschverbesserungsgesetz. Durch die Aufnahme zusätzlicher Daten und weiterer Stellen zur Nutzung des Registers sollte ein einheitlicher Datenpool für alle am Asylverfahren beteiligten Behörden geschaffen werden.

Grundsätzlich gilt der Datenschutz nicht nur für Inländer. Auf das den Datenschutz garantierende Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 GG i. V. m. Artikel 1 Absatz 1 GG können sich auch Ausländer berufen. Diesen Maßstab müssen alle Gesetze beachten.

So wurde meine Forderung, auf die beabsichtigte Ausweitung des automatisierten Zugriffs von Sicherheitsbehörden auf die Daten des AZR zu verzichten, aufgegriffen: Der ursprünglich vorgesehene Ausbau der Zugriffsmöglichkeiten des Bundesamtes für Verfassungsschutz im automatisierten Abrufverfahren wurde nicht umgesetzt, weil bereits nach geltender Rechtslage insoweit ausreichende Möglichkeiten bestanden.

Gerade die Datenspeicherung in zentralen Registern mit Zugriffsrechten einer Vielzahl von Stellen für unterschiedliche Zwecke bedarf stets einer genauen Prüfung der Erforderlichkeit der Speicherung, des Umfangs der zu speichernden Daten sowie der Zugriffsrechte von Behörden. Dies gilt in besonderer Weise für besondere Arten personenbezogener Daten, wie z. B. Gesundheitsdaten. Bloße Vereinfachungen im Verfahrensablauf oder Arbeitserleichterungen allein rechtfertigen nicht das Errichten zentraler Datenspeicher.

Aufgrund des massiven Ausbaus des AZR hat der Gesetzgeber nochmals klarstellend meine Rolle als Aufsichtsbehörde im Ausländerzentralregistergesetz hervorgehoben und regelmäßige Kontrollen gefordert (§ 34a AZR-Gesetz). Hinzu kommt die datenschutzrechtliche Aufsicht durch meine Kolleginnen und Kollegen in den Ländern, z. B. bezüglich der Ausländerbehörden. Der sich dadurch ergebende zusätzliche Aufwand für meine Dienststelle wird bisher allerdings nicht durch weitere personelle Ausstattung kompensiert. Ich appelliere daher an den Gesetzgeber, bei der Ausweitung von kontrollintensiven Verfahren stets auch die personelle Ausstattung der Aufsichtsbehörden im Auge zu behalten.

Bundesamt für Migration und Flüchtlinge

Mit dem starken Anstieg der Zahl von Asylverfahren ist auch das für deren Bearbeitung zuständige Bundesamt für Migration und Flüchtlinge (BAMF) gewachsen. Zur Zeit sind rund 10.000 Mitarbeiterinnen und Mitarbeiter in der Zentrale in Nürnberg und an den mehr als 80 über das gesamte Bundesgebiet verteilten Außenstellen tätig. Wegen des enormen personellen Bedarfs und des hohen politischen und öffentlichen Drucks war vielfach eine umfassende Einarbeitung der neuen Mitarbeiter nicht möglich. Bei einem Informationsbesuch in der Zentrale in Nürnberg konnten sich meine Mitarbeiter zwar davon überzeugen, dass bei den Beschäftigten des BAMF grundsätzlich die nötige Sensibilität für datenschutzrechtliche Belange besteht. Durch Beratungs- und Kontrollbesuche werde ich die Umsetzung der Neuregelungen in Zukunft datenschutzrechtlich begleiten.

10.2.4 Beratungsstelle Radikalisierung

Die Arbeit der Beratungsstelle Radikalisierung im Bundesamt für Migration und Flüchtlinge bedarf einer gesetzlichen Grundlage.

Die im BAMF angesiedelte Beratungsstelle Radikalisierung dient als erste Anlaufstelle u. a. für Angehörige, Freunde und Lehrer, die den Eindruck haben, ein Bekannter habe sich einer radikal islamistischen Gruppe zugewandt. Die Mitarbeiterinnen und Mitarbeiter geben Antworten auf häufige Fragen und vermitteln ggf. den Kontakt zu Hilfsangeboten vor Ort. Im Zuge dieser weiteren Beratung kooperiert das BAMF mit unterschiedlichen zivilgesellschaftlichen Trägern in den Ländern. Diese geben dem BAMF fortlaufend einen Überblick über den Stand der Beratung. Für diese Datenübermittlung und die darauf folgende Datenspeicherung, -verarbeitung und -nutzung durch das BAMF gibt es jedoch bislang keine ausreichende gesetzliche Grundlage. Da naturgemäß die Einwilligung der sich möglicherweise radikalisierenden Angehörigen nicht vorliegt, hat die Arbeit mit diesen personenbezogenen Daten derzeit keine gesetzlich verankerte Basis.

Im Rahmen eines Besuchs beim BAMF konnten sich meine Mitarbeiterinnen und Mitarbeiter über die gute und wichtige Arbeit der Beratungsstelle informieren. Die Rat suchenden Menschen werden hier kompetent betreut

und erhalten Unterstützung in einer vielfach ausweglos scheinenden Situation. Ich habe daher das Bundesministerium des Innern gebeten, diese wertvolle Arbeit durch eine gesetzliche Regelung zu stärken und die erforderlichen rechtlichen Grundlagen für die Verarbeitung der dabei anfallenden personenbezogenen Daten zu schaffen.

10.2.5 Immer wieder im Zentrum der Diskussion: die Videoüberwachung

Die Videoüberwachung bleibt sowohl in der datenschutzpolitischen Diskussion als auch in der praktischen Anwendung ein wichtiges Thema.

Vor dem Hintergrund der technologischen Entwicklung und des geänderten Sicherheitsbedürfnisses der Gesellschaft steht die Videoüberwachung immer wieder im Zentrum der Diskussion. Seit jeher gilt es, einen angemessenen Ausgleich zwischen den technischen Möglichkeiten, den berechtigten Interessen der Unternehmen und der öffentlichen Sicherheit einerseits und einem freien und unbeobachteten Verhalten der Menschen in Ausübung ihres Rechts auf informationelle Selbstbestimmung andererseits herzustellen.

So hat die Bedeutung der Videoüberwachung öffentlicher Räume durch Staat und Unternehmen in den letzten Jahren erheblich zugenommen. Videotechnik wird zur Überwachung von öffentlichen Straßen und Plätzen, öffentlichen Verkehrsmitteln und Bahnhöfen, aber auch in fast allen anderen Lebensbereichen eingesetzt, beispielsweise zur Überwachung von Kaufhäusern, Supermärkten, Gaststätten, Hotels und Geldinstituten. Rechtsgrundlage für die Videoüberwachung durch Unternehmen und Bundesbehörden ist § 6b BDSG. Soweit bereichsspezifische Gesetze des Bundes Regelungen zur Videoüberwachung enthalten (z. B. im Bundespolizeigesetz oder der Strafprozessordnung), finden ausschließlich diese Anwendung.

Im Berichtszeitraum hat der Düsseldorfer Kreis zwei wichtige Orientierungshilfen für den Bereich „Videoüberwachung“ beschlossen, die eine bundesweit einheitliche Auslegung und Praxis ermöglichen sollen:

Die Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ legt Kriterien fest, wann zur Wahrnehmung des Hausrechts und zum Schutz der Fahrgäste unter anderem in den Fahrgastbereichen der öffentlichen Verkehrsmittel Videoüberwachung zulässig ist.

Mit der Orientierungshilfe „Videoüberwachung in Schwimmbädern“ werden Hinweise zum zulässigen Einsatz der Videoüberwachung im Hinblick auf die schutzwürdigen Interessen der Schwimmbadbesucher gegeben.

Alle Beschlüsse des Düsseldorfer Kreises im Berichtszeitraum sowie die Orientierungshilfen sind im Kasten zu Nr. 10.2.5 aufgeführt und auf meiner Internetseite unter www.datenschutz.bund.de abrufbar.

Videoüberwachungsverbesserungsgesetz

Im Dezember 2016 beschloss das Bundeskabinett den Entwurf eines „Gesetzes zur Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz)“.

Der Entwurf ist eine Folge der Anschläge in Ansbach und München und soll im Ergebnis die Möglichkeiten zur Videoüberwachung durch private Betreiber von hochfrequentierten und besonders gefährdeten Orten wie Einkaufszentren, Stadien oder Bussen und Bahnen ausweiten.

Mit diesem Gesetz will die Bundesregierung insbesondere bei privatrechtlich betriebener Videoüberwachung an den genannten hochfrequentierten und gefährdeten Orten die Abwägungsentscheidung dahingehend verändern, dass auch wichtige Rechtsgüter der Öffentlichkeit (Leben, Gesundheit) besonders berücksichtigt werden müssen. Bisher dient die privatrechtliche Videoüberwachung unmittelbar zunächst nur den Interessen des Betreibers der Anlage, beispielsweise als Schutz vor Sachbeschädigungen oder Diebstahl.

Doch konnten unter bestimmten Umständen auch jetzt schon öffentliche Belange mittelbar als eigene Interessen berücksichtigt werden, zum Beispiel dann, wenn ein wirtschaftliches Interesse an einer möglichst großen Zahl von Besuchern besteht, die ausbleiben könnten, wenn sie Angst um ihre Sicherheit haben.

Oft scheitert die Rechtmäßigkeit der Videoüberwachung an diesen Orten allerdings nicht an der Interessenabwägung, sondern bereits an ihrer mangelnden Eignung. So entscheiden sich die Betreiber solcher Anlagen häufig aus Kosten- oder Verwaltungsgründen gegen die Errichtung einer Infrastruktur zur Echtzeitausweitung und beschränken sich stattdessen auf die reine Speicherung der Aufnahmen. In diesen Fällen mag durch die Überwachung zwar die Strafverfolgung erleichtert werden, aber ein größerer Schutz vor Gefahren wird hierdurch nicht erreicht.

Kasten zu Nr. 10.2.5

Beschlüsse des Düsseldorfer Kreises in den Jahren 2015 und 2016:

- Orientierungshilfe „Datenschutzanforderungen an Smart-TV-Dienste“
- Videoüberwachung in öffentlichen Verkehrsmitteln
- Videoüberwachung in Schwimmbädern
- Nutzung von Kameradrohnen durch Private
- Orientierungshilfe zur datenschutzrechtlichen Einwilligung in Formularen
- Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

10.2.6 Drohnen - mehr als ein flugtechnisches Geschicklichkeitsspiel?

Die Auswirkungen auf die Privatsphäre durch den Einsatz von Drohnen sind erheblich.

Unbemannte Luftfahrtsysteme - umgangssprachlich „Drohnen“ - haben in der gesellschaftlichen Wahrnehmung und in der alltäglichen Verwendung zugenommen. Drohnen werden mit Video- und Fotokameras ausgerüstet und sowohl im behördlichen als auch privaten Umfeld eingesetzt. Die dabei verwandte Technik wird immer leistungsfähiger und die Auswirkungen auf die Privatsphäre sind erheblich. Bereits in meinem letzten Tätigkeitsbericht hatte ich auf die Problematik ausführlich hingewiesen (vgl. 25. TB Nr. 5.6).

Im Berichtszeitraum wurde ich unter anderem auf die kommerzielle Nutzung der Drohne durch Postdienstleister aufmerksam gemacht.. Hierbei handelt es sich um einen stetig wachsenden Markt. Im Testbetrieb werden seit geraumer Zeit videoüberwachte Dienstleistungen zur Paketzustellung erbracht, die als Alternative zur privaten Abholung von Paketen etabliert werden sollen. Diese Entwicklung wird von mir aufmerksam verfolgt und im Falle meiner Zuständigkeit auf Beachtung der datenschutzrechtlichen Bestimmungen hin überprüft.

Nach meinen Informationen streben die EU-Verkehrsminister eine Harmonisierung des europäischen Luftraums für den Drohneneinsatz im Sichtflugbereich an. Daher wird auch die Aufnahme entsprechender datenschutzrechtlicher Vorgaben in das europäische Recht von mir ausdrücklich befürwortet (vgl. u. Nr. 2.4).

Auf nationaler Ebene setzt der Entwurf des Bundesministeriums für Verkehr und digitale Infrastruktur für eine Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten ein zentrales, datenschutzrechtliches Anliegen um.

Der Entwurf sieht vor, dass der Betrieb von unbemannten Luftfahrtsystemen, - also von Drohnen - und Flugmodellen über Wohngrundstücken verboten werden soll, wenn das Gerät oder seine Ausrüstung in der Lage ist, optische, akustische oder Funksignale zu empfangen, zu übertragen oder aufzuzeichnen. Mit dieser Regelung werden die Privatsphäre der Bürgerinnen und Bürger und damit auch ihr Recht auf informationelle Selbstbestimmung geschützt, indem etwa die Beobachtung von Wohngrundstücken mit kamerabestückten Drohnen verboten ist. Für Verstöße hiergegen sieht der Verordnungsentwurf Bußgelder vor. Dies begrüße ich ausdrücklich.

Der Verordnungsentwurf enthält lediglich drei Ausnahmen von diesem Verbot, die nachvollziehbar und daher unbedenklich sind.

Die erste Ausnahme greift, wenn der durch den Betrieb über dem jeweiligen Wohngrundstück in seinen Rechten betroffene Eigentümer oder sonstige Nutzungsberechtigte dem Überflug von unbemannten Luftfahrtsystemen und Flugmodellen, bei denen das Gerät oder seine Ausrüstung in der Lage ist, optische, akustische oder Funksignale zu empfangen, zu übertragen oder aufzuzeichnen, ausdrücklich zugestimmt hat.

Die zweite und dritte Ausnahme greifen dann, wenn der Betrieb von unbemannten Luftfahrtsystemen durch Behörden zur Erfüllung ihrer Aufgaben oder durch nichtbehördliche Organisationen im Bereich des Katastrophenschutzes und des Einsatzes bei Not- und Unglücksfällen oder unter deren jeweiliger Aufsicht erfolgt.

Das BMVI hat den Entwurf der Verordnung im Januar 2017 dem Bundesrat zur Zustimmung vorgelegt. Das Verfahren war bei Redaktionsschluss noch nicht abgeschlossen.

Auf ihrer Herbsttagung im November 2016 hat die 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder auch über das Thema „Autonome Systeme mit Videographie“ beraten. Hierbei wurde die Arbeitsgruppe Videoüberwachung, ein Arbeitsgremium des Düsseldorfer Kreises, beauftragt, eine rechtliche Bewertung vorzunehmen und die weitere Entwicklung kritisch zu begleiten.

Ich werde die Weiterentwicklung vor allem der kommerziellen Nutzung von Drohnen weiterverfolgen und die Beachtung datenschutzrechtlicher Vorgaben bei Bedarf einfordern.

10.2.7 Das neue Melderecht in der Praxis

Die Umsetzung des neuen Melderechts stellt die Praxis noch vor Herausforderungen.

Bereits in meinem letzten Tätigkeitsbericht hatte ich über das Gesetzgebungsverfahren zum Bundesmeldegesetz (BMG) berichtet (vgl. 25. TB Nr. 5.15). Das Gesetz ist nun zum 1. Januar 2015 in Kraft getreten. Damit gilt bundesweit ein einheitliches Melderecht. Wie sich aus den bei mir eingehenden Eingaben von Bürgerinnen und Bürgern, aber auch von Seiten der Wirtschaft und Interessenvertretungen zeigt, bereitet die Anwendung des Gesetzes teilweise noch Schwierigkeiten.

So wird z. B. von Betroffenen und kommunalen Mandatsträgern, aber auch von Seniorenverbänden kritisiert, dass die Datenweitergabe von Altersjubilaren z. B. an Presse oder Mandatsträger nunmehr erst ab dem 70. Geburtstag möglich ist, sofern hiergegen kein Widerspruch der betroffenen Person vorliegt (§ 50 Abs. 5 BMG). Bis zum Inkrafttreten des BMG konnten in einigen Ländern entsprechende Informationen auch bereits vor dem 70. Geburtstag weitergegeben werden. Andererseits erreichen mich aber auch Eingaben, bei denen Bürgerinnen und Bürger kritisieren, dass überhaupt eine Datenweitergabe erfolgt und es eines Widerspruchs bei der Meldebehörde bedarf, um dies zu unterbinden.

Die bestehende Widerspruchslösung ist angesichts der gegensätzlichen Kritiken ein geeigneter Kompromiss zwischen den unterschiedlichen Interessen.

Zudem haben mich Hinweise erreicht, nach denen vermehrt Abfragen zu Werbezwecken erfolgen sollen, ohne dass die erforderliche Einwilligung der Betroffenen gegenüber der anfragenden Stelle abgegeben worden ist. Aufgrund der vielfach bei den Meldebehörden bestehenden Unsicherheit möchte ich deswegen nochmals auf die Verteilung der Verantwortlichkeiten in diesem Bereich hinweisen: Die Meldebehörden haben nach § 44 Absatz 3 BMG stichprobenhaft das Vorliegen von Einwilligungserklärungen zu überprüfen. Liegen der Meldebehörde zur Einwilligungserklärung konkrete Anhaltspunkte für unrichtige Angaben der Auskunft verlangenden

Stelle vor, hat sie von Amts wegen zu ermitteln. Die Kontrolle des rechtmäßigen Umgangs mit den aus den Melderegistern abgefragten Daten (also insbesondere hinsichtlich der besonderen melderechtlichen Zweckbindung) ist Aufgabe der Datenschutzaufsichtsbehörden.

Sowohl von Seiten der Wirtschaft, als auch von Seiten der Meldebehörden wird darüber hinaus Kritik an der Regelung des sog. bedingten Sperrvermerks geübt. Ein solcher Vermerk ist von der Meldebehörde dann vorzunehmen, wenn eine Person z. B. in einer Justizvollzugsanstalt oder einer Pflegeeinrichtung untergebracht ist. Eine Melderegisterauskunft darf in diesem Fall nur erteilt werden, wenn eine Beeinträchtigung schutzwürdiger Interessen des Betroffenen ausgeschlossen werden kann (§ 52 Abs. 2 BMG). Dieser ist vor Erteilung einer Melderegisterauskunft zu hören. An dieser Regelung sollte festgehalten werden, da die Interessen der durch den bedingten Sperrvermerk geschützten Betroffenen damit wirksam berücksichtigt werden können.

Ich werde die weitere Entwicklung in der Praxis im Auge behalten und mich mit den Kolleginnen und Kollegen in den Ländern eng über deren Erfahrungen aus Kontrollbesuchen austauschen.

10.2.8 Nationales Waffenregister heute und in Zukunft

Das Nationale Waffenregister soll weiterentwickelt werden. Bereits heute erreichen mich zahlreiche Anfragen zur Datensicherheit.

Das Nationale Waffenregister ermöglicht die Zuordnung von Waffen sowie waffenrechtlichen Erlaubnissen, Ausnahmen, Anordnungen, Sicherstellungen oder Verboten zu bestimmten Personen. Neben den technischen Angaben zu den gespeicherten Waffen sind daher auch eine Vielzahl personenbezogener Daten im Register enthalten.

Im Berichtszeitraum erreichten mich wieder zahlreiche Eingaben besorgter Bürgerinnen und Bürger, die sich über die Sicherheit ihrer im Nationalen Waffenregister gespeicherten Daten Gedanken machten. Mehrere Petenten bezogen sich auf eine Äußerung eines bayerischen Landtagsabgeordneten, der in einer Debatte behauptet hatte, er habe Einblick in das Register nehmen können und verfüge über Kenntnisse zum Waffenbesitz eines Abgeordnetenkollegen. Die von mir erbetenen Protokollauswertungen des Bundesverwaltungsamtes (Registerbehörde) zeigten jedoch, dass der entsprechende Abgeordnete keine Zugriffsmöglichkeiten auf die Daten gehabt hatte. Auch im Übrigen konnte ein unberechtigter Datenabfluss ausgeschlossen werden. Im Rahmen der Eingabebearbeitung konnte ich keine Defizite der Datensicherheit im Bundesverwaltungsamt feststellen.

Im Rahmen eines Informationsbesuches bei der fachlichen Leitstelle in Hamburg konnten ich mich über deren Arbeit und die Datenbereinigung der in das Register überführten Datenbestände der lokalen Waffenbehörden informieren, die noch immer eine große Herausforderung darstellt.

Ich werde die Entwicklung weiterhin beobachten.

10.2.9 ... aus dem Bereich Innere Sicherheit: Polizei

Der Datenschutz im Bereich der Polizeibehörden ist in Bewegung. Auf der einen Seite haben die Entscheidung des Bundesverfassungsgerichts und die EU-Richtlinie für den Bereich Justiz und Inneres (JI-Richtlinie) neue rechtliche Maßstäbe gesetzt, die nun in Bundesrecht umzusetzen sind (vgl. Nr. 1.2.2, Nr. 1.3). Auf der anderen Seite sind durch neue Gesetze und laufende Gesetzgebungsverfahren große Veränderungen zu erwarten. Zu erwarten sind auch Veränderungen in der IT-Landschaft. Die Polizeibehörden werden in ihren Systemen künftig in größerem Umfang personenbezogene Daten verarbeiten. Vor allem aber besteht ein Trend, diese Daten innerhalb der Systeme stärker zu verknüpfen. Dies kann ich in meiner laufenden Tätigkeit bereits beobachten. Durch das neue Recht wird dieser Trend aber nochmals verstärkt, weil die bisherigen Dateigrenzen weitgehend entfallen.

Der Zusammenhang mit weiteren Themenbereichen, wie dem Austausch der Polizeibehörden mit den Nachrichtendiensten, der europäische Datenaustausch oder die weit im Gefahrenvorfeld stattfindende Auswertung von Daten in der Geldwäschebekämpfung darf dabei nicht übersehen werden. Nach der Rechtsprechung des Bundesverfassungsgerichts sind alle Maßnahmen, die insbesondere durch heimliche Ermittlungsmaßnahmen und Datenanalysen in das Grundrecht auf informationelle Selbstbestimmung eingreifen, stets im gesamten Zusammenhang zu betrachten. Dafür wurde der treffende Begriff der „Überwachungs-Gesamtrechnung“ geprägt.

10.2.9.1 Novellierung des BKAG

Der von der Bundesregierung beschlossene Gesetzentwurf zur Novelle des Bundeskriminalamtgesetzes wird die polizeiliche Datenlandschaft in Bund und Ländern grundlegend verändern. Ich sehe dabei viele datenschutzrechtliche Mängel.

Anlass des Entwurfs sollte eigentlich die Umsetzung der Urteile des Bundesverfassungsgerichts der jüngsten Zeit (vgl. o. Nr. 1.3), insbesondere zum Bundeskriminalamtgesetz, sowie der neuen EU-Richtlinie für den Datenschutz im Bereich Justiz und Inneres (JI-Richtlinie, vgl. o. Nr. 1.2.2) sein. Der Entwurf beschränkt sich aber nicht darauf, sondern schafft einen neuen relativ undifferenzierten Informationspool, führt zu wesentlich längeren Speicherfristen und berücksichtigt viele der datenschutzrechtlichen Forderungen an ein modernes polizeiliches Datenschutzrecht nicht.

Neuer Informationspool

Der Entwurf will die bisherigen Verbunddateien des bundesweiten INPOL-Systems abschaffen und durch einen neuen „Informationsverbund“ ersetzen. Die bisherige Differenzierung nach verschiedenen Dateien wird es dann in Zukunft nicht mehr geben. Dasselbe gilt für die internen Dateien des BKA, die der Gesetzentwurf durch ein „Informationssystem“ ersetzen will.

Das Bundesministerium des Innern und das BKA haben bislang keine konkreten Planungen für eine neue IT-Struktur vorgelegt. Diese sollten als erstes in schriftlicher und damit belastbarer Form vorliegen. Erst dann kann inhaltlich diskutiert werden, ob und ggf. welche gesetzlichen Anpassungen notwendig sind. Nach meiner Überzeugung kann das BKA die IT-Landschaft auch ohne die im Gesetzentwurf vorgesehenen fundamentalen Änderungen modernisieren. Insbesondere ist die vorgesehene vollständige Abkehr vom Dateibegriff dazu nicht notwendig. Solange konkrete Planungen fehlen, findet die Diskussion quasi im luftleeren Raum statt.

Die **Funktionalität der Systeme** soll nach dem Entwurf nur noch wenig begrenzt sein:

- Sämtliche Daten innerhalb des Informationssystems und des Informationsverbundes können prinzipiell miteinander verknüpft werden.
- Durch die Verknüpfung laufen die Aussonderungsprüffristen ins Leere.
- Alle Daten können miteinander abgeglichen werden.
- Die Methoden des Datenabgleichs sind nicht eingegrenzt.
- Jeder Abgleich kann zu weiteren Datenverknüpfungen führen und damit wiederum die Speicherdauer verlängern.
- Personen bleiben auch dann dauerhaft gespeichert, wenn ihre Daten in „strategische Analysen und Statistiken“ einfließen.

Durch die neue geplante Struktur werden die gespeicherten Daten nicht mehr einzelnen Dateien zugeordnet. Damit enthalten die in den jeweiligen Dateien zusammengefassten Daten **keine spezifischen Vorgaben mehr zum Zweck** der jeweiligen Speicherung, zu Aussonderungsprüffristen und zu den weiteren bislang in Errichtungsanordnungen vorgesehenen Verfahrenssicherungen.

Als Ersatz für die bisherigen Dateien wird nunmehr der Begriff der **Kategorien** benutzt. Es ist aber nicht klar, was darunter zu verstehen ist, wie die Kategorien genau gebildet werden sollen und wie sie voneinander abzugrenzen sind. Nicht hinreichend präzise ist geregelt und von den Behörden verbindlich festzulegen, zu welchen **Zwecken** in den jeweiligen Kategorien personenbezogene Daten gespeichert werden dürfen. Die Zweckbindung ist aber das zentrale Element der verfassungsgerichtlichen Rechtsprechung zum Datenschutz. Speichern und verknüpfen die Polizeibehörden personenbezogene Daten, dann kann dies intensiv in Grundrechte eingreifen. Die bisherige Rechtsprechung des Bundesverfassungsgerichts, die auf die Gefahren der automatisierten Datenverarbeitung hinweist, gilt weiterhin. Diese setzt voraus, für jedes gespeicherte Datum zu bestimmen, für welche konkreten Zwecke es gespeichert wird. Der **Grundsatz der Zweckbindung** gilt also weiterhin auch dann, wenn die Behörde die Daten nur intern und innerhalb derselben Aufgabenstellung verarbeitet.

Aussonderungsprüffristen

Wie der Gesetzentwurf ursprünglich vorsah, sollten diese künftig für alle zu einer Person gespeicherten Daten einheitlich an dem Tag beginnen, an dem die letzte Eintragung erfolgt ist. Diese Regelung orientiert sich nicht mehr daran, was für die Aufgabenerfüllung erforderlich ist und welchen Anlass der Betroffene für eine spätere Speicherung gegeben hat. Diese **„**Mitziehautomatik**“**, die einheitliche Speicherfristen ohne Differenzierung der einzelnen Speicherungen festlegt, hat der Bundestag aber im Gesetzgebungsverfahren gestrichen. Meine Kritik daran war also erfolgreich. Damit gilt insoweit weiter die bislang im BKAG vorgesehene Regelung.

Speicherungen zu einer Person können Ereignisse von unterschiedlichem Gewicht betreffen oder auf einer unterschiedlichen Tatsachenbasis beruhen. Der Betroffene kann rechtskräftig verurteilt sein oder nur wegen vager Verdachtsmomente gespeichert sein, etwa aufgrund einer später nicht verifizierbaren Anzeige, oder nur als Kontaktperson oder Opfer. Daher können nicht alle Fälle über einen Kamm geschoren werden. Eine „Mitziehautomatik“ in Verbundsystemen verstößt gegen Artikel 7 Absatz 2 der JI-Richtlinie und ist unverhältnismäßig.

Dieser Effekt wird durch neue IT-Strukturen nochmals verstärkt: Zunehmend basieren polizeiliche Datenbanken auf Systemen, die auf eine **Verknüpfung von Daten** ausgelegt sind (vgl. u. Nr. 10.2.9.3). Diese speichern nicht mehr personenorientierte Datensätze, sondern speichern ereignisorientiert. Die Daten zu einer Person werden mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignissen, Institutionen oder Sachen verknüpft wird. Die Zahl der Verknüpfungsebenen ist nicht begrenzt, so dass die zu einer Person gespeicherten Daten zunehmend diffundieren. Im Laufe der Zeit „reichern sie sich an“. Nach dem Entwurf soll die Berechnung der Fristen nicht mehr von dem zu der Person gespeicherten Ereignis abhängen. Das Gesetz will stattdessen auf die „letzte Eintragung“ und auf „alle zu einer Person gespeicherten Daten“ abstellen. Damit wird eine Person auch dann länger gespeichert, wenn zum Beispiel zu einem Mittäter später ein Eintrag ergänzt wird. Es „nützt“ dem Betroffenen dann nichts, wenn er inzwischen auf den Pfad der Tugend zurückgefunden hat („mitgefangen, mitgehangen“). Ich begrüße deshalb sehr, dass der Bundestag sich meiner Kritik angenommen hat und die Mitziehklausel aus dem Entwurf nicht übernommen hat.

Zusätzliche datenschutzrechtliche Änderungsvorschläge zur Novellierung des BKAG

1. **Datenschutzkontrolle:** Der Gesetzentwurf sollte die Datenschutzaufsicht stärken - sowohl hinsichtlich der Sachmittel- und Personalausstattung als auch der Kompetenzen. Sicherzustellen ist nicht nur die Kontrollbefugnisse auf dem Stand der Zeit zu halten, sondern auch die Durchsetzung. Stelle ich Verstöße gegen geltendes Recht fest, muss ich dagegen auch vorgehen können. Dazu bedarf es mindestens der Möglichkeit, ein gerichtliches Verfahren einzuleiten, damit unabhängige Richter entscheiden können.

2. **Zweckbindung:** Das Bundesverfassungsgericht hat in seinem Urteil zum BKAG (vgl. o. Nr. 1.3) den Grundsatz der Zweckbindung dogmatisch umrissen. Dabei hat es höhere Maßstäbe angelegt, wenn die Datenverarbeitung besonders intensiv in Grundrechte eingreift. Das Bundesverfassungsgericht hebt in verschiedenen Entscheidungen die spezifisch breitenwirksamen Grundrechtsgefährdungspotentiale hervor und betont dabei besonders die Auswirkungen der elektronischen Datenverarbeitung als intensiven Grundrechtseingriff. Wenn ein Datum im Einzelfall aufgrund eines Ermittlungsansatzes genutzt werden darf, be-

deutet dies nicht, es gleichzeitig in ein umfassendes Verknüpfungs- und Analysesystem einstellen zu dürfen. Begrenzungen und Verfahrenssicherungen dürfen nicht unverhältnismäßig gestrichen werden.

3. **Analysen und Profilbildung:** Computergestützte Analysen und Profilbildung mit Data-Mining-Methoden führen zu erheblichen Grundrechtseingriffen. Das Verknüpfen personenbezogener Daten ist deshalb gesetzlich zu begrenzen. Auch ein scheinbar harmloses Datum kann, wenn es in umfangreiche Datenbanken eingestellt und mit weiteren Daten verknüpft wird, tiefgreifende Aussagen zur Person des Betroffenen ermöglichen.

4. **Dateisysteme und verhältnismäßige Begrenzungen:** Die bisherige Aufteilung der Speicherungen in Dateien sollte beibehalten werden. Jede Speicherung ist ein eigenständiger Grundrechtseingriff. Deshalb müssen gesetzlich spezifische Eingriffsschwellen festgelegt werden. Je weniger „nah" eine Person mit einer konkreten Straftat oder Gefahr im Zusammenhang steht, desto weniger darf sie gespeichert werden. Die Aufhebung der abgegrenzten Dateistrukturen führt zu einer entgrenzten Datenverarbeitung, denn alle Daten sind dann nahezu beliebig miteinander verknüpfbar.

5. **Keine unreflektierte Aufgabenerweiterung:** Die Aufgaben des BKA dürfen nicht mit dehnbaren Begriffen wie „strategischen und operative Analysen" ausgeweitet werden, wenn gleichzeitig Aufgaben- und Befugnisnormen miteinander verschränkt werden.

6. **Errichtungsanordnungen:** An den bisherigen Errichtungsanordnungen ist festzuhalten. Darin sollte weiterhin der Inhalt der Dateien und der mit der Datei vorgesehene Verarbeitungszweck eingegrenzt werden. In Errichtungsanordnungen müssen die Polizeibehörden bislang Rechtsgrundlage und Zweck der Datei, Personenkreis und Inhalt der gespeicherten Daten, Prüffristen, Voraussetzungen, Empfänger von Datenübermittlungen und die Protokollierung festlegen. Durch die Beschreibung der Datei in einer Errichtungsanordnung wird die notwendige Transparenz geschaffen, auf die die Bürgerinnen und Bürger grundsätzlich einen Anspruch haben. Auch für die Beratungs- und Kontrollaufgabe der Datenschutzbeauftragten sind Errichtungsanordnungen essentiell. So wäre z. B. vor einer systematischen Kontrolle die Festlegung des Kontrollgegenstandes ohne dieses Wissen nicht möglich (vgl. u. Nr. 10.2.9.3).

7. **Unschuldsvermutung in polizeilichen Dateien:** Ein Kernanliegen des Datenschutzes ist es, die Unschuldsvermutung auch in polizeilichen Dateien zur Geltung zu bringen. Datenschutz ist rechtsstaatlicher Beschuldigtenschutz. Jedes Ermittlungsverfahren ist zunächst ergebnisoffen. Es kann sich herausstellen, dass der Betroffene die Tat nicht begangen hat oder sie ihm nicht nachgewiesen werden kann. Bislang müssen Daten aber erst dann gelöscht werden, wenn die Unschuld erwiesen ist. Wenn dem Beschuldigten lediglich die Tat nicht nachgewiesen werden kann, bedeutet das für ihn in der Regel, dass die Daten weiter gespeichert bleiben. Das kehrt die Unschuldsvermutung gegen die sonst geltenden Prinzipien um und widerspricht der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Bundesverfassungsgerichts. Bei der sog. **Negativprognose** ist daher der Grad des Tatverdachts zu berücksichtigen. Nach jedem gerichtlichen Freispruch sollte es künftig zur Regel werden, die Daten der betroffenen Person aus polizeilichen Datenbanken zu löschen. Dies sollte gesetzlich ausdrücklich klargestellt werden.

8. **Eng begrenzte Speicherung von „Prüffällen":** Die Speicherung so genannter Prüffälle habe ich immer wieder kritisiert (vgl. u. Nr. 10.2.9.3). Hier werden Daten zu Personen in Vorsorgedateien gespeichert, gegen die rechtlich im Zeitpunkt der Speicherung keine Negativprognose gestellt werden kann. Mit dem vorliegenden Entwurf sollen ausdrücklich Personen als „Prüffälle" gespeichert werden, obwohl sie keine Verdächtigen sind. Die „Anreicherung" ihrer Daten ist ausdrückliches Ziel. Eingriffsschwellen, die dem Eingriffsgewicht Rechnung tragen, wären datenschutzrechtlich der richtige Weg. Die Daten werden im Ergebnis zur Verdachtsgenerierung auf Vorrat gespeichert. Eine bloß befristete Speicherung löst das Problem nicht.

9. **Datenerhebungen:** In rechtspolitischen und verfassungsrechtlichen Diskussionen ist vielfach der Blick auf besonders spektakuläre Formen der Datenerhebung gerichtet. Dabei geraten allerdings leicht andere Befugnisse aus dem Blick. Diese mögen zwar im Einzelfall nicht so spektakulär sein, können aber in ihrer Tragweite gleichwohl erheblich sein. So ist der bisherige § 7 Absatz 2 BKAG recht unbestimmt und weit gefasst.

10.2.9.2 Polizeilicher Informations- und Analyseverbund in Betrieb

Der polizeiliche Informations- und Analyseverbund (PIAV) ist im Jahr 2016 mit einer ersten Datei in Betrieb gegangen. An dieser Datei wird sich zeigen, ob und welche Fragen sich im praktischen Betrieb des Systems stellen.

Vor der Einführung des PIAV hat eine Arbeitsgruppe der Datenschutzbeauftragten von Bund und Ländern die Planungen begleitet (vgl. 25. TB Nr. 5.13.2). Als praktisches Problem in der ersten eingerichteten Datei habe ich festgestellt, dass die Bundespolizei in ihrem Teilnehmersystem andere Fristen festgelegt hat als das Bundeskriminalamt im Zentralsystem. Derart unterschiedliche Fristen können zu Problemen führen. Ursache sind offenbar die Schnittstellen. Damit die Bundespolizei Daten an PIAV anliefern kann, muss diese aus technischen Gründen eine Transferdatei einrichten.

Eine weitere praktische Frage ist, wie mit Altdaten umgegangen wird, die aus bereits bestehenden Dateien in PIAV-Dateien übertragen werden. Für die Falldatei Rauschgift hat das Bundeskriminalamt z. B. ein Migrationskonzept vorgestellt (vgl. u. Nr. 10.3.2).

Ich werde die weitere Inbetriebnahme des Systems datenschutzrechtlich begleiten.

10.2.9.3 Zentralstellen- und Strafverfolgungsdateien beim BKA

Die Kontrolle der beim BKA gespeicherten personenbezogenen Daten führt immer wieder zu Schwierigkeiten und rechtlichen Problemen.

Die datenschutzrechtliche Kontrolle und Bewertung der polizeilichen Dateien sind Teil meiner ständigen Tätigkeit. Dies beginnt mit dem Anhörungsverfahren zu Errichtungsanordnungen für neue oder geänderte Dateien und setzt sich mit datenschutzrechtlichen Kontrollen im laufenden Betrieb fort. Auch Eingaben von betroffenen Bürgerinnen und Bürgern geben dafür oft wichtige Impulse. Dies hat im Bereich des Bundeskriminalamts im laufenden Berichtszeitraum wieder zahlreiche grundsätzliche Fragen aufgeworfen.

Die polizeiliche Datenverarbeitung entwickelt sich kontinuierlich weiter. Zunehmend werden Dateien auf der technischen Grundlage „b-case“ (vgl. u Nr. 10.3.4) betrieben. Diese speichern nicht mehr personenorientierte Datensätze, sondern sie arbeiten ereignisorientiert, d. h. die Daten zu einer Person werden mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignissen, Institutionen oder Sachen verknüpft wird. Da die Zahl der Verknüpfungsebenen nicht begrenzt ist, diffundieren die zu einer Person gespeicherten Daten zunehmend in größeren Datenbeständen (vgl. o. Nr. 10.2.9.1, Kasten zu Nr. 10.2.9.1). Dies spielt vor dem Hintergrund meiner Anregungen und Bewertungen immer eine Rolle.

Ein zentrales Problem stellt immer wieder die Rechtsgrundlage der Dateien dar. So führt das Bundeskriminalamt Dateien teilweise auf der Grundlage des § 483 Strafprozessordnung (StPO). Danach darf die Strafverfolgungsbehörde eine Datei für Zwecke „des Strafverfahrens“ führen, womit ein bestimmtes Strafverfahren gemeint ist. Diese Norm enthält keine Voraussetzungen und Bedingungen. Das ist verfassungsrechtlich akzeptabel, wenn man eine Datei auf ein einzelnes Strafverfahren begrenzt. In Betracht kommen hier vor allem besonders umfangreiche Verfahren, deren Akten mehrere Regalmeter enthalten können. Bedenken habe ich aber, auf

dieser Grundlage fallübergreifende Dateien zu führen. Dies würde letztlich die rechtlichen Begrenzungen für übergreifende Dateien und Verbundsysteme unterlaufen. Diese setzen engere Vorgaben, wenn etwa die Daten eines Beschuldigten oder eines Zeugen in künftigen Verfahren, also für die Gefahrenvorsorge, genutzt werden sollen. Würde man solche Dateien zulassen, könnten etwa die Daten zu Zeugen oder Geschädigten fallübergreifend und umfassend ausgewertet werden.

Darüber hinaus geht es vielfach um die Frage, in welchem Umfang Datenbanken auf die Generalklausel des § 7 Absatz 1 BKAG gestützt werden können. Dies betraf wie schon in früheren Berichtszeiträumen vor allem die so genannten **Prüffälle** (vgl. 24. TB Nr. 7.4.4). Unzulässig ist es z.B. eine Person zu speichern, bei der noch unklar ist, ob sie ausreichenden Anlass für eine Speicherung gegeben hat. Nicht tragbar ist es insbesondere, solche Personen nur mit dem Ziel der „Anreicherung" der Daten zu speichern.

Eine Besonderheit sind Prüfdateien, in denen Prüffälle in einem bislang nicht gekannten Umfang gespeichert werden. In einer neuen Datei speichert das Bundeskriminalamt die Daten aus den **Funkzellenabfragen** aus einer Vielzahl von Verfahren aus verschiedenen Bundesländern und gleicht diese miteinander ab. Nach meiner Auffassung handelt es sich der Sache nach um eine **Rasterfahndung** gemäß § 98a StPO. Das Bundeskriminalamt und das Bundesministerium des Innern sind jedoch der Auffassung, eine solche Datei auf die Generalklausel des § 7 Absatz 1 BKAG stützen zu können. Diese Datenverarbeitung hat eine hohe Streubreite und enthält die Daten einer Vielzahl von Personen, die selbst keinen Anlass für eine Speicherung gegeben haben. Dies kann nur auf Grundlage einer spezifischen Rechtsgrundlage erfolgen, die Voraussetzungen und Umfang verhältnismäßig regelt. Die Generalklausel genügt dafür nicht. Ich sehe mich durch einzelne Gerichtsentscheidungen bestätigt, die bei Funkzellenabfragen gleichzeitig einen Beschluss gemäß § 98a StPO fassen. Auf die Datei aufmerksam geworden bin ich im Verfahren der Anhörung zur Errichtungsanordnung. Ich beabsichtige, sie einer datenschutzrechtlichen Kontrolle zu unterziehen. Zahlen liegen mir noch nicht vor, ich gehe aber davon aus, dass eine solche Datei prinzipiell eine sehr hohe Anzahl von Daten enthalten kann.

In einer Vielzahl von Dateien führt das Bundeskriminalamt **„ermittlungsunterstützende Hinweise" (EHW) als neues Speicherdatum** ein. Betroffen sind auch bundesweite Verbunddateien. Zuvor waren nur „personengebundene Hinweise" (PHW) vorgesehen. Diese sind gesetzlich legitimiert und dienen der Eigensicherung der Polizei und dem Schutz der betroffenen Person (z. B. „bewaffnet", „gewalttätig", „Suizidgefahr"). Die neuen EHW sollen die betroffene Person aber darüber hinaus klassifizieren und eine schnelle Einstufung ermöglichen (z. B. „Rocker", „politisch motivierter Straftäter"). Anders als bei bisherigen PHW sind keine besonderen Fristen vorgesehen. Das „Etikett" hängt den Betroffenen also im Zweifel für die gesamte Speicherdauer an. Nach meiner Auffassung haben EHW einen stärker stigmatisierenden Charakter. Sie können nicht mit dem legitimen Zweck der Eigensicherung der eingesetzten Beamten gerechtfertigt werden. Wie bei allen polizeilichen Daten ist zu berücksichtigen, dass es nicht nur um verurteilte Straftäter geht. Ein Großteil aller polizeilichen Daten betrifft Personen, die nur wegen eines Verdachts gespeichert sind. Das mit dem EHW vergebene Etikett erhalten also auch solche Personen, deren Daten beispielsweise bei einer Demonstration erfasst wurden, gegen die ein Strafverfahren aber später wegen mangelnder Beweise eingestellt wurde oder die sogar freigesprochen wurden. Die Kriterien, nach denen EHW vergeben werden, sind völlig unklar. Ich habe das Bundesministerium des Innern gebeten, mir für alle geplanten EHW im Einzelnen zu erläutern, nach welchen genauen Kriterien und auf welcher Rechtsgrundlage diese jeweils vergeben werden. Leider habe ich bislang nur die allgemeine Antwort erhalten, die EHW seien von den Gremien der Innenministerkonferenz so beschlossen worden. Der Vorgang ist noch nicht abgeschlossen.

Die Reaktion auf meine Anmerkungen im **Anhörungsverfahren zu Errichtungsanordnungen** war auch in anderen Fällen nicht zufriedenstellend. So habe ich immer wieder auf die fehlende Protokollierung verschiedener Dateien hingewiesen. Eine Änderung der bestehenden Praxis wurde immer wieder abgelehnt. Leider ist es mir bislang verwehrt, in derartigen Fällem die Gerichte anzurufen. Das Anhörungsverfahren hat sich für meine Arbeit aber gleichwohl als sehr wichtig erwiesen, da es Ansatzpunkt für mein weiteres Tätigwerden und für datenschutzrechtliche Kontrollen bietet. Viele Problemlagen wären mir ohne das Anhörungsverfahren verborgen geblieben (vgl. a. u. Nr. 10.2.9.1).

Die hier aufgeworfenen Fragen führen auch in **Einzelfällen** zu Problemen, zu denen sich betroffene Bürgerinnen und Bürger mit der Bitte um Unterstützung an mich wenden. So habe ich in einem Fall festgestellt, dass die Speicherung eines Falls von der Auskunft an einen Petenten ausgenommen worden war; dies hat das BKA nunmehr nachgeholt. In einem anderen Fall habe ich bemerkt, dass ein Petent über 30 Jahre als Kontakt- und Begleitperson gespeichert war, obwohl der letzte nachgewiesene Kontakt in den 1980er Jahren stattgefunden hatte.

10.2.10 ... aus dem Bereich Innere Sicherheit: Nachrichtendienste

Die Nachrichtendienste sind wesentliche Säulen der Sicherheitsarchitektur (vgl. 23. TB Nr. 7.1.1, 22. TB Nr. 4.2, 21. TB Nr. 5.1) und müssen insbesondere auch international kooperieren; die Vorgaben des Bundesverfassungsgerichts sind aber - auch insoweit - stets zu beachten. Daraus ergeben sich Handlungspflichten für den Gesetzgeber - auch in Bezug auf die personelle Ausstattung der Kontrollorgane.

Innerhalb der Sicherheitsarchitektur der Bundesrepublik Deutschland nehmen die Nachrichtendienste eine zentrale Stellung ein. Zutreffend betont das Bundesverfassungsgericht in seinem Beschluss vom 13. Oktober 2016 (BVerfG, Beschluss des Zweiten Senats vom 13.10.2016, Az.: 2 BvE 2/15, Rn. 126): „Nachrichtendienste sind Ausdruck der Grundentscheidung des Grundgesetzes für eine wehrhafte Demokratie, des Selbstbehauptungswillens des Rechtsstaates und damit Bestandteil des Sicherheitssystems der Bundesrepublik Deutschland (...)."

Nachrichtendienste haben besondere Aufgaben und Befugnisse. Sie dürfen so frühzeitig wie keine andere Behörde und auch weitreichend und heimlich in die Grundrechte der Betroffenen eingreifen (vgl. o. Nr. 1.3). Die Kontrolle der Nachrichtendienste ist dabei eine notwendige Kompensation zum Schutz der Grundrechte der Betroffenen (vgl. o. Nr. 1.3). Diese Funktion hat das Bundesverfassungsgericht den Kontrollorganen und damit auch mir zugewiesen.

Die im Berichtszeitraum verübten Terroranschläge verdeutlichen in besonderer Weise, welche globalen Bedrohungen der freiheitlich demokratischen Grundordnung existieren, die nur durch eine intensive internationale Zusammenarbeit abgewehrt werden können. Der umfängliche Austausch personenbezogener Daten ist ein Wesenselement dieser Kooperationen.

Die Tätigkeit der Nachrichtendienste muss aber - auch im Rahmen dieser Kooperation - verfassungskonform erfolgen. Verfassungskonformität bedeutet auch, dass die Dienste im Sinne der verfassungsgerichtlichen Vorgaben effizient und wirksam kontrolliert werden müssen und der Gesetzgeber den zuständigen Kontrollorganen die hierfür notwendigen Voraussetzungen gewähren bzw. diese schaffen muss (vgl. o. Nr. 1.3). Effiziente Sicherheitsgewährleistung und wirksame Datenschutzkontrolle sind zwei Seiten derselben Medaille.

10.2.10.1 Effiziente und verfassungskonforme Abwehr des Terrorismus unerlässlich

Der Gesetzgeber hat die Befugnisse des Bundesamtes für Verfassungsschutz (BfV) und des Bundesnachrichtendienstes (BND) im Bereich der internationalen Zusammenarbeit gestärkt und für die Ausland-Ausland-Fernmeldeaufklärung des BND eine gesetzliche Rechtsgrundlage geschaffen. Ich teile die Intention des Gesetzgebers, sehe zugleich aber verfassungsrechtliche Risiken - auch im Hinblick auf die Beschränkung meiner Kontrollkompetenz.

Im Jahr 2016 sind im Sicherheitsbereich mit dem Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus und dem Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes weitere zentrale Gesetze in Kraft getreten.

Durch die Verbesserung des Informationsaustauschs bei der Terrorismusbekämpfung sollen die Erkenntnisse einer Vielzahl von Behörden national und insbesondere auch international zusammengeführt und übergreifend analysiert werden. Ich befürworte die gesetzgeberische Zielsetzung für eine verbesserte Zusammenarbeit, denn die Bedrohung durch den internationalen Terrorismus kann nur durch eine effiziente internationale Kooperation abgewendet werden (vgl. o. Nr. 1.3 und Nr. 10.2.10).

Zu Recht betont das Bundesverfassungsgericht in seinem Beschluss vom 13. Oktober 2016 (BVerfG, Beschluss des Zweiten Senats vom 13.10.2016, Az.: 2 BvE 2/15, Rn. 125): *„Straftaten mit dem Gepräge des Terrorismus zielen auf die Destabilisierung des Gemeinwesens und umfassen in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes. Die Bereitstellung von wirksamen Aufklärungsmitteln zu ihrer Abwehr ist ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht (...).“* Die auch in Deutschland erfolgten Terroranschläge verdeutlichen dies in dramatischer Weise.

Es ist das Wesensmerkmal des demokratischen Rechtsstaates, der globalen Bedrohung effizient und zugleich verfassungskonform zu begegnen. Dies sind zwei Seiten derselben Medaille, die untrennbar miteinander verbunden sind. Würde man dies aus dem Blick verlieren, hätte der Terrorismus sein Ziel erreicht.

Dies bedeutet: Wir müssen den internationalen Terrorismus effektiv abwehren und bekämpfen - aber unter Wahrung unserer Verfassung und der hierzu ergangenen Rechtsprechung des Bundesverfassungsgerichts.

Dies habe ich in meinen Stellungnahmen anlässlich der öffentlichen Sachverständigenanhörungen des Deutschen Bundestages zu den genannten Gesetzen deutlich gemacht.

Das Bundesverfassungsgericht hat in einer Reihe aktueller Entscheidungen grundlegende Anforderungen an Eingriffsschwellen, Eingrenzung des betroffenen Personenkreises sowie an Transparenz und Kontrolle aufgestellt (zuletzt in den Entscheidungen zum Bundeskriminalamtgesetz und zum Antiterrordateigesetz, vgl. o. Nr. 1.3, 25. TB Nr. 5.2).

Das Gericht hat mir dabei eine Kompensationsfunktion zum Schutz der Grundrechte der Betroffenen zugewiesen (vgl. o. Nr. 1.3). Insbesondere im Bereich der Nachrichtendienste ist der schwach ausgestaltete Individualrechtsschutz durch effiziente, wirksame und regelmäßige Datenschutzkontrollen zu kompensieren (vgl. o. Nr. 1.3 und Nr. 10.2.10).

Diese Vorgaben sind auch im Rahmen der internationalen Kooperation der Nachrichtendienste mit ausländischen Sicherheitsbehörden zu berücksichtigen (vgl. o. Nr. 1.3).

Mit den o. g. Gesetzen werden das BfV und der BND erstmals ermächtigt, gemeinsame Dateien mit ausländischen Sicherheitsbehörden im Inland zu führen und an gemeinsamen Dateien teilzunehmen, die von ausländischen Stellen im Ausland geführt werden. Zielsetzung ist, möglichst alle Erkenntnisse in einer Datei zusammen zu führen, diese allen zugänglich zu machen, sie automatisiert zu analysieren und daraus neue Erkenntnisse und Ermittlungsansätze zu gewinnen.

Die Besonderheit dieser gemeinsamen Dateien besteht - im Gegensatz zu einer Datenübermittlung - darin, dass jede Stelle für die von ihr dort gespeicherten Daten nach dem nationalen Recht ihres Staates ausschließlich - auch datenschutzrechtlich - verantwortlich ist (vgl. § 27 Abs. 2 BNDG; § 22b Abs. 6 BVerfSchG). D. h.: BfV und BND tragen für ihre Daten alleine die Verantwortung, dass die nach deutschem Recht bestehenden (Datenschutz-)Vorgaben auch in diesen Dateien beachtet werden.

Entsprechend der verfassungsgerichtlich vorgegebenen Kompensationsfunktion muss ich dies adäquat überprüfen können. Für eine effiziente Datenschutzkontrolle ist es deswegen u. a. erforderlich, die von deutscher Seite in einer von einem ausländischen Nachrichtendienste (AND) geführten gemeinsamen Datei gespeicherten Daten dort, d. h. in dieser Datei, sehen zu können. Es genügt beispielsweise nicht, im Inland beim BfV bzw. BND zu

prüfen, welche Daten dorthin übertragen worden sind. Dies verdeutlicht exemplarisch meine Kontrolle der Antiterrordatei. Nur durch einen Abgleich der Daten beim BfV mit den Speicherungen in der Antiterrordatei (ATD) habe ich feststellen können, dass das BfV nach dem Artikel-10-Gesetz erhobene und in seinen Dateien gekennzeichnete Daten automatisiert in die ATD übertragen hatte, diese Daten aber in der ATD ungekennzeichnet gespeichert waren (vgl. u. Nr. 10.3.5). Das Bundesministerium des Innern hat im Rahmen der Ressortberatungen erklärt, mir stünde keine Befugnis zur Kontrolle der Daten des BfV in einer von einem AND geführten Datei durch Einsichtnahme in die dort gespeicherten Daten des BfV zu.

Ich empfehle dem Gesetzgeber, eine entsprechende Klarstellung vorzunehmen und dadurch ein weiteres verfassungsrechtliches Risiko zu vermeiden.

10.2.10.2 Zusammenarbeit mit Gremien des Deutschen Bundestages

Die vertrauensvolle Zusammenarbeit aller Kontrollorgane ist für mich der Schlüssel zu der vom Bundesverfassungsgericht geforderten wirksamen, umfassenden und effizienten Kontrolle der Nachrichtendienste und zur Vermeidung von Kontrolllücken.

Das Bundesverfassungsgericht räumt einer wirksamen und umfassenden Kontrolle der von den Sicherheitsbehörden erhobenen personenbezogenen Daten eine große Bedeutung ein. In seiner Entscheidung zur Antiterrordatei (ATD) führt es hierzu aus (BVerfG, Urteil vom 24.04.2013, Az. 1 BvR 1215/07, Rn. 214 ff.; bekräftigt im Urteil zum BKAG, Urteil vom 20.04.2016, Az. 1 BvR 966/09, Rn. 140 ff. - vgl. Nr. 1.3):

„Weil eine Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen.“ (vgl. o. Kasten b zu Nr. 1.3).

In diesem Verständnis sind das legitime Dateninteresse der Dienste und der gebotene Schutz des Grundrechts auf informationelle Selbstbestimmung in unserem demokratischen Rechtsstaat - ebenso wie Sicherheit und Freiheit - zwei Seiten derselben Medaille.

Mit Blick auf die ATD-Entscheidung hatte bereits die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg die Entschließung „Effektive Kontrolle von Nachrichtendiensten herstellen!“ gefasst und darauf hingewiesen, eine Verteilung der Kontrolle auf mehrere Stellen dürfe nicht die Effektivität dieser Kontrolle einschränken (vgl. 25. TB Anlage 11).

Um diesem verfassungsgerichtlichen Kontrollauftrag gerecht zu werden, habe ich auch im zurückliegenden Berichtszeitraum die parlamentarischen Kontrollgremien, namentlich das Parlamentarische Kontrollgremium, das Vertrauensgremium des Haushaltsausschusses, die G-10-Kommission und den NSA-Untersuchungsausschuss in ihrer Arbeit unterstützt.
Unter Wahrung der Geheimschutzvorgaben habe ich die Gremien über die Ergebnisse meiner Arbeit, insbesondere auch über meine Kontrolle der Außenstelle des BND in Bad Aibling (vgl. u. Nr. 10.3.6), unterrichtet und an Sitzungen der Kontrollgremien teilgenommen und dort berichtet; einer meiner Mitarbeiter hat die Sitzungen des NSA-Untersuchungsausschusses begleitet.

Es ist mir ein wichtiges Anliegen, das verfassungsgerichtliche Leitbild der Kooperation in der Kontrollpraxis mit Leben zu füllen. In seiner vorgenannten Entscheidung (BVerfG, a. a. O., Rn. 216) führt das Bundesverfassungsgericht insoweit aus:

„Ebenfalls ist zu gewährleisten, dass im Zusammenspiel der verschiedenen Aufsichtsinstanzen auch eine Kontrolle der durch Maßnahmen nach dem Artikel-10-Gesetz gewonnenen Daten - die in einer Datei, welche maßgeblich auch vom Bundesnachrichtendienst befüllt wird, besondere Bedeutung haben - praktisch wirksam sichergestellt ist. Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen."

In der zweiten Jahreshälfte 2015 habe ich erstmalig eine gemeinsame ATD-Pflichtkontrolle mit der G-10-Kommission des Deutschen Bundestages beim BfV in Berlin durchgeführt, die zu mehreren Beanstandungen geführt hat (vgl. u. Nr. 10.3.5). Diese enge Kooperation hat für mich Vorbildcharakter. Ich werde mich dafür engagieren, den gemeinsamen Kontrollansatz auch bei künftigen Kontrollen weiterzuverfolgen. Dieser ist Garant dafür, etwaige Kontrolllücken bei Eingriffen in das Brief-, Post- und Fernmeldegeheimnis nach Artikel 10 GG auszuschließen (vgl. u. Nr. 10.2.10.3; 24. TB Nr. 7.7.2).

Nicht unerwähnt lassen möchte ich, dass am 30. November 2016 das Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes in Kraft getreten ist. Mit diesem wird die stärkere Verzahnung der parlamentarischen Kontrollgremien weiter vorangetrieben. Ich begrüße diese deutliche Stärkung der parlamentarischen Kontrolle und freue mich auf die künftige Zusammenarbeit mit dem neu gewählten Ständigen Bevollmächtigten sowie seinem Leitenden Beamten. Leider wurde das mit dem neuen BNDG geschaffene Unabhängige Gremium zur Kontrolle der Ausland-Ausland-Fernmeldeüberwachung vom Inland aus nicht beim Deutschen Bundestag angesiedelt. Dies darf aber nicht zu einer Zersplitterung der Kontrolllandschaft führen, sondern muss im Sinne der Grundrechtsträger ebenfalls zu einer Stärkung der Kontrolle beitragen. Auch insoweit hoffe ich auf eine enge und vertrauensvolle Zusammenarbeit mit den Mitgliedern dieses Unabhängigen Gremiums.

10.2.10.3 Kontrollfreie Räume - ein noch nicht (vollständig) gelöstes Problem

Zusagen und Vereinbarungen sind hilfreich - gesetzliche Klarstellungen jedoch unerlässlich.

Ich hatte bereits in meinem 24. Tätigkeitsbericht (Nr. 7.7.2) darauf hingewiesen, dass die äußerst restriktive Gesetzesauslegung des Bundesministeriums des Innern im Spannungsfeld der Kontrollzuständigkeiten von G-10-Kommission (§ 15 Abs. 5 Satz 2 G-10-Gesetz) und mir (§ 24 Abs. 2 Satz 1 Nr. 1 und Satz 3 BDSG) in der Kontrollpraxis zu kontrollfreien Räumen führt.

Im Berichtszeitraum ist es mir in zahlreichen Gesprächen gelungen, das BMI zu einer Änderung seiner Rechtsauffassung zu bewegen. Zusammen mit dem gemeinsamen Kontrollansatz G-10-Kommission/BfDI (vgl.. Nr. 10.2.10.2 und. Nr. 10.3.5) ist dies ein wichtiger Schritt hin zu einem besseren Schutz des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung. Diese geänderte Rechtsauffassung muss in der Kontrollpraxis allerdings zunächst noch mit Leben gefüllt werden und entstandene Unsicherheiten bei den beteiligten Behörden sind im Sinne eines effektiven Grundrechtsschutzes zu beseitigen.

Ich nenne drei Beispiele, bei denen noch Handlungsbedarf besteht. So fand etwa der - lange vor der Kontrolle angekündigte und bekannte - gemeinsame Kontrollansatz G-10-Kommission/BfDI bei der bereits erwähnten Pflichtkontrolle der Antiterrordatei beim BfV in Berlin (vgl. o. Nr. 10.2.10.2 und u. Nr. 10.3.5) trotz der geänderten Rechtsauffassung vor Ort zunächst keine Akzeptanz bei den anwesenden Mitarbeitern des BMI und des BfV, was den Ablauf der Kontrolle massiv beeinträchtigte.

Was meine formelle Beanstandung hinsichtlich der mangelnden Kennzeichnung von G-10-Daten anbelangt, wurden meine Sachfeststellungen zwar bestätigt. Vom BMI wird aber meine Befugnis zur Überprüfung dieser Kennzeichnung nunmehr mit der Behauptung der alleinigen Kontrollzuständigkeit der G-10-Kommission negiert und die Auffassung vertreten, derartige Rechtsverstöße dürfe ich nicht beanstanden. Diese Auffassung ist unzutreffend, denn das Antiterrordateigesetz als eine bereichsspezifische Regelung begründet auch meine Kontrollzuständigkeit.

Schließlich hatte ich - nach meinen Erfahrungen bei der Kontrolle der Außenstelle des BND in Bad Aibling (vgl. u. Nr. 10.3.6) - beabsichtigt, einen Informations- und Kontrollbesuch für den Bereich Technische Aufklärung des BfV durchzuführen. Auch dies ist mir in weiten Teilen zunächst mit dem Hinweis verwehrt worden, überwiegend sei ausschließlich eine Zuständigkeit der G-10-Kommission gegeben. Bis Redaktionsschluss konnte eine abschließende Klärung noch nicht herbeigeführt werden.

Unabhängig von der Klärung dieser Zuständigkeitsfragen, die sich im Übrigen nicht im Verhältnis der beiden Kontrollinstanzen G-10-Kommission und BfDI, sondern ausschließlich im Verhältnis zur Rechts- und Fachaufsicht der zu kontrollierenden Behörden zeigen, wäre es wünschenswert, wenn der Gesetzgeber eindeutige verfassungsgerichtliche Aufträge umsetzen würde. D. h. entsprechende gesetzliche Klarstellungen müssten sowohl im BDSG als auch im Artikel-10-Gesetz erfolgen. Das im Zuge der Umsetzung der europäischen Datenschutz-Grundverordnung zu erarbeitende Gesetz (vgl. o. Nr. 1.2 f.) bietet hierzu eine gute Gelegenheit, die nicht versäumt werden sollte.

10.2.10.4 Best-practice: Es geht auch anders

Erfahrungen belegen: Eine gute Kooperation ist ein Gewinn für alle!

Nach den Enthüllungen über die massenhafte anlasslose Kommunikationsüberwachung US-amerikanischer und britischer Geheimdienste ist die Tätigkeit der deutschen Nachrichtendienste in besonderer Weise in den Blickpunkt der Öffentlichkeit geraten. Die Aufarbeitung des NSA-Skandals hat auch meine Tätigkeit nachhaltig bestimmt (vgl. u. Nr. 10.3.6).

Positiv hervorzuheben ist hier die auch im Zuge dieser Aufarbeitung weiter intensivierte, konstruktive Zusammenarbeit mit der behördlichen Datenschutzbeauftragen des BND und ihrem Team. Intensiv und frühzeitig hat diese die betroffene Abteilung des BND nicht nur kontrolliert, sondern auch ihre datenschutzrechtlichen Schulungen ausgebaut und in enger Kooperation mit mir durchgeführt. Dadurch bin ich in der Lage, auftretende Fragen direkt zu beantworten, Defizite zu ermitteln, Kritik, Sorgen und Probleme unmittelbar aufzunehmen und gemeinsam mit den betroffenen Mitarbeiterinnen und Mitarbeitern des BND im offenen Dialog rechtskonforme Lösungen für bestehende Probleme zu entwickeln.

Ein weiteres positives Beispiel ist die durch das Engagement der behördlichen Datenschutzbeauftragten des Bundesministeriums der Verteidigung erzielte Lösung eines langjährigen Problems: In den Sicherheitsbehörden werden vielfach kleinere Datenmengen in Form von Excel-Listen verarbeitet. Diese Anwendungen konnten bisher nicht unter umfassender Nutzung von Protokolldaten kontrolliert werden, weil dies von Vertreten aller Sicherheitsbehörden als technisch nicht realisierbar erachtet wurde. Da das Programm Excel jedoch eine kostengünstige Anwendung zur Datenverarbeitung und -verwaltung darstellt, wird es dennoch häufig verwendet und ebenso häufig aufgrund des vorgenannten Defizits von mir beanstandet.

Um dieses Problem zu lösen, haben sich die Informatiker im Team der behördlichen Datenschutzbeauftragten des Bundesministeriums der Verteidigung intensiv mit den Möglichkeiten des Programms beschäftigt. Dabei wurde eine programmseitig implementierte Protokollierungsmöglichkeit gefunden, die für kleinere Anwendungen auch von meinen Mitarbeitern als ausreichend anerkannt wurde. Freundlicherweise haben die Datenschützer der Bundeswehr zugesagt, anderen Nutzern von Excel-Tabellen diese Funktion zu erläutern.

In jeder Legislaturperiode berate ich die Bundesregierung im Rahmen vieler Gesetzgebungsverfahren. Dabei sind die Zeitspannen, die mir zur Prüfung der oftmals sehr umfänglichen Gesetzentwürfe zur Verfügung stehen, entgegen den einschlägigen Vorgaben sehr oft außerordentlich kurz und lassen vielfach nur kursorische Prüfungen zu. Dies ist weder sachdienlich, noch entspricht es den ausdrücklichen Bestimmungen der Gemeinsamen Geschäftsordnung der Bundesministerien.

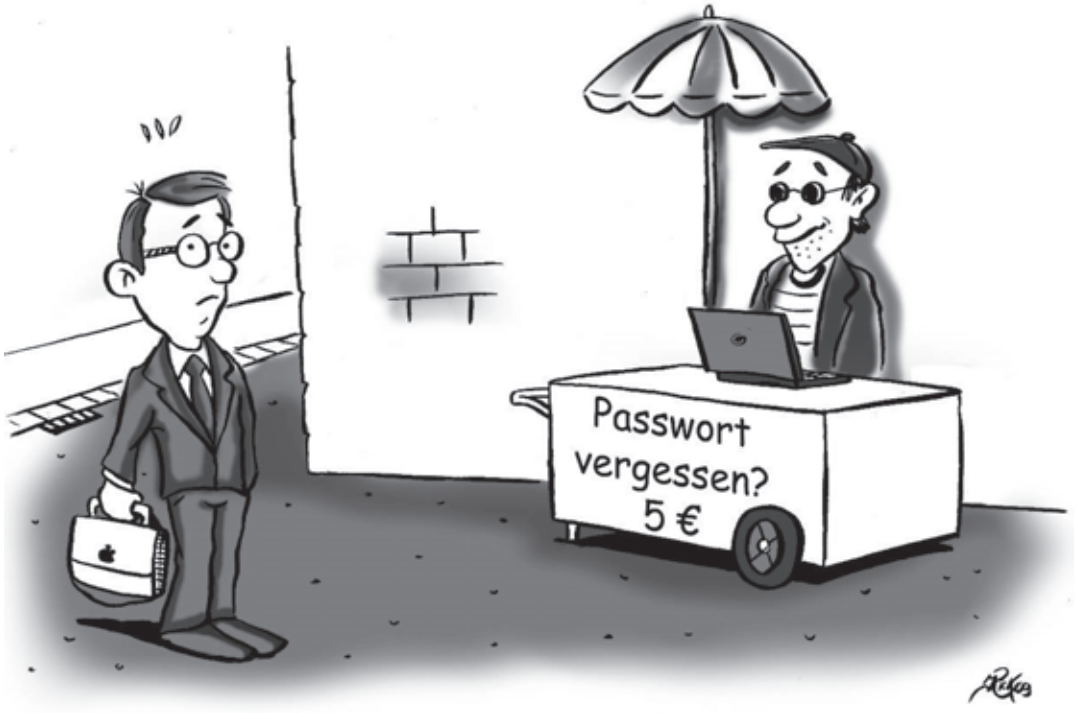
Eine besonders positive Ausnahme von dieser Praxis ist die im Berichtszeitraum fortgeführte Beratung zur Novellierung des Sicherheitsüberprüfungsgesetzes (SÜG). Dieses Gesetz betrifft auch den Umgang mit besonders sensiblen Daten bis hin zur Intimsphäre der überprüften Personen und bedarf auch aus diesem Grund einer besonderen datenschutzrechtlichen Begleitung. Das zuständige Fachreferat des federführenden Bundesministeriums des Innern hat diesem Erfordernis vorbildlich Rechnung getragen und die Vorgaben der GGO umgesetzt. Ich hoffe auf eine positive Ausstrahlwirkung.

10.2.11 … aus dem Bereich: Technologischer Datenschutz

Um einen sicheren Umgang mit Informationstechnik und den eigenen Daten gewährleisten zu können, ist es wichtig, die technischen Grundlagen unseres digitalen Lebens in den Blick zu nehmen. Dies beginnt ganz grundsätzlich bei der Auswahl sicherer Systeme und entsprechender Datenschutzeinstellungen und reicht über Verschlüsselungsmechanismen und deren Anwendung bis hin zur anonymen Nutzung von Diensten oder der Pflege und Wartung von Software. Ein zentrales Anliegen des technologischen Datenschutzes besteht darin, Technologien bereits von Beginn an so zu entwickeln und zu gestalten, dass datenschutzrechtliche Vorgaben umgesetzt und somit zu einer Selbstverständlichkeit bei der Nutzung von Informations- und Kommunikationstechnik werden. Die Datenschutz-Grundverordnung spricht hier von „privacy by design“ bzw. „privacy by default“. Neben diesen beiden ganz zentralen Prinzipien enthält die neue Verordnung viele weitere wichtige Instrumente und Verfahren im Bereich des technologischen Datenschutzes. Konkrete Beispiele dafür sind etwa die Datenschutzfolgenabschätzung, die Implementierung von Gütesiegeln oder das Recht auf Datenportabilität. Ein wichtiger Aspekt der Datenschutz-Grundverordnung besteht darin, dass Verantwortliche und Auftragsverarbeiter zukünftig geeignete technische und organisatorische Maßnahmen ergreifen müssen, um bei der Datenverarbeitung ein angemessenes Schutzniveau gewährleisten zu können. Denn die technischen Innovationen schreiten mit einem so hohen Tempo voran, dass ganz besonders dringender Handlungsbedarf besteht, um auch aus Datenschutzsicht mit den Entwicklungen Schritt halten zu können.

Die folgenden Beiträge zeigen einen Ausschnitt aus meiner vielfältigen Tätigkeit auf dem Gebiet des technologischen Datenschutzes, der Datensicherheit und der Informationstechnik.

Zum Thema Identitätsdiebstahl sind meine Hinweise aus dem 25. Tätigkeitsbericht (Nr. 5.14.3) nach wie vor gültig. Neben dem sorgsamen Umgang mit Zugangsdaten und Sicherheits-Token sind gut gewählte und regelmäßig geänderte Passwörter eine wichtige Maßnahme, um Identitätsdiebstähle zu verhindern.



Joachim Rick

10.2.11.1 IT-Sicherheitsgesetz

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist im Juli 2015 in Kraft getreten. Es soll einen Beitrag dazu leisten, Defizite im Bereich der IT-Sicherheit, vor allem bei Betreibern Kritischer Infrastrukturen, abzubauen und die digitalen Infrastrukturen in Deutschland insgesamt zu stärken.

Das IT-Sicherheitsgesetz stellt ein konkretes Ergebnis der Umsetzung der Digitalen Agenda der Bundesregierung dar. Sein Ziel ist die Verbesserung der IT-Sicherheit bei den Kritischen Infrastrukturen (KRITIS), also etwa der Strom- und Wasserversorgung oder der Telekommunikation. Hier sind Vorgaben zur Verbesserung der Verfügbarkeit und Sicherheit von IT-Systemen von ganz besonderer Bedeutung, weil ein Ausfall dieser Systeme schwerwiegende Folgen für Staat, Gesellschaft und Wirtschaft mit sich bringen kann. Um dies zu erreichen, ändert und ergänzt das IT-Sicherheitsgesetz andere, bereits bestehende Gesetze, wie das Telemedien-, das Telekommunikations-, das Energiewirtschafts- oder das BSI-Gesetz.

Betreiber Kritischer Infrastrukturen sollen zukünftig z. B. einen Mindeststandard an IT-Sicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das BSI melden. Sie müssen angemessene technische und organisatorische Vorkehrungen zum Schutz informationstechnischer Systeme garantieren und diese durch Standardisierungen und Auditierungen nachweisen. Auch die Anforderungen an Telekommunikationsunternehmen werden erhöht. Sie müssen z. B. ihre Kunden künftig warnen, wenn auffällt, dass deren Anschluss für Angriffe missbraucht wird - etwa im Rahmen eines sog. Botnet. Diese Regelungen dienen nicht nur dem Schutz vor unerlaubten Eingriffen in die Infrastruktur, sondern letztlich auch dem Schutz personenbezogener Daten. Kommen die Betreiber den Vorgaben nicht nach, drohen empfindliche Strafen.

Um Klarheit darüber zu schaffen, welche Unternehmen überhaupt vom IT-Sicherheitsgesetz als „Kritische Infrastrukturen“ erfasst werden, wurde das Gesetz um eine „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (22.04.2016, BGBl. I, S. 958) ergänzt. Diese bestimmt zunächst Kritische Infrastrukturen in den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation. Im Frühjahr 2017 sollen durch eine Änderungsverordnung auch die Sektoren Gesundheit, Finanz- und Versicherungswesen,

Transport und Verkehr behandelt werden. Die betroffenen Betreiber werden verpflichtet, dem BSI erhebliche Störungen ihrer Systeme zu melden und innerhalb von zwei Jahren die Einhaltung eines Mindeststandards an IT-Sicherheit nachzuweisen.

Die Entsprechung des IT-Sicherheitsgesetzes auf europäischer Ebene bildet die „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-Richtlinie), die im August 2016 in Kraft getreten ist. Auch wenn sie sich in weiten Teilen mit den Maßgaben des IT-Sicherheitsgesetzes deckt, sind ihre Vorgaben in nationales Recht umzusetzen und mögliche Konflikte zwischen europäischer und nationaler Rechtsprechung zu beachten. Dazu kommen die Neuregelungen der europäischen Datenschutz-Grundverordnung (DSGVO), die teilweise bis Mai 2018 noch einer Umsetzung in nationales Recht bedarf. Für den deutschen Gesetzgeber besteht die Herausforderung, alle drei Regelwerke in der Umsetzung miteinander zu verbinden und möglichst klare Vorgaben zu schaffen, um sowohl ein Höchstmaß an Sicherheit und Widerstandsfähigkeit von IT-Systemen als auch das Maximum zum Schutz personenbezogener Daten zu erreichen.

Die Ausarbeitung des IT-Sicherheitsgesetzes wurde von mir von Anfang an beratend begleitet. Informationssicherheit stellt eine Grundvoraussetzung dar, um die Grundrechte auf informationelle Selbstbestimmung, auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Dabei führt Informationssicherheit nicht automatisch zu einem hohen Datenschutzniveau. Vielmehr gilt es, in bestimmten Fällen auch eine Abwägung von IT-Sicherheitsinteressen und einer datenschutzgerechten Umsetzung von Prozessen zu treffen. Über vergleichbare Prozesse, nämlich meine Mitarbeit bei Maßnahmen des BSI im Zusammenhang mit dem Diebstahl von Identitätsdaten, habe ich bereits im 25. TB Nr. 5.14.3 berichtet.

Bei der Festlegung und Durchsetzung von Informationssicherheitsstandards müssen die Datenschutzaufsichtsbehörden daher weiterhin konsequent beteiligt und in die Meldewege eingebunden werden. Dies und die Mitarbeit bei den Mindeststandards werden künftige Schwerpunkte meiner Arbeit bilden. Das IT-Sicherheitsgesetz ist deshalb nicht nur mit einem Stellenzuwachs für das BSI verbunden, sondern auch meine Personalausstattung wird erfreulicherweise verbessert, um dem mit dem Gesetz verbundenen Aufgabenzuwachs nachkommen und die grundrechtlich verankerten Bestimmungen des Datenschutzrechts auch zukünftig effektiv umsetzen zu können.

10.2.11.2 Datenschutzzertifizierung – ein Wettbewerbsvorteil

Die Datenschutz-Grundverordnung führt eine Zertifizierung von Verarbeitungsvorgängen ein, die die korrekte Anwendung der Gesetzgebung unterstützen soll. Damit werden die Weichen für einen gestärkten Datenschutz in Europa in die richtige Richtung gestellt.

Mit der geplanten Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie der Vergabe von Datenschutzsiegeln auf Ebene der Europäischen Union schafft die Datenschutz-Grundverordnung erstmals die Möglichkeit für alle europäischen Datenschutzstellen, die Einhaltung ihrer Vorgaben auf Basis einheitlicher Regelungen zur Zertifizierung zu überprüfen. Neben den Kriterien für die Zertifizierung sind einheitliche Rahmenbedingungen für die Akkreditierung von Prüfstellen und die Anforderungen an Prüfkataloge abzustimmen und künftig anzuwenden. Im Arbeitsprogramm der Artikel-29-Gruppe wird das Thema der Zertifizierung daher auch besonders priorisiert. Es wurde eine Arbeitsgruppe eingerichtet, die entsprechende Vorgaben wie z. B. Verfahrensordnungen für die Akkreditierung und die Zertifizierung erarbeitet, die als ein Zertifizierungsprogramm im Sinne der ISO-Norm 17065 zu verstehen sind und auf deren Grundlage Akkreditierungen beantragt, begutachtet und erteilt werden können.

Durchgeführt werden soll die Zertifizierung durch entsprechende Zertifizierungsstellen oder durch die zuständige Aufsichtsbehörde. Über die Anzahl der Zertifizierungsstellen trifft die Datenschutz-Grundverordnung keine

Aussage, d. h., es sind sowohl eine Zertifizierungsstelle als auch mehrere Zertifizierungsstellen möglich. Der Verordnungsgeber beabsichtigt hierbei, aus dem Betrieb von Zertifizierungsstellen ein Geschäftsmodell machen zu können.

Die Definition der Zertifizierungskriterien obliegt grundsätzlich den Aufsichtsbehörden, dabei sollen neben den Maßnahmen zum technisch-organisatorischen Datenschutz auch Verhaltensregeln als Zertifizierungskriterien definiert werden. Die konkreten Rahmenbedingungen für dieses Verfahren werden aktuell auf europäischer und nationaler Ebene ausgestaltet. Denn die neue Aufgabe erfordert vielfältige Vorbereitungsmaßnahmen und Abstimmungsprozesse, sowohl in den europäischen Gremien als auch bei der Anpassung der nationalen Gesetzgebung. Diese muss u. a. festlegen, welchen Stellen welche Aufgaben zukommen und wie beispielsweise die nationale Akkreditierungsstelle, die Deutsche Akkreditierungsstelle (DAkkS), einzubinden ist. Die konkrete Ausgestaltung war bei Redaktionsschluss noch offen (vgl. hierzu Nr. 1.21 f.).

Zentral geregelt ist das Zertifizierungsverfahren in den Artikeln 42 und 43 der Datenschutz-Grundverordnung. Gegenstand von Zertifizierungen können letztlich sämtliche Verarbeitungsvorgänge sein. Nachgewiesen wird die ordnungsgemäße Anwendung der Verordnung, vor allem die Einhaltung der technischen und organisatorischen Anforderungen entsprechend Artikel 24 und 32 der Datenschutz-Grundverordnung. Sie hebt an einigen Stellen die Zertifizierung aber auch noch einmal gesondert als Instrument zur Erfüllung der Anforderungen von „privacy by design“ und „privacy by default“ und hinreichender und geeigneter Garantien bei der Auftragsdatenverarbeitung und bei der Drittstaatenübermittlung hervor. Grundsätzlich soll die Zertifizierung die Verwendung von privacy by design und privacy by default befördern.

Durch eine Zertifizierung kann der Auftragnehmer, z. B. ein Anbieter von Cloud-Diensten, nachweisen, dass er seine Verpflichtungen zu technisch-organisatorischen Maßnahmen bei der Auftragsdatenverarbeitung erfüllt. Im Zertifikat müssen die Art der Auftragsdatenverarbeitung, die Risikolage sowie der Maßnahmenkatalog enthalten sein. Ein wichtiger Punkt ist die Gewährleistung der Datensicherheit als grundlegendes Fundament des Datenschutzes, sie umfasst die Erreichung der Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit durch geeignete Maßnahmen wie zum Beispiel Pseudonymisierung oder Verschlüsselung. Darüber hinaus sind Schutzklassen ein wichtiges Instrument, um individuellen Schutzbedarf und dessen Erfüllung durch zertifizierte Dienste praxisgerecht auszudrücken. Hier bietet besonders der Maßnahmenkatalog des Standard-Datenschutzmodells (vgl. u. Nr. 10.2.11.5) eine geeignete Grundlage.

Zertifikate sind nicht unbeschränkt gültig. Nach spätestens 3 Jahren bzw. bei Änderung der Datenverarbeitung oder der Risikolage kann eine Nachzertifizierung beauflagt werden. Bei Verstößen bzw. fehlender Nachzertifizierung, d. h., wenn die Voraussetzungen für die Zertifizierung nicht mehr erfüllt sind, muss das Zertifikat entzogen werden.

Eine grundlegende Voraussetzung für die Zertifizierung ist die Akkreditierung der Zertifizierungsstellen. Zu akkreditierende Zertifizierungsstellen müssen Zertifikate im Sicherheitsmanagement und umfangreiche Erfahrungen in der Datenschutzberatung nachweisen. Akkreditierende Stellen wiederum benötigen fachlich versiertes Personal, das auf dem aktuellen Stand im Bereich Sicherheitsmanagement und Datenschutz ist. Sie müssen die gemäß Artikel 55 oder 56 zuständige Aufsichtsbehörde und/oder die nationale Akkreditierungsstelle sein. Zertifizierungsstellen kann die Akkreditierung entzogen werden, wenn z. B. fehlende oder nicht aktualisierte Zertifikate im Sicherheitsmanagement oder Mängel bei der Datenschutzberatung festgestellt werden. Dies setzt eine regelmäßige Überprüfung der akkreditierten Stellen voraus. Die Höchstdauer der Akkreditierung beträgt 5 Jahre.

Die Einführung von europaweit einheitlichen datenschutzspezifischen Zertifizierungsverfahren durch die Datenschutz-Grundverordnung stellt eine wichtige und zentrale Neuerung der europäischen Bemühungen um einen gestärkten Datenschutz dar. Darüber hinaus bietet sie für Auftragnehmer einen möglichen Wettbewerbsvorteil. Jetzt gilt es, die Herausforderungen der Umsetzung dieser Vorgaben anzunehmen und die entsprechende Ausgestaltung effektiv zu begleiten. Über diese Entwicklungen werde ich auch in den kommenden Tätigkeitsberichten informieren.

10.2.11.3 Windows XP - ein langer Abschied

Der Support für das Betriebssystem Windows XP wurde am 14. April 2014 eingestellt. Obwohl der Hersteller Microsoft die Öffentlichkeit bereits im April 2009 darüber informiert hatte, kam das Ende des Supports für viele überraschend. In meinem Zuständigkeitsbereich hat die Ablösung teilweise längere Zeit beansprucht, nicht zuletzt wegen der sehr unterschiedlichen Einsatzszenarien.

Die Einstellung des Supports durch Microsoft bedeutet für die Nutzung von Windows XP, dass keine Produktaktualisierungen in Form von Service Packs und Sicherheitsupdates (sog. Hotfixes etc.) mehr bereitgestellt werden. Dadurch bestand für die Arbeitsplatzsysteme in der Bundesverwaltung das Risiko, dass Sicherheitslücken ausgenutzt und nicht behoben werden könnten und somit auch der Schutz personenbezogener Daten auf diesen Systemen nicht mehr gewährleistet wäre. Um mir einen Überblick über den Stand der Ablösung von Windows XP in der Bundesverwaltung zu verschaffen, habe ich Ende 2015 eine entsprechende Abfrage bei den verantwortlichen Stellen durchgeführt. Diese umfasste Angaben zur Netzwerkanbindung dieser Systeme, zu möglichen Gefahren für die Vertraulichkeit und Integrität von personenbezogenen Daten durch den Einsatz von veralteten Systemen, sowie zur geplanten Ablösung dieser Systeme (Zeitpunkt und Übergangslösung - vgl. Kasten zu Nr. 10.2.11.3).

Zusammenfassend kann festgestellt werden, dass in allen Behörden der Bundesverwaltung Maßnahmen zur Ablösung kritischer Arbeitsplatzsysteme ergriffen wurden und entsprechend Planung bis Ende 2015 bzw. 2016 größtenteils abgeschlossen werden sollen.

Ausnahmen betreffen sogenannte „Embedded Systems“, hierbei handelt es sich um spezielle Systeme, die im Normalfall nicht an ein Netzwerk angeschlossen sind und keinen Internetzugang haben. Eine weitere Ausnahme bildet leider die Deutsche Rentenversicherung, wo mit der Umstellung in kleineren Außenstandorten und der mobilen IT-Systeme mit Anbindung an das Datennetz der DRV-Bund bis Ende 2016 noch immer nicht begonnen wurde. Entsprechend DRV Bund soll die vollständige Umstellung auf Windows 7 bis zum Ende des ersten Halbjahres 2017 abgeschlossen sein (vgl. u. Nr. 3.2.3.4).

Einige große Behörden wie das Bundeministerium der Verteidigung haben mit der Firma Microsoft Sonderverträge abgeschlossen, um auch nach dem Supportende für einen begrenzten Zeitraum Sicherheitsupdates und Unterstützung erhalten zu können.

Behörden, die diese Möglichkeit nicht nutzen können, haben überwiegend das Problem, aufgrund der fehlenden Möglichkeit, Fach-/Spezialanwendungen auf ein anderes Betriebssystem zu portieren, kritische Arbeitsplatzsysteme nicht kurzfristig und mit vertretbarem finanziellem Aufwand ablösen zu können. Dies haben auch Kontrollen meinerseits bestätigt. In den meisten Fällen sind diese Systeme nicht an ein Netzwerk angeschlossen bzw. es wurden Maßnahmen ergriffen, diese Systeme entsprechend abzusichern. Für spezielle Systeme, wie z. B. medizinische Geräte oder Systeme zur Authentisierung von Sicherheitstoken, kann nur der Hersteller dieser Systeme eine Lösung bereitstellen.

Daher fordere ich alle Hersteller von Produkten, die ein sog. „embedded Windows XP“ oder ein anderes veraltetes Betriebssystem nutzen, auf, schnellst möglich eine Lösung auf Basis eines aktuellen Betriebssystems bereitzustellen.

Mit Blick auf das Supportende 2020 für das Betriebssystem Windows 7 bzw. 2025 für Windows 8 begrüße ich die Bereitstellung eines einheitlichen, sicheren und transparenten Clientbetriebssystems für die Bundesverwaltung im Rahmen der IT-Konsolidierung des Bundes und hoffe, dass dieses Angebot umfangreich und rechtzeitig durch die Bundesverwaltung in Anspruch genommen wird.

Kasten zu Nr. 10.2.11.3

Das **Ergebnis der Abfrage** entspricht dem Stand von Dezember 2015 und ist in der unten stehenden Tabelle zusammengefasst. In der rechten Spalte ist die Rückmeldung der Bundesbehörden dargestellt.

Deutsche Bundesbank	Es gibt noch ca. 50 Systeme mit Windows XP ohne Netzanschluss, deren Bestand kontinuierlich zurückgeführt wird.
Bundesarbeitsgericht	Es gibt noch 4 Systeme mit Windows XP, der Zeitpunkt der Ablösung ist noch offen. Hier wird zeitnah um Aktualisierung gebeten.
Bundessozialgericht	Es gibt noch 4 Systeme mit Windows XP, der Zeitpunkt der Ablösung ist noch offen. Hier wird zeitnah um Aktualisierung gebeten.
Bundesversicherungsamt	Es gibt noch ca. 34 Systeme mit Windows XP ohne Netzanschluss, deren Ablösung bis Ende 2016 vorgesehen ist.
DRV Bund	Es gibt noch ca. 20.150 Systeme mit Windows XP, deren Ablösung bis Mitte 2016 vorgesehen ist. Aktualisierung Stand 3/2017: 90 % dieser Systeme wurden bis Oktober 2016 umgestellt.
DRV Knappschaft-Bahn-See	Es gibt noch ca. 5.300 Systeme mit Windows XP, deren Ablösung bis Ende 2015 vorgesehen ist.
Bundesagentur für Arbeit	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Arbeit und Soziales - Ressortbereich	Es gibt noch ca. 22.700 Systeme mit Windows XP, deren Ablösung für 2015/2016 vorgesehen ist.
Die Beauftragte der Bundesregierung für Kultur und Medien - Ressortbereich	Es gibt noch ca. 132 Systeme mit Windows XP ohne Netzanschluss, davon sollen 102 Systeme bis Ende 2015 abgelöst werden.
Deutsche Nationalbibliothek DNB	Es gibt noch ca. 58 Systeme mit Windows XP, davon 5 Systeme ohne Netzanschluss, deren Ablösung für November 2015 vorgesehen ist.
Akademie der Künste	Es gibt noch 8 Systeme mit Windows XP, davon 4 Systeme ohne Netzanschluss, deren Ablösung für Ende 2015 bzw. 2016 vorgesehen ist.
Bundesministerium für Bildung und Forschung	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesinstitut für Berufsbildung	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Wirtschaft und Energie	Es gibt noch ca. 990 Systeme mit Windows XP, deren Ablösung für 2016 vorgesehen ist.
Deutscher Bundestag	Es gibt noch 27 Systeme mit Windows XP, deren Ablösung für 2016 vorgesehen ist.
Presse- und Informationsamt der Bundesregierung	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium der Justiz und für Verbraucherschutz - Ressortbereich	Es gibt noch 336 Systeme mit Windows XP, davon 58 Systeme ohne Netzanschluss, deren Ablösung für Mitte 2016 vorgesehen ist. Für weitere 73 Systeme ist eine Ablösung für 2016/2019 vorge-

	sehen. Für 205 Systeme gibt es noch keinen Termin. Hier wird zeitnah um Aktualisierung gebeten.
Bundesanstalt für Immobilienaufgaben	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesrat	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesrechnungshof	Es gibt noch 13 Systeme mit Windows XP ohne Netzanschluss, für 2 Systeme davon ist eine Ablösung bis Ende 2015 vorgesehen.
Auswärtiges Amt	Es gibt noch ca. 250 Systeme mit Windows XP ohne Netzanschluss, deren Ablösung für Ende 2015 vorgesehen ist.
Deutsches Archäologisches Institut	Es gibt noch 85 Systeme mit Windows XP, deren Ablösung für Mitte 2016 vorgesehen ist.
Bundeskriminalamt	Es gibt noch ca. 100 Systeme mit Windows XP ohne Netzanschluss, deren Ablösung für Ende 2015 vorgesehen ist.
Bundeskanzleramt	Es gibt noch 3 Systeme mit Windows XP, deren Ablösung für Ende 2015 vorgesehen ist.
Bundesnachrichtendienst	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium des Innern	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesverwaltungsamt - Bundesstelle für Informationstechnik	Es gibt noch 2 Systeme mit Windows XP ohne Netzanschluss, deren Ablösung für Ende 2015 vorgesehen ist.
Bundesamt für Migration und Flüchtlinge	Es gibt noch 26 Systeme mit Windows XP ohne Netzanschluss, der Zeitpunkt der Ablösung ist noch offen.
Bundesanstalt für Finanzdienstleistungsaufsicht	Es gibt noch 1 System mit Windows XP, der Zeitpunkt der Ablösung ist noch offen. Hier wird zeitnah um Aktualisierung gebeten.
Statistisches Bundesamt	Es gibt noch 12 Systeme mit Windows XP, davon 1 System ohne Netzanschluss, deren Ablösung für Ende 2015 bzw. Mitte 2016 vorgesehen ist.
Bundesministerium der Finanzen	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Familie, Senioren, Frauen und Jugend - Ressortbereich	Es gibt noch 611 Systeme mit Windows XP, davon 26 Systeme ohne Netzanschluss, deren Ablösung für Anfang 2016 vorgesehen ist.
Bundesdruckerei	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Verkehr und digitale Infrastruktur	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Ernährung und Landwirt-	Es gibt noch 361 Systeme mit Windows XP ohne Netzanschluss, für 33 Systeme davon ist eine Ablö-

schaft - Ressortbereich	sung bis Ende 2016 vorgesehen.
Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit Ressortbereich	Es gibt noch 122 Systeme mit Windows XP, deren Ablösung für 2016 vorgesehen ist.
Bundespräsidialamt	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Gesundheit	Es gibt noch 9 Systeme mit Windows XP ohne Netzanschluss, der Zeitpunkt der Ablösung ist noch offen.
Bundeministerium der Verteidigung	Es gibt noch ca. 12.000 Systeme mit Windows XP ohne Netzanschluss, deren Ablösung für Ende 2016 vorgesehen ist. Für diese Systeme gibt es Sonderverträge mit Microsoft.
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung	Es gibt noch 2 Systeme mit Windows XP ohne Netzanschluss, der Zeitpunkt der Ablösung ist noch offen.

10.2.11.4 Windows 10

Neue Betriebssysteme werben mit personalisierten Diensten und benötigen hierfür personenbezogene Daten. Hierüber informieren sie die Nutzerinnen und Nutzer in ihren Datenschutzerklärungen. Sind diese Datenschutzerklärungen jedoch verständlich und klar formuliert und, vor allem, halten sich die Hersteller daran? Ein guter Grund, sich die Datenschutzerklärung am Beispiel von Windows 10 einmal genauer anzusehen.

Der Trend bei der Entwicklung von Betriebssystemen geht in den letzten Jahren immer mehr in Richtung Onlinefunktionalität. Dabei ist der Austausch von Daten über das Internet, z. B. des Clientsystems mit einer Cloud, zum Standard geworden. Microsoft, der Hersteller des Betriebssystems Windows 10, folgt diesem Trend und bietet umfangreiche Dienste an, die dem Nutzer die tägliche Arbeit erleichtern und eine unbegrenzte Verfügbarkeit der Daten sicherstellen soll. Auch andere Hersteller wie Apple oder Google bieten diese Dienste an und nutzen die ständige Verbindung der Clientsysteme mit dem Internet. Allen Herstellern gemein ist, dass sie dafür Daten des Clientsystems, z. B. Positionsdaten, und Daten des Nutzers verwenden. Die größte Funktionalität bieten hier personalisierte Dienste, wie die Hersteller hervorheben. Um aber einen Dienst zu personalisieren, bedarf es personenbezogener Daten. Wie die Daten erhoben, verarbeitet und gespeichert werden und um welche Daten es sich handelt, darüber muss der Hersteller die Nutzerinnen und Nutzer in einer entsprechenden Datenschutzerklärung informieren.

Die Datenschutzerklärung von Microsoft zu Windows 10, die über die Webseite des Herstellers abgerufen werden kann, beschreibt sehr umfangreich, welche Daten vom Betriebssystem selbst und den dazugehörigen Diensten erhoben werden (Stand: Anfang März 2017). Gerade bei den Diensten wird deutlich, dass sich Microsoft vorbehält, umfangreiche personenbezogene Daten zu erheben und zu verarbeiten. Doch auch wenn man diese Dienste nicht nutzen will und deaktiviert, werden personenbezogene Daten erhoben und an den Hersteller gesendet, wie die Datenschutzerklärung verrät.

Bei der Aktivierung von Windows 10 werden neben einem Produktschlüssel, der dem Gerät zugeordnet wird, Daten zur Software und zum Gerät erhoben. Diese nicht genauer definierten Daten werden „bei Bedarf einer Lizenzvalidierung“ erneut erhoben und an Microsoft gesendet, wobei nicht erläutert wird, wie diese Daten verarbeitet, an wen sie weitergegeben und wie lange sie gespeichert werden.

Bei mobilen Geräten, auf denen Windows 10 installiert ist, werden Geräte- und Netzwerkidentifizierungsmerkmale („device and network identifiers“) erhoben. Da diese Identifizierungsmerkmale für jedes Gerät einmalig

sind und ein Bezug zu weiteren auf dem Gerät gespeicherten, persönlichen Daten hergestellt werden kann, können diese Daten als personenbezogene Daten angesehen werden. Das Auslesen und Verarbeiten dieser Daten wird seit Jahren von Datenschützern kritisiert. Darüber hinaus wird die Position des Gerätes beim Einschalten erfasst.

Jedem Nutzer, der sich auf einem Windows 10 System anmeldet, wird ein Identifizierungsmerkmal, die Werbe-ID, zugeordnet („unique advertising ID for each user on a device“), durch das der Nutzer eindeutig identifiziert werden kann. Der Zugriff auf diese Werbe-ID muss explizit abgeschaltet werden, dabei wird sie allerdings nicht gelöscht.

Microsoft erfasst die präzise Position von Geräten, auf denen Windows 10 installiert ist. Dafür werden GPS-Daten, WLAN-Daten und die IP-Adresse des Gerätes ausgewertet und in einer Datenbank bei Microsoft gespeichert. Das Unternehmen gibt an, alle Daten, über die sich eine Person oder ein Gerät identifizieren lassen, vor der Weitergabe an Dritte zu entfernen. Dabei sagt es aber nicht, um welche Daten es sich bei den entfernten Daten handelt. Bei einer IP-Adresse handelt es sich z. B. um ein personenbezogenes Datum, über das die Position eines Gerätes in manchen Fällen bis auf einen Postleitzahlenbereich eingegrenzt werden kann. Der Lokalisierungsdienst kann durch den Nutzer abgeschaltet werden, die erhobenen Daten verbleiben jedoch in der Datenbank von Microsoft.

Microsoft bietet mehrere Dienste zur Gewährleistung der Sicherheit und zum Schutz des Gerätes an, wie Smart Screen und Windows Defender. Entsprechend seiner Datenschutzerklärung behält sich das Unternehmen vor, Dateien, die heruntergeladen werden bzw. sich auf dem System befinden und möglicherweise Schadsoftware enthalten können („it may also send files that could contain malware“), an Microsoft zu senden. Außerdem senden diese Dienste Berichte und wenn Microsoft personenbezogene Daten in diesen Berichten vermutet („report is likely to contain personal data“), muss der Nutzer den Versand bestätigen. Diese Dienste müssen explizit abgeschaltet werden.

Unter dem Merkmal „Getting to know you“ sammelt Microsoft personenbezogene Daten wie z. B. Sprachdaten, handschriftliche Daten und Daten, die über die Tastatur eingegeben werden. Letztere werden um IDs, IP-Adressen und andere mögliche Identifizierungsmöglichkeiten bereinigt („we scrub to remove IDs, IP addresses, and other potential identifiers“). Weitere Dienste erheben darüber hinaus Namen, Spitznamen, Kalenderdaten, Kontaktdaten, Namen von bevorzugten Orten und benutzten Anwendungen, allerdings erfolgt die Übertragung nur mit Zustimmung des Nutzers. Ein Teil dieser bei Microsoft gespeicherten Daten, wie Kontakte und Kalenderdaten, kann über ein Microsoft-Konto gelöscht werden, was mit den anderen personenbezogenen Daten passiert, wird nicht erklärt.

Ein umfangreicher Teil der erhobenen Daten betrifft die sogenannten Telemetriedienste. Telemetrie umfasst alle Daten eines Systems, die auf diesem System gemessen/erhoben und an Microsoft übertragen werden. Entsprechend der Datenschutzerklärung handelt es sich um Diagnose- und Nutzungsdaten, die das Unternehmen zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems nutzt. Bedenklich sind hier zwei Aspekte, die Microsoft in seiner Datenschutzerklärung angibt. Zum einen werden diese an Microsoft übertragenen Daten mit einem oder mehreren eindeutigen Identifizierungsmerkmalen verknüpft, die es dem Unternehmen ermöglichen, einen individuellen Nutzer auf einem individuellen Gerät und dessen Nutzungsmuster (wieder) zu erkennen („stored with one or more unique identifiers that can help us recognize an individual user on an individual device“). Zum anderen können diese Telemetriedienste nicht vollständig abgeschaltet werden und somit kann eine Übertragung personenbezogener Daten, wie z. B. der IP-Adresse, an Microsoft nicht verhindert werden.

Wie zusammenfassend festzustellen ist, kann bei der Verwendung von Windows 10 auch trotz optimaler Konfiguration aller Datenschutzeinstellungen die Übertragung und Verarbeitung personenbezogener Daten auf Serversystemen von Microsoft in den USA nicht verhindert werden. Dies bestätigen u. a. Untersuchungen des Bayerischen Landesamtes für Datenschutzaufsicht, das sich im Rahmen seiner Mitarbeit in der Artikel-29-Gruppe der europäischen Datenschutzbehörden mit Windows 10 beschäftigt. Das Bundesamt für Sicherheit in der In-

formationstechnik (BSI) ist zu den gleichen Erkenntnissen gekommen. Die ausgelesenen Daten können nicht geprüft werden, da sie verschlüsselt übertragen werden. Weder gegenüber dem BSI noch gegenüber meinen europäischen Kollegen, die sich bereits in zwei Briefen an Microsoft gewandt haben, hat das Unternehmen offengelegt, welche Daten gesammelt und wofür sie verwendet werden.

Solange der Hersteller hier nicht für Transparenz sorgt, muss ich ihn in Form seiner Datenschutzerklärung beim Wort nehmen und davon ausgehen, dass personenbezogene Daten erhoben und übertragen werden. Des Weiteren muss der Hersteller neben der nötigen Transparenz dem Nutzer ermöglichen, die Übertragung seiner Daten ganz zu unterbinden bzw. die gesammelten Daten einsehen und vollständig löschen zu können. Hier hat der Hersteller nur halbherzig Maßnahmen ergriffen.

Das intransparente Vorgehen von Microsoft kritisiere ich und empfehle dem Hersteller, hier für Klarheit und Abhilfe zu sorgen. Dies auch vor dem Hintergrund, dass die neue Datenschutz-Grundverordnung jeden Verantwortlichen ab Mai 2018 verpflichten wird, die Grundsätze von privacy by design und privacy by default zu beachten und Verletzungen dieser Grundsätze mit hohen Geldbußen belegt. Ich werde die weitere Entwicklung bei Windows 10 beobachten und - insbesondere im Rahmen eines möglichen Einsatzes in der Bundesverwaltung - kritisch begleiten.

10.2.11.5 Das Standard-Datenschutzmodell

Die Arbeiten am „Standard-Datenschutzmodell“ (SDM) wurden weitergeführt. Der Blickwinkel richtete sich zunächst auf die Definition von geeigneten Schutzzielen und Verfahren zur Herstellung von Datensicherheit.

Schutzziele und ein darauf aufbauendes IT-Sicherheitsmanagement werden schon seit einigen Jahren im Bereich der IT-Sicherheit eingesetzt, beispielsweise in den IT-Sicherheitsbewertungskriterien, dem sog. Orange Book oder den Common Criteria. Bei der Umsetzung werden allerdings auch Defizite dieser Verfahren und Schutzziele erkennbar. So bringen sie keine Struktur in den Bereich der Schutzziele, sodass im Laufe der Zeit eine immer unübersichtlichere Sammlung von nebeneinander stehenden Schutzzielen entstanden ist und weiter entsteht. Die verschiedenen Verfahren beschäftigen sich auch nicht mit Wechselwirkungen von Schutzzielen, d. h. ob und inwiefern sich diese gegenseitig verstärken oder schwächen oder gar implizieren oder gegenseitig ausschließen. Aufgrund dieser mangelnden Harmonisierung gibt es keine Gesamtschau von den einzeln nebeneinander stehenden Schutzzielen und keine Überlegungen zu ihrer Vollständigkeit.

Nach vielen Jahren des Erprobens solcher Verfahren entwickelte Mitte der 1990er Jahre das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Modell des Grundschutzes, um die Umsetzung solcher Verfahren zu vereinfachen. In der Zwischenzeit ist der IT-Grundschutz zu einem praktikablen Werkzeug zur Sicherstellung der IT-Sicherheit geworden. Das Verfahren beruht auf einem einfachen Modell (vgl. Kasten a zu Nr. 10.2.11.5).

Das BSI überarbeitet zwar derzeit den Grundschutz, aber an den grundsätzlichen Erwägungen wird sich auch in Zukunft nichts ändern. Bereits in meinem 15. Tätigkeitsbericht (Nr. 30.8) habe ich den Einsatz von Grundschutz befürwortet und dies auf eine einfache Formel gebracht:

DATENSCHUTZ = Grundschutz + X

In den vielen Jahren der Anwendung dieser Formel wurde darüber diskutiert, wie denn die X-Komponente zu bestimmen und welcher „Wert“ angemessen sei. Dies hängt natürlich von den konkreten Rahmenbedingungen, Systemen, Daten usw. ab und konnte bislang nur sehr rudimentär ermittelt werden.

Deswegen wurde bereits vor Jahren eine Arbeitsgruppe der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eingerichtet. Diese hat ihre Aufgabe auf der Basis des Grundschutzmodells neu fokussiert und das „Standard-Datenschutzmodell“ (SDM) mit sechs sog. Gewährleistungszielen entwickelt.

Zu den „klassischen“ Gewährleistungszielen im SDM zählen:

1. Verfügbarkeit,
2. Integrität und
3. Vertraulichkeit.

Wie bereits in meinem 25. TB (Nr. 5.14.1) berichtet, reichen diese Ziele allerdings nicht aus, um Datenschutz und Datensicherheit zu gewährleisten. Dazu werden noch folgende ergänzende Gewährleistungsziele benötigt:

4. Nichtverkettung,
5. Transparenz und
6. Intervenierbarkeit.

Diese sechs Gewährleistungsziele und die daraus abgeleiteten Maßnahmen können dazu dienen, die X-Komponente in der obigen Formel mit Inhalt zu füllen. Gleichzeitig ergänzt dieses Modell in idealer Form das Grundschutzmodell des BSI und wendet die gleiche Methode an (vgl. Kasten b zu Nr. 10.2.11.5).

Blickt man auf die künftig geltende Datenschutz-Grundverordnung, ergeben sich noch weitere Vorteile aus dem SDM.

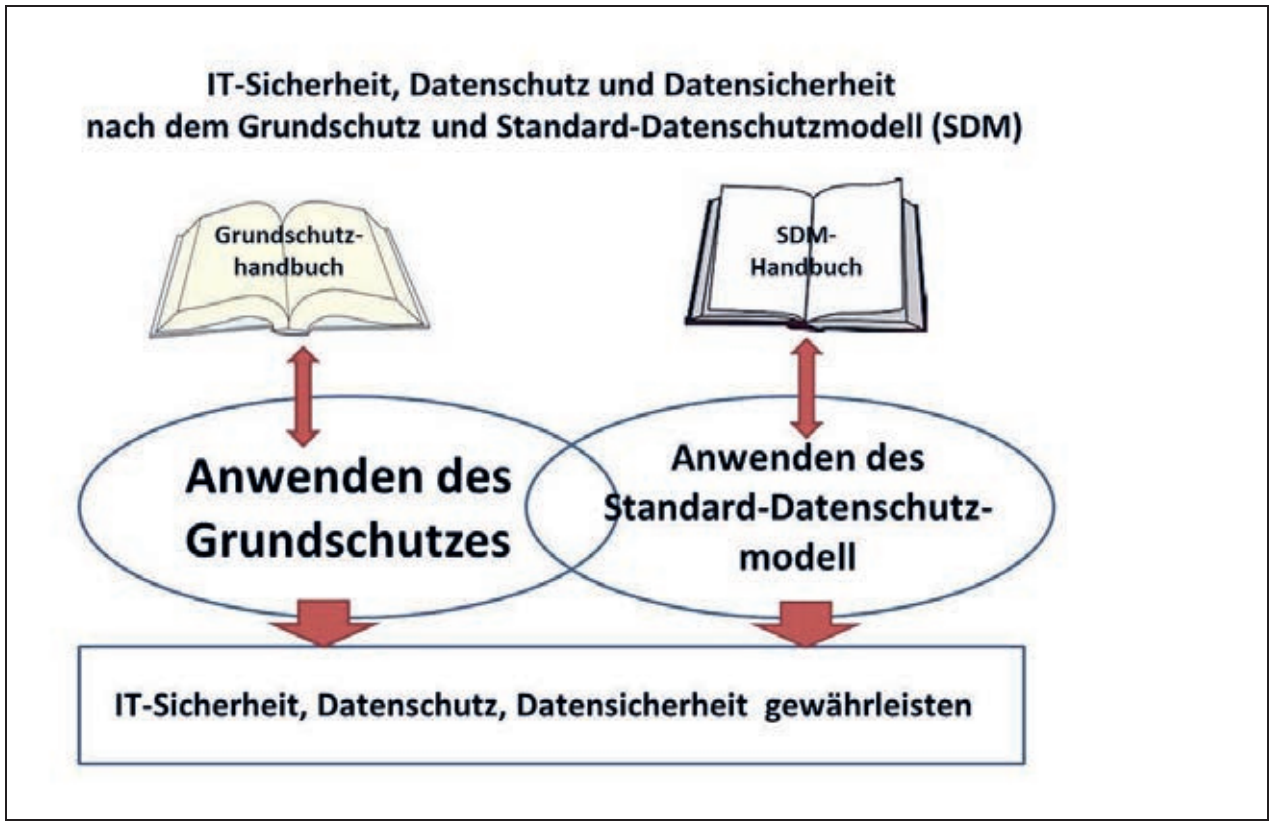
Mit Hilfe der Gewährleistungsziele überführt das SDM die rechtlichen Anforderungen der DSGVO in den von der Verordnung geforderten Katalog aus technischen und organisatorischen Maßnahmen. Dieser Referenzkatalog ermöglicht zudem, die Maßnahmen auf ihre Wirksamkeit zu überprüfen. Derartig standardisierte Maßnahmenkataloge bieten eine sehr gute Grundlage für die in der DSGVO vorgesehenen datenschutzspezifischen Zertifizierungen.

Eine solche Standardisierung unterstützt somit die von der Verordnung vorgegebene Zusammenarbeit der Aufsichtsbehörden, die mit einheitlichen Beratungs- und Prüfkonzepten die modernen Verfahren zur automatisierten Verarbeitung personenbezogener Daten begleiten. Das SDM als ganzheitliches Prüf- und Beratungskonzept kann dabei zu einem abgestimmten, transparenten und nachvollziehbaren System der datenschutzrechtlichen Bewertung führen.

Das SDM sollte jetzt im Einsatz getestet und ähnlich wie das Grundschutzmodell mit einem Maßnahmenhandbuch versehen werden. Derzeit sind im SDM Version 1.0 (abrufbar unter www.datenschutz.bund.de) schon eine Reihe von Maßnahmen erarbeitet worden, die direkt angewendet werden können. Gleichwohl müssen diese aufgrund von technologischen Weiterentwicklungen immer wieder angepasst und ergänzt werden. Auch neue Techniken werden in Zukunft die Erarbeitung neuer Maßnahmen nach sich ziehen. Das Modell soll zukünftig sowohl für die Datenschutzaufsicht im Bereich der privaten Wirtschaft als auch im Bereich der öffentlichen Verwaltung einen wesentlichen Beitrag leisten, um einen an Grundrechten orientierten Datenschutz durchzusetzen.

Kasten a zu Nr. 10.2.11.5

Kasten b zu Nr. 10.2.11.5



10.2.11.6 IT-Konsolidierung Bund

Die Neuaufstellung der IT des Bundes macht Fortschritte. Nachdem das BMI bereits seit 2006 die IT-Konsolidierung für fast alle Behörden in seinem Geschäftsbereich plant, wurde im Mai 2015 von der Bundesregierung die Konsolidierung der IT der gesamten Bundesverwaltung beschlossen, bei deren Umsetzung ich beratend einbezogen bin.

Die Konsolidierung der Informationstechnik des Bundes verfolgt das Ziel, die Informationssicherheit in der Bundesverwaltung dauerhaft mit hoher Qualität zu gewährleisten. Die zunehmende Geschwindigkeit der technologischen Entwicklung macht es notwendig, flexibel reagieren zu können, um die Leistungsfähigkeit eines stabilen IT-Betriebs sicherzustellen.

Die Umsetzung der IT-Konsolidierung bildet ein ressortübergreifendes Projekt, das sich aus mehreren Teilprojekten zusammensetzt. Die Bundesregierung hat mich frühzeitig sowohl auf der Ebene der Gesamtprojektleitung als auch im Rahmen der einzelnen Teilprojekte um Beratung aus datenschutzrechtlicher Sicht gebeten. Daher habe ich die Konsolidierung von Beginn an begleitet und deutlich gemacht, welche datenschutztechnischen und -rechtlichen Rahmenbedingungen im Zuge der Anpassung der IT-Betriebe erfüllt sein müssen.

Neben Informations- und Beratungsgesprächen habe ich im Verlauf des Verfahrens unter anderem auch zum Entwurf der Rahmenvereinbarung zwischen dem Bundesministerium des Innern, dem Bundesministerium für Verkehr und digitale Infrastruktur und dem Bundesministerium der Finanzen für die Übertragung von Betriebsaufgaben auf das Informationstechnikzentrum Bund (ITZBund) Stellung genommen. Dabei habe ich besonders auf die Problematik der Auftragsdatenverarbeitung aufmerksam gemacht. Denn sowohl das BDSG als auch die europäische Datenschutz-Grundverordnung (DSGVO) fordern eine für die Verarbeitung personenbezogener Daten verantwortliche Stelle. Lässt die Stelle diese Verarbeitung in ihrem Auftrag durch einen Dritten durchführen, müssen die Vorgaben des § 11 BDSG zur Auftragsdatenverarbeitung beachtet werden.

Mit der Übergabe des IT-Betriebs gehen zwar weitere Aufgaben auf das ITZBund über, aber die Verantwortlichkeit für die ordnungsgemäße Verarbeitung personenbezogener Daten bleibt bei der auftraggebenden Behörde. Deshalb finden die Vorgaben des § 11 BDSG zur Auftragsdatenverarbeitung hier Anwendung und die dort vorgesehenen Vereinbarungen zur Festlegung technisch-organisatorischer Maßnahmen zur Gewährleistung eines datenschutzgerechten Betriebs müssen vor der Betriebsübernahme verbindlich geschlossen sein.

Das BDSG sieht, genauso wie die DSGVO, umfangreiche Kontrollrechte und -pflichten für die datenverarbeitende Stelle vor. So umfasst § 11 BDSG auch die Pflicht der verantwortlichen Stelle, sich vor und in regelmäßigen Abständen während des laufenden Betriebs eines IT-Verfahrens von der ordnungsgemäßen Durchführung der technisch-organisatorischen Maßnahmen zu überzeugen.

Weil diese Kontrollrechte und -pflichten, die jeden einzelnen Auftraggeber und jedes von ihm übertragene Verfahren betreffen, im laufenden Betrieb die Personalressourcen eines Rechenzentrums stark belasten können, empfehle ich eine Zertifizierung des IT-Sicherheitsmanagements des ITZBund zum Beispiel nach dem Standard ISO 27001 (Zertifizierung auf Basis von IT-Grundschutz).

Eine Zertifizierung und regelmäßige Re-Zertifizierung des IT-Sicherheitsmanagements erleichtert den Auftraggebern die Erfüllung ihrer Kontrollpflichten erheblich und entlastet in Folge auch die Personalressourcen des ITZBund. Im Rahmen eines (Re-) Zertifizierungsprozesses wird einmalig für alle nach einem standardisierten Schema geprüft, was sonst jeder Auftraggeber für sich für jedes Verfahren wiederholen müsste.

In meiner beratenden Funktion bringe ich mich außerdem in die Ressortabstimmungen zu den einzelnen Maßnahmen ein. Beispiele dafür sind der Entwurf des Rechenzentrums-Konsolidierungsplans 2017, die Weiterentwicklung der IT-Steuerung des Bundes oder der Entwurf einer Architekturrichtlinie für die IT des Bundes. Ein zentraler Aspekt ist dabei Sorge dafür zu tragen, dass die datenschutzrechtlichen Prinzipien der Erforderlichkeit und der Verhältnismäßigkeit beachtet werden.

Meine Beratungstätigkeit wird dabei teilweise auch durch den Austausch und die Zusammenarbeit mit dem BSI ergänzt, damit Aspekte der Informationssicherheit und des Datenschutzes gleichermaßen Berücksichtigung erfahren.

Die Bundesregierung macht im Rahmen der IT-Konsolidierung von meinem Beratungsangebot Gebrauch und will, soweit bislang erkennbar, meinen Empfehlungen folgen. Aufgrund des ambitionierten Zeitplans sehe ich allerdings den rechtzeitigen Abschluss bestimmter Maßnahmen mit einer gewissen Sorge.

Mit Beschluss vom 28. September 2016 hat der Haushaltausschuss des Deutschen Bundestags die Bundesregierung aufgefordert, mich in beratender Funktion in die einzelnen Teilprojekte weiterhin mit einzubeziehen. Damit bildet die datenschutzrechtliche und -technische Unterstützung der IT-Konsolidierung Bund für mich weiterhin eine wichtige Aufgabe, über die ich nicht nur an den Haushaltsausschuss, sondern auch im Rahmen weiterer Tätigkeitsberichte berichten werde.

10.3 Aus Beratung und Kontrolle

10.3.1 Beratungs- und Kontrollbesuche beim Statistischen Bundesamt: Forschungsdatenzentrum und IT-Migration im Fokus

Neben einem Informationsbesuch beim Forschungsdatenzentrum des Statistischen Bundesamtes in Wiesbaden mit erfreulichem Ergebnis habe ich weitere Kontrollbesuche zur Überprüfung der immer noch nicht datenschutzgerecht vollzogenen IT-Migration des Statistischen Bundesamtes auf die Bundesstelle für Informationstechnik des Bundesverwaltungsamts durchgeführt.

§ 16 Absatz 6 Bundesstatistikgesetz (BStatG) ermöglicht die Übermittlung von Daten zur Durchführung wissenschaftlicher Vorhaben durch die Forschungsdatenzentren des Bundes und der Länder. Das Angebot des von mir besuchten Forschungsdatenzentrums des Statistischen Bundesamtes (FDZ) umfasst derzeit rund 150 amtliche Statistiken mit einem inhaltlichen Schwerpunkt in den Bereichen Sozial-, Steuer- und Unternehmensstatistiken. Die gesetzlichen Vorgaben erlauben einerseits die Übermittlung von faktisch anonymisierten Einzeldaten. Die Vorschrift regelt aber auch die Zugangsberechtigungen zu formal anonymisierten Daten für Wissenschaft und Forschung in speziell abgesicherten Bereichen des Statistischen Bundesamts und unter Einhaltung wirksamer Vorkehrungen zur Wahrung der Geheimhaltung. Mein Besuch im Frühjahr 2015 diente der Abrundung meiner datenschutzrechtlichen Begleitung des Zensus 2011. Bei meinem Besuch ging es daher um die interne Organisation des Zugangs zu Mikrodaten des Zensus 2011. Dabei habe ich die Aufteilung der Aufgaben und Verantwortung im statistischen Verbund zwischen dem Statistischen Bundesamt, dem Forschungsdatenzentrum NRW und dem Forschungsdatenzentrum Bayern näher untersucht. Als Ergebnis kann ich festhalten, dass die im statistischen Verbund agierenden Forschungsdatenzentren in einem hohen Maß professionell handeln und den berechtigten Anliegen des Datenschutzes eine hohe Priorität eingeräumt werden.

Der IT-Betrieb des Statistischen Bundesamtes ist Anfang des Jahres 2013 im Zuge der IT-Konsolidierung im Geschäftsbereich des BMI auf die Bundesstelle für Informationstechnik des Bundesverwaltungsamts (BIT) übergegangen. Wegen unvollständiger bzw. fehlender schriftlicher Regelungen zur Auftragsdatenverarbeitung nach dem BDSG habe ich das Verfahren Ende 2013 gegenüber dem zuständigen Ministerium als Weisungsgeber förmlich beanstandet (vgl. 25. TB Nr. 5.9).

In seinen Bemühungen, die Mängel abzustellen, die zur Beanstandung geführt haben, habe ich das Statistische Bundesamt im Berichtszeitraum fortwährend beraten. Hierfür habe ich weitere Beratungs- und Kontrollbesuche im März 2015 und zuletzt im Dezember 2016 durchgeführt. Dabei habe ich deutlich gemacht, dass die Kriterien des § 11 Absatz 2 BDSG für eine Verarbeitung personenbezogener Daten im Auftrag grundsätzlich für jedes der rund 130 in Betracht kommenden statistischen Fachverfahren des Bundesamts in entsprechenden Vereinbarungen abzubilden sind. Soweit dabei eine Zusammenfassung gleichförmiger Arbeitsschritte in „Rahmen-“ oder „Gruppen-Service-Level-Agreements“ sinnvoll erscheint, ist eine solche gebündelte Darstellung möglich. Wichtig ist dabei die nachvollziehbare Erfassung sämtlicher IT-Verfahren, die eine Verarbeitung personenbezogener Daten umfassen. Auf der Grundlage eines mir zwischenzeitlich vorgelegten Mustervertrags „Vereinbarung zur

Auftragsdatenvereinbarung nach § 11 BDSG“ sowie von „Muster“-Leistungsbeschreibungen für die einzelnen Verfahren hat mir das Bundesamt eine vollständige und endgültige Umsetzung der gesetzlichen Vorgaben des § 11 BDSG innerhalb des Jahres 2017 zugesagt.

10.3.2 Kontrolle der „Falldatei Rauschgift“

Beim Bundeskriminalamt und im Bereich der Zollfahndung habe ich die „Falldatei Rauschgift“ geprüft. An dieser datenschutzrechtlichen Kontrolle haben auch die Landesbeauftragten für Datenschutz in einem Großteil der Bundesländer teilgenommen und die von den jeweiligen Landespolizeibehörden gespeicherten Daten geprüft. Bei einer Vielzahl der gespeicherten Datensätze fehlte die gesetzlich geforderte Dokumentation. Bundesweit gespeichert waren zahlreiche Bagatellfälle.

Die Falldatei Rauschgift wird seit den 1980er Jahren beim BKA als **bundesweite Verbunddatei** geführt. Verantwortlich für den Inhalt der gespeicherten Daten sind die jeweiligen Verbundteilnehmer. Neben dem BKA nehmen das Zollkriminalamt (ZKA) für den Bereich der Zollfahndung und die Polizeibehörden der Länder an der Datei teil. Aus diesem Grund hatte ich angeregt, diese Datei sowohl aus Bundes- als auch aus Landessicht zu kontrollieren. Die Kolleginnen und Kollegen auf Landesebene sind dieser Anregung zum großen Teil gefolgt und haben die entsprechenden Einspeicherungen der Polizeien der Länder kontrolliert. Bei einer ersten Kontrolle beim **BKA** stellte ich fest, dass dieses selbst nur Fälle sehr schwerer Drogenkriminalität gespeichert hatte, gleichzeitig fiel aber die Speicherung vieler Fälle der Bagatellkriminalität auf.

In einem Fall ging es etwa um einen Apotheker, der in den hinteren Bereich seines Ladengeschäfts gegangen war, um ein Rezept zu prüfen. In diesem Moment entwendete der Kunde ein als Betäubungsmittel eingestuftes Medikament. In der Datei gespeichert wurde aber der Apotheker. In weiteren Fällen ging es um den Besitz geringer Mengen (z. B. ein „Joint“) oder darum, dass Wohnungsinhaber bei einer Privatfeier geduldet hatten, dass einzelne Gäste einen „Joint“ rauchen („Tatort: Toilette“).

Mit Stand Juli 2015 enthielt der Falldatei Rauschgift insgesamt 680.665 Einspeicherungen.

Die Speicherung derartiger Fälle in einer bundesweiten Verbunddatei ist nur verhältnismäßig, wenn zusätzlich weitere Gründe die Notwendigkeit dokumentieren. In einer so genannten Negativprognose sind Tatsachen festzuhalten, aus denen sich ergibt, dass gegen den Betroffenen in Zukunft Strafverfahren zu führen sein werden. Hierzu müssen der Fall und die Person umfassend gewürdigt werden und die Verhältnismäßigkeit ist zu beachten (§ 8 Abs. 2 BKAG). Zudem muss der Fall eine länderübergreifende oder internationale Bedeutung haben oder es muss sich um einen besonders erheblichen Fall handeln. Die als Stichproben gezogenen Fälle wurden von den Landesbeauftragten für Datenschutz in eigener Zuständigkeit geprüft.

Im Bereich des **ZKA** habe ich selbst geprüft und dabei festgestellt, dass durchgehend dokumentierte Negativprognosen fehlten. Deshalb ließ sich nicht abschließend untersuchen, ob die gesetzlichen Voraussetzungen für eine Speicherung vorlagen. Gerade in Fällen, die von den Hauptzollämtern an das ZKA gemeldet worden waren, ging es jedoch oft um geringe Mengen Betäubungsmittel (hierbei insbesondere Cannabis),so dass eine bundesweite Speicherung nicht verhältnismäßig war. Dies habe ich gegenüber dem Bundesministerium der Finanzen beanstandet.

In Folge meiner Beanstandung hat das Bundesministerium der Finanzen das ZKA gebeten, die Negativprognosen, bei denen auch der Grad des Restverdachts und die jeweilige Tatbeteiligung zu berücksichtigen sind, nachzuholen und die Daten nach § 8 Absatz 2 BKAG in den Fällen zu löschen oder zu anonymisieren, in denen diese Bedingungen nicht erfüllt sind. Sollte diese Überprüfung zeitnah nicht durchgeführt werden können, sind die Daten zu löschen bzw. bis zum Abschluss der Prüfung zu sperren.

Gegenüber dem BKA habe ich angeregt, als Zentralstelle stärker auf die Einhaltung der gesetzlichen Verbundregeln hinzuwirken. Dies gilt insbesondere für Fälle, in denen bei Auswertung der Daten oder aufgrund der Dokumentationslage die Speicherung vieler Bagatellfälle zutage tritt. Die Prüfung der Speichervoraussetzungen bleibt aber Sache der Verbundteilnehmer, also hauptsächlich der Landesbehörden.

Als Ergebnis der Kontrolle stelle ich zudem fest, dass sich die im Bundeskriminalamtgesetz vorgesehene Zusammenarbeit zwischen Datenschutzbeauftragten des Bundes und der Länder als effektiv erwiesen hat. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat einen gemeinsamen Bericht erstellt und die Ergebnisse in einer **Entschließung** zusammengefasst (vgl. u. Anlage 6).

Nach Angaben des BKA wird die Falldatei Rauschgift mittelfristig abgeschafft. Ich gehe davon aus, dass dies etwa Anfang 2018 geschehen wird. Die weiterhin erforderlichen Daten sollen in das neue Verbundsystem PIAV (Polizeilicher Informations- und Analyseverbund, vgl. o. Nr. 10.2.9.2) übertragen werden. In einem weiteren Informationsbesuch beim BKA hat mir dieses ein Filtersystem vorgestellt. Damit will es allen Verbundteilnehmern erleichtern, den Datenbestand zu reduzieren und die weiterhin speicherungsfähigen Daten auszuwählen, die in die neue Datei übertragen werden können. Dabei wird unter anderem technisch nach den sichergestellten Mengen von Betäubungsmitteln gefiltert. Fälle mit Mindermengen können auf diesem Wege technisch aussortiert werden.

Ich begrüße die Anstrengungen, nunmehr einen datenschutzkonformen Zustand herzustellen.

10.3.3 Die europäische Fingerabdruckdatei für Asylsuchende - Eurodac

Die Kontrolle der Datei Eurodac beim Bundeskriminalamt (BKA) als nationaler Zugangsstelle führte kleinere Fehler zutage, die als „Kinderkrankheiten" beim Umgang mit dem neuen System gelten können. Perspektivisch erwarte ich eine deutliche Steigerung der bislang sehr geringen Abfragen.

Im Juli 2015 ist die europäische Verordnung (EU) Nr. 603/2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten in Kraft getreten (vgl. hierzu Nr. 22.11). Die Einrichtung dieser Fingerabdruckdatei soll der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 dienen, die bestimmt, welcher Mitgliedsstaat für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedsstaat gestellten Antrags auf internationalen Schutz zuständig ist. Gleichzeitig legt die Eurodac-Verordnung Erlaubnis- und Verfahrensvorschriften fest, nach denen die **Gefahrenabwehr- und Strafverfolgungsbehörden** der Mitgliedsstaaten sowie Europol Anträge auf **Abgleich mit Eurodac-Daten** stellen dürfen. Die Datei Eurodac wird bei der europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA) geführt.

Die Verordnung sieht sog. operative Stellen in den Mitgliedsstaaten vor, die berechtigt sind, einen Abgleich mit Eurodac-Daten zu beantragen. Dies können nur ausdrücklich von den Mitgliedsstaaten benannte Gefahrenabwehr- und Strafverfolgungsbehörden sein. Anträge der operativen Stellen werden von einer Prüfstelle daraufhin untersucht, ob die Voraussetzungen der Verordnung für einen solchen Antrag vorliegen. Ist das der Fall, wird der Antrag über die sog. **nationale Zugangsstelle** an eu-LISA weitergeleitet.

Nach den Bestimmungen der Eurodac-Verordnung muss **jedes Jahr** von einer unabhängigen Stelle **eine Überprüfung** der Verarbeitung personenbezogener Daten für Zwecke der Gefahrenabwehr und der Strafverfolgung, einschließlich einer stichprobenartigen Analyse der in elektronischer Form übermittelten begründeten Anträge, durchgeführt werden. Eine derartige Kontrolle habe ich erstmals 2016 beim BKA durchgeführt. Das BKA bot sich dafür deshalb an, weil es entsprechend der Eurodac-Verordnung sowohl die nationale Zugangsstelle darstellt als auch selbst eine Prüfstelle sowie operative Stellen besitzt. Innerhalb des BKA sind operative Stellen bestimmte Referate, die aufgrund ihres Tätigkeitsgebietes (Verhütung, Aufdeckung und Untersuchung von terroristischen oder sonstigen schweren Straftaten) dazu besonders bestimmt sind.

Das BKA als nationale Zugangsstelle hatte seit Inkrafttreten der Verordnung 20 Anträge an Eurodac weitergeleitet, davon elf eigene. Von diesen elf erfolgten drei Anträge in Amtshilfe für Bundesländer, die zu diesem Zeitpunkt noch nicht in der Lage waren, die Anfragen eigenständig durchzuführen.

Ich habe mir die Ablauforganisation sowie das Verfahren zeigen lassen und auch stichprobenartig die Anträge geprüft. Dabei habe ich insgesamt nur kleinere Fehler feststellen können, die damit zu erklären sind, dass den Mitarbeitern das Verfahren wegen der geringen Fallzahlen noch nicht hinreichend bekannt war. Das BKA hat bereits die Ankündigung meiner Kontrolle zum Anlass genommen, die Mitarbeiter nochmals zu schulen und ggf. Anpassungen am Verfahren vorzunehmen, um die bereits selbst erkannten Mängel abzustellen. Inhaltliche Fehler waren erfreulicherweise nicht zu verzeichnen. Die Vorgaben der Verordnung, u. a. das vorherige Abfragen anderer, vorrangiger Datenbanken, wurden immer beachtet.

Perspektivisch ist davon auszugehen, dass sich die Fallzahlen und damit auch mein Kontrollaufwand deutlich erhöhen werden. Einerseits handelt es sich hier noch um ein recht „junges“ Verfahren, dessen Nutzung sich - sowohl bei der Erfassung, wie auch bei der Abfrage - erst noch einspielen muss. Andererseits existieren bei der Europäischen Kommission bereits konkrete Pläne, den **Anwendungsbereich** von Eurodac zu **erweitern** (vgl. Nr. 2.3.1). So sollen die Mitgliedsstaaten künftig die Daten von Drittstaatsangehörigen oder Staatenlosen, die keinen Asylantrag gestellt haben, speichern und suchen können. Damit würde Eurodac nicht mehr nur eine „Asyldatenbank“ sein, sondern auch weiteren Zuwanderungszwecken dienen, da beispielsweise Fingerabdruckabgleiche von aufgegriffenen illegalen Einwanderern möglich werden. Zudem sollen künftig neben Fingerabdrücken auch Fotos, Name, Geburtsdatum, Nationalität und Identitätsdokumente in Eurodac gespeichert werden, wodurch eine Personenidentifizierung möglich würde, ohne dass der einspeichernde Staat kontaktiert werden muss. Auch ist beabsichtigt, das Alter für die Abnahme von Fingerabdrücken von 14 auf sechs Jahre abzusenken.

10.3.4 Die Dateien „@rtus-Bund“ und „b-case“ bei der Bundespolizei

Bei der Bundespolizei habe ich eine datenschutzrechtliche Kontrolle der Dateien „@rtus-Bund“ und „b-case“ durchgeführt. Ursprünglich sollte dabei vor allem die Speicherung von Daten zu Kindern geprüft werden, es stellten sich aber auch einige grundsätzliche Fragen, die während der Anhörung zu den Errichtungsanordnungen aufgetreten waren.

Die Datei „@rtus-Bund“ dient zunächst der **Vorgangsbearbeitung**. Darüber hinaus legt eine Dienstanweisung fest, dass eine Nutzung der erfassten Daten zum Zwecke der strategischen oder operativen Auswertung möglich ist. Die Bundespolizei nutzt diese Datei für fallübergreifende Analysen, und zwar sowohl für laufende als auch für abgeschlossene Verfahren. Die Datei sieht keine unterschiedlichen Zugriffsrechte nach dem jeweiligen Bearbeitungsstadium vor.

„b-case“ nutzt die Bundespolizei als **Fallbearbeitungssystem**. Diese Datei dient ihr dazu, die polizeiliche Fallbearbeitung bei Komplex- und Strukturermittlungen sowie bei der Recherche und der Analyse von Informationen zur Aufklärung von Straftaten zu unterstützen. Erfasst werden Daten beispielsweise in den Bereichen Migration, Fahrkartenbetrug, Taschendiebstahlsbanden und Schleusung.

Strukturell ist in erster Linie zu bemängeln, dass beide Dateien nicht zwischen den verschiedenen gesetzlich zulässigen Speicherzwecken (Aufgabenerfüllung, Gefahrenvorsorge und Strafverfolgungsvorsorge sowie befristete Dokumentation und Vorgangsverwaltung) differenzieren.

Nachdem die Vorgangsbearbeitung als Aufgabenerfüllung abgeschlossen ist, dürfen die Daten zur Gefahrenvorsorge und Strafverfolgungsvorsorge nur unter engeren Voraussetzungen und Bedingungen gespeichert werden (§ 29 Abs. 2 und 3 BPolG). Dies berücksichtigen beide Dateien nicht ausreichend. Für die Datei „@rtus-Bund“ kommt darüber hinaus nach Abschluss der Bearbeitung eines Vorgangs in Betracht, diesen zur befristeten Dokumentation zu speichern (§ 29 Abs. 5 BPolG). Das bedingt aber eine organisatorische Trennung der Daten vom übrigen Datenbestand. Die **Zugriffsregelungen** müssen dann entsprechend dem begrenzten Zweck ausgestaltet werden. Derartige organisatorische Vorkehrungen fehlen für die Datei „@rtus-Bund“.

Die fehlende Differenzierung wirkt sich bei der **Speicherung von Daten zu Kindern** in besonderer Weise aus, zumal hier der Grundsatz der Verhältnismäßigkeit stärker zu beachten ist.

Speziell für Kinder ist festzuhalten, dass diese keine Beschuldigten sein können. Daher ist auch eine **Speicherung** als Verdächtige einer Straftat **nur mit erheblichen Einschränkungen zulässig**. Als Zeugen, Hinweisgeber und in vergleichbarer Rolle können Kinder ohnehin nur mit den für diese Personengruppe gesetzlich vorgesehenen Restriktionen gespeichert werden.

Nicht zu beanstanden ist, wenn Kinder zur Aufgabenerfüllung mit entsprechend begrenztem Zweck gespeichert werden. Dies kann bei der Strafverfolgung für kurze Zeit der Fall sein, um der Staatsanwaltschaft den Vorgang mit dem Ziel der Einstellung zuzuleiten. Das kann aber auch zur Gefahrenabwehr zulässig sein, etwa wenn ein Kind vermisst oder sonst gefährdet wird.

Eine darüber hinausgehende Speicherung - insbesondere in der Datei „b-case“ - ist aber in der Regel unzulässig. Ziel der Datei ist es, Daten aus einem Ermittlungsverfahren für weitere Verfahren zur Verfügung zu stellen, um mögliche Zusammenhänge zu ermitteln. Dazu soll nicht nur das Ereignis mit den handelnden Personen für sich isoliert abgebildet werden, sondern die gespeicherten Personen, Objekte, Institutionen, Sachen und Ereignisse sollen fallübergreifend verknüpft werden. Daher ist jedes gespeicherte Datum prinzipiell darauf angelegt, „angereichert“ zu werden. Die in „b-case“ gespeicherten Daten stehen daher unbegrenzt für Zwecke der Gefahrenabwehr und der Strafverfolgung zur Verfügung. Für Kinder verstößt eine solche Speicherung gegen den Grundsatz der Verhältnismäßigkeit. Auch die für eine Speicherung notwendige Negativprognose ist in diesen Fällen nicht möglich.

Eine Speicherung von Zeugen und Hinweisgebern in „b-case“ kommt nicht in Betracht, denn diese Datei erfüllt nicht die für diese Personen zu beachtenden gesetzlichen Restriktionen.

Die Kontrolle hat zu datenschutzrechtlichen Beanstandungen geführt. Derzeit befinde ich mich mit der Bundespolizei im Dialog zur Neugestaltung der Dateien.

10.3.5 ATD-Pflichtkontrollen - wichtig und unbedingt auszubauen

Die verfassungsgerichtlich und gesetzlich vorgegebenen Pflichtkontrollen der Antiterrordatei (ATD 5 beim BfV, BND und beim Militärischen Abschirmdienst (MAD) bildeten einen Schwerpunkt meiner Tätigkeit. Allerdings verfüge ich noch nicht über ausreichende personelle Ressourcen, die verfassungsgerichtlichen und gesetzlichen Vorgaben voll zu erfüllen (vgl. o. Nr. 1.3).

Die Kontrollen bei BND und MAD waren bei Redaktionsschluss noch nicht vollständig abgeschlossen, so dass ich mich vorliegend im Wesentlichen auf die ATD-Pflichtkontrolle beim BfV in Berlin beschränke, die in der zweiten Jahreshälfte 2015 gemeinsam mit Mitarbeitern des Sekretariats der G-10-Kommission des Deutschen Bundestages durchgeführt wurde, (vgl. o. Nr. 10.2.10.2).

Ohne die Ergebnisse vorwegnehmen zu wollen, kann ich aber schon jetzt sagen, dass der organisatorische Ablauf der Kontrollen beim BND und MAD sowie die Unterstützung, die meinen Mitarbeitern dort insbesondere durch die behördlichen Datenschutzbeauftragten zu Teil wurde, sehr erfreulich waren. Vergleichbares kann ich auch über eine entsprechende Kontrolle beim BKA als dateiführender Stelle sagen.

Den im Rahmen der Kontrolle beim BfV erstmalig verfolgten gemeinsamen Kontrollansatz mit der G-10-Kommission des Deutschen Bundestages betrachte ich als zukunftsweisendes Modell, das es zur Vermeidung kontrollfreier Räume auch künftig zu verfolgen gilt (vgl. o. Nr. 10.2.10.2).

Gemäß § 3 Absatz 3 Antiterrordateigesetz (ATDG) sind Daten, die aufgrund einer anderen Rechtsvorschrift zu kennzeichnen sind, auch bei der Speicherung in der ATD entsprechend zu kennzeichnen. Dies trifft regelmäßig auf Daten zu, die im Rahmen einer Telekommunikationsüberwachung nach dem Artikel 10 - Gesetz gewonnen werden. Ich hatte bereits in meinem 23. Tätigkeitsbericht (Nr. 7.1.2) ausgeführt, dass das BfV entgegen der im ATDG normierten gesetzlichen Voraussetzungen alle Daten, die durch heimliche Telekommunikationsüberwachungen erhoben worden waren und daher besonders gekennzeichnet werden mussten, ungekennzeichnet in die ATD übertragen hatte.

Auf meine Aufforderung hin hatte das BfV zugesagt, unverzüglich die gesetzlich vorgeschriebene Kennzeichnung durchzuführen und sämtliche Empfänger über ihre Kennzeichnungspflicht zu unterrichten. Auf eine formelle Beanstandung hatte ich deshalb seinerzeit verzichtet. Im Lichte dessen war ein Schwerpunkt meiner Prüfung die Umsetzung dieser Zusage. Bei meiner neuerlichen Kontrolle musste ich leider feststellen, dass das BfV für diese Problematik immer noch keine Lösung gefunden hat und sich stattdessen weitere Kennzeichnungsverstöße gezeigt haben. Dies stellt einen schwerwiegenden Gesetzesverstoß dar, den ich formell beanstandet habe.

Gemäß § 24 Absatz 4 BDSG ist das BfV als öffentliche Stelle des Bundes verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen. Vor dem Hintergrund der verfassungsgerichtlichen Rechtsprechung und meines hieraus resultierenden Kontrollauftrags („Kompensationsfunktion“; vgl. o. Nr. 10.2.10.2), kommt dieser Unterstützung bei den die Nachrichtendienste betreffenden Kontrollen eine noch größere Bedeutung zu.

Das BfV hat mir allerdings nicht in hinreichendem Maße ermöglicht, die mir gemäß § 10 Absatz 1 ATDG zugewiesene datenschutzrechtliche Kontrollfunktion auszuüben. Mir wurden die im Vorfeld der Kontrolle erbetenen Daten und Informationen nur zu einem äußerst geringen Anteil und zudem verspätet zur Verfügung gestellt. Die wenigen überhaupt zur Verfügung gestellten Daten waren nicht praktikabel auswertbar. Die von mir für die Kontrolle als notwendig erachteten technischen und organisatorischen Voraussetzungen wurden im Vorfeld nicht geschaffen und konnten auch während der Kontrolle nur in geringem Umfang hergestellt werden. So war ein hinreichender Systemzugriff nicht möglich. Die anwesenden Mitarbeiter des BfV verfügten nicht über die notwendigen Berechtigungen und/oder waren nicht in der Lage, die Systeme adäquat zu bedienen. Diese unzureichenden Unterstützungen begründen ebenfalls einen schwerwiegenden Gesetzesverstoß, den ich formell beanstandet habe.

10.3.6 NSA-Skandal: Kontrolle des BND mit ungeahnten Folgen

Meine Kontrolle der Außenstelle des BND in Bad Aibling belegt die Notwendigkeit, insbesondere im Bereich der Nachrichtendienste den Vorgaben des Bundesverfassungsgerichts entsprechende Datenschutzkontrollen durchzuführen.

Die Auswirkungen des NSA-Skandals (vgl. 25. TB Nr. 2.1.1) hat meine Tätigkeit auch in diesem Berichtszeitraum nachhaltig bestimmt. Zwischenzeitlich liegen Kontrollergebnisse vor, über die ich aus Gründen des Geheimschutzes an dieser Stelle nicht detailliert berichten darf. Bei meiner Kontrolle habe ich Rechtsverstöße festgestellt und förmlich beanstandet. Es obliegt allein der Entscheidung des Gesetzgebers, diese Vorgaben zu ändern bzw. anzupassen, um legitimen Informationsinteressen der Öffentlichkeit gerecht werden zu können.

Meine Erkenntnisse habe ich unter Wahrung der Vorgaben des Verschlusssachenschutzes an das für die Kontrolle der Nachrichtendienste des Bundes zuständige Parlamentarische Kontrollgremium (PKGr), die G-10-Kommission des Deutschen Bundestages und den ersten Untersuchungsausschuss des Deutschen Bundestages in der 18. Wahlperiode (NSA-Untersuchungsausschuss) (vgl. o. Nr. 10.2.10.2; 25. TB Nr. 2.1.1) übersandt.

Von herausragender Bedeutung bei meiner Kontrolle waren die jeweils mehrtägigen Vor-Ort-Prüfungen im Oktober 2013 und im Dezember 2014. Aufgrund meiner unerwarteten Feststellungen im ersten Termin habe ich das Kontrollteam zwingend verstärken müssen. Da ich für die Kontrolle der Nachrichtendienste nur Personal

einsetzen darf, das besondere Sicherheitsüberprüfungen durchlaufen hat, war diese Verstärkung nur schwierig zu realisieren.

Die intensiven Vorbereitungen, die Vor-Ort-Termine, die Nachbereitungen mit umfangreichem weiteren schriftlichen und mündlichen Informationsaustausch, die Aufbereitung und Strukturierung der umfänglichen und - auch in technischer Hinsicht - sehr komplexen Informationen haben die Ressourcen dieses Kontrollteams über lange Zeit nahezu vollständig gebunden. Dessen beschränkte Kapazitäten wurden darüber hinaus durch die intensiven Erörterungen mit dem BND und dem für die Aufsicht über den BND zuständigen Bundeskanzleramt sowie die Unterstützungsleistungen für den NSA-Untersuchungsausschuss des Deutschen Bundestages weiter gefordert.

Es besteht die dringende Notwendigkeit, derartige Kontrollen auszubauen und weiter zu intensivieren, um die vom Bundesverfassungsgericht geforderte Kompensationsfunktion (vgl. o. Nr. 1.3 und Nr. 10.2.10) zu erfüllen. Derzeit ist dies mit den zur Verfügung stehenden Ressourcen nicht möglich.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.3; 1.6; 12.3.2; 21.1; 21.2; 21.3; 21.4; 21.5; 22-11; 22.12

11 Ausschuss für Kultur und Medien

11.1 Auswirkungen der DSGVO auf diesen Themenbereich

Die Datenschutz-Grundverordnung (DSGVO) ist ab dem 25. Mai 2018 auch im Bereich von Kultur und Medien unmittelbar in Deutschland anzuwenden.

Zwar ist der Kulturbereich ein Politikfeld, das nicht in die ausschließliche Zuständigkeit der Europäischen Union fällt, allerdings kann das Ziel der DSGVO, eine Vollharmonisierung im Bereich des Datenschutzrechts herzustellen, nur dann ausreichend verwirklicht werden, wenn die Unionsregelung gilt (Art. 5 Abs. 3 Vertrag über die Europäische Union). Daher ist die DSGVO als eine solche vollharmonisierende Regelung zu verstehen, die damit auch im Bereich der Kultur ab dem 25. Mai 2018 anzuwenden ist.

Für den Bereich der Medien führt die DSGVO in ihrem Artikel 85 das so genannte Medienprivileg fort. Danach sind die Mitgliedstaaten einerseits verpflichtet, durch Rechtsvorschriften einen Ausgleich zwischen dem Datenschutz und dem Recht auf freie Meinungsäußerung und Informationsfreiheit herzustellen. Andererseits sieht Artikel 85 Absatz 2 DSGVO zahlreiche Ausnahmen von den Regelungen der DSGVO vor, sofern diese erforderlich sind, um das Recht auf Datenschutz mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen. Die insoweit in Bund und Ländern bestehenden Regelungen des Medien-, Rundfunk-, Presse- und Zivilrechts erfüllen ganz überwiegend diesen Anspruch.

Zur Gewährleistung einer wirksamen unabhängigen Datenschutzkontrolle müssen die Regelungen in Zukunft so ausgestaltet werden, dass für die Verarbeitung personenbezogener Daten zu wirtschaftlich-administrativen Zwecken auch bei Medienunternehmen die Zuständigkeit der jeweiligen Datenschutzaufsichtsbehörden gegeben ist. Denn in diesem Bereich sind Eingriffe in Meinungs-, Presse- oder Rundfunkfreiheit nicht zu befürchten. Die bisher bei der Mehrzahl der Landesrundfunkanstalten und bei der Deutschen Welle insoweit bestehenden Kontrolllücken sind europarechtlich nicht mehr haltbar. Hinsichtlich der Datenschutzkontrolle bei der Deutschen Welle bin ich hierüber mit der Beauftragten für Kultur und Medien im Gespräch.

Auch das Archivrecht ist an die Vorgaben der Datenschutz-Grundverordnung anzupassen:

Diese erkennt die besonderen Belange des Archivwesens an und enthält daher in Artikel 89 einige Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken. Auf Bundesebene sind mit dem Bundesarchiv, dem Politischen Archiv des Auswärtigen Amtes und der Behörde des Bundesbeauftragten für die Stasi-Unterlagen als Sonderarchiv insbesondere drei große Archive betroffen. Die möglichen Ausnahmen für die Verarbeitung personenbezogener Daten bedürfen der Umsetzung durch nationales Recht. Entsprechende Regelungen sind im Entwurf des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU enthalten.

11.2 Einzelthemen

11.2.1 Neufassung des Bundesarchivgesetzes

Bei der Neufassung des Bundesarchivgesetzes bestand an zwei Stellen wesentlicher Nachbesserungsbedarf.

Ziel des Gesetzentwurfs ist die grundlegenden Überarbeitung und Aktualisierung der bisherigen aus dem Jahr 1988 stammenden Fassung des Gesetzes. In dem im Herbst 2016 an den Deutschen Bundestag übermittelten Regierungsentwurf waren aus meiner Sicht zwei wesentliche Punkte überarbeitungsbedürftig:

Unterlagen die bereits nach einem Informationszugangsgesetz zugänglich waren

In der geltenden Fassung des Bundesarchivgesetzes unterfallen einmal nach dem Informationsfreiheitsgesetz des Bundes zugängliche Unterlagen nach einer Übernahme durch das Bundesarchiv nicht mehr den archivrechtlichen Schutzfristen. Dies sollte nach dem Willen der Bundesregierung geändert werden. Zuvor nach einem Informationszugangsgesetz zugängliche Unterlagen sollten mit der Übergabe an das Bundesarchiv zunächst wieder grundsätzlich der 30-jährigen Schutzfrist unterliegen.

Anbietungspflicht der Nachrichtendienste

Weiter sah der Entwurf eine Regelung vor, nach der die Nachrichtendienste des Bundes selbst über die Anbietung von Unterlagen an das Bundesarchiv entscheiden sollten.

Nachdem meine Bedenken in den Ressortberatungen keine Berücksichtigung gefunden hatten, habe ich mich zunächst mit einem Schreiben an den Ausschuss für Kultur und Medien des Deutschen Bundestages gewandt und auf diese aus meiner Sicht missglückten Regelungsvorschläge hingewiesen. Einer Einladung des Ausschusses folgend habe ich die Möglichkeit genutzt, im Rahmen einer Öffentlichen Anhörung nochmals auf diese Punkte hinzuweisen.

Ich freue mich, dass zum ersten Punkt die von mir vorgeschlagene Änderung Eingang in das Gesetz gefunden hat. Demnach werden Unterlagen also mit der Umwandlung in Archivgut auch künftig nicht wieder den archivrechtlichen Schutzfristen unterfallen, sondern sind weiterhin nach den Kriterien der Informationszugangsgesetze zu bewerten. Ich begrüße diese Änderung ausdrücklich, da hierdurch die mit den Informationszugangsgesetzen geschaffene Transparenz nicht nachträglich wieder eingeschränkt werden kann.

Die Regelung zur eingeschränkten Anbietungspflicht der Nachrichtendienste ist jedoch in modifizierter Form weiterhin im Gesetz verankert. Dies bedauere ich sehr. Auch ohne diese Sonderregelungen für die Nachrichtendienste wären hinreichende Schutzmöglichkeiten für dort entstandene Unterlagen vorhanden gewesen. Durch die nun erfolgte Regelung könnten die Nachrichtendienste künftig ohne die Möglichkeit einer effektiven Kontrolle selbst darüber entscheiden, ob und welche Unterlagen sie an das Bundesarchiv abgeben. Dadurch wird unter anderem die Forschung zur Arbeit der Nachrichtendienste erheblich erschwert werden.

11.2.2 Gemeinsames Bund-Länder-Portal zum Kulturgutschutz

Im Bereich des Kulturgutschutzes entsteht das erste gemeinsame Verfahren nach § 11 des Gesetzes zur Förderung der elektronischen Verwaltung (EGovG).

Durch das Gesetz zur Neuregelung des Kulturgutschutzrechts (KGSG) wurde das derzeit lediglich auf einer Bund-Länder-Vereinbarung beruhende Infoportal www.kulturgutschutz-deutschland.de auf eine gesetzliche Grundlage gestellt. Gemäß § 79 KGSG führen Bund und Länder zum Schutz des nationalen Kulturgutes nun ein gemeinsames Verfahren im Sinne von § 11 EGovG ein. Sie sind befugt, Informationen einschließlich personenbezogener Daten in diesem gemeinsamen Verfahren zu verarbeiten. Dabei handelt sich um den ersten praktischen Anwendungsfall von § 11 EGovG. Für die entsprechende datenschutzrechtliche Kontrolle bin ich auf Grundlage des BDSG zuständig.

Meine Kontrollbefugnis umfasst u. a. die technische Ausgestaltung des Verfahrens, grundsätzliche Festlegungen zu den zu speichernden personenbezogenen Daten, Rollen- und Berechtigungskonzepte, Löschfristen sowie die Protokollierung.

Die Zusammenarbeit mit der BKM im Vorfeld und während des Gesetzgebungsverfahrens zum neuen KGSG war vorbildlich. Im Nachgang zum Gesetzgebungsverfahren wurde mit mir bereits das neue Rollen- und Berechtigungskonzept abgestimmt.

Nach Implementierung plane ich einen Beratungs- und Kontrollbesuch bei der BKM, um das neue Kulturgüterschutzportal in der Praxis zu begutachten.

11.2.3 Expertenkommission zur Zukunft der Behörde des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

Die Aufarbeitung eines der dunkelsten Kapitel der neueren deutschen Geschichte wird fortgesetzt.

Das Stasi-Unterlagen-Gesetz (StUG) aus dem Jahre 1991 weist der Behörde des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU) folgende Kernaufgaben zu:

- die Sicherung, Erfassung und Erschließung der Stasi-Unterlagen,
- die Gewährung von Akteneinsicht,
- die Verwendung der Unterlagen z. B. zum Zweck der Rehabilitation, aber auch zur Überprüfung auf eine frühere Stasi-Tätigkeit und
- die Forschungs- und Bildungsarbeit.

Im Juli 2014 hat der Deutsche Bundestag eine Expertenkommission zur Klärung der Entwicklungsperspektiven für diese bislang von der BStU erfüllten Aufgaben eingesetzt (Bundestagsdrucksache 18/1957). Im Frühjahr 2016 hat die Expertenkommission ihren Bericht vorgelegt. Darin empfiehlt sie unter anderem, die Stasi-Unterlagen bis zum Ende der nächsten (19.) Wahlperiode in das Bundesarchiv zu integrieren und die Standorte der Akten und damit die Zugangsmöglichkeiten im Beitrittsgebiet zu erhalten, die Forschungsaufgaben einer selbständigen „Forschungsstelle DDR-Staatssicherheit“ zu übertragen, und dem Bundesbeauftragten u. a. die Aufgaben eines Ansprechpartners bzw. einer Ombudsperson für Opfer der kommunistischen Diktatur und Betroffene im Sinne des StUG mit Beratungsfunktion auch für den Deutschen Bundestag, die Bundesregierung und die Bundesbehörden zu übertragen (Bundestagsdrucksache 18/8050).

Die Kommission hat dem Deutschen Bundestag vorgeschlagen, ihre Handlungsempfehlungen in ein Artikelgesetz umzusetzen, damit „noch in der 18. Legislaturperiode notwendige Entscheidungen für die zukünftige Fortführung der Aufgaben der/des BStU getroffen werden können“.

Dieses Gesetzgebungsverfahren steht noch aus. Die bei Redaktionsschluss bereits weit fortgeschrittene aktuelle Novellierung des Bundesarchivgesetzes (vgl. u. Nr. 11.2.1) enthält noch keine Regelungen über den Informationszugang zu Stasi-Unterlagen.

11.3 Aus Beratung und Kontrolle
Beratungs- und Kontrollbesuche beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

Im Berichtszeitraum führten meine Mitarbeiter zwei Beratungs- und Kontrollbesuche in den Außenstellen Erfurt und Schwerin des BStU durch. Ferner fand ein Informations- und Beratungsbesuch bei der Außenstelle in Leipzig statt.

Der Schwerpunkt beider Beratungs- und Kontrollmaßnahmen lag bei den technischen und organisatorischen Maßnahmen zur Absicherung der Aktenbestände und der Liegenschaft.

Als generelles Ergebnis meiner Prüfung konnte ich erneut feststellen, dass Mitarbeiterinnen und Mitarbeiter des BStU sich durch hohe Sachkunde und Gewissenhaftigkeit im Umgang mit den sensiblen personenbezogenen

Unterlagen auszeichnen. Über die Funktionsfähigkeit des Haussicherungssystems konnte ich mich durch Begehung der Liegenschaft und - in der Außenstelle Schwerin - durch die Durchführung eines Probealarms überzeugen.

Gleichwohl habe ich zwei Verbesserungsvorschläge zur datenschutzkonformen Überarbeitung des bestehenden Entsorgungsauftrags zur Übernahme und Vernichtung sensibler Unterlagen sowie die Einführung eines einheitlichen Löschdatums für Posteingangsbücher - für alle Außenstellen - unterbreitet, die sich bereits in der Umsetzungsphase befinden.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.6; 21.1; 21.5

12 Ausschuss für Recht und Verbraucherschutz

12.1 Auswirkungen der DSGVO auf diesen Themenbereich

Bisher gilt das nationale Bundesdatenschutzgesetz nur für den administrativen Bereich der Justiz. Dies wird auch künftig mit der europäischen Datenschutz-Grundverordnung (DSGVO) so bleiben.

Mit dem Justizprivileg (Art. 55 Abs. 3) klärt die DSGVO den sachlichen Geltungsbereich für die Justiz. Im Rahmen ihrer justiziellen Tätigkeit unterstehen die Gerichte nicht der Datenschutzaufsicht. Nur bei Verwaltungsangelegenheiten der Gerichte können die Datenschutzaufsichtsbehörden tätig werden. Dies entspricht der bisherigen Rechtslage nach § 1 Absatz 2 Nummer 2b BDSG.

Die Datenschutz-Grundverordnung wird sich auch auf den Verbraucherschutz auswirken. Einerseits geht die Stärkung der Betroffenenrechte - bei allen Unterschieden - häufig auch einher mit einer Stärkung des Verbraucherschutzes. Mit der Ausübung der durch das Datenschutzrecht gewährten Rechte nehmen die Betroffenen ein wichtiges Freiheitsrecht - das Recht auf informationelle Selbstbestimmung - wahr. Der Verbraucherschutz sichert hingegen den Schutz des Einzelnen vor einer auf wirtschaftlichem Ungleichgewicht beruhenden Benachteiligung und verfolgt damit ein anderes Ziel. Dennoch können z. B. eine höhere Transparenz bei der Verarbeitung personenbezogener Daten oder gesetzliche Anforderungen an eine datenschutzrechtliche Einwilligung auch zu einem verbesserten Verbraucherschutz beitragen.

Andererseits enthält Artikel 80 Absatz 2 DSGVO eine ganz unmittelbare Schnittstelle zwischen Daten- und Verbraucherschutz. Die Norm ermöglicht es den Mitgliedstaaten, Regelungen einzuführen, die es Datenschutzverbänden erlauben, unabhängig von einem Auftrag einer betroffenen Person bei den Aufsichtsbehörden Beschwerden einzulegen oder gerichtliche Hilfe gegen Entscheidungen der Aufsichtsbehörden oder gegen Verantwortliche zu beanspruchen. Insoweit wird zu prüfen sein, ob das Unterlassungsklagegesetz im Hinblick auf die im Jahre 2015 geschaffene datenschutzrechtliche Verbandsklage (vgl. 25. TB Nr. 6.1) angepasst werden muss.

12.2 Einzelthemen

12.2.1 Die Justiz wird digitalisiert

Auch im Bereich der Justiz schreitet die Digitalisierung weiter voran.

Die zunehmende Digitalisierung erreicht immer mehr auch den Bereich der Justiz. Die flächendeckende Einführung elektronischer Akten bei Gerichten und im Strafverfahren ist wohl nur noch eine Frage der Zeit. Mit dem Justizkommunikationsgesetz wurden bereits 2005 die rechtlichen Voraussetzungen für die elektronische Aktenbearbeitung an Gerichten geschaffen. Wider Erwarten haben die Regelungen jedoch bis heute noch nicht zu einer flächendeckenden elektronischen Aktenbearbeitung geführt. Die Papierakte hält sich tapfer.

Eine Wende könnte jedoch das Inkrafttreten weiterer Vorschriften des Gesetzes über die Förderung des elektronischen Rechtsverkehrs mit den Gerichten bringen. Ab 2018 sind diese verpflichtet, einen elektronischen Zugang zu eröffnen, damit Schriftstücke und insbesondere Klagen auch elektronisch eingereicht werden können. Ab 2022 sind Behörden und Rechtsanwälte verpflichtet, Schriftsätze bei Gericht nur noch elektronisch einzureichen.

Neben vielen praktischen und arbeitsorganisatorischen Herausforderungen ist die Einführung einer elektronischen Aktenführung immer auch eine Herausforderung für den Datenschutz. Das gilt insbesondere im Hinblick auf die langen Aufbewahrungs- bzw. Speicherfristen für Gerichtsakten. Elektronische Speichermedien haben

bisher nur eine limitierte Lebensdauer. Es muss jedoch sichergestellt werden, dass die Daten aus den elektronischen Akten bis zum Ende der Speicherfrist lesbar bleiben. Auf der anderen Seite muss auch technisch gewährleistet sein, dass personenbezogene Daten am Ende der jeweiligen Speicherfrist gelöscht werden können.

Im Berichtszeitraum gab es diverse Gesetzgebungs- und Verordnungsverfahren, die die Digitalisierung der Justiz zum Gegenstand hatten:

Elektronische Akte im Strafverfahren

Ein erster Entwurf wurde bereits im Juni 2012 der Justizministerkonferenz vorgestellt. Das Bundeskabinett hat den Gesetzentwurf zur elektronischen Akte im Strafverfahren nun verabschiedet und in das parlamentarische Verfahren eingebracht (Bundestagsdrucksache 18/9416). Zu dem Gesetzentwurf hatte ich im Rahmen der Ressortberatungen ausführlich Stellung genommen (25. TB Nr. 6.3). Leider haben meine Anregungen bislang keine Resonanz gefunden. Mir liegen auch keine Vorschläge vor, wie das Verfahren der elektronischen Akte in der Praxis durchgeführt werden soll. Hierbei geht es insbesondere um 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.

Ungeklärt ist zudem die Frage, ob die Justizbehörden eine technische Grundlage schaffen wollen, die von den Polizeibehörden mitgenutzt werden kann oder ob der umgekehrte Weg eingeschlagen werden soll. Denkbar wäre etwa, die Vorgangsbearbeitungssysteme der Polizeibehörden um ein entsprechendes Modul zu erweitern. Wollen Justizbehörden und Polizeibehörden für ein und dieselbe „Akte“ unterschiedliche Systeme nutzen, stellt sich die Frage nach den Schnittstellen und der Zusammenarbeit. Daraus ergeben sich neben ökonomischen auch datenschutzrechtliche Fragen.

Ebenso wie beim Entwurf für ein neues Bundeskriminalamtgesetz (BKAG, vgl. Nr. 10.2.9.1) sollten zunächst die grundlegenden Fragen zur angestrebten Architektur geklärt sein. Mit anderen Worten: Was genau wollen Gesetzgeber und Praxis erreichen? Erst dann kann optimal gesagt werden, welche Vorgaben der Gesetzgeber, insbesondere hinsichtlich der Verantwortlichkeiten und Zugriffsregelungen, schaffen sollte.

Außerdem müssen die aktuellen Vorgaben des Bundesverfassungsgerichts in seiner Entscheidung zum BKAG (Nr. 1.3) berücksichtigt werden. Diese betreffen etwa die zweckändernde Verwendung von Daten. Der Gesetzentwurf zur elektronischen Akte im Strafverfahren will hier sehr weitgehende und niedrigschwellige Zweckänderungen freigeben, unabhängig von der Sensibilität der Daten und ihrer Erhebung. Dies führt zu verfassungsrechtlichen Risiken, wenn die Daten auch an die Nachrichtendienste übermittelt werden.

Kritisch zu bewerten ist auch der Umstand, dass Daten u. a. zu Opfern und Zeugen in der elektronischen Akte in einem Umfang gespeichert werden können, der weit über den Inhalt der Informationssysteme der Polizeibehörden hinausgeht.

Elektronisches Urkundenarchiv

Das BMJV hat im August 2016 den Entwurf eines Gesetzes zur Neuordnung der Aufbewahrung von Notariatsunterlagen und Einrichtung des elektronischen Urkundenarchivs vorgelegt. Kern des Gesetzentwurfs ist die Einrichtung eines elektronischen Urkundenarchivs bei der Bundesnotarkammer. In diesem sollen notarielle Unterlagen künftig vorrangig aufbewahrt werden und zwar bis zum Ende der gesetzlichen Aufbewahrungsfrist von grundsätzlich 100 Jahren. Die Bundesnotarkammer soll verpflichtet werden, dieses Archiv bis spätestens 2022 zu errichten.

Daneben enthält der Gesetzentwurf Regelungen zum besonderen elektronischen Notarpostfach und zum elektronischen Notarverzeichnis. Das elektronische Notarverzeichnis existiert bereits auf freiwilliger Basis und wird nun auf eine gesetzliche Grundlage gestellt.

Bereits der erste Referentenentwurf hat datenschutzrechtliche Aspekte weitgehend berücksichtigt. Zudem wurden die von mir im Rahmen der Ressortabstimmung ausgesprochenen Empfehlungen vollständig in den Gesetzesentwurf eingearbeitet. Dies begrüße ich sehr.

Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer

Mit der neuen Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (RAVPV) wird von der Verordnungsermächtigung des § 31c Bundesrechtsanwaltsordnung Gebrauch gemacht. Die RAVPV enthält spezifische Regelungen über das besondere elektronische Anwaltspostfach sowie über die Rechtsanwaltsverzeichnisse der Anwaltskammern und das Gesamtverzeichnis der Bundesrechtsanwaltskammer.
Weiter sieht die RAVPV Bestimmungen zum Inhalt, zur Berichtigung, Löschung und Sperrung von Eintragungen in den Rechtsanwaltsverzeichnissen vor. Auch für das besondere elektronische Anwaltspostfach werden in der RAVPV die Einrichtung, Ausgestaltung, Sperrung und Löschung der Postfächer geregelt.
Die Vorschriften wurden durch das BMJV datenschutzkonform ausgestaltet.

Die Digitalisierung in der Justiz wird mich sicher auch in den kommenden Jahren noch intensiv beschäftigen.

12.2.2 Vorratsspeicherung von Daten 2.0

Nachdem zunächst das Bundesverfassungsgericht (Urteil vom 02.03. 2010, Az. 1 BvR 256/08) und später der Europäische Gerichtshof (Urteil vom 08.04.2014, Az. C-293/12 und C-594/12) die gesetzlichen Grundlagen für die Vorratsspeicherung von Telekommunikationsverkehrsdaten auf nationaler und europäischer Ebene für grundrechtswidrig erklärt hatten, wagte der Gesetzgeber bereits im Frühjahr 2015 einen neuen Anlauf.

Leider erfolgte dies nicht im Stile eines Mittel- oder Langstreckenlaufs, bei dem man sein Tempo wohlüberlegt gestaltet, sondern vielmehr in Form eines 100-Meter-Sprints. Im Mai 2015 legte das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) einen Gesetzentwurf zur Wiedereinführung der Vorratsspeicherung von Daten vor. Dieser wurde - entgegen der Vorgaben der Gemeinsamen Geschäftsordnung der Bundesministerien - mit extrem kurzen Stellungnahmefristen und ohne Durchführung einer Ressortbesprechung innerhalb von nur sieben Tagen vom Kabinett beschlossen. Bei einem umfangreichen Gesetzgebungsverfahren, das massive Eingriffe in die Grundrechte der Bürgerinnen und Bürger zur Folge hat, ist dies deutlich zu kritisieren.
Doch nicht nur beim Verfahren weist das neue Gesetz Defizite auf. Die neuen Regelungen erhielten mit „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ zwar einen neuen Namen. Inhaltlich finden sich aber auch hier in vielen Punkten dieselben rechtlichen Probleme, die schon in vorherigen Gesetzen angelegt waren. Auch wenn die Eingriffe durch das neue Gesetz, beispielsweise durch eine Verkürzung der Speicherfristen und die Ausnahme für E-Mails, weniger weitgehend sind als bei dem vom Bundesverfassungsgericht (BVerfG) für nichtig erklärten ersten Gesetz, und Anforderungen des Gerichts zur Sicherheit der Daten berücksichtigt wurden, bestehen nach wie vor erhebliche Zweifel, ob die neuen Regelungen grundrechtkonform sind (vgl. Kasten a zu Nr. 12.2.2).

Hinsichtlich der Auflistung sämtlicher Defizite verweise ich auf meine im Gesetzgebungsverfahren gegenüber dem Deutschen Bundestag abgegebene ausführliche Stellungnahme (abrufbar unter: www.datenschutz.bund.de). An dieser Stelle möchte ich gleichwohl zwei wesentliche Argumente für meine Bewertung nennen: Unabhängig von der bereits erwähnten „restriktiveren“ Ausgestaltung handelt es sich auch bei der aktuellen Version der Vorratsspeicherung von Daten um einen schwerwiegenden Grundrechtseingriff von besonderem Ausmaß. Sowohl das BVerfG als auch der Europäische Gerichtshof (EuGH) haben in ihren Urteilen klargestellt, dass bei

entsprechenden Maßnahmen hohe Anforderungen an deren Ausgestaltung zu stellen sind, um sie im Ergebnis als angemessen beurteilen zu können. Auch wenn erkennbar versucht worden ist, diesen Maßstäben gerecht zu werden, reißt das Gesetz mehrfach die von den obersten Gerichten aufgestellten Hürden.

Zum einen missachtet das Gesetz - jedenfalls im Bereich der Überwachung der Internetnutzung - die vom BVerfG aufgestellte und in wissenschaftlichen Beiträgen als „Überwachungs-Gesamtrechnung“ bezeichnete Vorgabe, keine anlasslose Datenspeicherungen vorzunehmen, die - auch im Zusammenspiel mit anderen Datenerfassungen - zu einer weitgehenden Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen können. Gerade dies wird jedoch aufgrund des Trends der vergangenen Jahre, die Befugnisse staatlicher Behörden vor allem bei der Erfassung und Auswertung von IP-Adressen zu erweitern, in immer größerem Rahmen möglich.

Die erhobenen IP-Adressen sind geeignet dazu beizutragen, detaillierte Informationen über die im Internet genutzten Inhalte zu gewinnen. Bei Telemediendiensten erhobene Nutzungsdaten können im Zusammenspiel mit den im Rahmen der Vorratsspeicherung von Daten erfassten IP-Adressen grundsätzlich einzelnen Nutzern zugeordnet werden. Deren Surfverhalten kann dann zumindest über mehrere Wochen in nicht unerheblichem Maße überwacht werden.

Zum anderen wurde die Vorgabe des EuGH aus dem Eingangs erwähnten Urteil nicht berücksichtigt, nach dem unter anderem die von der Vorratsspeicherung von Daten betroffenen Personen auf solche beschränkt werden müssen, die in irgendeiner Weise in eine schwere Straftat verwickelt sind oder deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten. Das Gesetz greift daher unverhältnismäßig in die durch die Charta der Grundrechte der Europäischen Union (Charta) garantierten Rechte auf Achtung des Privat- und Familienlebens in Artikel 7 und des Schutzes personenbezogener Daten in Artikel 8 ein.

Die Anwendbarkeit der Charta als Maßstab auch für die nationale Gesetzgebung hat der EuGH zudem erst kürzlich noch einmal in einem Urteil zu entsprechenden schwedischen und englischen Gesetzen klargestellt (Urteil vom 21.12.2016, Az. C-203/15 und C-698/15). In diesem Zusammenhang wiederholte das Gericht zudem unmissverständlich, dass eine allgemeine und unterschiedslose Vorratsspeicherung von Daten sämtlicher Verkehrs- und Standortdaten aller Telekommunikationsnutzer europarechtswidrig ist. Lediglich eine gezielte Vorratsspeicherung von Daten, die hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist, sei zulässig.

Forderungen nach einer erheblichen Ausweitung der in der Vorratsspeicherung von Daten geregelten Speicherpflichten, beispielsweise durch die Miteinbeziehung der bei der Nutzung von E-Mail- und Messengerdiensten anfallenden Daten sowie nach einer Verlängerung der Speicherfristen würden die Vorratsspeicherung von Daten auf ein über das im verfassungswidrigen Gesetz von 2010 hinausgehende Maß ausdehnen.

Unabhängig davon bestehen meines Erachtens erhebliche Bedenken, dass das aktuelle Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten den hohen Anforderungen von BVerfG und EuGH genügt. Die letztliche Entscheidung hierüber wird aber wieder einmal von eben diesen Gerichten getroffen werden. Eine Prüfung der deutschen Vorratsspeicherung von Daten vor dem EuGH ist aufgrund seiner Entscheidung zur Anwendbarkeit der Charta jedenfalls nicht unwahrscheinlich. Beim BVerfG wurden bereits mehrere Verfassungsbeschwerden gegen das Gesetz eingereicht.

Ich werde die Verfahren selbstverständlich begleiten und zudem im Rahmen meiner Aufsichtsfunktion über Unternehmen der Telekommunikationsbranche die Umsetzung unter datenschutzrechtlichen Gesichtspunkten in der Praxis kontrollieren.

Katalog, Verordnung, Richtlinie

Die Regelungen zur Vorratsspeicherung von Daten im TKG verlangen nicht nur die Erstellung eines Anforderungskatalogs, sondern verweisen auch auf die TKÜV und TR TKÜV. Auch diese Vorschriften müssen angepasst werden.

Die Telekommunikationsanbieter müssen bei der Vorratsspeicherung von Daten einen besonders hohen Standard der Datensicherheit und Datenqualität gewährleisten. Auch dies war eine Forderung des BVerfG, die in das Gesetz übernommen wurde. Wie das konkret erfolgen soll, regelt das Telekommunikationsgesetz (TKG) nur im Ansatz und verlagert stattdessen die Aufgabe der Konkretisierung gemäß § 113f TKG in einen Anforderungskatalog. Diesen hat die Bundesnetzagentur (BNetzA) zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und mir erstellt. Sofern die zur Vorratsspeicherung Verpflichteten die hier festgelegten Vorgaben berücksichtigen, sollte man diesbezüglich von einem ausreichenden Sicherheitsniveau ausgehen können.

Die Speicherung der Verkehrsdaten soll in einer zentralen Speicherinfrastruktur vorgenommen werden, die sowohl physisch als auch logisch durch Firewall-Systeme gegen Angriffe geschützt ist (vgl. Kasten b zu Nr. 12.2.2).

Über die Grundarchitektur hinaus mussten bei der Erstellung des Katalogs allerdings viele technisch-organisatorische Detailfragen geklärt werden. Dies gestaltete sich nicht immer einfach, da einerseits ein sehr hohes Schutzniveau erreicht werden musste, das andererseits aber in der Praxis mit einem noch vertretbaren Aufwand umsetzbar sein sollte.

Eine der Anforderungen war z. B., die irreversible Löschung der speicherpflichtigen Verkehrsdaten nach Ablauf der Speicherfrist zu gewährleisten. Moderne Speichermedien (magnetische Festplatten wie auch SSD) können fehlerhafte Sektoren deaktivieren, also dem Zugriff des Betriebssystems entziehen. Damit ist ein zuverlässiges Löschen nicht mehr möglich. Daher ist vorgesehen, die „Vorratsdaten“ mit Tagesschlüsseln verschlüsselt zu speichern. Wenn der Tagesschlüssel nach Ablauf der vorgesehenen Speicherdauer zuverlässig gelöscht wird, gelten auch die verschlüsselten Daten als gelöscht. Hierzu ist ein zuverlässiges Schlüsselmanagement erforderlich. Eine tatsächliche Löschung der verschlüsselten Daten ist zwar weiterhin erforderlich, muss jedoch nicht mehr mit besonderem Aufwand betrieben werden.

Eine weitere besondere Herausforderung ist auch die sichere Gestaltung des Abfragesystems. Das TKG verweist hierzu in § 113c Absatz 3 auf die Regelungen der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV) und die Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR TKÜV). Auch wenn diese Verweisung wohl Synergien mit bereits bestehenden Abfragesystemen für andere Auskunftszwecke (z. B. Bestands- und Verkehrsdatenauskünfte aus betrieblich genutzten Daten) schaffen sollte, führt sie bei der Gestaltung des Anforderungskatalogs eher zu Problemen.

Statt im Rahmen des Anforderungskatalogs die Auskunft der Daten beim oben bereits dargestellten Gesamtkonstrukt mit zu regeln, musste das Thema ausgeklammert und im Rahmen der Überarbeitung der TKÜV und der zugehörigen Technischen Richtlinie umgesetzt werden. Dabei wäre es zumindest sinnvoll gewesen, diese Vorschriften parallel zur Erstellung des Anforderungskatalogs anzupassen. Da aber die Federführung für die Er- und Überarbeitung der jeweiligen Regelung bei unterschiedlichen Stellen liegt, wurde zuerst der Anforderungskatalog erstellt und im Nachgang die Überarbeitungen der TKÜ und sodann der TR TKÜV in Angriff genommen. Deswegen konnten letztere bis Redaktionsschluss noch nicht fertig gestellt werden. Erste Entwürfe dafür liegen mir bereits vor und eine finale Veröffentlichung der Vorschriften noch vor dem Beginn der verpflichtenden Speicherung im Juli 2017 ist nach derzeitigem Stand wahrscheinlich. Ob aufgrund der Umsetzungsfristen bzw. der Zeit für eine technische Realisierung Übergangslösungen eingesetzt werden müssen, bleibt abzuwarten.

In der TKÜV wurde insbesondere ein neuer Teil für die Beauskunftung der Verkehrsdaten eingeführt, der auch die Regelung für die Protokollierung enthält. Für betrieblich gespeicherte und speicherpflichtige Verkehrsdaten wird dabei kein grundsätzlicher Unterschied gemacht, d. h. die hohen Anforderungen gelten auch für betrieblich genutzte Daten.

Auch für einige weitere Bereiche wurden Anpassungen durchgeführt. Erfreulicherweise ist nicht mehr vorgesehen, Anordnungen per Telefax zu übermitteln. Ebenso wird die Beantwortung des Auskunftsersuchens künftig nur noch elektronisch erfolgen können. Weitere Anpassungen betreffen z. B. die Ausland-Ausland-Fernmeldeaufklärung (vgl. Nr. 10.2.10.1). Ganz unauffällig soll auch eine Fernwartung der Einrichtungen des Bundesnachrichtendienstes zugelassen werden. Bisher durfte überhaupt keine Fernwartung erfolgen, nun darf keine *unbefugte* Fernwartung stattfinden.

Die TR TKÜV regelt neben der technischen Umsetzung von Überwachungsmaßnahmen auch die Maßnahmen, mit denen die Erteilung und Übermittlung von Auskünften umgesetzt werden sollen. Bei größeren Anbietern wird die sogenannte „ETSI-ESB“ vorgeschrieben. (ETSI bezieht sich auf die Normungsorganisation, das Europäische Institut für Telekommunikationsnormen, das den zu Grunde liegenden europäischen Standard erstellt hat, und ESB bedeutet *Spezifikation der elektronischen Schnittstelle für Auskunfts- und Verbindungsdatenersuchen sowie Telekommunikationsüberwachungen und Ortungen* oder kurz *Elektronische Schnittstelle Behörden*.) In der TR TKÜV wurden insbesondere die Anforderungen für die Vorratsdatenspeicherung ergänzt. Kleinere Anbieter mit weniger als 100.000 Nutzern können auch die weniger aufwändige „E-Mail-ESB“ nutzen, bei der die Anordnungen - nach Ankündigung - per verschlüsselter E-Mail entgegen genommen und beantwortet werden sollen.

Ob diese neuen Regelungen im Detail tatsächlich den Anforderungen an ein hohes Datenschutz- und Datensicherheitsniveau genügen, kann erst beurteilt werden, wenn die finale Fassung der Vorschriften vorliegt. Da die Vorgaben des TKG jegliche Verarbeitung von Vorratsdaten bei Telekommunikationsanbietern umfassen - also neben der Erhebung und Speicherung auch die Prozesse zur Auskunftserteilung - müssen die Bestimmungen im Anforderungskatalog der Verordnung und Richtlinie als zusammenhängende Einheit betrachtet werden. Die der BNetzA in Zusammenarbeit mit dem BSI und mir übertragene Aufgabe der Konkretisierung der allgemeineren TKG-Regelungen ist damit erst abgeschlossen, wenn dieses in sich aufeinander verweisende Gesamtkonstrukt bis zur letzten Regelung fertiggestellt und in Kraft getreten ist. Inwieweit diese Vorschriften dann hoffentlich völlig widerspruchsfrei in der praktischen Umsetzung durch die Unternehmen zusammenspielen, wird sich in der Praxis zeigen müssen. Ich werde mich durch Beratungs- und Kontrollbesuche bei verschiedenen Telekommunikationsanbietern davon überzeugen.

Kasten a zu Nr. 12.2.2

Die wesentlichen Vorgaben der Vorratsspeicherung von Daten 2.0 auf einen Blick

Verpflichtete (*§ 113a TKG*)

- Erbringer öffentlich zugänglicher Telekommunikationsdienste (nicht jedoch Hotels, Cafés, o. ä.)

Zu speichernde Daten (*§ 113b TKG*)

- *bei Telefonverbindungen, SMS und MMS*:
  - die Nummern oder Kennungen der an der Verbindung/Übermittlung beteiligten Anschlüsse
  - die Datums- und Zeitangabe des Beginns und Ende der Verbindung/Übermittlung
  - im Mobilfunk zusätzlich die SIM-Kartennummer (IMSI), Kennung des benutzten Gerätes (EMEI) und die Funkzellen, in der die Verbindung begonnen wurde
  - bei IP-Telefonie zusätzlich die IP-Adressen der beteiligten Anschlüsse und zugewiesene Benutzerkennung
- *bei Internetnutzung*:
  - die IP-Adresse
  - die Anschluss- und Benutzerkennung
  - die Datums- und Zeitangabe des Beginns und Ende der Internetnutzung unter einer IP-Adresse
  - bei mobiler Internetnutzung zusätzlich die Funkzelle, in der die Verbindung begonnen wurde

Speicherfristen (*§ 113b TKG*)

- Standortdaten (Funkzellen) für vier Wochen
- alle anderen Daten für zehn Wochen

Abfrageberechtigte Stellen (*§ 113 c TKG*)

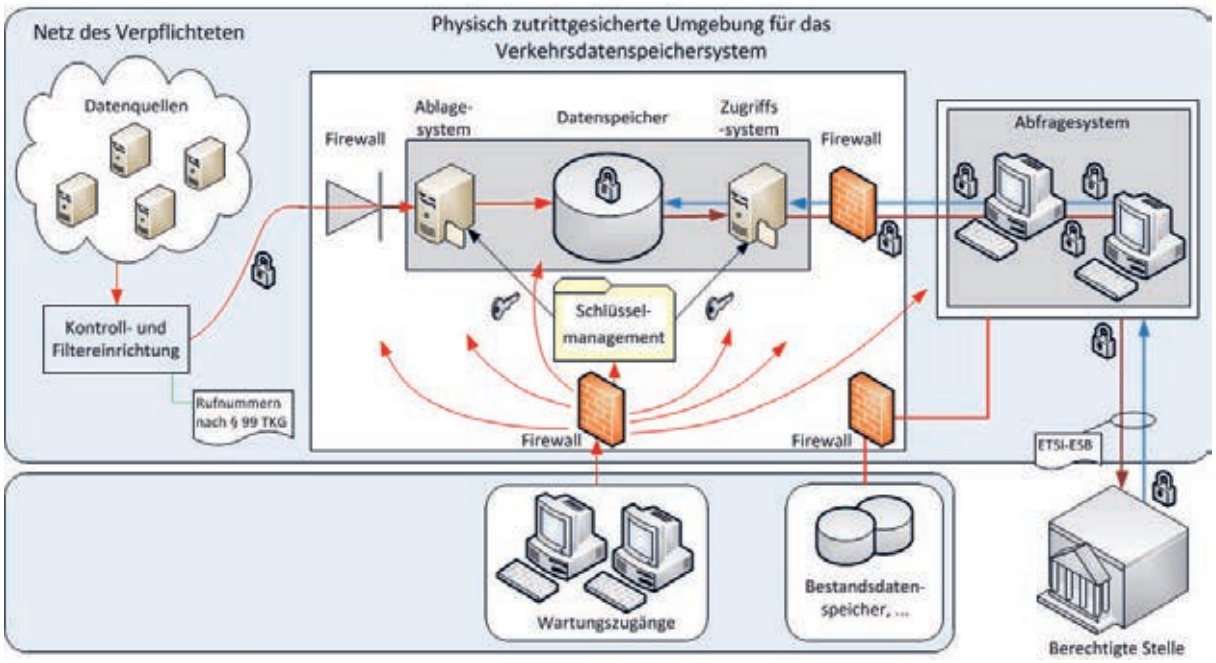
- Strafverfolgungsbehörden von Bund und Ländern
- Gefahrenabwehrbehörden der Länder

Sonstiges

- die Daten dürfen nur zur Verfolgung von in der Strafprozessordnung gesondert ausgewiesenen schweren Straftaten oder zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand des Bundes oder eines Landes verwendet werden; einzige Ausnahme ist die Zuordnung einer IP-Adresse zu einem konkreten Anschlussinhaber (*§ 113c TKG*)
- die Daten müssen nach dem Stand der Technik (z. B. durch sichere Verschlüsselung, vom Internet entkoppelter Speicherung, Vier-Augen-Prinzip beim Zugriff) vor missbräuchlicher Verwendung geschützt werden (*§ 113d TKG*)
- Zugriffe auf die Daten müssen protokolliert werden (*§ 113e TKG*)
- Die BNetzA erstellt zusammen mit der BfDI und dem BSI einen Anforderungskatalog (*§ 113f TKG*)
- Die Speicherpflicht beginnt am 1. Juli 2017

Kasten b zu Nr. 12.2.2

Umsetzungsbeispiel der Grundarchitektur



12.2.3 Datenschutzrechtliche Probleme bei Mietspiegeln?

Die Erstellung von Mietspiegeln soll angeblich auf datenschutzrechtliche Hürden stoßen. Aus diesem Grund sollten Sonderregelungen im BGB geschaffen werden.

Im September 2015 nahmen meine Mitarbeiter auf Einladung des BMJV an einem Expertentreffen zum Thema Mietspiegel teil. Im Rahmen dieses Gesprächs sowie im Vorfeld des Treffens teilten verschiedene professionelle Mietspiegelersteller mit, sie stießen bei der Erstellung der Mietspiegel immer wieder auf datenschutzrechtliche Hürden. Insbesondere würden sie benötigte Daten nicht erhalten. Leider wurden von den Mietspiegelerstellern keine konkreten datenschutzrechtlichen Bestimmungen genannt, die einer Übermittlung der benötigten Daten entgegenstehen könnten.

Im April 2016 übersandte mir das BMJV dann einen Referentenentwurf, der insbesondere Vorschriften zur Mietspiegelerstellung enthielt. Darunter waren auch datenschutzrechtliche Spezialregelungen für die Mietspiegelerstellung. Gegen die vorgeschlagenen Bestimmungen bestanden aus Datenschutzsicht zahlreiche Bedenken. Insbesondere erschloss sich mir der Bedarf für die neuen Vorschriften nicht. Bereits nach geltenden bundes- und landesrechtlichen Regelungen ist die Erstellung von Mietspiegeln datenschutzkonform möglich. Auch die Gesetzesbegründung konnte nicht schlüssig darlegen, aus welchen Gründen diese Spezialregelungen benötigt würden.

Meine Bedenken habe ich dem BMJV in einer Stellungnahme ausführlich dargelegt. Im Anschluss daran fand auf Einladung des BMJV ein sehr konstruktives Gespräch zwischen Vertretern des BMJV, des BMI und der BfDI statt. Ich konnte meine Vorbehalte nochmals mündlich vortragen. Das BMJV hat mir zugesichert, die datenschutzrechtlichen Regelungen grundlegend zu überarbeiten.

12.2.4 Erfahrungsaustausch der BfDI mit den Datenschutzbeauftragten der Bundesgerichte

2016 fand auf meine Initiative hin der erste Erfahrungsaustausch der BfDI mit den Datenschutzbeauftragten der Bundesgerichte statt.

Auf meine Einladung hin haben sich am 23. Juni 2016 die behördlichen Datenschutzbeauftragten (bDSB) der Bundesgerichte zu einem ersten Erfahrungsaustausch in meiner Dienststelle in Bonn getroffen. Die angereisten bDSB der Bundesgerichte und meine Mitarbeiter nutzten die Gelegenheit, um sich persönlich kennenzulernen und aktuelle datenschutzrechtliche Themen zu besprechen. Gegenstand der Diskussion war insbesondere:

- die Stellung der bDSB an den Bundesgerichten,
- die Auswirkungen der Datenschutz-Grundverordnung auf die Justiz sowie
- Entwicklungen im Bereich des elektronischen Rechtsverkehrs und der elektronischen Akte.

Diese Themen werden alle Beteiligten in den kommenden Jahren intensiv begleiten (vgl. a. u. Nr. 1.6). Ich freue mich daher, dass alle Teilnehmer ihr Interesse an einer Fortsetzung des Erfahrungsaustauschs bekundet haben.

Von einem regelmäßigen Erfahrungsaustausch mit den bDSB der Bundesgerichte verspreche ich mir eine Stärkung des Datenschutzes an den Bundesgerichten, auch in die Bereiche hinein, die meiner Kontrolle entzogen sind.

12.2.5 Öffentlichkeitsfahndung nach den Vorgaben der Richtlinien für das Straf- und Bußgeldverfahren

Das BMJV will die RiStBV nicht einem Beschluss der Justizministerkonferenz entsprechend ändern. Ebenso sollen die gesetzlichen Vorschriften nicht angepasst werden.

Die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) regeln näher, was die Strafverfolgungsbehörden bei der öffentlichen Fahndung nach Beschuldigten oder Zeugen zu beachten haben. Nach einem Beschluss der Justizministerkonferenz sollen die Möglichkeiten erweitert werden, soziale Netzwerke für die Fahndung zu nutzen. Das hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisiert (vgl. 25. TB Nr. 6.2). Ich begrüße daher, dass die erweiterte Nutzung sozialer Netzwerke zumindest für Bundesbehörden nicht in der RiStBV verankert wird. Das BMJV teilte mir allerdings mit, dass es die Regelungen der in den Ländern neu gefassten RiStBV nicht für rechtswidrig halte.

Ebenso hatte ich gebeten, die gesetzlichen Fahndungsvoraussetzungen in der Strafprozessordnung zu prüfen. Denn die Öffentlichkeitsfahndung im Internet ist besonders eingriffsintensiv. Einmal veröffentlichte Daten und Bilder lassen sich nicht mehr zurückholen. Teilweise wurde die Öffentlichkeitsfahndung in der Vergangenheit mit richterlicher Genehmigung sogar bei Fundunterschlagungen eingesetzt. In einem mir bekannten Fall stellte sich die abgebildete Person später als unschuldig heraus. Daher sollte darüber nachgedacht werden, ob auf gesetzlicher Ebene höhere Schwellen gezogen werden müssen. Dem hat das BMJV allerdings ebenfalls eine Absage erteilt.

12.3 Aus Beratung und Kontrolle

12.3.1 Datenschutzrechtliche Kontrolle am Bundesverwaltungsgericht - es gibt für alles ein erstes Mal!

Meine Mitarbeiter haben mit dem Bundesverwaltungsgericht (BVerwG) erstmals einen datenschutzrechtlichen Beratungs- und Kontrollbesuch an einem Bundesgericht durchgeführt.

Aufgrund der den Berufsrichtern in Artikel 97 GG gewährten Unabhängigkeit beschränkte sich der Kontrollteil meines Besuchs auf die Stellung des behördlichen Datenschutzbeauftragten sowie auf die Verwaltung des Gerichts (§ 24 Abs. 3 BDSG).

Die Funktion des Datenschutzbeauftragten wird am BVerwG durch einen Berufsrichter ausgeübt. Eine Freistellung für die Wahrnehmung dieser Funktion ist entgegen § 4f Absatz 5 Satz 1 BDSG nicht erfolgt. Auch wenn Berufsrichter ihre Dienstzeit in großem Umfang frei steuern und die Einteilung seiner Aufgaben unabhängig gestalten können, messe ich einer tatsächlichen Entlastung von den hauptamtlichen Aufgaben als Berufsrichter eine hohe Bedeutung zu. Ich halte es aufgrund der vielfältigen Aufgaben eines behördlichen Datenschutzbeauftragten für geboten, eine Freistellung über eine Reduzierung der dem Berufsrichter als Berichterstatter zugewiesenen Verfahren zu bewirken (vgl. a. u. Nr. 1.6).

Ich habe das BVerwG über meine Rechtsauffassung informiert und um Umsetzung gebeten.

Die Akten der Gerichtsverwaltung werden bereits seit dem Jahr 2012 ausschließlich elektronisch geführt. Für sämtliche elektronischen Vorgänge wurde dabei ohne Differenzierung eine Archivierungsfrist von zehn Jahren im entsprechenden IT-Verfahren „EVA“ (Elektronische Verwaltungsakte) festgelegt. Dies steht jedoch im Gegensatz zu dem für die Gerichtsverwaltung geltenden Erlass über die „Bestimmungen zur Regelung der Aufbewahrung und Vernichtung von Akten im Geschäftsbereich des Bundesministeriums der Justiz“ aus dem Jahr 1991, der differenzierte Aufbewahrungsfristen für das Schriftgut vorsieht. Darin ist beispielsweise für die Aufbewahrung von Bewerbungen am Gericht lediglich eine Archivierungsfrist von drei Jahren vorgesehen. Auf der anderen Seite sollen Organisations- und Geschäftsverteilungspläne des Gerichts sogar für einen Zeitraum von 30 Jahren aufbewahrt werden.

Die Gültigkeit des o. g. Erlasses hatte sich das BVerwG zuletzt im Jahr 2010 vom BMJV bestätigen lassen. Ich habe daher das Gericht gebeten, den Erlass im IT-Verfahren „EVA“ für das Schriftgut der Gerichtsverwaltung umzusetzen.

Gleichzeitig habe ich gegenüber dem BMJV aber auch eine Überarbeitung des 25 Jahre alten Erlasses unter Berücksichtigung des aktuellen Bedarfs der Bundesgerichte für die Archivierung von Schriftgut angeregt. Ich hoffe, dass die Umsetzung meiner Anregung im BMJV nicht genauso viel Zeit in Anspruch nimmt, wie die Verabschiedung der aufgrund § 2 des Schriftgutaufbewahrungsgesetzes zu erlassenden Rechtsverordnung über die Archivierung des Schriftguts aus gerichtlichen Verfahren, die bereits seit mehr als zehn Jahren auf sich warten lässt.

12.3.2 Beratung und Kontrolle im Deutschen Patent- und Markenamt sowie bei der Vergabestelle für Berechtigungszertifikate

Das Deutsche Patent- und Markenamt ist bei seiner elektronischen Schutzrechtsakte inklusive der elektronischen Akteneinsicht gut aufgestellt. Dasselbe gilt für die Vergabestelle für Berechtigungszertifikate zur Nutzung der eID-Funktion des Personalausweises.

Beim **Deutschen Patent- und Markenamt** (DPMA) habe ich mir im Berichtszeitraum die Umsetzung des Projekts „Elektronische Schutzrechtsakte“ vor Ort angesehen und dies mit einer Kontrolle zu Querschnittsthemen verbunden.

Das Patent- sowie das Marken- und Gebrauchsmusterrecht gewähren grundsätzlich jedem einen Anspruch auf Akteneinsicht. Dies dient potentiellen Anmeldern zur Orientierung, ob bereits bestimmte Schutzrechte in Deutschland eingetragen sind. Als Konsequenz müssen personenbezogene Daten wie Name und Adresse des Anmelders bzw. Schutzrechtsinhabers von Gesetzes wegen einer beschränkten Öffentlichkeit zugänglich gemacht werden. Bei der Umstellung von der Papier- auf die elektronische Akte hat das DPMA auch die Akteneinsicht auf ein elektronisches Verfahren umgestellt. Neue Verfahren werden ausschließlich elektronisch geführt, Altbestände bei Bedarf sukzessive digitalisiert. Über die Internetseite des DPMA können Interessierte nach Schlagworten oder auch Aktenzeichen suchen und bekommen Aktenteile elektronisch angezeigt. Bei der

Digitalisierung von Papierakten sowie bei der Bereitstellung von elektronischen Dokumenten für die Online-akteneinsicht muss allerdings berücksichtigt werden, dass bestimmte personenbezogene Daten dem Antragsteller nicht zugänglich gemacht werden dürfen. Dazu zählen eigene Aktenteile wie das Gebührenrecht (insbesondere Kontoverbindungsdaten) und die Verfahrenskostenhilfe. Auch eventuelle ärztliche Gutachten, mit denen belegt werden soll, warum eine Frist nicht eingehalten werden konnte, dürfen nicht veröffentlicht werden. Durch ein Rechte- und Rollenkonzept sowie ein Sperrkonzept bei personenbezogenen Daten im Bereich des Zahlungsverkehrs sowie der Verfahrenskostenhilfe oder der Wiedereinsetzung ist gewährleistet, dass nur diejenigen Mitarbeiter des DPMA personenbezogene Daten zur Kenntnis nehmen können, die diese Daten zur Aufgabenerledigung benötigen.

Meine Mitarbeiter haben den Besuch beim DPMA zudem genutzt, um auch allgemeine datenschutzrechtliche Themen zu prüfen. Ein Schwerpunkt lag auf der Stellung der behördlichen Datenschutzbeauftragten (bDSB). Engagement, Kenntnisse und Stellung der bDSB innerhalb der Behörde sind vorbildlich. Lediglich hinsichtlich ihrer Freistellung sehe ich Verbesserungsbedarf. Bereits ab einer Größe von 1.000 Mitarbeitern ist allein aufgrund des Personaldatenschutzes eine vollständige Freistellung der bDSB erforderlich. Da das DPMA über 2.500 Mitarbeiter hat, habe ich die vollständige Freistellung der bDSB und eine zusätzliche Unterstützung durch ihre Mitarbeiter empfohlen. Hierdurch kann die bDSB mehr eigene Initiativen zur Stärkung des Datenschutzes im DPMA ergreifen und verstärkt präventiv tätig werden (vgl. auch Nr. 1.6). Weitere Kontrollthemen waren das Besuchermanagement, die Videoüberwachung, Auftragsdatenverarbeitungen nach § 11 BDSG sowie die Angaben im Verfahrensverzeichnis. Meine Mitarbeiter haben hier in Einzelfällen Verbesserungsbedarf festgestellt. Insgesamt ist das DPMA beim Datenschutz jedoch gut aufgestellt.

Für die **Vergabestelle für Berechtigungszertifikate** (VfB) im Bundesverwaltungsamt konnte ich feststellen, dass die Prüfung datenschutzrechtlicher Aspekte bei der Vergabe von Berechtigungszertifikaten für die Nutzung der eID-Funktion des Personalausweises in guten Händen ist. Unternehmen wie auch Behörden, die die eID-Funktion für ihre Online-Prozesse nutzen möchten, benötigen hierfür ein sog. Berechtigungszertifikat, das die VfB vergibt. Hierzu prüft sie vorab, welche Daten aus dem Ausweischip für welche Identifizierungsprozesse ausgelesen werden sollen. Durch dieses Genehmigungsverfahren wird zum einen sichergestellt, dass nur diejenigen Daten übermittelt werden, die für den genannten Zweck unbedingt erforderlich sind. Zum anderen wird auch geprüft, ob die Geschäftszwecke oder hoheitlichen Aufgaben, für die die Daten benötigt werden, auch mit dem Personalausweisgesetz vereinbar sind. Bürger, die ihre eID-Funktion online einsetzen, können so auf eine gesetzeskonforme Verarbeitung ihrer Daten vertrauen. Durch das Zertifikat als Voraussetzung für den Einsatz der eID-Funktion können die Kunden darüber hinaus sichergehen, dass ihr Gegenüber (also die Firma oder die Behörde), das die entsprechende Internetseite betreibt, auch tatsächlich die Institution ist, für die sie sich ausgibt. Ich konnte mich beim Besuch vor Ort überzeugen, dass die VfB ihre Arbeit sehr gewissenhaft verrichtet. Nach dem Willen der Bundesregierung soll sich das Verfahren der Genehmigung von Berechtigungszertifikaten allerdings grundlegend ändern (vgl. Nr. 10.2.1).

Es ist bedauerlich, dass die eID-Funktion des Personalausweises immer noch ein Nischendasein führt, obwohl sie eine sehr sichere und datenschutzgerechte Möglichkeit der Online-Identifizierung ist. Ich hoffe, dass sich dies bald ändert und die eID-Funktion auch beispielweise in Massenverfahren wie dem Online-Banking Einzug hält.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2.1; 1.6; 21.1; 21.5; 22.4

13 Sportausschuss

13.1 Auswirkungen der DSGVO auf diesen Themenbereich

Auch im Bereich des Sports wird die Datenschutz-Grundverordnung gelten. Die Akteure sollten sich daher frühzeitig mit ihren Auswirkungen beschäftigen.

Auch wenn die Datenschutz-Grundverordnung (DSGVO) keine expliziten Regelungen für den Bereich des Sports vorsieht, sind ihre Bestimmungen auch hier zu beachten (vgl. Nr. 1.1, Nr. 1.2 f.). Dies gilt insbesondere für die Rechtmäßigkeit der Verarbeitung der Daten, der Verarbeitung besonderer Kategorien personenbezogener Daten wie z. B. Gesundheitsdaten und die Rechte der Betroffenen nach Kapitel III der DSGVO. Die umfangreichen Informationspflichten und Auskunftsrechte treffen auch die für eine Datenverarbeitung Verantwortlichen. Ich empfehle daher auch den Akteuren im Sport, sich frühzeitig und intensiv mit den neuen Regelungen vertraut zu machen.

13.2 Einzelthemen

Big Data im Sport

Big Data gewinnt auch im Bereich des Sports immer mehr an Bedeutung. Der Datenschutz sollte dabei frühzeitig berücksichtigt werden.

Der Sportausschuss des Deutschen Bundestages hatte mich zu einer öffentlichen Anhörung zum Thema Big Data im Spitzensport am 1. Juni 2016 eingeladen. Ich habe diese Gelegenheit genutzt, um auf die Nutzungsmöglichkeiten, vor allem aber auch auf datenschutzrechtliche Risiken und Probleme hinzuweisen. Die Sammlung und Auswertung großer Datenmengen wird vermutlich mittlerweile in nahezu allen Sportarten u. a. zur Gegneranalyse und zur Analyse der eigenen Leistung und deren Optimierung genutzt. Neben Trackern zur Ermittlung der Laufleistung und der physischen Fitness werden auch Kameradaten, bis hin zu Aufzeichnungen durch Kameradrohnen, genutzt. Problematisch ist hierbei, inwieweit die vorgenommenen Datenverarbeitungen durch Einwilligungen der Betroffenen gedeckt sind sowie die Nutzung und Sicherung der gespeicherten Daten. Mangels gesetzlicher Grundlage ist für die Erhebung personenbezogener Daten stets eine Einwilligung der betroffenen Sportlerinnen und Sportler einzuholen. Ob diese unter allen Umständen frei von jeglichem Zwang ist, kann zumindest fraglich sein. Aufgrund des großen Wertes der Daten gerade auch für Konkurrenten im bezahlten Spitzensport besteht die nicht zu unterschätzende Gefahr des Datendiebstahls. Die erhobenen Daten sind deshalb durch technische und organisatorische Maßnahmen abzusichern. Auch wenn sich das Thema Big Data im Sport aus Sicht des Datenschutzes und nach dem gegenwärtigen Kenntnisstand zu den bisher bekannten Anwendungen mit dem derzeit vorhandenen datenschutzrechtlichen Instrumentarium erfassen, regeln und steuern lässt, mag ich künftigen gesetzgeberischen Handlungsbedarf zum Schutz der Betroffenen nicht ausschließen.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 21.1; 21.5

14 Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit

14.1 Aus Beratung und Kontrolle

Beratungs- und Kontrollbesuche beim Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit und in dessen Geschäftsbereich

Meine Kontrollen beim Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit und einer Behörde seines Geschäftsbereichs haben keine Verstöße gegen datenschutzrechtliche Bestimmungen ergeben.

- Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit

Das Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) ist meiner Empfehlung gefolgt, seinen behördlichen Datenschutzbeauftragten und auch dessen Mitarbeiterin zu jeweils 50 Prozent für den behördlichen Datenschutz freizustellen (vgl. oben Nr. 1.6).

Außerdem habe ich dem BMUB empfohlen, ein Datenschutzkonzept zu erstellen und sein IT-Sicherheitskonzept insbesondere um ein Löschkonzept zu ergänzen. Das BMUB hat die Umsetzung dieser beiden Empfehlungen in Angriff genommen und wird mich über deren Abschluss informieren.

- Bundesamt für Strahlenschutz

Bei der Kontrolle des Bundesamtes für Strahlenschutz (BfS) in Salzgitter stand neben der Überprüfung der Stellung und Aufgabenerfüllung der behördlichen Datenschutzbeauftragten (bDSB, vgl. oben Nr. 1.6) der Umgang mit personenbezogenen Daten im Zusammenhang mit Forschungsprojekten des Bundesamtes im Fokus.

Hierzu hat mir das BfS exemplarisch die Vorgehensweise zu Aufbau, Betrieb und Dokumentation der in ihrer Verantwortung stehenden Bioprobenbank über Uranbergbauarbeiter der ehemaligen Wismut AG erläutert. Das Projekt umfasst insgesamt 450 auf freiwilliger Basis erhobene Blutproben ehemaliger Bergbauarbeiter, die über einen Gesamtzeitraum von über 40 Jahren unterschiedlich hohen Strahlenbelastungen ausgesetzt waren. Die mir dargestellten Verfahren zum Aufbau der Datenbank sowie zur Auswertung und zur weiteren Nutzung der Bioproben lassen auf eine hohe Sensibilität für die Einhaltung datenschutzrechtlicher Vorgaben schließen.

Meine Mitarbeiter konnten sich vor Ort überzeugen, dass die bDSB ihre Aufgaben im erforderlichen Umfang wahrnimmt. Bedingt durch die organisatorische Aufteilung des BfS auf mehrere weit voneinander entfernt liegende Dienstsitze, ist eine wünschenswerte persönliche Präsenz der bDSB allerdings nur eingeschränkt realisierbar. Ich habe empfohlen, die bDSB in weiterem Umfang freizustellen, um sämtliche Dienststellen zwecks Beratung der dort tätigen Mitarbeiterinnen und Mitarbeiter regelmäßig aufsuchen zu können.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2.1; 1.6; 21.1; 21.5

15 Ausschuss für Verkehr und digitale Infrastruktur

15.1 Einzelthemen

Änderung des Straßenverkehrsgesetzes

Bei der Rechtssetzung im Verkehrsbereich wurde ich vom Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) an zahlreichen Ressortabstimmungen entsprechender Rechtsetzungsvorhaben beteiligt. Zu erwähnen ist hier insbesondere der Entwurf zur Änderung des Straßenverkehrsgesetzes (Bundestagsdrucksache 18/11300).

Ziel dieser Gesetzesinitiative ist es, die rechtlichen Grundlagen für das automatisierte Fahren auf Deutschlands Straßen zu schaffen (vgl. hierzu auch Nr. 1.4). So soll zur Klärung von haftungsrelevanten Fragen mit dem Entwurf die elektronische Aufzeichnung von Fahrdaten für Fahrzeuge mit sogenannten automatisierten Fahrfunktionen verbindlich festgeschrieben werden.

Ich habe dem BMVI mitgeteilt, dass in dem vorliegenden Entwurf die zur Wahrung der berechtigten Interessen der betroffenen Fahrer erforderlichen datenschutzrechtlichen Regelungen fehlen. Unbestritten notwendig müssen zur Klärung haftungsrechtlicher Fragen im Falle eines Unfalls Aussagen darüber getroffen werden können, ob das Auto autonom oder der Fahrer gefahren ist. Es ist auch nachvollziehbar, dass aufgezeichnet werden soll, wann ein Fahrer die Aufforderung erhalten hat, die Fahrzeugsteuerung wieder zu übernehmen. Gleiches gilt für die Dokumentation von technischen Störungen der hoch- bzw. vollautomatisierten Fahrsysteme.

Hierbei muss aber konkret und abschließend geregelt werden, welche Daten dazu über welchen Zeitraum aufgezeichnet werden dürfen. Weiter muss zudem präzise und eindeutig bestimmt werden, wer Daten aus dem Fahrzeug erheben und für welchen Zweck an wen übermitteln darf. Sollte der Entwurf in der vorliegenden Form verabschiedet werden, besteht die Gefahr, auf dieser Basis obligatorisch elektronische Fahrtenschreiber in Privatfahrzeugen mit automatisierten Fahrfunktionen einzuführen. Zur Aufklärung von Unfallursachen ist aber nur eine „Blackbox“ erforderlich, die einen eng begrenzten Zeitraum vor dem Eintritt eines Unfalls aufzeichnet.

Damit die Rechte der Fahrer von Fahrzeugen mit automatisierten Fahrfunktionen gewahrt bleiben, muss jede gesetzliche Regelung zur verpflichtenden Einführung elektronischer Fahrdatenspeicher datenschutzrechtlich normenklar und bestimmt sein. Sie muss dazu Regelungen zum Umfang, zur Erhebung, Verarbeitung und Nutzung, zur Zweckbestimmung und zur Löschung der in Rede stehenden personenbezogenen Daten enthalten.

Für eine gesetzliche Regelung zur verpflichtenden Einführung elektronischer Fahrdatenspeicher bedeutet dies konkret:

- diejenigen Daten abschließend aufzuzählen, die aufgezeichnet werden sollen und die nach Übermittlung an Dritte gespeichert werden dürfen,
- die maximale Aufzeichnungsdauer festzulegen,
- die Anforderungen an das zur Aufzeichnung verwendete Speichermedium festzuschreiben und diese datenschutzgerecht zu gestalten,
- die Zwecke für die Übermittlung der aufgezeichneten Daten zu konkretisieren,
- zu regeln, wer die aufgezeichneten Daten übermitteln darf und
- den Löschzeitpunkt für die übermittelten Daten festzulegen.

Diese datenschutzrechtlich zwingenden Anforderungen sind im Rahmen der Ressortabstimmung vom BMVI leider nicht berücksichtigt worden. Entsprechend habe ich meine Bedenken dem Ausschuss für Verkehr und digitale Infrastruktur des Deutschen Bundestages mitgeteilt.

Das Thema automatisiertes und vernetztes Fahren ist auch Bestandteil der digitalen Agenda und der Strategie „intelligente Vernetzung“ der Bundesregierung und basiert ganz wesentlich auf der massenhaften Verarbeitung von Daten, die in der Regel personenbezogen sind, weil sie durch das Fahrverhalten beeinflusst werden oder gar Aufschluss über gefahrene Strecken geben können. Dieses Thema bildet deshalb auch einen Schwerpunkt meiner Arbeit, worüber ich ausführlich in Nr. 1.4 berichte.

15.2 Aus Beratung und Kontrolle

Beratungs- und Kontrollbesuche im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur

Ich habe in drei Behörden Beratungs- und Kontrollbesuche durchgeführt. Nicht alles war datenschutzkonform, Beanstandungen musste ich aber nicht aussprechen.

Kraftfahrt-Bundesamt

Gegenstand des Besuchs beim Kraftfahrt-Bundesamt (KBA) war der Umgang mit personenbezogenen Daten im Zusammenhang mit dem Fahreignungsregister.

Im Mittelpunkt stand die Umsetzung des „Fünften Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze“ durch das KBA. Mit den zum 1. Mai 2014 in Kraft getretenen Regelungen wurde das bis dahin unter dem Begriff „Verkehrszentralregister“ geführte Register novelliert und unter dem Begriff „Fahreignungsregister“ geführt.

Aufgrund der mit der Novelle verbundenen Fokussierung auf die Eintragung fahreignungsbedingter Verstöße mussten Eintragungen über nicht fahreignungsbedingte Verstöße am 1. Mai 2014 gelöscht werden (§ 65 Abs. 3 Satz 1 Straßenverkehrsgesetz - StVG).

Zum Zeitpunkt meines Besuchs hatte das KBA diese Löschverpflichtung noch nicht vollständig umgesetzt und begründete dies mir gegenüber nachvollziehbar mit hierfür nicht ausreichend vorhandenen personellen Ressourcen. Diese ermöglichten es lediglich, Löschungen im obigen Sinne sowohl im elektronischen, als auch im noch ausschließlich papiergebundenen Teil des Fahreignungsregisters nur jeweils dann vorzunehmen, wenn im Zuge anderweitig ausgelöster Sachbearbeitung festgestellt werde, dass eine nach § 65 Absatz 3 Satz 1 StVG zu löschende Eintragung noch vorhanden war.

Schon während des Besuchs herrschte Einvernehmen, die vom KBA begonnenen Löschungen künftig schneller vorzunehmen. Dieser Empfehlung hat das KBA entsprochen und mittlerweile die Löschungen nach § 65 Absatz 3 Satz 1 StVG vollständig vorgenommen.

Bundesamt für Güterverkehr

Meine Mitarbeiter haben sich über die ausschließlich elektronische Führung der Verkehrsunternehmensdatei nach der Verkehrsunternehmensdatei-Durchführungsverordnung (VUDat-DV) beim Bundesamt für Güterverkehr (BAG) informiert.

Die Erteilungsbehörden für Berechtigungen und Genehmigungen im Güterkraftverkehrsbereich sowie Genehmigungen im Kraftomnibusbereich dürfen im Rahmen ihrer Zuständigkeit nicht allgemein zugängliche Daten der Verkehrsunternehmen sowie deren Registrierungsnummer automatisiert abrufen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist (§ 3 Abs. 2 VUDat-DV). Das BAG hat bei jedem zehnten dieser Abrufe Protokolle zu fertigen, die die beim Abruf verwendeten Daten, den Tag und die Uhrzeit des Abrufs, die abrufende öffentliche Stelle und die abgerufenen Daten enthalten müssen (§ 3 Abs. 3 Satz 3 VUDat-DV). Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden (§ 3 Abs. 3 Satz 4 VUDat-DV).

Das BAG räumte ein, abweichend hiervon jeden Abruf nach § 3 Absatz 3 Satz 3 VUDat-DV zu protokollieren.

Entsprechend meiner Empfehlungen hat mir das BAG inzwischen mitgeteilt, künftig regelungskonform ausschließlich jeden zehnten Abruf zu protokollieren und bereits vorliegende Protokolle, die über diese Verpflichtung hinausgehen, unverzüglich zu löschen.

Zudem ist das BAG meinem Hinweis gefolgt, den behördlichen Datenschutzbeauftragten und seine Stellvertreterin zur angemessenen Wahrnehmung ihrer diesbezüglichen Aufgaben zu jeweils 50 Prozent freizustellen (vgl. a. u. Nr. 1.6).

Bundesanstalt für Straßenwesen

Schwerpunkt dieses Kontrollbesuchs war die Stellung des behördlichen Datenschutzbeauftragten.

Der Bundesanstalt für Straßenwesen (BASt) habe ich empfohlen, den behördlichen Datenschutzbeauftragten zu 30 Prozent seinen Stellvertreter zu 15 Prozent und eine weitere Mitarbeiterin zu 5 Prozent für den Bereich des behördlichen Datenschutzes freizustellen (vgl. a. u. Nr. 1.6), damit diese in ausreichendem Maße ihren Aufgaben aus dem BDSG nachkommen können.

Eine Reaktion der BASt hierzu lag mir zum Redaktionsschluss noch nicht vor.

A. Zudem von besonderem Interesse

Nr. 1.1: 1.2.1; 1.4; 1.6; 21.1; 21.5; 22.13

16 Verteidigungsausschuss

16.1 Auswirkungen der DSGVO auf diesen Themenbereich

Das Bundesdatenschutzgesetz gilt bisher auch für die Bundeswehr. Ob dies künftig auch bei der Datenchutz-Grundverordnung (DSGVO) so ist, scheint fraglich.

Anders als beim Justizprivileg (Art. 55 Abs. 3 DSGVO), findet sich in der DSGVO kein ausdrücklicher Hinweis auf den sachlichen Geltungsbereich für die Bundeswehr. Ob die DSGVO unmittelbar für die Bundeswehr zur Anwendung kommt, hängt davon ab, ob die DSGVO insoweit durch die Bestimmungen des Vertrages über die Europäische Union eingeschränkt wird. In diesem Zusammenhang sind zwei Fragen zu beantworten: Fällt die Bundeswehr überhaupt in den Geltungsbereich des Unionsrechts und wenn ja, in welchem Umfang.

Artikel 42 Absatz 2 Satz 1 des Vertrages über die Europäische Union (EUV) sieht vor, dass schrittweise eine gemeinsame Verteidigungspolitik festgelegt werden soll; diese haben die EU-Mitgliedsstaaten allerdings noch nicht beschlossen. Daher zählt die Verteidigung nach wie vor zu den nationalen Aufgaben. Gemäß ihrem Artikel 2 Absatz 2 Buchstabe a gilt die DSGVO allerdings nur für Tätigkeiten, die dem Unionsrecht unterliegen. Die Verteidigung fällt nicht in den Anwendungsbereich des Unionsrechts. Folglich ist der sachliche Anwendungsbereich der DSGVO für Zwecke der Verteidigung nicht eröffnet, allerdings für andere Zwecke schon.

Für die Bereiche der Bundeswehr, die nicht dem Zweck der Verteidigung dienen, ist die DSGVO somit unmittelbar anwendbar. Dazu gehören z. B. Fragen des Beschäftigtendatenschutzes in der Bundeswehr, die Datenverarbeitung in Bundeswehrkrankenhäuser oder der behördliche Datenschutzbeauftragte, sofern er in den von der DSGVO erfassten Bereichen tätig wird.

Es ist Aufgabe des Gesetzgebers, auch für die Bundeswehr insgesamt eine ab dem 25. Mai 2018 geltende Rechtslage zu schaffen, die einen angemessenen Datenschutz gewährleistet.

16.2 Einzelthemen

Gesetz zur Änderung des Soldatengesetzes

Der Gesetzgeber plant die Erweiterung der Sicherheitsüberprüfung auf alle neu einzustellenden Soldatinnen und Soldaten.

Das Bundesministerium der Verteidigung (BMVg) hatte mir im April 2016 den Referentenentwurf eines 16. Gesetzes zur Änderung des Soldatengesetzes mit Gelegenheit zur Stellungnahme übersandt: künftig sollen danach alle Bewerber, deren Berufung in das Soldatenverhältnis beabsichtigt ist (Berufssoldaten/-innen, Soldaten/-innen auf Zeit, freiwillig Wehrdienst Leistende) einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterzogen werden. Dadurch soll die Bundeswehr vor Innentätern geschützt und vermieden werden, dass sich Terroristen bei der Bundeswehr an Waffen ausbilden lassen.

In meiner Stellungnahmen habe ich inhaltliche Bedenken zum Gesetzentwurf geäußert. Danach soll künftig jeder Soldat einer einfachen Sicherheitsüberprüfung unterzogen werden.

Während bisher Sicherheitsüberprüfungen dann eingeleitet wurden, wenn jemand eine sicherheitsempfindliche Tätigkeit ausüben sollte, soll der Anknüpfungspunkt für eine Sicherheitsüberprüfung künftig allein die beabsichtigte Einstellung als Soldat/-in sein, die mit einer Ausbildung an Waffen verbunden ist.

Meine hiergegen geäußerten Bedenken wurden zu meinem Bedauern im Rahmen des Gesetzgebungsverfahrens nicht berücksichtigt.

Durch die beabsichtigte Erweiterung erhöht sich die Zahl der Sicherheitsüberprüfungen im Bereich der Bundeswehr um ein Vielfaches. Dies wird auch den Umfang meiner Kontrolltätigkeit in diesem Bereich deutlich erhöhen.

16.3 Aus Beratung und Kontrolle

16.3.1 Einzelfälle

Atteste zur Prüfungsuntauglichkeit an einer Bundeswehruniversität

Ein Petent, der an einer Universität der Bundeswehr studiert, wandte sich an mich, nachdem er krankheitsbedingt nicht an einer Prüfung seines Studiengangs teilnehmen konnte. Die Prüfungsunfähigkeit hatte er mittels eines truppenärztlichen Attestes des örtlichen Sanitätsversorgungszentrums nachgewiesen, in dem durch Auswahl eines Ankreuzfeldes bestätigt wurde, er sei wegen einer akuten kurzfristigen Erkrankung nicht in der Lage gewesen, an der Prüfung teilzunehmen.

Trotz des vorgelegten Attestes hat der zuständige Prüfungsausschuss den Petenten nachträglich aufgefordert, die Ärzte des örtlichen Sanitätsversorgungszentrums von ihrer Schweigepflicht zu entbinden und ein ausführliches Attest über die Prüfungsunfähigkeit nach einer versäumten Prüfung vorzulegen. Darin sollten die Ärzte im Hinblick auf eine krankheitsbedingte Studier- und/oder Prüfungsunfähigkeit Krankheitssymptome aufführen und die sich dadurch ergebenden Auswirkungen der Erkrankung auf das Leistungsvermögen beschreiben.

Die grundsätzliche Entscheidung des Prüfungsausschusses zum Wechsel von einem einfachen auf ein ausführliches Attest ist datenschutzrechtlich nicht zu beanstanden. Dieser Schritt soll einem potentiellen Missbrauch des krankheitsbedingten Prüfungsrücktritts effektiver entgegenwirken und damit die Chancengleichheit für alle Studenten wahren. Die Erhebung der sensiblen Gesundheitsdaten beruht auf der Ausbildungs- und Prüfungsordnung und damit auf einer gesetzlichen Grundlage.

Auch das Formblatt des ausführlichen Attestes, das für solche Fälle heranzuziehen ist, begegnet keinen datenschutzrechtlichen Bedenken. Der Prüfungsausschuss erhebt damit keine Diagnosen oder Krankheitsverläufe, sondern beschränkt sich auf die Mitteilung von Krankheitssymptomen, d. h. Tatsachenfeststellungen aufgrund eigener Wahrnehmung des untersuchenden Arztes. Aufgrund dieser festgestellten Tatsachen werden die negativen Auswirkungen auf das Leistungsvermögen (laienverständlich) beschrieben, die in eine Empfehlung des untersuchenden Arztes über den Ausschluss von bestimmten Studiertätigkeiten münden. Bei konsequenter Umsetzung dieses Verfahrens halte ich es für vertretbar, dass der Prüfungsausschuss sachgerecht über das Bestehen einer Prüfungsuntauglichkeit entscheidet, obwohl in dem Gremium selbst kein Arzt vertreten ist.

Im vorliegenden Fall war das Vorgehen des Prüfungsausschusses gleichwohl nicht datenschutzkonform. Denn dieser hatte sich erst nach dem Rücktritt des Petenten dazu entschlossen, ein ausführliches Attest zu verlangen. Der Petent ist durch dieses nachträgliche Verlangen in seinem Vertrauensschutz und in seiner Entscheidungsfreiheit darüber, ob und unter welchen Voraussetzungen er seinen Arzt von der Schweigepflicht entbinden und ein ärztliches Attest verwenden möchte, unangemessen beeinträchtigt worden.

Umgang mit dem Kommunikationsmittel E-Mail

Mehrere Eingaben haben mich zum Umgang der Bundeswehr und ihrer Dienststellen mit dem Kommunikationsmittel E-Mail erreicht.

a) Ein Petent, der nicht gleichzeitig Angehöriger der Bundeswehr ist, wandte sich mit folgendem Sachverhalt an mich: Er habe sich bei der Bundeswehr als freiwilliger Helfer für den Einsatz im Rahmen der Ebola-Epidemie beworben, weil er aus den Medien erfahren habe, die Bundesministerin der Verteidigung hätte in ihrem Geschäftsbereich einen Aufruf für freiwillige Helfer als Tagesbefehl erlassen. Dieser Tagebefehl galt allerdings nur für Bundeswehrangehörige. Freiwillige Zivilisten, die sich trotzdem gemeldet hatten, wurden per E-Mail dem Deutschen Roten Kreuz (DRK) gemeldet. Damit sind personenbezogene Daten mehrerer hundert Freiwilliger übermittelt worden. Erst danach sind die zivilen Freiwilligen über die Weiterleitung ihrer Daten unterrichtet worden.

Auf meine Nachfrage räumte das BMVg ein, für diese Übermittlung habe keine Rechtsgrundlage bestanden. Auch sei eine die Übermittlung alternativ legitimierende Einwilligung von den Freiwilligen nicht eingeholt worden.

Das BMVg hat daraufhin die Löschung der Daten des Petenten veranlasst und das Verfahren unverzüglich umgestellt. Freiwillige wurden seither gebeten, sich mit ihrer Bewerbung direkt an das DRK zu wenden. Eine Beanstandung dieses Datenschutzverstoßes habe ich daher nicht für notwendig erachtet.

b) In einer weiteren Eingabe ging es um den Umgang mit einer Beschwerde an den Wehrbeauftragten des Deutschen Bundestages. Im Rahmen der Beschwerdebearbeitung hat das BMVg seine Antwort nicht nur an den Wehrbeauftragten, sondern auch an fünf Organisationsbriefkästen verschiedener Dienststellen versandt.

Wie das Ministerium eingeräumt hat, sei die Weiterleitung der Stellungnahme an so viele Empfänger nicht erforderlich und auch unter dem Gesichtspunkt des Informationsflusses nicht zu rechtfertigen gewesen. Zudem hätte sich der Verfasser der E-Mail vor Absendung bei den empfangenden Dienststellen rückversichern müssen, ob dort alle Personen mit Zugriff auf den Organisationsbriefkasten zur Kenntnisnahme der in der Stellungnahme enthaltenen personenbezogenen Daten des Petenten berechtigt gewesen seien. Dies ist jedoch unterblieben. Insofern konnte das BMVg nicht ausschließen, dass auch unberechtigte Personen Zugriff auf die Stellungnahme und damit auf Daten des Petenten gehabt hatten.

Das Ministerium hat nachweisen können, dass es grundsätzlich die erforderlichen organisatorischen Maßnahmen getroffen hat, um einen korrekten Umgang mit E-Mails zu gewährleisten und fehlerhafte Übermittlungen auszuschließen. Es handelte sich im vorliegenden Fall um eine fehlerhafte Einzelentscheidung. Daher habe ich auch in diesem Fall von einer Beanstandung abgesehen.

c) Ein Soldat informierte mich über einen weiteren Sachverhalt, in dem personenbezogene Daten unbefugt per E-Mail versendet und damit Dritten zugänglich gemacht worden sind.

Er hatte vor dem Verwaltungsgericht ein Urteil gegen das Bundesamt für das Personalmanagement der Bundeswehr (BAPersBw) erstritten, mit dem ihm entstandene Nachteile wegen einer zu späten Beförderung ausgeglichen werden sollten.

Das BAPersBw berichtete anschließend der Fachaufsicht im BMVg über den Ausgang des Klageverfahrens und übersandte eine Kopie des vollständigen Urteils mit den personenbezogenen Daten des Petenten, da Rechtsmittel zu prüfen waren und das Verfahren zur Umsetzung des Urteils zugunsten des Soldaten festzulegen war. Darüber hinaus kam dem Fall eine grundsätzliche Bedeutung im Hinblick auf die Anwendung des Beförderungserlasses zu. Da diese Übermittlung des Urteils zum Zweck der Personalführung und -bearbeitung erfolgt ist, hatte ich hiergegen keine Bedenken.

Datenschutzrechtlich problematisch war allerdings, dass das BMVg das Urteil - weiterhin nicht anonymisiert - zur allgemeinen Information über die Anwendung des Beförderungserlasses an mehrere Dienststellen weiterversandt hatte. In diesem Fall war die Übermittlung der Angaben des Petenten im Urteil des Verwal-

tungsgerichts nicht erforderlich. Die personenbezogenen Daten hätten vorab geschwärzt werden müssen. Zwar war dem BMVg der Fehler noch selbst aufgefallen und es hatte eine Woche später den Empfängerkreis informiert, eine anonymisierte Version des Urteils übersandt und um Löschung der ersten E-Mail gebeten. Allerdings hatte das personalisierte Urteil zu diesem Zeitpunkt bereits weitere Kreise gezogen.

Das BMVg hat im Rahmen der Eingabe alle beteiligten Dienststellen noch einmal eindringlich aufgefordert, das Urteil in personalisierter Form zu löschen und die Umsetzung zu bestätigen.

Nachdem der Petent von Kameraden auf die Weiterleitung des vollständigen Urteils aufmerksam gemacht worden war, bat er das BMVg zunächst selbst um Auskunft über diesen Vorgang. Unverständlicherweise ist ihm gegenüber die bundeswehrinterne Verteilung des Urteils zuerst abgestritten worden. Das BMVg ist jedoch meiner Aufforderung gefolgt und hat seine Auskunft über die Empfänger des Urteils gegenüber dem Petenten korrigiert.

16.3.2 Personalakten der Reservisten - wem gehören sie?

Eine Kontrolle im größten Personalaktenlager der Bundeswehr hat unvorhergesehene rechtliche Fragen aufgeworfen.

Im Berichtszeitraum haben meine Mitarbeiter dem größten Personalaktenlager der Bundeswehr einen Besuch abgestattet. Hier werden sämtliche Personalakten der Reservisten verwaltet, die nicht mehr der Wehrüberwachung unterliegen. Die Akten werden bei Bedarf an die zuständigen Dienststellen der Bundeswehr zur Erteilung von Auskünften versendet. Zudem wird ihre Vernichtung nach Ablauf der gesetzlichen Archivierungsfristen überwacht.

Datenschutzrechtliche Probleme bereitete hierbei die organisatorische Einbindung des Aktenlagers. Die Einrichtung und ihre Mitarbeiter gehören planmäßig zum Bundesamt für das Personalmanagement der Bundeswehr (BAPersBw). Der Gesetzgeber hat die Verantwortung für die Personalakten der Reservisten jedoch den Karrierecentern der Bundeswehr (KarrC Bw) übertragen (§ 5 Abs. 1 Satz 1 der Verordnung über die Führung der Personalakten der Soldaten und der ehemaligen Soldaten (SPersAV) i. V. m. § 2 Wehrverwaltungsaufgabenübertragungsgesetz). Bei den KarrC Bw handelt es sich um die Rechtsnachfolger der Kreiswehrersatzämter und dem BAPersBw nachgeordnete Behörden.

Aufgrund der vorstehend genannten gesetzlichen Aufgabenzuweisung an die KarrC Bw, ist fraglich, ob eine Aufbewahrung der Akten durch das BAPersBw nach geltender Rechtslage möglich ist.

Da insoweit noch Klärungsbedarf besteht, habe ich die Vertreter des BMVg und des BAPersBw Anfang 2017 zu einem gemeinsamen Gespräch in meine Dienststelle in Bonn eingeladen. Das rechtliche Problem wurde von den Vertretern des BMVg erkannt. Sie sagten mir eine Klärung zu.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 1.6; 21.1; 21.5; 22.2

17 Ausschuss für Wirtschaft und Energie

17.1 Auswirkungen der DSGVO auf diesen Themenbereich

Die Datenschutz-Grundverordnung (DSGVO) bringt für die Unternehmen in Deutschland und Europa zahlreiche Veränderungen mit sich. Anders als bei der Verarbeitung personenbezogener Daten durch Behörden und öffentliche Stellen enthält die DSGVO für den nicht-öffentlichen Bereich nur sehr wenige Regelungsspielräume für den nationalen Gesetzgeber, sodass ihre Vorschriften unmittelbar durch die Unternehmen anzuwenden sind.

In meinem Zuständigkeitsbereich spielen dabei die Post- und Telekommunikationsunternehmen eine herausgehobene Rolle, da ich hier auch zukünftig die datenschutzrechtliche Aufsicht ausüben werde. Hierfür ist es allerdings dringend notwendig, die Zuständigkeitszuweisungen in § 42 Absatz 3 Postgesetz und in § 115 Absatz 4 Telekommunikationsgesetz an die neue Rechtslage anzupassen, da die geltenden Regelungen noch auf die Vorschriften des BDSG verweisen, das es ab dem 25. Mai 2018 nicht mehr in der bisherigen Form geben wird. Bedauerlicherweise ist das zuständige Bundesministerium für Wirtschaft und Energie hier bislang nicht aktiv geworden. Es ist für die betroffenen Unternehmen von erheblicher Bedeutung, dass auch künftig keine Zweifel an der Zuständigkeit der BfDI bestehen und insoweit Rechtssicherheit geschaffen wird.

Inhaltlich sind die Unternehmen gefordert, ihre Datenverarbeitung, den Umgang mit den Rechten der Betroffenen sowie ihre organisatorischen Abläufe und technischen Prozesse an die DSGVO anzupassen. Wie bisher werde ich den Unternehmen als Beraterin und Ansprechpartnerin für ihre datenschutzrechtlichen Fragen zur Seite stehen. Zu den Schwerpunkten werden dabei neben der Einrichtung von Verfahren zur Datenschutzfolgenabschätzung und zur Meldung von Datenschutzverletzungen auch die neuen Regelungen zur Zertifizierung und Akkreditierung gehören, deren genaue Ausgestaltung bereits von den Aufsichtsbehörden in Deutschland, aber auch in Europa vorbereitet wird.

Von besonderer Bedeutung sind die Befugnisse zur Durchsetzung des Datenschutzrechts, die sich gegenüber den Post- und Telekommunikationsunternehmen im Vergleich zur geltenden Rechtslage deutlich verändern werden. Während ich bisher lediglich die Möglichkeit habe, Verstöße gegen das Datenschutzrecht bei der Bundesnetzagentur zu beanstanden, werde ich künftig im Anwendungsbereich der DSGVO die Möglichkeit haben, unmittelbar gegenüber den Unternehmen z. B. durch verbindliche Anordnungen die Einhaltung des Datenschutzes durchzusetzen. Darüber hinaus werde ich auch Bußgelder für Verstöße gegen die DSGVO unmittelbar gegenüber den Post- und Telekommunikationsanbietern verhängen können. Hierfür sieht die DSGVO einen Bußgeldrahmen von maximal 20 Millionen Euro oder 4 % des Weltjahresumsatzes vor, je nachdem, welcher Betrag höher ist. Damit kommt auf mich auch eine völlig neue Aufgabe zu.

Abgesehen vom Telekommunikations- und Postgesetz sind im Bereich von Wirtschaft und Energie eine Reihe weiterer Vorschriften an das neue Europäische Datenschutzrecht anzupassen. Dabei sind vor allem die datenschutzrechtlichen Vorschriften des Telemediengesetzes (TMG) von Bedeutung, bei denen zu prüfen ist, ob und in welchem Umfang diese Vorschriften überhaupt beibehalten werden können. Weiteren Anpassungsbedarf wird es z. B. im Energierecht, Vergaberecht und im Gewerberecht geben. Hierzu hatte das BMWi im Berichtszeitraum bereits mit den Vorbereitungen begonnen.

17.2 Einzelthemen

17.2.1 Digitalisierung der Energiewende - Smart Metering

Das Gesetz zur Digitalisierung der Energiewende ist da und setzt Maßstäbe!

Ich habe in den vergangenen Tätigkeitsberichten bereits mehrfach darüber berichtet, wie ich in die Schaffung der rechtlichen und technischen Rahmenbedingungen für die Einführung intelligenter Messsysteme im Energiebereich eingebunden worden bin (vgl. zuletzt 25. TB Nr. 8.2). Diese so genannten Smart Meter sind zweifelsohne ein bedeutender Baustein für eine intelligente Energieinfrastruktur der Zukunft, ohne die die gesamtgesellschaftlich gewollten grundlegenden Veränderungen der Energieproduktion (Stichwort „Energiewende“) 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 Sicherheit in der Informationstechnik (BSI) zusammen, um eine hinreichende datenschutzrechtliche Flankierung bei der Einführung intelligenter Messsysteme zu erreichen.

Im Berichtszeitraum habe ich das BMWi bei der Erarbeitung des Gesetzes zur Digitalisierung der Energiewende vom 29. August 2016 (BGBl I, 2016, S. 2034) intensiv beraten. Kernstück dieses Gesetzes ist mit Artikel 1 das Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz). Darin werden die erlaubte Nutzung von Messdaten umfassend geregelt und strenge Mindestanforderungen an die IT-Sicherheit festgeschrieben. Normenklar werden die Verwendungszwecke für die Messdaten und die zur Verarbeitung der Messwerte berechtigten Stellen bestimmt. Dem Datenvermeidungsprinzip wird insofern gefolgt, als jede Stelle nur die zur Erfüllung ihrer Aufgaben erforderlichen Daten erhält und Daten generell anonymisiert oder wenigstens pseudonymisiert werden müssen, wenn zur Erfüllung der jeweilige Aufgabe ein direkter Bezug zum Letztverbraucher nicht erforderlich ist.

Datenschutzrechtlich sehr sensibel sind und bleiben die mit Smart Metern fortlaufend erhobenen Verbrauchswerte. Mit dem Gesetz wird nunmehr geregelt, in welchen Fällen diese detaillierten Verbrauchswerte auch genutzt werden dürfen. Sehr zu meinem Bedauern gehört dazu auch die vom Gesetzgeber mit dem Ziel der Energieeinsparung gewünschte Nutzung flexibler Tarife. Mit § 12 Stromnetzzugangsverordnung hatte der Gesetzgeber eigentlich zur Abwicklung der Stromlieferverträge für Verbrauchergruppen mit einem Jahresverbrauch unterhalb von 100.000 kWh die Anwendung vereinfachter Verfahren (Standardlastprofile) vorgeschrieben. Diese fehlen jedoch für Verbraucher mit flexiblen Tarifen, so dass in diesen Fällen die Lastgänge herangezogen werden müssen. Ich werde mich auch weiterhin dafür einsetzen, das Instrument der Standardlastprofile so weiter zu entwickeln, dass Verbraucher ihre detaillierten Verbrauchswerte nicht preisgeben müssen, wenn sie einen flexiblen Stromtarif wählen.

Mit der Festschreibung der Anforderungen an den Datenschutz und die Cybersicherheit der Kommunikationsinfrastruktur und des Smart-Meter-Gateways setzt das Gesetz zur Digitalisierung der Energiewende Maßstäbe auch für andere Sektoren der Wirtschaft. Im internationalen Vergleich gelten insbesondere die Datenschutzanforderungen als besonders streng. Die obligatorisch einzusetzenden richtlinienkonformen Smart-Meter-Gateways befolgen mustergültig das Prinzip des privacy by design. Sie bieten einen effektiven Schutz vor Cyberangriffen und gewähren den Verbrauchern maximalen Einblick in die Nutzung ihrer Daten. Damit ist das Smart-Meter-Gateway beispielhaft für die Gestaltung von Kommunikationskomponenten in anderen Sektoren der Wirtschaft, in denen mit der angestrebten Digitalisierung und Vernetzung keine neuen Risiken für die Rechte und Freiheiten der Bürger geschaffen werden sollen und ein zuverlässiger Schutz gegen Cyberangriffe sichergestellt werden muss. Ich werde mich dafür einsetzen, dass Kommunikationskomponenten nach diesem Beispiel auch in anderen Wirtschaftsbereichen zum Einsatz kommen. Insbesondere für den Smart-Home-Bereich bietet es sich an, etwaige Kommunikation mit externen Diensten ausschließlich über ein Smart-Meter-Gateway zuzulassen.

17.2.2 Änderung datenschutzrechtlich relevanter Vorschriften im Gewerberecht

Die mit § 34a GewO-E umgesetzten Verschärfungen des Bewachungsgewerbes sind zu unbestimmt und schießen in ihrer Gesamtheit über das Ziel hinaus:

Der Gesetzgeber nahm „verschiedene Vorfälle“ zum Anlass, das gewerbliche Bewachungsrecht zu verschärfen. Der „Entwurf eines Gesetzes zur Änderung bewachungsrechtlicher Vorschriften“ modifizierte zu diesem Zweck § 34a Gewerbeordnung (GewO), was bei mir auf datenschutzrechtliche Bedenken stieß.

Problem und Zielsetzung des Gesetzentwurfs waren auf die „besondere Situation bei der Bewachung von Flüchtlingsunterkünften“ gerichtet. Der Anwendungsbereich von § 34a GewO-E erstreckt sich allerdings auch auf „Großveranstaltungen“. Die eingebrachte Lösung geht daher über den dargestellten Problem- und Zielbereich hinaus. Die verfassungsrechtlich notwendige Erforderlichkeit hierfür wird im Entwurf nicht (hinreichend) nachgewiesen. Entsprechendes gilt für die alle drei Jahre durchzuführende Wiederholung der Zuverlässigkeitsüberprüfung. Selbst nach dem Sicherheitsüberprüfungsgesetz (§ 17 Abs. 2 Satz 1 SÜG) erfolgt eine Wiederholungsüberprüfung regelmäßig erst nach zehn Jahren - und Überprüfungen nach dem SÜG sind z. B. für Mitarbeiter von Geheimdiensten vorgesehen, die Zugang zu Verschlusssachen haben sollen. Weshalb im Bewachungsgewerbe strengere Regelungen gelten sollen, leuchtet mir nicht ein.

Wer ein Bewachungsgewerbe ausüben will, bedarf der Erlaubnis der Behörde. Diese Erlaubnis ist zu versagen, wenn der Antragsteller unzuverlässig ist. Nach § 34a Absatz 1 Satz 4 Nummer 3 GewO-E ist unzuverlässig, wer einzeln oder als Mitglied einer Vereinigung Bestrebungen und Tätigkeiten im Sinne des § 3 Absatz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG) verfolgt oder unterstützt oder in den letzten fünf Jahren verfolgt oder unterstützt hat. Schon der hier verwandte Begriff der „Bestrebung“ ist weit, da das BVerfSchG den erfassten Personenkreis wenig bestimmt.

Nach § 34a Absatz 1a GewO-E holt die Behörde zur Überprüfung der Zuverlässigkeit die Stellungnahme einer in der Vorschrift näher bestimmten Wohnortpolizeibehörde ein. Darin soll Auskunft darüber geben werden, ob „tatsächliche Anhaltspunkte bekannt sind, die Bedenken gegen die Zuverlässigkeit begründen können.“ Eine derartige Formulierung ist im Bundesrecht an anderen Stellen nicht auffindbar. Es ist völlig unbestimmt, worauf die Polizeibehörde ihre Bedenken stützen soll. Genannt werden zwar „tatsächliche Anhaltspunkte“. Es ist jedoch völlig unklar, worauf diese sich beziehen sollen. Es sind keinerlei Fristen genannt, wie alt die Sachverhalte sein dürfen, auf die sich die Landespolizei berufen darf. Es stellt sich ebenfalls die Frage, ob die verwendeten Informationen gegenüber dem Betroffenen stets transparent gemacht werden.

Nach § 34a Absatz 1a Satz 4 GewO-E kann die zuständige Behörde zusätzlich zum Zweck der Überprüfung der Zuverlässigkeit und ohne weitere Voraussetzung bei einer zuständigen Verfassungsschutzbehörde die Abfrage des nachrichtendienstlichen Informationssystems (NADIS-WN) „veranlassen“. Was aus dieser veranlassten Abfrage folgt, ist jedoch unklar. Offenbar soll die Gewerbehörde direkt auf die Daten aus NADIS-WN zugreifen können, weil nach der Gesetzesbegründung die Einrichtung einer Schnittstelle zum automatisierten Abgleich geplant ist. Dies mit einer Formulierung wie „Abgleich veranlassen“ zu verschleiern, halte ich für verfassungsrechtlich problematisch. Auch stellt sich die Frage nach der Verhältnismäßigkeit eines solchen Eingriffs.

Die erneute, regelmäßige Überprüfung im Abstand von drei Jahren steht in Widerspruch zum SÜG (s. o.) und begegnet erheblichen Bedenken im Hinblick auf die Wahrung des Verhältnismäßigkeitsgebots.

Eine NADIS-WN Abfrage ist ein erheblicher, d. h. grundrechtsintensiver Eingriff. Nach dem SÜG ist dieser nur auf der Grundlage einer wirksam erteilten Einwilligung (d. h. einer Sicherheitserklärung - vgl. § 13 SÜG) und nur unter qualifizierten Voraussetzungen und Verfahrenssicherungen zulässig. Der vorliegende Gesetzesentwurf enthält keine vergleichbaren Vorgaben, obgleich ein entsprechender Eintrag für den Betroffenen (potentiell) weitreichende Folgen hat. Verdachtsunabhängige „Regelabfragen“ Betroffener bei Verfassungsschutzbehörden sind im Hinblick auf die Beachtung des Verhältnismäßigkeitsgebots kritisch zu bewerten - zumal die Informationen dieser Behörden oftmals nicht auf „harten“ Fakten, sondern auf „weichen“ Informationen beruhen, deren Validität nicht nachgewiesen ist.

§ 34a Absatz 6 GewO-E sieht schließlich die Errichtung eines Bewacherregisters vor. Es bestehen auch hier erhebliche verfassungsrechtliche Bedenken, ob für eine solche Errichtung das Verhältnismäßigkeitsgebot im

ausreichenden Maße beachtet wurde. Denn bereits in Bezug auf die „bloße“ Speicherung dieser Daten war die Erforderlichkeit im Gesetzesentwurf nicht (hinreichend) belegt. Das vorgesehene Register sieht jedoch nunmehr auch vor, Daten des Bewachungspersonals nicht nur verdachtsunabhängig zu speichern, sondern auch elektronisch auswertbar vorzuhalten.

Meine datenschutzrechtlichen Bedenken habe ich dem Ausschuss für Wirtschaft und Energie, dem Innenausschuss und dem Ausschuss für Recht und Verbraucherschutz mitgeteilt. Sie blieben im Wesentlichen jedoch unberücksichtigt. Lediglich die Intervalle der regelmäßigen Überprüfung wurden von drei auf fünf Jahre angehoben. Die Verschärfungen des Bewachungsrechts traten am 1. Dezember 2016 in Kraft (BGBl. I, S. 2456).

17.2.3 Trusted Cloud - die dunklen Wolken verziehen sich

Mit der neuen Datenschutz-Grundverordnung wird ab 2018 europaweit ein Rechtsrahmen für Datenschutzzertifizierungen geschaffen. Das im Projekt „Trusted Cloud“ des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelte „Trusted Cloud Datenschutz Profil“ (TCDP) ist weiter gereift.

Zum Thema Cloud Computing habe ich in den vergangenen Tätigkeitsberichten (vgl. 25. TB Nr. 8.5 und 24. TB Nr. 5.3) ausführlich berichtet und dabei zuletzt auch die geplante Datenschutzzertifizierung des „Trusted-Cloud Projektes“ des BMWi angesprochen. Das TCDP bildet die gesetzlichen Anforderungen an eine Auftragsdatenverarbeitung in einen Prüfstandard ab und unterscheidet sich deshalb von sonstigen Datenschutzgütesiegeln. Zudem hilft der modulare Aufbau erneute Überprüfungen von bereits zertifizierten Teilen zu vermeiden. Mitte 2016 wurde das TCDP in der Version 1.0 finalisiert und veröffentlicht. Hiermit können nun Cloud Dienste nach dem Bundesdatenschutzgesetz zertifiziert werden. Bereits auf der CeBIT 2016 konnte als Testlauf der Methodik ein erstes Zertifikat nach TCDP 0.9 ausgehändigt werden (siehe auch http://www.tcdp.de/).

Das Projekt „Trusted-Cloud“ habe ich in den letzten Jahren intensiv begleitet und dabei wiederholt deutlich gemacht, wie wichtig das Thema für Datenschützer ist. Mit der Verwaltung der nun fertigen Dokumente ist die Stiftung Datenschutz beauftragt worden; dies begrüße ich. Die eventuell notwendigen Anpassungen und die Weitentwicklung des TCDP werde ich im Auge behalten.

Weiter hat das Bundesamt für Sicherheit in der Informationstechnik einen Anforderungskatalog zum Cloud Computing entwickelt. Dieser richtet sich in erster Linie an professionelle Cloud-Diensteanbieter sowie deren Prüfer und Kunden. Darin wird festgelegt, welche Anforderungen die Cloud-Diensteanbieter erfüllen müssen bzw. auf welche Anforderungen sie mindestens verpflichtet werden sollten (siehe auch http://www.bsi.de).

In der vorliegenden Form setzt der Anforderungskatalog seinen Schwerpunkt in der Beurteilung der Informationssicherheit bei Cloud-Diensten, das TCDP seinen direkt bei § 9 BDSG und den technischen und organisatorischen Maßnahmen. Der Anforderungskatalog des BSI referenziert daher nicht unmittelbar zu den - insbesondere aus § 11 BDSG folgenden - datenschutzrechtlichen Anforderungen. Er erscheint mir aber als ein gut geeignetes Instrument, um die rechtlichen Vorgaben aus § 11 BDSG inhaltlich mit Leben zu erfüllen. Danach muss sich der Auftraggeber (Cloud-Kunde) vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überzeugen und hat das Ergebnis zu dokumentieren. Diese Überprüfungs- und Dokumentationspflicht kann auch durch Zertifizierungen des Auftragnehmers (Cloud-Dienstanbieters) erreicht werden.

Die Datenschutz-Grundverordnung (DSGVO) enthält eine Regelung zur Zertifizierung. Die Zertifizierung nach Trusted Cloud Datenschutz Profil entspricht den Prinzipien, die der Regelung der DSGVO zugrunde liegen. Von den Projektbeteiligten wird daher angestrebt, die TCDP-Zertifizierung zu einer Datenschutz-Zertifizierung auf der Grundlage der DSGVO weiterzuentwickeln. Dabei sollen TCDP-Zertifikate in einem vereinfachten Verfahren in Zertifikate nach DSGVO überführt werden können. Zusätzlich kann das TCDP-Schutzklassenkonzept als Grundlage für ein Schutzklassenkonzept einer künftigen Zertifizierung nach DSGVO dienen. Daher kann ich bereits jetzt allen Cloud-Dienstanbietern eine Datenschutzzertifizierung auf der Grundlage des TCDP empfehlen.

17.2.4 ... aus den Bereichen Telekommunikation, Telemedien und Post

17.2.4.1 Die Reform der ePrivacy-Richtlinie

Im Rahmen der Reform des europäischen Datenschutzrechts wird nach der Datenschutz-Grundverordnung nun auch die ePrivacy-Richtlinie überarbeitet.

Mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) muss auch die ePrivacy-Richtlinie überarbeitet werden. Die Reform zielt darauf ab, das Verhältnis zwischen der Datenschutz-Grundverordnung und den Regelungen im Bereich der elektronischen Kommunikation zu klären, ohne allerdings Regeln festzulegen, die über die Vorschriften der DSGVO hinausgehen - dies ist in Artikel 95 DSGVO eindeutig so vorgegeben. Damit ist jedoch keineswegs der Anwendungsbereich der geltenden Richtlinie von einer Änderung oder Erweiterung ausgeschlossen.

Die elektronischen Kommunikationsdienste befinden sich in einem Prozess der ständigen Erweiterungen und Neuerungen, dem die Regelungen Rechnung tragen müssen. Um einen Überblick über die aus Sicht der Betroffenen notwendigen Änderungen zu erhalten, hat die Europäische Kommission im Frühjahr 2016 eine öffentliche Anhörung durchgeführt, an der Vertreter verschiedener Interessengruppen - Netzwerk-Provider, Service-Provider, Verbraucherverbände und Bürger - teilgenommen haben. Die Fragen der Kommission reichten von der Erweiterung des Anwendungsbereichs über Sonderregelungen für die Vertraulichkeit der Kommunikation sowie für Verkehrs- und Lokalisierungsdaten bis hin zum Opt-in bei Cookies, Nutzer-Tracking und Werbeanrufen. Je nach Interessenlage fielen die Antworten aus den beteiligten Gruppen unterschiedlich aus. Vertreter der europäischen Datenschutzbehörden hatten kurz vorher die Gelegenheit, in einem Workshop ihre Positionen zu diskutieren.

Im Juli 2016 hat die Artikel-29-Gruppe in einer Stellungnahme die gemeinsame Position der europäischen Datenschutzbeauftragten zu den Fragen der Europäischen Kommission abgegeben. Hieran habe ich mitgearbeitet und unterstütze das Papier in allen Punkten.

Von besonderer Bedeutung ist die Erweiterung des Anwendungsbereichs der ePrivacy-Richtlinie auf die sog. **OTT-Dienste**, und zwar auf solche, die ein Äquivalent zu den „klassischen“ Telekommunikationsdiensten darstellen (vgl. Kasten zu Nr. 17.2.4.1). Schon seit einiger Zeit wird kontrovers diskutiert, ob Kommunikationsdienste, die für die Signalübertragung das Internet nutzen, überhaupt als Telekommunikationsdienste angesehen werden können. Die Inklusion der OTT-Dienste in die ePrivacy-Verordnung bedeutet auch endlich die Klärung der Streitfrage bzgl. der Zuständigkeiten für WhatsApp und GoogleMail.

Die Artikel-29-Gruppe hat eine Erweiterung ausdrücklich befürwortet, um die **Vertraulichkeit der Kommunikation** für diese OTT-Dienste zu gewährleisten. Wenig überraschend ist das Votum der Bürger in der öffentlichen Anhörung zu dieser Frage: die Mehrheit ist für die Erweiterung.

Bestätigt wird diese Sichtweise auch vom Verwaltungsgericht Köln, das im November 2015 die Frage, ob GoogleMail ein Telekommunikationsdienst sei und somit dem deutschen Telekommunikationsgesetz (TKG) unterfalle, eindeutig bejaht hat. Die Signalübertragung erfolge zwar nicht über eine eigene Netzinfrastruktur, sondern werde von einem Internetprovider erbracht. Bei einer funktionalen Betrachtung sei jedoch der gesamte Kommunikationsvorgang Google als Anbieter bzw. Erbringer zuzurechnen. Google ist zwar zwischenzeitlich seiner Meldepflicht nach § 6 TKG nachgekommen, hat aber gegen das Urteil Widerspruch eingelegt. Das OVG Münster wird hierzu im Laufe des Jahres 2017 entscheiden.

Neben der Erweiterung auf OTT-Dienste ist auch die Einbeziehung der Anbieter von öffentlich zugänglichem **„privaten“ WLAN** in Hotels, Cafés etc. sinnvoll, die ihren Gästen einen Internetanschluss zur Mitbenutzung

zur Verfügung stellen und bisher ohne klare gesetzliche Vorgaben für den Umgang mit deren Daten agieren. Oftmals müssen die Gäste Nutzungsbedingungen akzeptieren, die - z. B. bei der Speicherung der Surfdaten - über die Vorschriften des TKG hinausgehen. Auch die „Lockerung“ im Telemedienrecht bei der Haftungsprivilegierung der Anbieter für fremde Inhalte hat hier leider keine durchgreifende Änderung gebracht. Die Einbeziehung der „privaten“ WLAN-Anbieter in den Anwendungsbereich wird daher nicht nur für diese, sondern auch für die Mitbenutzer die erforderliche Rechtssicherheit bringen.

Ein altbekanntes Problem betrifft den Artikel 5 Absatz 3 der Richtlinie, den sog. **Cookie-Paragraphen**, der durch die Unsicherheiten bei seiner praktischen Anwendung eine Überarbeitung dringend erforderlich macht. Eingesetzt werden Cookies einerseits, wenn sie für Konfigurationszwecke und die technische Erbringung des Dienstes benötigt werden, andererseits und auch sehr gerne, um den Nutzern bei ihren Surfbewegungen im Internet nachzuspüren, neudeutsch Tracking genannt. Während der Einsatz von Cookies im ersten Fall datenschutzrechtlich zulässig ist, fordert die Artikel-29-Gruppe in ihrer Stellungnahme, einerseits klare Erlaubnistatbestände für das Tracking von Nutzerdaten festzulegen (z. B. Datensicherheitszwecke, Verwendung von anonymisierten Daten und solchen mit geringen oder keinen Auswirkungen auf den Datenschutz). In anderen Fällen, z. B. der Profilbildung für Werbezwecke, wird ein Browser-Plugin (z. B. DNT) als geeignete Lösung angesehen. Damit kann der Nutzer ohne großen Aufwand und für alle Anbieter festlegen, ob oder unter welchen Bedingungen er einem Tracking zustimmt.

Mit der zu erwartenden Überarbeitung des Cookie-Paragraphen wird sich die von mir immer wieder angemahnte Anpassung der entsprechenden Regelung im Telemediengesetz an die Vorgaben der Richtlinie erübrigen (vgl. 25. TB Nr. 8.9.1). Das BMWi kann die Angelegenheit nun endlich ad acta legen!

In der Aufsichtspraxis hat sich auch gezeigt, dass die **Einwilligung** des Nutzers beim Setzen eines Cookies oftmals nicht freiwillig ist, ohne ausreichende Information erfolgt und im Grunde nur der Erfüllung der gesetzlichen Verpflichtungen dient. Dies wird deutlich beim sog. *Cookie Wall*, der nach dem Prinzip „alles oder nichts“ funktioniert. Daher nennt die Stellungnahme mehrere Fälle, in denen die in diesem Sinne erzwungene Einwilligung unzulässig sein soll, z. B. bei besonders sensiblen Daten (Daten zur Gesundheit, politischen oder sexuellen Orientierung) oder bei der gebündelten Einwilligung für Daten mit niedrigem und hohem Schutzbedarf.

Es verwundert nicht, dass die freie Wahl für die große Mehrheit der Nutzer (77 Prozent) besonders wichtig ist, wie die Anhörung der Europäischen Kommission ergeben hat. Denn sie lehnen das mögliche Recht der Anbieter ab, ihnen den Zugang zu den jeweiligen Diensten ohne Einwilligung in Cookies oder andere Tracking-Verfahren zu verweigern. Die Wirtschaft sieht das naturgemäß anders.

Der Entwurf der Europäischen Kommission ist am 11. Januar 2017 vorgestellt worden.

Kasten zu Nr. 17.2.4.1

OTT-Dienste

Over-**t**he-**T**op-Dienste werden über das offene Internet erbracht, wobei der Anbieter nicht in die Übermittlung der Signale bzw. Daten involviert ist, sondern ein Internetprovider diese durchführt. Nach ihrem Schwerpunkt sind zwei Arten zu unterscheiden.

OTT-Kommunikationsdienste, zu denen neben Instant-Messaging- und VoIP-Diensten wie *WhatsApp* und *Skype* die sog. Webmailer wie *GoogleMail* oder *WEB.DE* gehören, entsprechen in ihrer Funktion den „klassischen" Sprachtelefonie- und SMS-Diensten.

OTT-Inhaltsdienste dienen in erster Linie nicht der Kommunikation, sondern der Vermittlung von Inhalten. Die Angebote sind sehr vielfältig, z. B. Suchmaschinen, Streaming-Dienste wie *Spotify* und Dienste für Video- und Audioinhalte wie *YouTube*.

Soziale Netzwerke stellen eine Mischform dar, da dort sowohl Inhalte gepostet als auch private Nachrichten an andere Nutzer versendet werden können.

17.2.4.2 Fürs Telefonieren vorab bezahlen? Nur noch mit Ausweisnummer!

Zwar mag eine Verifikation der erhobenen Kundendaten gerade im Bereich der im Voraus bezahlten Mobilfunkdienste notwendig sein, die im § 111 TKG eingeführte zusätzliche Pflicht zur Vorratsdatenspeicherung von Ausweisinformationen aller Prepaid-Kunden geht aber eindeutig zu weit.

Schon immer sind Telekommunikationsanbieter verpflichtet, die zur Erbringung ihres Dienstes erhobenen Bestandsdaten ihrer Kunden bei entsprechenden Anfragen den Sicherheitsbehörden zur Verfügung zu stellen. Diese Daten sind von den Unternehmen in der Regel auch immer gut gepflegt worden, da sie die Basis für die Abrechnung mit den Kunden sind.

Dies änderte sich mit dem Aufkommen der Prepaid-Karten im Mobilfunk. Insbesondere bei den über das Internet vertriebenen Karten häuften sich die „Unregelmäßigkeiten" im Datenbestand. So berichtete beispielsweise ein Journalist, bei einem Selbstversuch habe er diverse Prepaid-Verträge auf den Namen seines Hundes abschließen können. Die deswegen vermehrt auftauchenden Kunden namens „Hasso von der Vogelweide" oder „Donald Duck" haben die Sicherheitsbehörden veranlasst, regelmäßig eine gründlichere Überprüfung der von den Anbietern im Prepaid-Bereich erhobenen Daten anzumahnen.

Im Rahmen der allgemeinen Ausweitung sicherheitsbehördlicher Befugnisse im Nachgang verschiedener terroristischer Anschläge in Europa entschied sich der Gesetzgeber dazu, bei dieser Gelegenheit auch gleich eine Verifikationspflicht der bei Prepaid-Verträgen angegebenen Daten einzuführen.

Anstatt dabei aber die entsprechende Novellierung des Telekommunikationsgesetzes darauf zu beschränken, für die Telekommunikationsanbieter die Pflicht einzuführen, vor Freischaltung einer Prepaid-Karte die Richtigkeit der vom Kunden angegebenen Daten über die Vorlage eines amtlichen Ausweisdokumentes zu überprüfen, ging man noch ein paar Schritte weiter. Die Anbieter sind nunmehr zusätzlich verpflichtet, die Art des Verfahrens, das zur Überprüfung eingesetzt wurde, die Art des Ausweisdokumentes, dessen Nummer und die es ausstellende Stelle zu speichern und, wenn angefordert, Sicherheitsbehörden zur Verfügung zu stellen.

Nicht nur, dass der Gesetzgeber damit zum Ausdruck bringt, er traue den Telekommunikationsunternehmen nicht zu, ihren gesetzlichen Verpflichtungen zur Verifikation der von ihnen erhobenen Daten ordnungsgemäß nachzukommen, und ihnen damit faktisch vorab unterstellt, sich rechtswidrig zu verhalten. Vielmehr erweitert

er den Katalog der bisher nach § 111 TKG zu speichernden Daten und führt damit eine massenhafte Speicherung von sensiblen Daten zu Identitätsdokumenten ein, ohne dass zum Zeitpunkt der Speicherung überhaupt absehbar ist, ob diese Daten jemals benötigt werden; per Definition handelt es sich also um eine weitere Vorratsspeicherung von Daten.

Besonders kritisch ist dabei, dass es sich hier um Daten handelt, die von den Anbietern selbst zur Erbringung des Dienstes in keiner Weise benötigt werden. Die Regelung konstituiert somit eine Pflicht, Daten zu erheben und zu speichern, die ausschließlich für sicherheitsbehördliche Zwecke verwendet werden. Sogar in der Gesetzesbegründung wird explizit ausgeführt, die gespeicherten Angaben zum Identitätsdokument sollen lediglich dem Zweck dienen, Sicherheitsbehörden *„einen Anknüpfungspunkt für weitere Ermittlungen zur Feststellung des Anschlussinhabers zu ermöglichen“*. Der bisher im TKG vorherrschende Grundsatz, dass Telekommunikationsanbietern nur die für ihre Diensterbringung erforderlichen Daten erheben dürfen, diese dann aber auch Sicherheitsbehörden zur Verfügung stellen müssen, wird komplett auf den Kopf gestellt. Telekommunikationsanbieter werden quasi als „Hilfssheriffs“ vereinnahmt, für Sicherheitsbehörden Daten zu erheben, die vielleicht etwas in offiziellen Melderegistern, nicht jedoch in der Kundendatendatei eines Privatunternehmens zu suchen haben.

Eine Rechtfertigung dieser Art der Vorratsspeicherung von Daten lässt sich auch nicht mit den Vorgaben des Bundesverfassungsgerichts begründen. In seinem Beschluss vom 24. Januar 2012 (1 BvR 1299/05) führte dieses aus, durch § 111 TKG solle lediglich eine verlässliche Datenbasis geschaffen werden, die es bestimmten Behörden erlaube, Telekommunikationsnummern individuellen Anschlussinhabern zuzuordnen. Dies kann aber bereits durch die neue Verpflichtung zur Überprüfung der angegebenen Daten durch ein Identitätsdokument erreicht werden. So lange nicht durch praktische Erfahrungen belegbar ist, dass die neu einzuführende Verifikationspflicht nicht zu dem gewünschten Effekt einer Verbesserung der Datenqualität führt, geht die zusätzlich eingeführte Speicherpflicht von Ausweisdaten über die Vorgaben des Bundesverfassungsgerichts hinaus und ist damit weder erforderlich noch verhältnismäßig.

Neben diesen rechtlichen Schwierigkeiten stellt der neugestaltete § 111 TKG die Telekommunikationsanbieter aber vor allem auch in der Praxis vor erhebliche Probleme. Die neuen Auflagen sind jedenfalls dann durchaus herausfordernd, wenn - anders als in einer Ladenfiliale des Anbieters - ein Vertriebsweg (wie z. B. Vertriebspartner, Internet, etc.) vorsieht, dass ein Kunde selbstständig seine Daten angibt und ihm dabei kein Mitarbeiter des Unternehmens gegenüber steht, der mal eben auf den Ausweis sehen kann. Um Lösungen für dieses praktische Problem zu finden, wurde der Bundesnetzagentur in § 111 Absatz 1 Satz 4 TKG die Aufgabe zugewiesen, Verfahren vorzugeben, die sie für eine Identitätsüberprüfung im Sinne der Norm als geeignet betrachtet.

Interessant ist beispielsweise, dass im Rahmen der Verifikation keine gerooteten oder gejailbreakten Mobiltelefone verwendet werden dürfen. Eine Erläuterung dieses Verbots oder eine nur ansatzweise Erklärung, inwieweit die Firmware eines Mobiltelefons die Bildübertragung bei einem Videochat beeinflussen und damit die Verifikation des in diesem Rahmen vorgezeigten Ausweisdokuments beeinträchtigen kann, findet sich in der Verfügung leider nicht.

Eine weitere Verpflichtung, die für alle der oben genannten alternativen Verifikationsmethoden auferlegt wird, ist die Anfertigung einer Kopie, eines Scans oder Screenshots des Ausweisdokuments und dessen Übermittlung an den Anbieter. Zwar sind hier ausweislich der Verfügung datenschutzrechtliche Vorgaben zu beachten. Wie dies in der Praxis allerdings genau umgesetzt werden soll, wird sich erst noch zeigen. So müssen beispielsweise nicht relevante Informationen auf den Ausweisdokumenten (wie z. B. Größe oder Augenfarbe) bereits bei der Erstellung der Kopie maskiert werden. Da zur Verifikation verschiedenste Ausweisdokumente verwendet werden dürfen, stelle ich es mir durchaus anspruchsvoll vor, immer die entsprechende Schablone für die Maskierung bereitzuhalten. Zudem muss sichergestellt werden, die Daten nur über einen sicher verschlüsselten Kanal zu übertragen. Ich werde daher genau kontrollieren, wie die datenschutzrechtlichen Vorgaben in der Praxis umgesetzt werden.

Aus meiner Sicht rechtswidrig ist die Vorgabe, nach der die verifizierende Person beim Verdacht einer Täuschung durch den Antragsteller die angegebenen Daten weiter erheben und dann, gesondert gekennzeichnet, an den Diensteanbieter übermitteln soll. Wie dieser dann damit verfahren soll, ist nicht geregelt, sondern lediglich ein Verbot der Speicherung in der Kundendatei nach § 112 TKG. Eine Freischaltung der Prepaid-Karte soll selbstverständlich ebenfalls nicht erfolgen.

Die Bundesnetzagentur (BNetzA) will mit dieser Vorgabe Betrügern die Möglichkeit nehmen, festzustellen, an welcher Stelle des Verifikationsprozesses die versuchte Täuschung gescheitert ist. Auch wenn dies aus prozesstechnischen Gesichtspunkten sicherlich nachvollziehbar ist, rechtfertigt es trotzdem keine rechtsgrundlose Erhebung personenbezogener Daten. Denn sobald eine Täuschung vermutet und daraufhin die Entscheidung getroffen wird, dem Kunden ein Telekommunikationsangebot zu verweigern, fällt auch der Rechtsgrund für die Datenerhebung nach § 95 Absatz 1 TKG weg.

Es bleibt abzuwarten, ob die BNetzA diese Vorgabe korrigiert und Telekommunikationsanbieter oder für diese handelnde Verifikationspartner tatsächlich entsprechende Datenerhebungen vornehmen. Ich werde dies datenschutzrechtlich begleiten.

17.2.4.3 Telefonbuch de Luxe

Innerhalb der rekordverdächtigen Zeit von „nur“ knapp 14 Jahren scheint es gelungen zu sein, sich endlich auf eine Verordnung über die Umsetzung der so genannten Jokersuche bei der automatisierten Bestandsdatenauskunft nach § 112 TKG zu einigen. Das Ergebnis lässt aber - aus datenschutzrechtlicher Sicht - Wünsche offen.

Das von der BNetzA seit dem Jahr 1999 betriebene automatisierte Auskunftsverfahren ermöglicht es verschiedenen Behörden, Auskunft über den Inhaber einer Rufnummer oder die von einer Person genutzten Rufnummern abzufragen. Eine direkte Anfrage bei allen Telekommunikationsanbietern wäre zu umständlich.

Ist die exakte Schreibweise des Namens oder die genaue Adresse einer Person nicht bekannt, können die Daten jedoch nicht abgefragt werden. Deshalb legte § 112 TKG im Jahre 2004 fest, eine Rechtsverordnung solle Ersuchen mit unvollständigen Abfragedaten und die Suche mittels einer „Ähnlichenfunktion“ regeln. Auch weitere Daten, z. B. das Geburtsdatum, könnten abgefragt werden (vgl. 20. TB Nr. 13.5). Nach mehreren Anläufen und weiteren Änderungen im TKG liegt nun ein Entwurf der Kundendatenauskunftsverordnung (KDAV) vor, der voraussichtlich 2017 in Kraft treten wird.

Im Entwurf der KDAV ist vorgesehen, dass bestimmte Angaben, z. B. Vorname oder Hausnummer fehlen dürfen oder dass durch Platzhalter bzw. eine phonetische Suche ungenaue Angaben gemacht werden können. So kann etwa mit M[ae][iy]er sowohl Maier als auch Meyer gefunden werden. Auch eine rein anschriftenbasierte Suche soll möglich sein.

Diese Möglichkeiten führen jedoch zu mehrfachen Treffern, bei denen auch Daten von weiteren Personen übertragen werden. Um hier keine unverhältnismäßigen Datenübermittlungen zu riskieren, wird die Anzahl der angezeigten Ergebnisse auf maximal 40 begrenzt. Liegt die Anzahl der ausgeworfenen Ergebnisse bei einem Anbieter über dieser Schwelle, werden keine Datensätze, sondern lediglich die Anzahl der Treffer übermittelt.

Bei dieser Schwelle hatte ich im Vorfeld für einen etwas niedrigeren Wert plädiert. Besonders problematisch ist jedoch, dass die Begrenzung auf 40 Treffer für jeden Anbieter einzeln gilt, die Abfrage aber parallel bei allen an das automatisierte Auskunftsverfahren angeschlossenen Unternehmen durchgeführt wird und die BNetzA sämtliche von den Anbietern erhaltenen Daten an die ersuchende Behörde übermittelt. So könnte es passieren, dass ein großer Anbieter nur mitteilt, er habe 200 Treffer, einige kleinere Anbieter jedoch jeweils bis zu 40 Teilnehmerdaten weitergegeben. Im Ergebnis kann so eine Behörde auf eine Anfrage die Bestandsdaten von weit über hundert Anschlussinhabern erhalten.

Eine solche einerseits unvollständige, gleichzeitig aber ggf. äußerst umfangreiche Datenübermittlung halte ich für unverhältnismäßig. Deswegen hatte ich eine Prüfung bei der BNetzA vor Übermittlung an die anfragende Behörde gefordert, diese wurde aber leider nicht in die Verordnung übernommen.

Wie wichtig in diesem Zusammenhang entsprechende Protokollierungen für die Durchführung einer Datenschutzkontrolle des automatisierten Auskunftsverfahrens sind, zeigen zwei Protokollprüfungen, die ich im Berichtszeitraum auf Initiative von Polizeibehörden durchgeführt habe. Im ersten Fall kam eine missbräuchliche Anfrage ans Licht, die im Zusammenhang mit einem Stalking-Fall steht. Im zweiten Fall habe ich noch keine Rückmeldung, ob ein Missbrauch des Verfahrens vorliegt. Unter dem Strich gab es aber auch in den vergangenen Jahren nur wenige Bitten um eine Protokollprüfung. Seit ich in Nr. 13.5 des 20. Tätigkeitsberichts zuletzt über diese Protokollprüfungen berichtet habe, hat sich daran nichts geändert.

17.2.4.4 Big Data im TK-Bereich

Der Begriff Big Data ist in aller Munde - der Datenschutz wird dabei oft als Hemmschuh für die wirtschaftliche Nutzbarkeit der Daten angeprangert. Es gibt indes gute Beispiele, wie Daten trotz einer Anonymisierung sinnvoll genutzt werden können.

Bei großen Datensammlungen von Telekommunikationsanbietern ist zwischen personenbezogenen und anonymisierten Datensammlungen zu unterscheiden. Eine Anonymisierung von Daten gilt nicht als Verarbeitung und ist somit zulässig. Dies gilt auch für sensible Daten, wie etwa Standortdaten von Mobilfunknutzern. Solche Bewegungsdaten sind auch ohne Personenbezug für Verkehrsbetriebe, Werbetreibende, Planer von Einkaufszentren und viele mehr eine wertvolle Informationsquelle. Allerdings sind solche umfangreichen Datensammlungen jedenfalls dann kritisch zu bewerten, wenn die Gefahr besteht, Anonymisierungsprozesse könnten nicht sauber durchgeführt werden und damit werde eine Re-Personalisierung von teilweise sehr sensiblen Informationen möglich. Sofern aber die Unternehmen den erforderlichen Aufwand bei der Anonymisierung betreiben und diese gewissenhaft umsetzen, können neben den Interessen der Wirtschaft auch die Interessen und Rechte der betroffenen Bürger gewahrt werden.

Wie bereits in meinem 25. Tätigkeitsbericht (Nr. 8.8.4) berichtet, wurden mir Projekte vorgestellt, die Standortdaten der Mobilfunkteilnehmer nutzbar machen wollen. Diese habe ich seit mehreren Jahren eng begleitet und hierbei regelmäßig Empfehlungen zur Einhaltung und Verbesserung des Datenschutzniveaus gegeben; ein gutes Beispiel für „privacy by design und default“. Zuletzt habe ich mir auch die praktische Anwendung der eingesetzten Verfahren bei zwei Beratungs- und Kontrollbesuchen detailliert erläutern lassen. Auch wenn dabei keine signifikanten Mängel festgestellt wurden, werde ich mich weiterhin regelmäßig über die Weiterentwicklung der Projekte informiert halten.

Im Kern besteht das Anonymisierungsverfahren darin, einzelne „Bewegungsspuren“ über einen jeweils begrenzten Zeitraum zu erzeugen, die keiner Person mehr zugeordnet oder miteinander verknüpft werden können. Dabei kann z. B. ein Hashalgorithmus aus der Rufnummer und einem täglich wechselnden „Salt“ eine neue Kennung berechnen (vgl. Kasten zu Nr. 17.2.4.4). Ein Zurückrechnen ist damit nicht möglich und wegen des wechselnden „Salt“ können die Bewegungsspuren nicht über mehrere Tage miteinander verknüpft werden.

Auch wenn diese Daten bereits als faktisch anonym angesehen werden können, werden sie bei den mir vorgestellten Projekten von den Telekommunikationsanbietern dennoch wie personenbezogene Daten behandelt und nicht an Dritte übermittelt. Weitergegeben werden nur Summen, z. B. wie viele Personen in einem vorgegebenen Zeitraum am potentiellen Standort vorbeigelaufen sind. Dabei sind die zur Verfügung gestellten Informationen nicht geeignet, Rückschlüsse auf einzelne Personen zuzulassen. Auch durch einen Angriff mit Zusatzwissen und einem unverhältnismäßig großen Aufwand könnte man aus diesen statistischen Informationen keine Rückschlüsse zum Verhalten einzelner Personen mehr gewinnen.

Noch interessanter sind die Statistiken, wenn zusätzliche Informationen über das Alter, Geschlecht und Wohnort (auf - teilweise sogar verkürzter - Postleitzahlenbasis) ergänzt werden. Zur Anreicherung mit diesen Informationen werden verschiedene Verfahren - auch unter Nutzung der Bestandsdaten - eingesetzt. Diese sind nicht nur zu komplex, um sie hier vollständig und verständlich zu erläutern, sondern sie unterliegen auch dem Betriebs- und Geschäftsgeheimnis. Es werden dabei an verschiedenen Stellen Mechanismen eingesetzt, die eine Zuordnung zu einer Person verhindern. Wenn eine Person beispielsweise einen sehr abgelegenen Wohnort oder Arbeitsplatz hat, an dem sonst fast keine Daten anderer Personen anfallen, könnte sie auch wenn ihre Daten noch so sicher verhasht sind - durch einfaches Beobachten der Situation vor Ort identifiziert werden. Um dies zu vermeiden, werden entsprechende Informationen unterdrückt.

Eine Einwilligung zur Verarbeitung der in diesem Verfahren verwendeten Daten ist nicht erforderlich, da sie - wie dargestellt - keinen Personenbezug mehr aufweisen. Umso erfreulicher ist es, dass die Unternehmen hier dennoch überobligatorisch ein Opt-Out anbieten. Somit können Kunden individuell entscheiden, ob ihre Daten in den Anonymisierungsprozess einbezogen werden.

Kasten zu Nr. 17.2.4.4

Was ist ein Salt? - Das Salz in der Daten-Suppe!

Eine **Hashfunktion** ist eine Funktion, die eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge abbildet. Dabei ist ein Zurückrechnen nicht möglich. Hier könnte aus einer Zeichenfolge, z. B. einer Rufnummer, eine andere Zeichenfolge gebildet werden. Da dies jederzeit wiederholbar ist und ein Ausprobieren aller Rufnummern mit heutigen Computern wenig Zeit beansprucht, spricht man vorliegend lediglich von einer einfachen Form einer Pseudonymisierung, nicht jedoch von einer Anonymisierung.

Durch einen **„Salt“**, eine weitere, meist zufällig gewählte Zeichenfolge, die an die erste Zeichenfolge (hier z. B. die Rufnummer) angehängt wird, wird das Ergebnis verändert. Sobald der „Salt“ gelöscht wird, kann die Hashfunktion nicht mehr wiederholt werden, ein Ausprobieren wird somit unmöglich. Wenn der Salt nicht mehr verfügbar ist und die sonstigen Rahmenbedingungen stimmen, spricht man von einer Anonymisierung. Werden Daten mit einem unterschiedlichen „Salt“ verhasht, sind sie auch nicht miteinander verknüpfbar.

17.2.4.5 Noch einmal: IP-Adressen - der EuGH hat entschieden

Der Bundesgerichtshof (BGH) hatte im Oktober 2014 die Frage der Personenbeziehbarkeit von dynamischen IP-Adressen dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vorgelegt. Nun hat der EuGH sein Urteil gesprochen.

Über die Frage der Personenbeziehbarkeit von dynamisch vergebenen IP-Adressen wurde in der Vergangenheit viel diskutiert und ebenso viel geschrieben (vgl. 25. TB Nr. 8.8.2). Dabei wurden zwischen den unterschiedlichen Lagern immer wieder dieselben Argumente ausgetauscht, die den jeweiligen Interessen entsprachen, den Gegner aber nicht überzeugen konnten. Der EuGH hat nun bestätigt, dass dynamische IP-Adressen personenbezogene Daten darstellen, und damit die dringend benötigte Rechtssicherheit geschaffen.

Das Gericht kommt in seiner Entscheidung zu dem Schluss, die IP-Adressen der Nutzer beim Besuch einer Website seien personenbezogene Daten, wenn der Anbieter der Website die rechtliche Möglichkeit habe, über zusätzliche Informationen - auch mit Hilfe eines Dritten - die Identität des Nutzers bestimmen zu lassen. Dies ist z. B. im Falle von Cyberattacken möglich.

Die zweite vom BGH vorgelegte Frage betrifft die Umsetzung der Datenschutzrichtlinie (95/46/EG) in deutsches Recht, was letztendlich zu dem langen Rechtsstreit geführt hat. Hierzu stellt der EuGH klar, es müsse

Website-Anbietern möglich sein, die IP-Adressen ihrer Nutzer zur Störungsbeseitigung und Missbrauchsprävention zu verwenden, um die Funktionsfähigkeit ihrer Dienste zu gewährleisten. Das geltende Telemediengesetz sieht jedoch nur die Nutzung der IP-Adresse für die Inanspruchnahme des Dienstes und die Abrechnung kostenpflichtiger Angebote vor.

Der Gesetzgeber muss nun das Telemediengesetz anpassen und sich dabei eng an die Vorgaben des EuGH halten. Dies gilt für die vom Gericht definierten Zwecke und vor allem für die Speicherungsfrist, die analog zur bestehenden Vorschrift im TKG nicht mehr als sieben Tage betragen sollte.

Ein entsprechender Gesetzentwurf liegt mir bisher nicht vor.

17.2.4.6 Die Meldepflicht nach § 109a TKG

Wie bereits in meinem letzten Tätigkeitsbericht vorhergesagt, ist die Anzahl der von Telekommunikationsanbietern gemeldeten Datenschutzverstöße in den letzten beiden Jahren noch einmal angestiegen; insgesamt erreichten mich im Jahr 2015 258 Meldungen und im Jahr 2016 bereits 814 Meldungen.

Meine Analyse der gemeldeten Vorfälle zeigt, dass ein Großteil der Datenschutzvorfälle auf manuellen Arbeitsfehlern oder strukturellen Defiziten bei den betroffenen Prozessabläufen basiert. Mit Ausnahme eines systembedingten Problems bei einem Unternehmen, das zu gut einem Drittel der Meldungen geführt hat, lassen sich jedoch keine Muster oder anderweitige Besonderheiten erklären, die den Anstieg objektiv erklären könnten. Dieser ist daher meines Erachtens weniger auf eine Zunahme der tatsächlichen Datenschutzvorfälle zurückzuführen, sondern zeigt vor allem, dass die Unternehmen, die sich hier Anfangs recht zögerlich verhielten, ihrer gesetzlichen Meldepflicht mittlerweile weitgehend nachkommen. Ich begrüße diese Entwicklung, da sie einerseits belegt, dass das Bewusstsein der TK-Anbieter für die Belange der Nutzer mittlerweile ausgeprägter ist und andererseits auch zu einer größeren Transparenz bei allen Beteiligten führt.

Die Unternehmen nutzen zur Meldung ein von mir zusammen mit der Bundesnetzagentur entwickeltes Meldeformular, in dem Angaben zum Datenschutzvorfall selbst, darüber hinaus aber auch zu den daraufhin eingeleiteten Maßnahmen gemacht werden müssen. Letzteres umfasst vor allem die Information, ob und – wenn ja – wie die vom Vorfall betroffenen Personen benachrichtigt worden sind. Das Gesetz gibt den Unternehmen diesbezüglich vor, wie sie die Betroffenen über die von der Datenschutzverletzung für sie ausgehenden Risiken aufklären, Vorschläge für potentielle Abhilfemaßnahmen unterbreiten und schnellstmöglich die ursächlichen Fehler beheben müssen. Anhand der im Meldeformular abgefragten Angaben ist es mir möglich, zu überprüfen, ob die Unternehmen dieser Verpflichtung im gebotenen Umfang nachkommen. Sollte ein Unternehmen beispielsweise auf eine Benachrichtigung verzichten wollen, obwohl diese aus meiner Sicht im gemeldeten Fall erforderlich wäre, kann ich das Unternehmen auffordern diese nachzuholen. Auch wenn ein derartiges Einschreiten nur in äußerst seltenen Fällen notwendig wird, ist es dennoch erforderlich, jeden gemeldeten Vorfall individuell zu betrachten und zu bewerten.

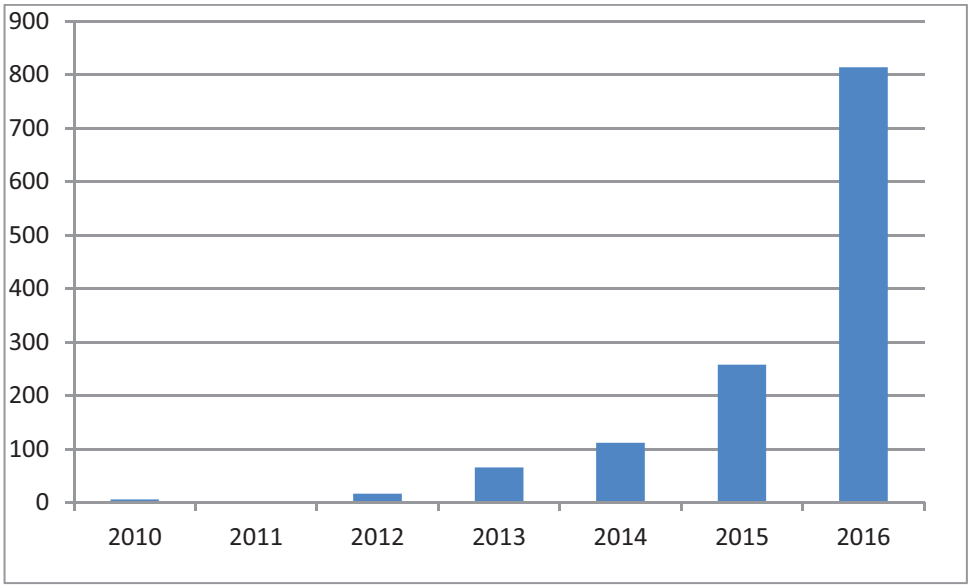
Das ebenfalls im letzten Bericht angesprochene gemeinsame Projekt der BfDI mit der Europäischen Agentur für Netz- und Informationssicherheit ein Verfahren zur Bewertung der Schwere von Datenschutzvorfällen zu erstellen, konnte erfreulicherweise abgeschlossen werden. In diesem Rahmen wurde über das Verfahren hinaus eine Datenbanklösung entwickelt, über die in Zukunft die Meldungen einfacher abgewickelt werden können. Um eine Optimierung des Meldeverfahrens für alle beteiligten Parteien zu erreichen, soll das System nun schnellstmöglich implementiert werden

Weniger erfreulich ist, dass die von mir angeregte Gesetzesänderung zur Beseitigung eines offensichtlichen Wertungswiderspruchs im Wortlaut des § 109a TKG nach wie vor nicht erfolgt ist. Obwohl die Norm im Rahmen der Änderung des IT-Sicherheitsgesetzes (vgl. Nr. 10.2.11.1) an anderer Stelle geändert wurde, sind meine entsprechenden Hinweise unberücksichtigt geblieben. In der Frage, ob beispielsweise Vertriebspartner, die an

der Erbringung von Telekommunikationsdiensten lediglich i. S. d. § 3 Nummer 6 b) TKG mitwirken, einen bei ihnen erfolgten Datenschutzverstoß melden müssen, besteht damit nach wie vor eine große Rechtsunsicherheit.

Kasten zu Nr. 17.2.4.6

Jahr	Meldungen
2010	6
2011	3
2012	17
2013	66
2014	112
2015	258
2016	814



Anzahl der Meldungen nach § 109a TKG

17.2.4.7 App und zu datenschutzgerecht: Mobile Applikationen von Bundesbehörden

Kein Smartphone mehr ohne Mobile Applikationen (Apps). Nicht alle Apps von Bundebehörden sind jedoch datenschutzrechtlich optimal gestaltet.

Bereits in den Jahren 2013 und 2014 habe ich Apps von Bundesbehörden datenschutzrechtlich untersucht (vgl. 25. TB Nr. 8.9.4) und die Anbieter für dabei auftretende Datenschutzprobleme sensibilisiert. Hauptkritikpunkt bei vielen Apps ist die unzureichende Information der Nutzer über den Zugriff auf Geräteressourcen und die Datenerhebung und -nutzung. Was zunächst harmlos klingt, kann aus datenschutzrechtlicher Perspektive sehr kritisch sein, wenn Daten (z. B. Standortdaten) missbräuchlich genutzt werden.

Im Regelfall werden Standortdaten von Apps jedoch benötigt, um entsprechende standortabhängige Dienste (Beispiele: Warnung vor lokalen Unwettergefahren, Informationen zur ehemaligen Berliner Mauer) anbieten zu können. Aus datenschutzrechtlicher Sicht soll die Datenerhebung und -nutzung eindeutig und nachvollziehbar in

der Datenschutzerklärung dargestellt sein. Leider mangelt es bei einigen Angeboten von Bundesbehörden hier an Transparenz. Deswegen habe ich Anbieter aufgefordert, Abhilfe zu schaffen.

Gut, dass es aber auch positive Beispiele gibt, bei denen die datenschutzrechtlichen Aspekte sowohl in der Datenschutzerklärung der App selbst als auch auf der Website der Behörde zu finden sind. Zusätzlich ist die GPS-Standortbestimmung zunächst standardmäßig deaktiviert und muss vom Nutzer bewusst in Betrieb genommen werden.

Meine kontinuierlichen Prüfungen von Mobilen Applikationen der Bundesbehörden sollen dazu beitragen, den Datenschutz bei diesen „Helfern im Alltag“ zu verbessern.

17.2.4.8 Konzerndatenschutzrichtlinie der Deutschen Post DHL - Zielvorgabe noch nicht erreicht

Bereits in der Vergangenheit (vgl. 24. TB Nr. 6.12.1) habe ich über die Konzerndatenschutzrichtlinie der Deutschen Post DHL und deren Billigung durch mich im Jahr 2011 berichtet. Diese umfasst alle global genutzten IT-Services des Unternehmens. Inzwischen konnte die Umsetzung der Konzerndatenschutzrichtlinie nach Angaben der Deutschen Post beinahe abgeschlossen werden. Von den ca. 900 Gesellschaften des Konzerns verbleiben nach Angaben des Konzerns noch etwa zwei Dutzend, die den Regelungen noch beitreten müssen, um die 100-prozentige Beitrittsquote faktisch zu erreichen. Ausgenommen vom Beitritt sind Gesellschaften mit Minderheitsbeteiligung der Deutschen Post, bei denen ihre Rechte zur Umsetzung nicht ausreichen sowie Gesellschaften ohne Personalkörper.

In der Praxis trägt die Konzerndatenschutzrichtlinie zu einer unternehmensweiten Hervorhebung der Bedeutung des Datenschutzes bei, die auch ich immer wieder gefordert hatte. Nach Angaben des Konzerns konnten in fast allen Gesellschaften ein Datenschutzansprechpartner etabliert werden, der die operationale Verantwortung der Beratung der jeweiligen Länder in den Bereichen Audit, Schulungen und Untersuchungen wahrnimmt.

Um Datenschutzbelange dauerhaft durch den Konzern bis in die Gesellschaften umzusetzen, wurde ein Datenschutz-Lenkungsausschuss eingerichtet, der sich u. a. mit der Darstellung des internen Audit-Konzepts sowie der Vorstellung des Aktionsplans bzgl. der Umsetzung der EU-DSGVO beschäftigt hat.

17.3 Aus Beratung und Kontrolle

17.3.1 Kontrollen im Telekommunikationsbereich

Nicht immer werden datenschutzrechtliche Defizite in angemessener Zeit behoben. Manchmal ist aber auch etwas Licht am Ende des Tunnels zu sehen.

Beratungs- und Kontrollbesuche bei Unternehmen der Telekommunikationsbranche sind eine meiner wichtigsten Aufgaben in diesem Bereich. Zum einen dienen sie dazu, sowohl individuelle als auch systemische Fehler bei der Datenverarbeitung durch diese Unternehmen zu identifizieren und - im Idealfall - zeitnah zu beseitigen, was wiederum zu einer unmittelbaren Verbesserung des Datenschutzniveaus für die betroffenen Kunden führt. Zum anderen erhalte ich durch diese Vor-Ort-Termine einen Überblick über die praktischen Auswirkungen datenschutzrelevanter Themen und die aktuellen technischen Entwicklungen im Telekommunikationsbereich, der in einer rein theoretischen Behandlung der Datenschutzfragen in diesem Umfang oft nicht möglich wäre. Ebenso fördern die Besuche den persönlichen Kontakt mit den betrieblichen Datenschutzbeauftragten der Unternehmen, die als Schnittstelle zwischen operativem Bereich der Unternehmen und mir meine ersten und wichtigsten Ansprechpartner sind. Schließlich sind meine Kontrollen nicht selten Ausgangspunkt für datenschutzrechtliche Diskussionen und Beratungen zu Fragen oder Projekten, die eigentlich nicht im Zusammenhang mit dem konkreten Prüfgegenstand stehen.

Was lange währt ...

In meinem 25. Tätigkeitsbericht (Nr. 8.3) hatte ich von drei Beanstandungen gegen drei bzw. aufgrund einer Fusion jetzt nur noch zwei große Mobilfunkanbieter berichtet. Ursache war vor allem die zu lange Speicherung von Verkehrsdaten netzinterner Verbindungen bei so genannten Flatrate-Tarifen. Ebenso wurden u. a. Funkzelleninformationen (Standortdaten) nicht schnell genug gelöscht und - aufgrund eines branchenweiten technischen Defizits - die Inhalte von SMS gespeichert. Hier konnte ich bei verschiedenen Nachkontrollen „Vollzug“ feststellen.

Telefónica hatte mir mitgeteilt, dass die Umstellungen zur Herstellung einer gesetzeskonformen Speicherung von Verkehrsdaten bis Ende Dezember 2016 weitgehend abgeschlossen wurden. Auch bei der Speicherung der SMS-Inhalte wurde eine Lösung in Aussicht gestellt.

Ebenso waren bei *E-Plus* erhebliche Bemühungen erkennbar, die offenen Punkte abzuarbeiten. Einiges wurde dadurch erledigt, dass im Rahmen der Zusammenführung der Unternehmen die Telefónica-Systeme verwendet werden.

Auch bei *Vodafone* konnte bei der Speicherung von Verkehrsdaten ein erheblicher Fortschritt erzielt werden. Seit Mitte 2016 werden die Funkzellendaten, IMEI (Seriennummer des Handys) und die Daten von Flatrate-Verbindungen nach Rechnungsstellung gelöscht. Auch wenn die Umsetzung einzelner Punkte der Beanstandung noch nicht abgeschlossen ist (insbesondere beim Data-Warehouse - DWH), konnte eine deutliche Verbesserung verzeichnet werden.

Dies belegt den positiven Effekt meiner Beanstandungen, auch wenn nicht von einer zeitnahen Reaktion gesprochen werden kann.

Man sieht sich immer zweimal

Bei zwei Unternehmen wurden Kontrollen zu Themen durchgeführt, die in vergleichbarer Form bereits einige Jahre zuvor schon einmal Gegenstand eines Besuchs gewesen sind.

Bei dem einen Unternehmen betraf die erste Kontrolle den Festnetzbereich. Damals waren Anruflisten eines der Themen, die ausführlich diskutiert wurden und zu Änderungen in der Software führten. Bereits in meinem 20. Tätigkeitsbericht (Nr. 13.4) hatte ich auf diese Problematik aufmerksam gemacht, insbesondere darauf, dass Anruflisten nur im Auftrag des Kunden geführt werden dürfen und z. B. die Speicherdauer wählbar sein soll. Das Unternehmen bietet auch Mobilfunkleistungen an, die nun Gegenstand meiner Kontrolle waren. Dabei fiel auf, dass die Anruflisten bei Mobilfunkkunden immer aktiv waren. Das Unternehmen hatte hier eine neue Software eingesetzt und dabei die Wahlmöglichkeiten für Anruflisten nicht implementiert. Diese datenschutzrechtliche Problematik war wohl bereits wenige Jahre nach der ersten Kontrolle im Festnetzbereich aus dem Fokus geraten. Inzwischen wurden die erforderlichen Änderungen umgesetzt bzw. zugesagt.

Bei dem anderen Unternehmen - hier bezog sich die Prüfung auf die Verarbeitung von Bestands- und Verkehrsdaten - wurde seitens des Unternehmens erklärt, im DWH würden die Daten anonymisiert, so dass keine Präsentation geplant sei. Wie ein Blick in die sieben Jahre alte Akte zeigte, war schon bei einem früherem Besuch ein Vorsystem des DWH angesprochen worden. Auch damals erklärte man, es erfolge eine Anonymisierung. Mit meiner zwischenzeitlich gewonnenen Erkenntnis, welches datenschutzrechtlich problematische Verständnis mancher Anbieter von der Anonymisierung - insbesondere in Abgrenzung zur Pseudonymisierung - hat, habe ich diese Aussage hinterfragt. Wie eine daraufhin spontan ermöglichte Präsentation zeigte, fand sehr wohl eine personenbezogene Verarbeitung von Bestands- und Verkehrsdaten im DWH statt. Die Kontrolle ist noch nicht abgeschlossen.

Diese Beispiele belegen die Notwendigkeit, Prüfungen mit einigem zeitlichen Abstand zu wiederholen,. Insofern werde ich auch in Zukunft immer wieder Unternehmen erneut kontrollieren, wenn seit der letzten Prüfung bereits einige Jahre vergangen sind.

Immer wieder Data-Warehouse

Bei meinen Beratungs- und Kontrollbesuchen habe ich zweierlei festgestellt: man sollte weder überrascht sein, wie umfangreich manche Datensammlungen sind, noch sollte man erwarten, dass dem Unternehmen die Sensibilität der gesammelten Daten wirklich bewusst ist. Die Ausführungen in meinem 25. Tätigkeitsbericht (Nr. 8.8.4) zu dieser Thematik sind daher nach wie vor aktuell.

Ein besonders schlechtes Beispiel für eine Anonymisierung bot eine Datenbank eines Telekommunikations-Anbieters mit verhashten Verbindungsdaten. Kritisiert habe ich die Nutzung eines einfachen Hashverfahren, das auch langfristig nicht geändert wurde. Zwar war grundsätzlich gewährleistet, dass man nicht von den Hashwerten auf die Rufnummern zurückrechnen konnte. Sollte aber eine Zuordnung durch einen Angriff mit anderen Mitteln erst einmal erfolgt sein, würden auch alle älteren Verkehrsdaten offen gelegt. Ein solcher Angriff wäre durch einen Vergleich mit einem Einzelverbindungsnachweis oder bei bekanntem Hashverfahren durch Brute Force, also durch Ausprobieren, denkbar. In Folge meiner Kritik wurde das Verfahren so geändert, dass das Hashverfahren durch einen monatlich wechselnden „Salt“ variiert wird, der am Monatsende gelöscht wird. Somit ist ein Brute-Force-Angriff nicht mehr möglich. Ein Vergleich mit einem Einzelverbindungsnachweis könnte zwar unter günstigen Voraussetzungen zu einem Kunden führen, jedoch nur für den Monat, über den man ohnehin mittels des Einzelverbindungsnachweises Informationen hat. Mit dieser Änderung konnte das Verfahren akzeptiert werden.

Das kenne ich doch irgendwoher ...

Ein Klassiker bei Kontrollen ist immer wieder die zu lange Speicherung von nicht abrechnungsrelevanten Verkehrsdaten, z. B. bei netzinternen Gesprächen mit Flatrate-Tarifen oder bei Gesprächen, die gar nicht erst zustande kommen. Diese werden oft, obwohl sie nach § 97 Absatz 3 Satz 3 TKG nach Ermittlung der Abrechnungsirrelevanz unverzüglich zu löschen sind, zusammen mit den abrechnungsrelevanten Verkehrsdaten gespeichert. Dabei betrug die Speicherdauer bis zu 180 Tage. Diese Nicht-Differenzierung „by design“ kann für die Unternehmen zu einem hohen - auch finanziellen - Mehraufwand führen, wenn sie nachträglich ihre Software ändern müssen. Oft sind die IT-Systeme historisch gewachsen und aufgrund der Komplexität dann schwer zu warten.

Ebenso problematisch ist es, sich bei der Speicherdauer an der gesetzlichen Höchstfrist zu orientieren, statt an der vom Gesetz geforderten Erforderlichkeit. So verweise ich bei Kontrollen regelmäßig auf den von mir in Zusammenarbeit mit der BNetzA erstellten „Leitfaden zur Speicherung von Verkehrsdaten“ (vgl. 24. TB Nr. 6.7). In diesem plädiere ich beispielsweise für eine Speicherung der für Abrechnungszwecke verwendeten Verkehrsdaten für drei statt sechs Monate, denn in diesem Zeitraum sind Einwände gegen Rechnungen entsprechend den üblichen AGBs bereits erfolgt.

Bei einem Anbieter habe ich die Speicherung der Vormieterdaten eines Festnetzanschlusses von 28 Monaten festgestellt. Eine Begründung dafür konnte nicht geliefert werden. Vormieterdaten sind nur für den kurzen Zeitraum einer Vor-Ortinstallation notwendig. Nach erfolgtem Anschluss sind diese Daten nicht mehr erforderlich und eine Speicherung somit nicht zulässig.

Bei Vertragsabschlüssen ist die Struktur der Beratungsgespräche durch das Formular vorgegeben. Mit den datenschutzkonformen Formularen wird der Kunde aber zumindest über alle Optionen informiert. Sind die Formulare jedoch mangelhaft, kann dies nur schwer durch die Mitarbeiter ausgeglichen werden. Bisher habe ich stets Verbesserungsbedarf festgestellt, sei es die fehlende Mitbenutzererklärung bei der Beantragung eines Einzel-

verbindungsnachweises bei Anschlüssen im Haushalt, die nach § 99 Absatz 1 TKG den Kunden verpflichtet, alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber zu informieren. Oder seien es die Angaben zur Eintragung in Telefonverzeichnisse nach § 104 TKG, die mangelhaft ausgestaltet sind oder fehlen. Wiederholt habe ich weder die Option zum Einzelverbindungsnachweis noch zum Telefonbucheintrag im Formular gefunden. Diese Erklärungen kann ein Kunde oft erst nach Abschluss des Vertrags online abgeben. Damit kommen diese Anbieter ihrer gesetzlichen Pflicht nach § 93 Absatz 1 TKG nicht hinreichend nach, Kunden auf ihre Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Unternehmen wurden aufgefordert, entsprechende Anpassungen vorzunehmen.

E-Mail zum Wohle des Kunden ...

Wiederholt ist mir aufgefallen, dass E-Mail-Provider die Verkehrsdaten zur E-Mail nicht entsprechend den gesetzlichen Fristen löschen, sondern diese „zum Wohle des Kunden“ bis zu 30 oder gar 40 Tage aufbewahren, um Kundenanfragen, z. B. ob eine E-Mail wirklich versendet wurde, beantworten zu können.

Ein E-Mail-Diensteanbieter hat den Datenschutz hingegen wirklich beeindruckend umgesetzt. Obwohl es sich um einen gebührenpflichtigen Dienst handelt, hat das Unternehmen einen Weg gefunden, weder Bestandsdaten im Sinne des § 95 TKG noch Verkehrsdaten nach § 97 TKG für den Betrieb zu benötigen und diese folglich auch nicht zu erheben oder dauerhaft zu speichern. Wie mir berichtet wurde, zweifeln viele Sicherheitsbehörden, die Auskunft nach § 113 TKG verlangen, diese Praxis an und versuchen, teilweise gerichtlich nicht vorhandene Daten einzuklagen.

Was sonst noch so passieren kann ...

... wenn die BfDI vor der Tür steht und eine fast spontane Kontrolle bei einem Shop eines Telekommunikationsanbieters durchführen will: Mit gut drei Monaten Vorlauf hatte ich die Datenschutzbeauftragten der Telekommunikationsunternehmen über mein Vorhaben informiert, in verschiedenen Shops das Verfahren eines Vertragsabschlusses ohne vorherige langfristige Terminvereinbarung durchzugehen.

In einem Shop hat mich der Geschäftsführer trotz meiner mündlichen und schriftlichen Aufklärung über die Rechtslage und meine Befugnisse aufgefordert, sein Geschäft sofort zu verlassen, andernfalls würde er die Polizei holen. Den Ratschlag, den Datenschutzbeauftragten des Telekommunikationsunternehmens, dessen Produkte er vertrieb, zu kontaktieren, lehnte er ab. Dies veranlasste mich zu einer Beanstandung. Im Nachgang habe ich problemlos einen weiteren Shop desselben Unternehmens geprüft und festgestellt, dass meine Rechte und Befugnisse und damit vor allem auch der Datenschutz bei den Shops dieses Anbieters nunmehr offensichtlich präsent waren. So kann auch eine misslungene Kontrolle Positives bewirken.

De-Mail oder begriffliche Missverständnisse

Weder beim Systemdesign noch bei der Zertifizierung oder der Re-Zertifizierung war aufgefallen, dass Anbieter und Zertifizierender den Begriff „Rechnung“ verwendeten, aber darunter einmal die reine Rechnung und das andere Mal die Rechnung plus Einzelverbindungsnachweis verstanden. Da Rechnungen aus steuerlichen Gründen zehn Jahre gespeichert werden müssen, landeten unbesehen auch Verkehrsdaten über die Einzelverbindungsnachweise in der Datei für steuerliche Zwecke, obwohl sie maximal sechs Monate gespeichert werden dürften.

Ich habe trotz dieses Mangels von einer förmlichen Beanstandung abgesehen, da der Anbieter unverzüglich umfangreiche Maßnahmen ergriffen hat, diesen Missstand abzustellen und bereits nach drei Monaten die vollständige Umsetzung melden konnte.

BDBOS revisited - was hat sich verbessert[1]?

Im 24. Tätigkeitsbericht hatte ich unter Nr. 6.11 von meiner ersten Kontrolle bei der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) berichtet.

Kurz vor der Gesamtabnahme des BOS-Digitalfunksystems war ich erneut vor Ort. Deutliche Verbesserungen hat es vor allem bei den organisatorischen Maßnahmen zum Datenschutz gegeben. So wurde die Weitergabe von Verkehrsdaten an die Bundesländer zwecks Fehler- und Einsatzanalyse auf meine Initiative hin datenschutzrechtlich wesentlich verbessert.

Gleichwohl bleibt mein Hauptkritikpunkt an der pauschalen 90-Tage-Speicherung aller Verkehrsdaten zur Fehler- und Einsatzanalyse bestehen. Bei meiner ersten Kontrolle hatte ich akzeptiert, dass in der „Einführungsphase“ des Digitalfunks alle Verkehrsdaten für einen Zeitraum von 90 Tagen pauschal zur Fehlererkennung und -beseitigung gespeichert bleiben dürfen. Nach der Gesamtabnahme des Tetra-Systems müssen die Speicherfristen jedoch sukzessive minimiert werden, um einen datenschutzkonformen Betrieb zu garantieren. Hier habe ich die BDBOS aufgefordert, entsprechende Konzepte zu erarbeiten und die Speicherfristen für die Verkehrsdaten datenschutzgerecht anzupassen.

WhatsApp

Der Fall *WhatsApp* hat im Herbst 2016 für Proteste der Nutzer gesorgt und die Datenschutzaufsichtsbehörden auf den Plan gerufen. Anlass waren die geänderten Nutzungsbedingungen, die der Nutzer innerhalb von 30 Tagen akzeptieren sollte, wenn er den Dienst weiterhin in Anspruch nehmen wollte. Das hieß für ihn auch, in die Übermittlung seiner Account-Daten an Facebook und in deren Verwendung für Werbezwecke und Verbesserung des Angebots einzuwilligen. Bei der Übernahme von WhatsApp durch Facebook im Februar 2014 war allerdings genau das ausgeschlossen worden. Zwar ist ein Widerspruch in die Verwendung der Daten durch Facebook für Werbezwecke möglich, dies ändert aber nichts daran, dass die Daten nach der Übermittlung im Besitz von Facebook sind - für welche Verwendungen?

WhatsApp hat diese Übermittlung auf ein s. E. berechtigtes Interesse gemäß Artikel 7 Buchstabe f der Richtlinie 95/45/EG und die Einwilligung des Nutzers gestützt. Diese Begründung trägt nach meiner Bewertung rechtlich nicht. Vielmehr führt eine rechtliche Einschätzung meinerseits zu dem Ergebnis, dass es sich bei der Einwilligung nicht um eine datenschutzrechtlich wirksame Einwilligung i. S. d. § 94 TKG i. V. m. § 4a BDSG handelt. Ein berechtigtes Interesse liegt nicht vor. Die Prüfung war allerdings zum Redaktionsschluss noch nicht vollständig abgeschlossen.

Leider kann die heute noch unklare Rechtslage im Bereich der OTT-Dienste auch dazu führen, dass diese sich meiner Kontrolle und damit möglichen Aufsichtsmaßnahmen entziehen. Ordnet man die OTT-Kommunikationsdienste der Telekommunikation zu, ist aufgrund des Angebots an deutsche Nutzer das TKG anwendbar und somit - unabhängig von einer deutschen Niederlassung - meine Zuständigkeit gegeben. WhatsApp jedoch sieht seinen Dienst nicht als Telekommunikation an und beruft sich - im Widerspruch zu europäischen Gesetzen - auf US-amerikanisches Recht, solange keine europäische Niederlassung existiere.

Aufgrund des Einschreitens mehrerer europäischer Datenschutzbehörden hat WhatsApp inzwischen die Übermittlung der Daten von EU-Nutzern an Facebook bis zur Klärung der rechtlichen Fragen gestoppt. Auch die Artikel-29-Gruppe hat sich eingeschaltet und wird in einem koordinierten Vorgehen weitere Schritte einleiten.

Sonstiges

Bereits mehrfach hatte ich über die lange Speicherdauer der Verkehrsdaten bei der Interconnection, der Zusammenschaltung öffentlicher Telefonnetze, berichtet (vgl. 23. TB Nr. 6.3 und 25. TB Nr. 8.8.3). Hier wurde mir nun von der BNetzA mitgeteilt, die Zusammenschaltung der Netze werde noch länger mit der leitungsvermittelten Technik aufrechterhalten, die komplexere Abrechnungsmodalitäten erfordere. Erst wenn ausschließlich eine Zusammenschaltung mit der IP-Technik erfolge, also vermutlich 2019, werde eine Neubewertung vorgenommen. Ob eine Reduzierung der Speicherdauer von sechs auf drei Monate möglich sein wird, kann ich wohl erst im übernächsten Tätigkeitsbericht mitteilen.

17.3.2 „Da werden Sie geholfen ...“ - Datenschutzkonforme Einwilligung zur Gesprächsaufzeichnung in Callcentern

„Zur Qualitätssicherung und zu Schulungszwecken werden vereinzelt Gespräche aufgezeichnet. Wenn Sie damit nicht einverstanden sind ...“ Jeder kennt diese Ansagetexte der Callcenter. Aber ist dieses Verfahren auch datenschutzkonform?

Die Einwilligung zur Gesprächsaufzeichnung in Callcentern ist in vielen Fällen nicht datenschutzgerecht ausgestaltet. Die Speicherung von Mitschnitten stellt eine automatisierte Erhebung und Verarbeitung personenbezogener Daten gemäß §§ 4, 4a BDSG dar, die eine explizite Einwilligung des Betroffenen erfordert. Das Schweigen nach dem Hinweis auf eine mögliche Widerspruchsmöglichkeit (Widerspruchslösung) erfüllt diese Anforderungen nicht.

Ich habe bereits seit Jahren zu verschiedenen Anlässen - unter anderem in meinem 25. Tätigkeitsbericht (Nr. 8.8.3) sowie mehrfach im Rahmen des Jour fixe Telekommunikation - darauf hingewiesen, dass es aus datenschutzrechtlicher Sicht für Gesprächsaufzeichnungen zwingend einer Einwilligung im Wege der Opt-in-Lösung bedarf. Im Juli 2015 habe ich erstmals eine breit angelegte telefonische Kontrolle der Verfahren von Servicerufnummern der Telekommunikations- und Postdienstleister durchgeführt und diese seitdem in regelmäßigen Abständen wiederholt, zuletzt im Januar 2016.

Im Postbereich gab es nur bei einer Rufnummer Hinweise auf eine mögliche Gesprächsaufzeichnung, die kurzfristig durch eine datenschutzgerechte Einwilligungslösung ersetzt wurde. Bei den Telekommunikationsdienstleistern wurden insgesamt 30 Servicerufnummern überprüft. Bei neun Servicerufnummern musste ich feststellen, dass lediglich eine Widerspruchsmöglichkeit angeboten wurde (Stand: 25.01.2016). Aufgrund dieser Datenschutzverstöße habe ich die Verfahren der jeweiligen Anbieter gegenüber der BNetzA formal beanstandet.

Infolge der ausgesprochenen Beanstandungen wurde bisher bereits in fünf Fällen das Verfahren auf ein Opt-in-Verfahren umgestellt, ein Anbieter verzichtet nun vollständig auf Gesprächsaufzeichnungen. Bei den übrigen drei Anbietern ist das Verfahren noch nicht abgeschlossen.

17.3.3 Internetangebote der Bundesbehörden

Im Rahmen meiner Zuständigkeit kontrolliere ich die Einhaltung der datenschutzrechtlichen Vorgaben auch bei den Internetangeboten der Bundesbehörden.

Der Anbieter von Websites hat die Nutzer nach § 13 Absatz 1 Telemediengesetz (TMG) über die Art, den Umfang und den Zweck der Datenerhebung und -verarbeitung in allgemein verständlicher Form zu unterrichten. Dieser Unterrichtung kommt er mit der Datenschutzerklärung nach. Diese muss für die Nutzer jederzeit und von jeder Stelle des Internetangebotes aus abrufbar sein. Wird sie lediglich als Unterpunkt in das Impressum integriert, ist die Auffindbarkeit nicht hinreichend gegeben und § 13 Absatz 1 TMG nicht erfüllt.

Wie ich bei der Bearbeitung von Petenteneingaben und auch bei routinemäßigen Prüfungen von Internetangeboten der Bundesbehörden bei einigen Websites bemerkt habe, war die **Datenschutzerklärung** nicht als eigenständiger Menüpunkt, sondern als Teil des Impressums aufgeführt, in einigen Fällen fehlte sie sogar vollständig. Ich habe die behördlichen Datenschutzbeauftragten aufgefordert, umgehend die entsprechenden Anpassungen vornehmen zu lassen.

Zwei Behörden-Websites verwenden sog. **Google-Captchas** (engl.: Completely Automated Public Turing test to tell Computers and Humans Apart). Dabei handelt es sich um eine Form von Eingabefenster, mit dem festgestellt werden soll, ob der Zugriff von einem Menschen getätigt wird oder maschinell erfolgt. In den konkreten Fällen sollten die Captchas die Verfälschung von Umfragen durch automatisiert erstellte Antworten verhindern. Aus datenschutzrechtlicher Sicht ist die Einbindung von Captchas jedoch kritisch zu sehen, da, je nach verwendetem Captcha, die Übertragung von personenbezogenen Daten (hier: IP-Adresse) an Dritte nicht auszuschließen ist. Ich habe deshalb die Betreiber aufgefordert, entweder die verwendeten Captchas zu entfernen oder diese durch datenschutzgerechte Varianten zu ersetzen.

17.3.4 Kontrollen im Postbereich

Bei meinen stichprobenartigen Kontroll-, Informations- und Beratungsbesuchen bei Postdienstunternehmen habe ich insgesamt ein gutes Datenschutzniveau festgestellt. Alle beteiligten Unternehmen, ob groß oder klein, waren kooperativ und zeigten sich gegenüber Datenschutzthemen, nicht zuletzt auch im eigenen Interesse, sehr aufgeschlossen.

Im Postdienstleistungsbereich sind viele geringfügig Beschäftigte tätig. Gleichzeitig handelt es sich angesichts der Vielzahl der kleinen Unternehmen durchaus um eine größere Beschäftigtenanzahl, die mit personenbezogenen Daten in Kontakt kommt. Bei Kontrollen war es mir daher besonders wichtig, zu prüfen, ob alle Beschäftigten ordnungsgemäß auf das Daten- und Postgeheimnis (§ 5 BDSG und § 39 PostG) verpflichtet sind und durch regelmäßige Awareness-Maßnahmen geschult werden. In einem Fall verfügte ein Teil der Beschäftigten über unzureichende Deutschkenntnisse, um die von ihnen zu unterschreibenden Verpflichtungserklärungen sowie die Arbeitsanweisungen zu verstehen. Hier habe ich auf Informationsmaterialien in den relevanten Fremdsprachen gedrängt. Dieser Vorgabe wurde entsprochen.

Bei meinen Besuchen habe ich lizensierte Postdienstunternehmen, die Subunternehmer mit und ohne eigene Postlizenz einsetzen, immer wieder darauf hingewiesen, dass sie als die verantwortliche Stelle die Verantwortlichkeit für die ordnungsgemäße Durchführung von Verpflichtungen und Schulungen sowie für eventuelle Konsequenzen bei einer fehlerhaft durchgeführten Maßnahme nicht ausschließlich auf einen Dritten verlagern können, sondern selbst bei einer Delegation die Eigenverantwortung fortbesteht. Dies gilt auch bei einer Funktionsübertragung gem. § 5 der Postdienste-Datenschutzverordnung (PDSV), also nicht nur bei einem Auftragsdatenverarbeitungsverhältnis gem. § 11 BDSG.

Wie kommt meine Telefonnummer auf den Adressaufkleber und woher kennt der Postdienstleister meine E-Mail-Adresse?

Der Trend bei vielen großen Postdienstleistern geht zu einer angekündigten und sogar flexiblen Zustellung von Päckchen und Paketen, bei der Empfänger im Voraus informiert werden, wann eine Sendung ausgeliefert wird, sowie zur zeitlichen oder räumlichen Umlenkung der Sendung noch kurz vor der Zustellung. Diesen Service unterstützt der Versandhandel, der dazu eigenverantwortlich, nach vorheriger Einwilligung seines Kunden, die E-Mail-Adresse oder auch die Telefonnummer an den Postdienstleister weitergibt. So kann dieser den Kunden nicht nur per E-Mail, sondern auch telefonisch über den Zeitpunkt der Zustellung informieren und gleichzeitig sicherstellen, dass der Zusteller den Weg nicht umsonst macht. Es kommt allerdings immer wieder vor, dass sich der ein oder andere Empfänger über die „angereicherte Adresse“ wundert und dann verständlicherweise auch mich nach der Herkunft dieser Daten fragt.

Diese Verfahrensweise liegt aber nicht im Verantwortungsbereich der Postdienstunternehmen, sondern ausschließlich beim Absender. Ich habe daher im Rahmen meiner Möglichkeiten darauf hingewirkt, dass die Postdienstleister die Absender, meist Versandhändler, auf ihre Verpflichtung zur Einholung der Einwilligung zur Datenweitergabe der E-Mail-Adresse und ggf. der Telefonnummer nochmals ausdrücklich hinweisen. Als problematisch sehe ich es an, dass diese Art der Einwilligung bisher für Unternehmen oder Privatpersonen nicht möglich ist, die einen vorgefertigten Online Shop bei einen Anbieter wie z. B. Amazon betreiben, um dort als

sogenannter „Drittanbieter“ Waren verkaufen zu können, da die entsprechende Konfigurationsmöglichkeit fehlt. Der Amazon.de Marketplace wird in Luxemburg betrieben, deswegen kann nur der luxemburgische Datenschutzbeauftragte die datenschutzrechtlichen Anpassungen der Plattform einfordern.

A. Zudem von besonderem Interesse

Nr. 1.1;1.2 f.; 1.6; 12.2.2; 21.1; 21.5

18 Petitionsausschuss

Im Berichtszeitzeitraum haben sich Betroffene nicht nur an mich gewandt, sondern in einigen Fällen auch parallel an den Petitionsausschuss des Deutschen Bundestages. Es ist gut, wenn die Betroffenen die Möglichkeit haben, sich hilfesuchend an mehrere Petitionsstellen wenden zu können. Dies betraf beispielsweise den Fall eines Bürgers, der sich gegen die Fehlinterpretation der Gutachterregelung in § 200 Absatz 2 SGB VII wandte (vgl. Nr. 3.2.3.2). In den Fällen, in denen sich Betroffene auch an den Petitionsausschuss wenden, gibt mir dieser Gelegenheit, ihm meine Auffassung zu den datenschutzrechtlichen Fragen darzulegen. Ich begrüße dies ausdrücklich.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 3.2.3.2; 21.1; 21.5

19 Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung

Änderung der Geschäftsordnung

Am 15. Oktober 2015 führte ich ein Gespräch mit dem 1. Ausschuss des Deutschen Bundestages, Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung. Dabei ging es im Wesentlichen um die Möglichkeit, meinen Tätigkeitsbericht künftig im Plenum des Deutschen Bundestages vorstellen und meine Stellungnahmen im Rahmen von Ressortabstimmungen den Gesetzgebungsvorhaben der Bundesregierung bei Einbringung in die parlamentarische Beratung beifügen zu können. Der Ausschuss griff damit meine entsprechenden Empfehlungen aus dem 25. Tätigkeitsbericht auf.

Erforderlich wäre hierfür eine Änderung der Geschäftsordnung des Deutschen Bundestages. Einige Bundesländer haben ihren Landesdatenschutzbeauftragten bereits entsprechende Befugnisse eingeräumt, z. B. Berlin, Brandenburg, Sachsen und Thüringen.

Meine Beratungsaufgabe gegenüber dem Deutschen Bundestag könnte ich zudem wirksamer erfüllen, wenn meine Stellungnahmen im Rahmen von Ressortabstimmungen den Gesetzgebungsvorlagen der Bundesregierung bei Einbringung in die parlamentarische Beratung beigefügt würden. Hierdurch könnte der Gesetzgeber unmittelbar auf die datenschutzrechtlichen Implikationen eines Gesetzgebungsvorhabens aufmerksam gemacht werden. Vergleichbar wäre dies mit der Funktion des Nationalen Kontrollrates, dessen Stellungnahmen zu den verursachten Bürokratiekosten eines Gesetzes dem betreffenden Gesetzentwurf beigefügt werden.

Der Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung des Deutschen Bundestages hat eine Prüfung meiner Vorschläge zugesagt. Ein Ergebnis lag bei Redaktionsschluss zu diesem Tätigkeitsbericht noch nicht vor.

A. Zudem von besonderem Interesse

Nr. 1.1; 1.2 f.; 21.1; 21.5

20 Weitere Ausschüsse

Nachfolgend habe ich dargestellt, welche Beiträge meines Berichtes für weitere Ausschüsse des Deutschen Bundestages von besonderem Interesse sein können

Ausschuss Digitale Agenda	Nr. 1.1 Endspurt zur Europäischen Datenschutzreform und JI-Richtlinie; Nr. 1.2 f. Umsetzung der Europäischen Datenschutzreform in nationales Recht; Nr. 10.2.11 ff. Einzelthemen aus dem Bereich Technologischer Datenschutz; Nr. 12.2.1 Die Justiz wird digitalisiert; Nr. 17.2.1 Digitalisierung der Energiewende – Smart Metering; Nr. 21.5 Öffentlichkeitsarbeit
Haushaltsausschuss	Nr. 1.1 Endspurt zur Europäischen Datenschutzreform und JI-Richtlinie; Nr. 1.2 f. Umsetzung der Europäischen Datenschutzreform in nationales Recht; Nr. 1.3 Grundsatzentscheidungen im Sicherheitsbereich mit weitreichenden Folgen; Nr. 10.2.11.6 IT-Konsolidierung Bund; Nr. 21.1 Organisatorische Verselbständigung vollzogen; Nr. 21.5 Öffentlichkeitsarbeit
Ausschuss für Menschenrechte und humanitäre Hilfe	Nr. 1.1 Endspurt zur Europäischen Datenschutzreform und JI-Richtlinie; Nr. 1.2 f. Umsetzung der Europäischen Datenschutzreform in nationales Recht; Nr. 2 ff. Schwerpunktthemen – europäisch und international; Nr. 21.5 Öffentlichkeitsarbeit
Ausschuss für Tourismus	Nr. 1.1 Endspurt zur Europäischen Datenschutzreform und JI-Richtlinie; Nr. 1.2 f. Umsetzung der Europäischen Datenschutzreform in nationales Recht; Nr. 2 ff. Schwerpunktthemen – europäisch und international; Nr. 21.5 Öffentlichkeitsarbeit
Ausschuss für wirtschaftliche Zusammenarbeit und Entwicklung	Nr. 1.1 Endspurt zur Europäischen Datenschutzreform und JI-Richtlinie; Nr. 1.2 f. Umsetzung der Europäischen Datenschutzreform in nationales Recht; Nr. 21.5 Öffentlichkeitsarbeit

21 Aus meiner Dienststelle

21.1 Organisatorische Verselbstständigung vollzogen

Nachdem die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zum 1. Januar 2016 unabhängig geworden ist, gilt es nun, die erforderlichen personellen und finanziellen Rahmenbedingungen zu schaffen und zu sichern, um die Unabhängigkeit auch umzusetzen.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist seit dem 1. Januar 2016 eine eigenständige oberste Bundesbehörde. Damit wurde die seit 1995 bestehende europarechtliche Verpflichtung zur Herstellung der völligen Unabhängigkeit der Datenschutzaufsicht vollzogen. Die seit Errichtung der Behörde im Jahr 1978 geltende Dienstaufsicht des BMI sowie die Rechtsaufsicht der Bundesregierung wurden beendet. Jetzt unterstehe ich ausschließlich parlamentarischer und gerichtlicher Kontrolle.

Aufgrund der vielfältigen und stetig zunehmenden Aufgaben wächst meine Dienststelle dynamisch - und dies sowohl in personeller als auch in organisatorischer und finanzieller Hinsicht. Mit dem Nachtragshaushalt 2015 wurden drei zusätzliche Planstellen bewilligt; mit dem Haushalt 2016 erhielt ich weitere 20,5 zusätzliche Planstellen. Damit weist meine Dienststelle im Jahr 2016 insgesamt 110,5 Planstellen und Stellen auf. Entsprechend wurde der Haushalt von 9,3 Millionen € in 2015 auf 13,7 Millionen € für das Jahr 2016 aufgestockt (vgl. Kasten zu Nr. 21.1).

Dieses Wachstum setzt sich auch mit dem im Jahr 2016 verhandelten Haushalt 2017 fort. Für das Jahr 2017 wurden meiner Dienststelle 49 neue Planstellen bewilligt. Davon sind allerdings 20 Planstellen zum Ende des Jahres 2017 nach Vorlage einer Personalbedarfsermittlung zu entsperren.

Meine weiter wachsenden Aufgaben - insbesondere aufgrund der europäischen Datenschutz-Grundverordnung sowie durch die Rechtsprechung des Bundesverfassungsgerichts zur notwendigen datenschutzrechtlichen Kontrolle der Sicherheitsbehörden - machen auch künftig ein erhebliches personelles und finanzielles Wachstum erforderlich. Hierauf werde ich gegenüber Bundesregierung und Parlament weiterhin mit Nachdruck hinweisen und die sachlich gebotenen Personalaufstockungen vollumfänglich geltend machen.

Kasten zu Nr. 21.1

Übersicht Personalstellen BfDI - 2007 - 2017

	Stellen
2007	65
2008	69
2009	67
2010	81
2011	81
2012	89
2013	87,5
2014	87
2015	90
2016	110,5
2017	160,5

Erläuterung zum Haushaltsjahr 2017: Zusätzlich zu 49 neuen Planstellen eine Umsetzung aus dem Statistischen Bundesamt.

Nach erfolgter Umstrukturierung wird die BfDI auch die Initiierung von Forschungsvorhaben wieder aufnehmen. Für die Zukunft ist beabsichtigt, zwei Forschungsvorhaben auf den Weg zu bringen. Dies betrifft zum einen die „Car2x-Kommunikation“. Die Automobilindustrie will damit eine intelligente Verkehrssteuerung sowie eine deutlich bessere Unfallvermeidung erreichen. Fahrzeuge und Infrastrukturkomponenten („Road Site Units“) sollen hierzu in hoher Frequenz Daten aussenden, um Kollisionen zu vermeiden. Dieses Vorhaben wirft datenschutzrechtliche Fragen auf, etwa in Bezug auf die Möglichkeit der Rekonstruktion von Fahrtrouten.

Ein weiteres Forschungsvorhaben betrifft die Zertifizierung nach der europäischen Datenschutz-Grundverordnung. Hier stellt sich die Frage, welche Ansätze mit geltendem Recht vereinbar sind und wie die Zertifizierung konkret ausgestaltet werden sollte, z. B. hinsichtlich der Gültigkeitsdauer eines Zertifikats. Auch sind Regelungen zur Akkreditierung der Zertifizierungsstellen nach der europäischen Datenschutz-Grundverordnung festzulegen.

21.2 BfDI als Ausbildungsbehörde

Referendare, Praktikanten und Anwärter zeigen Interesse am Datenschutz.

Das Interesse an Praktikumsaufenthalten in meiner Dienststelle ist unverändert groß. Aufgrund der Umorganisation sowie eingeschränkter räumlicher Kapazitäten konnten im Berichtszeitraum allerdings nur zwei Referendare Teile ihrer Ausbildung in meinem Hause absolvieren. Ferner leistete ein Anwärter des gehobenen Verwaltungsdienstes sein Pflichtpraktikum in meiner Dienststelle ab. Ab dem Jahr 2017 bietet meine Dienststelle wieder in deutlich mehr Fällen die Möglichkeit, hier Teile der Ausbildung bzw. Pflichtpraktika zu absolvieren. Darüber hinaus wird zur Deckung des künftigen Personalbedarfs an der Schnittstelle zwischen den klassischen Verwaltungstätigkeiten und dem Bereich der Informationstechnik im Jahr 2018 die Möglichkeit zur Teilnahme am Studiengang Verwaltungsinformatik bei der Hochschule des Bundes angeboten werden.

21.3 Das Verbindungsbüro in Berlin

Das Verbindungsbüro in Berlin stellt eine wirkungsvolle und direkte Teilnahme am politischen Geschehen in Berlin sicher.

Derzeit umfasst das Verbindungsbüro in Berlin Mitte dreizehn Mitarbeiterinnen bzw. Mitarbeiter. Seit seiner Inbetriebnahme im Jahr 2008 wird ein Großteil der Termine in Berlin von den dortigen Mitarbeiterinnen und Mitarbeitern wahrgenommen. Dies betrifft insbesondere die Ausschusssitzungen des Deutschen Bundestages und Besprechungen mit den Bundesressorts. Damit wird eine wirkungsvolle und direkte Teilnahme am politischen Geschehen in der Bundeshauptstadt sichergestellt. Zugleich wird der Dienstreiseaufwand meiner Bonner Dienststelle deutlich reduziert. Zudem werden auch Besuchergruppen im Verbindungsbüro in Berlin empfangen.

21.4 Verschlüsselte Kommunikation mit der BfDI

Verschlüsselte Kommunikation wird immer wichtiger, insbesondere bei sensiblen personenbezogenen Daten. Vorhandene Angebote sollten aber auch genutzt werden.

Das Thema Verschlüsselung ist so aktuell wie nie. Mit meiner Dienststelle kann schon seit einigen Jahren verschlüsselt kommuniziert werden. Den Austausch vertraulicher Nachrichten unterstütze ich über das Programm Pretty Good Privacy (PGP) oder GnuPG.

Die Landesbeauftragten für den Datenschutz (LfD) hatten sich bereits vor längerer Zeit auf eine gemeinsam genutzte Verschlüsselung auf Basis von PGP geeinigt. Eine zentrale Stelle (hier der LfD Mecklenburg-Vorpommern) verwaltet einen zentralen Schlüsselbund. Die daraus von den LfDs und von meinem Haus abgeleiteten eigenen Schlüssel sind vertrauenswürdig.

Der Schlüssel und eine kurze Anleitung ist auf meiner Website unter „Kontakt“ (https://www.bfdi.bund.de/DE/Service/Kontakt/kontakt_node.html) dargestellt.

21.5 Öffentlichkeitsarbeit

Im Berichtzeitraum konnte die Öffentlichkeitsarbeit weiter ausgebaut werden. Neben der aktiven Teilnahme an Veranstaltungen mit einem Informationsstand meines Hauses wurden Besuchergruppen von Mitgliedern des Deutschen Bundestages betreut. Zudem steht allen interessierten Bürgerinnen und Bürgern ein umfangreiches Informationsangebot zur Verfügung.

Veranstaltungen

Meine Dienststelle nahm in den Jahren 2015 und 2016 am Tag der offenen Tür der Bundesregierung in Berlin mit einem Informationsstand im neuen Gebäude des Bundesministeriums des Innern teil.

Neben dem Tag der offenen Tür der Bundesregierung präsentierte sich meine Dienststelle unter anderem auf dem Europäischen Datenschutztag und dem Symposium zum 10-jährigen Bestehen des Informationsfreiheitsgesetzes.

Besuchergruppen

Neben diesen Veranstaltungen betreuen Mitarbeiterinnen und Mitarbeiter meines Berliner Verbindungsbüros auf Wunsch auch Besuchergruppen von Mitgliedern des Deutschen Bundestages. Im Berichtszeitraum zeigten 22 Besuchergruppen der verschiedenen Parteien mit jeweils 50 Teilnehmerinnen und Teilnehmern großes Inte-

resse an Fragen des Datenschutzes und der Informationsfreiheit. Im Vergleich zum vorhergehenden Berichtszeitraum war die Nachfrage von Mitgliedern des Deutschen Bundestages geringer. Ich werbe nachdrücklich bei den Mitgliedern des Deutschen Bundestages dafür, den Besuch bei der BfDI in das Programm der Besuchergruppen aufzunehmen.

Informationsmaterial

Im Berichtzeitraum konnten wieder zahlreiche Broschüren und Flyer publiziert werden; darunter sind eine umfangreiche Informationsbroschüre zur europäischen Datenschutz-Grundverordnung und ein Flyer zu den Auswirkungen der Datenschutz-Grundverordnung auf Bürgerinnen und Bürger.

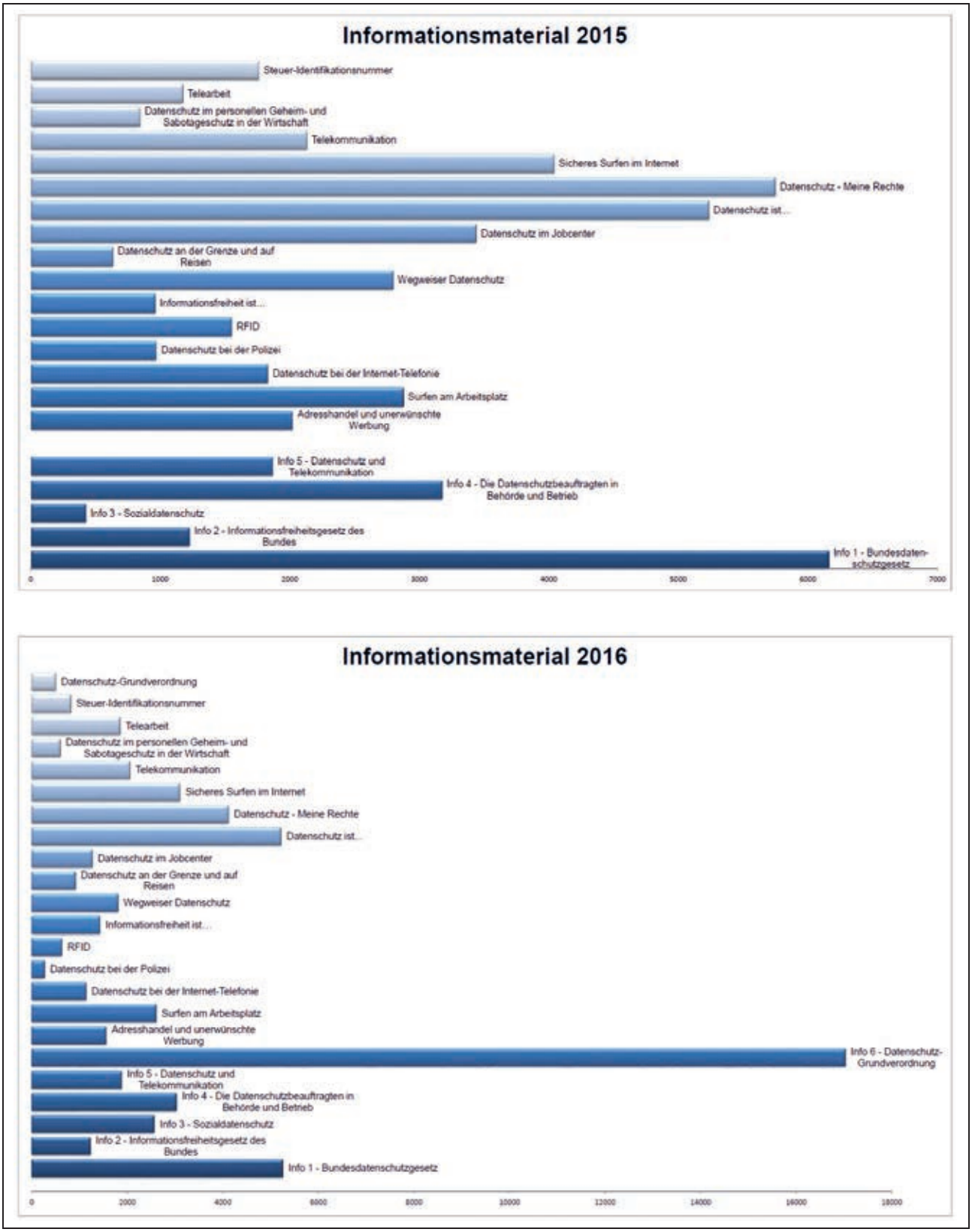
Die sechs Informationsbroschüren der „Info"-Reihe wenden sich an Leserinnen und Leser, die sich vertieft in ein Themengebiet einarbeiten wollen und ein Nachschlagewerk in Ergänzung zu den gesetzlichen Vorschriften benötigen. Die knapperen und handlicheren Flyer sprechen vor allem Bürgerinnen und Bürger an, die kurze Informationen und klare Handreichungen zum Datenschutz und zur Informationsfreiheit suchen. Das Themenspektrum reicht hier von den Grundlagen des Datenschutzes und der Informationsfreiheit über Tipps für das sichere Surfen im Internet bis hin zu Informationen über Datenschutzrechte im Bereich der Telekommunikation. Die hohen Bestellzahlen zeigen das große Interesse an diesen Themen (vgl. Kasten zu Nr. 21.5). Das Informationsangebot werde ich auch in den kommenden Jahren stetig aktualisieren und weiter ausbauen. Das Informationsmaterial ist abrufbar auf meiner Internetseite unter www.datenschutz.bund.de.

Datenschutz kompakt

Mein Informationsangebot habe ich um die Publikationsreihe „Datenschutz kompakt" erweitert. Insbesondere für die Abgeordneten des Deutschen Bundestages werden in diesem Format aktuelle Themen des Datenschutzes übersichtlich und pointiert aufbereitet.

Dadurch stehen zu komplexen Themen knappe Informationen für die parlamentarische Arbeit oder als Argumentationshilfe für die Wahlkreisarbeit oder Bürgergespräche bereit.

Kasten zu Nr. 21.5



21.6 Besuche ausländischer Delegationen

Verschiedene Gruppen von Datenschutzexperten aus Osteuropa, Nordafrika und insbesondere aus Asien besuchten meine Dienststelle, um aktuelle Fragen des Datenschutzes zu diskutieren und Erfahrungen auszutauschen.

Wie in den Vorjahren habe ich auch im Berichtszeitraum wieder ausländische Delegationen in meiner Dienststelle empfangen. So konnte ich den Erfahrungsaustausch mit Datenschutzexperten aus Japan fortsetzen (vgl. 25. TB Nr. 22.3). Zwei Delegationen der neu gegründeten „Personal Information Protection Commission“ (PIPC) informierten sich über das Konzept des Datenschutzes in Deutschland und die nationalen Erfahrungen mit dem europäischen Datenschutzrecht.

Zudem habe ich Delegationen der Datenschutzbehörden aus Bosnien-Herzegowina und aus der Ukraine empfangen. Themen der hierbei geführten Gespräche waren die gesetzlichen Regelungen und die praktischen Erfahrungen hinsichtlich des Datenschutzes sowie aktuelle datenschutzrechtliche Fragen, wie z. B. die europäische Datenschutzreform.

Es ist Ziel, auch künftig den Aufbau und die Tätigkeit neuer Datenschutzbehörden zu unterstützen und zu diesem Zweck den Erfahrungsaustausch mit ausländischen Datenschutzexperten fortzusetzen.

22 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. 24. TB Nr. 2.2.5, 25. TB Nr. 7.5 **Foreign Account Tax Compliance Act (FATCA)**

Das bilaterale FATCA-Abkommen zwischen Deutschland und den USA ist am 11. Dezember 2013 in Kraft getreten.

Meldende deutsche Finanzinstitute sind verpflichtet, sich bei der amerikanischen Steuerbehörde (Internal Revenue Service - IRS) registrieren zu lassen und die zu erhebenden Daten zu US-amerikanischen meldepflichtigen Konten an das Bundeszentralamt für Steuern (BZSt) zu melden. Die Daten sind jährlich zu erheben und bis zum 31.07. des Folgejahres an das BZSt zu übermitteln. Dieses leitet die Daten dann an den IRS weiter.

Die technischen Einzelheiten wurden mit der amerikanischen Seite in einem „Competent Authority Arrangement“ festgelegt. Im September 2015 wurden erstmals Daten in die USA übermittelt. Auch der IRS stellt im Gegenzug den deutschen Steuerbehörden Daten über in Deutschland Steuerpflichtige mit Konten in den USA zur Verfügung. Diese werden vom BZSt an die zuständigen inländischen Landesfinanzverwaltungen weitergegeben.

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. Ich werde das Verfahren auch weiterhin datenschutzrechtlich begleiten.

2. 25. TB Nr. 11.1.2 **Kontrolle des Instituts für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr (WehrMedStatInstBw)**

Bereits im vergangenen Berichtszeitraum habe ich über die Probleme bei der Aussonderung und Vernichtung von Gesundheitsunterlagen berichtet, die vom WehrMedStatInstBw auf Mikrofilm archiviert und deren Fundstellen in einer eigens dafür betriebenen Datenbank festgehalten werden.

Das Institut hat im Nachgang zu meinem Kontrollbesuch seine Fundstellendatenbank weiterentwickelt und mir die Änderungen bei einem erneuten Informationsbesuch im Jahr 2016 vorgestellt. Die jetzt als Dokumentenfundstelleninformationssystem (DFIS) bezeichnete Datenbank kann nun erstmals sicherstellen, dass alle enthaltenen Fundstellen über auf Mikrofilm archivierte Gesundheitsunterlagen fristgerecht gelöscht werden können.

Ich begrüße diese Weiterentwicklung. Sie stellt jedoch nur einen ersten wichtigen Schritt zur Umsetzung der eigentlichen Verpflichtung des Instituts dar, nicht mehr erforderliche Unterlagen mit Gesundheitsdaten zu löschen. Denn trotz der Löschung der Fundstelle wird die eigentlich zu löschende Unterlage weiterhin auf Mikrofilm vorgehalten, bis die Archivierungsfrist auch der letzten der auf dem gesamten Mikrofilm enthaltenen Gesundheitsunterlagen abgelaufen ist.

Meine Empfehlung an das Bundesministerium der Verteidigung, eine technische Lösung zur Datenlöschung nach Ablauf der Archivierungsfristen entwickeln zu lassen, halte ich daher aufrecht.

3. 25. TB Nr. 12.1 **Online-Wahl beim Bundesfreiwilligendienst**

Nach meiner Beteiligung beim Verfahren zum Erlass der Verordnung zur Wahl der Sprecherinnen und Sprecher des Bundesfreiwilligendienstes in den Jahren 2012 und 2013 habe ich mir im Jahr 2015 die

Durchführung der Online-Wahl beim Bundesamt für Familie und zivilgesellschaftliche Aufgaben (BAFzA) angesehen.

Die Teilnahme an der Wahl setzt voraus, dass sich die Bundesfreiwilligendienstleistenden (Bufdis) zunächst auf einer Internetseite für die Wahl registrieren. Daraufhin erhalten die registrierten Bufdis einen Transaktionscode als Legitimation per E-Mail zugesandt. Mit diesem Transaktionscode können sie in der zweiten Phase an der Wahl teilnehmen und ihre Stimme abgeben. Für den Wahlvorstand im BAFzA ist im Wahlverfahren anschließend nur ersichtlich, ob ein/e registrierte/r Wahlberechtigte/r seine Stimme bereits abgegeben hat, nicht jedoch, für welche/n Bewerber/in er sich entschieden hat.

Das IT-Verfahren zur Durchführung der Wahl wird im Rahmen einer Auftragsdatenverarbeitung durch einen IT-Dienstleister bereitgestellt. Dazu schließt das BAFzA jährlich einen Vertrag mit dieser Firma. Bei der Gestaltung des Vertrages habe ich auf einige Verbesserungen gedrungen:

So wurde der Vertrag für die Wahl 2015 erst mehrere Wochen nach Beginn des Wahlverfahrens abgeschlossen, so dass der IT-Dienstleister zwischenzeitlich personenbezogene Daten von Bufdis ohne Auftrag verarbeitet hat. Darüber hinaus habe ich vertragliche Anpassungen empfohlen, die den Dienstleister verpflichten, Unterauftragsverhältnisse beim BAFzA anzuzeigen. Zudem sollte im Rahmen der Beauftragung klargestellt werden, dass die BAFzA als Auftraggeber die datenschutzrechtlichen Kontrollrechte gegenüber dem Dienstleister ausübt und dies nicht dem Dienstleister selbst überlässt.

4. 25. TB Nr. 6.6.1 **Schwierigkeiten beim gemeinsamen Vollstreckungsportal der Länder**

Im 25. Tätigkeitsbericht hatte ich über die geplante Änderung der Schuldnerverzeichnisführungsverordnung (SchuFV) berichtet. Zwischenzeitlich ist die Änderung der Verordnung zum 1. Oktober 2015 in Kraft getreten. Die von mir vorgeschlagene Möglichkeit, bei Verwechselungsgefahr einen Warnhinweis anbringen zu lassen, wurde zu meinem Bedauern nicht aufgegriffen.

Die geänderten Suchkriterien nach § 8 SchuFV werde ich künftig unter meiner Beteiligung zu überprüfen. Ich werde die Überprüfung aktiv begleiten und anschließend prüfen, welche datenschutzrechtlichen Konsequenzen aus dem Ergebnis zu ziehen sind.

5. 24. TB Nr. 12.1.3.7. **Übermittlung von Sozialdaten an Vermieter**

Ich hatte bereits im 24. Tätigkeitsbericht über die unzulässige Praxis verschiedener Jobcenter berichtet, bei der Bewilligung von Arbeitslosengeld II den Leistungsempfänger zu verpflichten, vom jeweiligen Vermieter eine Bescheinigung über seine Mietwohnung ausfüllen oder sogar mit Unterschrift bestätigen zu lassen. Hierbei werden dem Vermieter in unzulässiger Weise Sozialdaten bekannt. Zwar benötigt ein Jobcenter zur Berechnung der Leistungen für Unterkunft und Heizung die jeweils erforderlichen Daten; als Nachweis für die Mietkosten kommen jedoch bereits der Mietvertrag sowie Unterlagen über Neben-, Heiz- und sonstige Kosten in Betracht. Auch weitere Angaben zur Wohnung müssen nicht beim Vermieter selbst erhoben werden.

Leider musste ich im aktuellen Berichtszeitraum feststellen, dass sich einzelne Jobcenter weiterhin über diese Vorgaben hinwegsetzen. Deshalb habe ich bei Eingaben zu diesem Thema und bei Besuchen vor Ort einzelfallabhängig das Vorgehen der Jobcenter geprüft und bewertet. Erfreulicherweise wurden aufgrund meiner Interventionen unzulässige Verfahrensweisen umgestellt.

Durch wiederholte Hinweise im Einzelfall stelle ich nunmehr eine hohe Bereitschaft der Jobcenter fest, die von mir vertretene Rechtsauffassung bundesweit anzunehmen. Die Durchsetzung meiner datenschutzrechtlichen Auffassung und die Sensibilisierung der Jobcenter waren mir im vergangenen Be-

richtszeitraum ein wichtiges Anliegen, das ich auch zukünftig weiter verfolgen werde. Gleichzeitig möchte ich an dieser Stelle erneut auf die Eigenverantwortung jedes Jobcenters hinweisen, nur die jeweils erforderlichen Daten zu erheben und Datenübermittlungen an Dritte nicht über Mitwirkungspflichten zu erzwingen.

6. 25. TB Nr. 9.2.1 **Die JOBBÖRSE der Bundesagentur für Arbeit**

Die BA hat Vermittlungsvorschläge in Arbeitgeber-Accounts in der JOBBÖRSE nicht gelöscht, obwohl ein Zugriff der Arbeitgeber auf die Kontaktdaten und beruflichen Werdegänge der Bewerber nicht mehr erforderlich war. Die BA hatte seinerzeit mitgeteilt, umgehend für Abhilfe sorgen zu wollen. Die notwendigen technischen Änderungen wurden von der BA leider erst im April 2016 umgesetzt, obwohl mir dies für April 2015 zugesagt worden war. Diese nicht gerechtfertigte Verzögerung habe ich nach § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG als Verstoß gegen die Vorschriften §§ 67b Absatz 1, 67c Absatz 1 SGB X beanstandet. Inzwischen wurde der festgestellte Datenschutzverstoß durch die BA beseitigt.

7. 24. TB Nr. 12.2.3 **Gesundheitsdaten bei den Agenturen für Arbeit**

Beantragt eine Arbeitnehmerin oder ein Arbeitnehmer Arbeitslosengeld, müssen die Fachkräfte der Agenturen für Arbeit neben den beruflichen Kenntnissen und Fähigkeiten auch gesundheitliche Einschränkungen berücksichtigen. Dazu ist die Erhebung von Gesundheitsdaten notwendig, die sensible persönliche Daten i. S. d. § 67 Absatz 12 SGB X darstellen. Wie ich berichtet habe, bestand zwischen der BA und mir Uneinigkeit darüber, welche Angaben die Antragsteller machen müssen, um ihre Mitwirkungspflichten aus §§ 60 ff. SGB X zu erfüllen.

Inzwischen habe ich mich in dieser Frage mit dem Bundesministerium für Arbeit und Soziales und der BA geeinigt. Um die gesundheitlichen Einschränkungen strukturiert zu erfassen und dem Ärztlichen Dienst der BA eine erste Einschätzung der Einschränkungen zu ermöglichen, muss zunächst ein Gesundheitsfragebogen ausgefüllt werden. Anschließend gibt es verschiedene Möglichkeiten, die Auswirkungen der vorgetragenen gesundheitlichen Einschränkungen auf die berufliche Eingliederung zu ermitteln. Entweder müssen die behandelnden Ärzte von der Schweigepflicht entbunden oder die Unterlagen müssen dem Ärztlichen Dienst übermittelt werden oder die Person muss sich beim Ärztlichen Dienst untersuchen lassen. Füllen die Antragsteller bereits den Gesundheitsfragebogen nicht aus, liegt in der Regel eine Verletzung der Mitwirkungspflicht vor, so dass gemäß § 66 Absatz 1 SGB I Leistungen entzogen bzw. versagt werden können. Verweigern die Antragsteller eine weitere Mitwirkungsleistung, muss die Agentur für Arbeit jeden Einzelfall gesondert betrachten und entscheiden, ob nicht eine andere Möglichkeit besteht, den Gesundheitsstatus zu bestimmen.

Die BA hat bereits 2015 zugesagt, ihren Praxisleitfaden für die Mitarbeiter der BA zur Einschaltung des Ärztlichen Dienstes und das zum Gesundheitsfragebogen gehörige Informationsblatt für die Antragsteller entsprechend anzupassen. Die Veröffentlichung des neuen Leitfadens liegt nun endlich vor. Ich erwarte, dass die BA auch das Informationsblatt schnellstmöglich neu fasst.

8. 25. TB Nr. 13.10 **Fehlende Löschkonzepte bei gesetzlichen Krankenkassen**

In meinem 25. Tätigkeitsbericht habe ich auf fehlende Löschkonzepte bei einer Vielzahl gesetzlicher Krankenkassen hingewiesen. Durch meine Ankündigung, eine Missachtung von datenschutzrechtlichen Regelungen aufgrund fehlender Konzepte oder technische Anwendungen zukünftig zu beanstanden, konnte ich erreichen, dass die Erstellung und Umsetzung von Löschroutinen auf der Prioritätenliste der Krankenkassen nach oben gerückt ist. Deswegen haben die beiden größten IT-Dienstleister im Segment der gesetzlichen Krankenversicherung für ihre Kunden Softwarelösungen entwickelt, die die von mir geforderten Löschkomponenten enthalten. Da den Krankenkassen bei der individuellen Implementie-

rung der Software jedoch ein gewisser Spielraum verbleibt, werde ich den Fortgang des Umsetzungsprozesses bei den einzelnen Kassen im Blick behalten und mahne in dieser Hinsicht weiterhin zur Eile.

9. 25. TB Nr. 9.4 **Wie viele Daten dürfen für Projekte des Europäischen Sozialfonds erhoben werden?**

Über meine datenschutzrechtlichen Erfahrungen auf diesem Gebiet habe ich in meinem letzten Tätigkeitsbericht berichtet und dabei vor allem kritisiert, dass auch die Situation des Haushalts („household situation") eines Teilnehmenden verpflichtend abgefragt wird. Hier werden Merkmale Dritter erhoben, die nicht im Zusammenhang mit der eigentlichen ESF-Förderung stehen. Das Bundesministerium für Arbeit und Soziales (BMAS) hat diese Problematik an die Europäische Kommission herangetragen. Diese hat die Bedenken aufgegriffen und vorgeschlagen, die Datenerhebung der Haushaltsangehörigen nur noch stichprobenartig durchzuführen. Dies halten sowohl das BMAS als auch ich noch nicht für ausreichend. Das BMAS setzt sich daher weiterhin für eine vollständige Streichung der Datenerhebung der Haushaltssituation ein.

10. 25. TB Nr. 9.5 **Ist die Regelung zur wissenschaftlichen Forschung im SGB X noch zeitgemäß?**

In meinem 25. Tätigkeitsbericht hatte ich auf den Modernisierungsbedarf bei § 75 SGB X hingewiesen, der aus dem Bereich der Wissenschaft und Forschung an mich herangetragen worden war. Im Berichtszeitraum hatten die maßgeblichen Bundesministerien für Arbeit und Soziales, für Gesundheit und für Bildung und Forschung eine Arbeitsgruppe eingerichtet, an der ich beteiligt war und die sich mit dem Zugang zu Sozialdaten bei den gesetzlichen Sozialversicherungen, für die Wissenschaft auseinandergesetzt hat. Man war sich einig, dass die Regelung an die heutigen Gegebenheiten angepasst werden muss. Bedauerlicherweise lag am Ende des Berichtszeitraums aber noch kein Entwurfstext vor, an dem man hätte weiterberaten können.

11. 25. TB Nr. 5.16 **Eurodac**

Mit dem Namen „Eurodac" wird eine gemeinsame Datenbank für Fingerabdrücke von Asylbewerbern und in der EU aufgegriffenen illegalen Einwanderern bezeichnet. Sie wird derzeit von den 28 Mitgliedstaaten der EU sowie von Island, Norwegen, Liechtenstein und der Schweiz genutzt. Die Verarbeitung personenbezogener Daten im Zentralsystem der Datenbank einschließlich der Übermittlung von Daten daraus an die Mitgliedstaaten überwacht der Europäische Datenschutzbeauftragte (EDPS). Die Datenschutzbehörden in den Mitgliedstaaten kontrollieren die Verarbeitung von Daten durch die einzelstaatlichen Behörden sowie die Übermittlung dieser Daten an die Zentraleinheit. Um einen gemeinsamen Ansatz bei der Datenschutzkontrolle zu gewährleisten, versammeln sich der EDPS und Vertreter der Aufsichtsbehörden aus den Anwenderstaaten mindestens zweimal pro Jahr in einer gemeinsamen Gruppe zur Koordination der Datenschutzaufsicht. An den Beratungen und Tätigkeiten dieser Gruppe nehme ich regelmäßig teil.

Im September 2015 organisierte die gemeinsame Gruppe einen Besuch bei der Europäischen Agentur für IT-Großsysteme oder euLISA, bei der Eurodac geführt wird. Dabei wurden keine schweren Verstöße gegen datenschutzrechtliche Vorschriften festgestellt. Gleiches gilt für einen weiteren Besuch im Oktober 2016. Der abschließende Bericht dazu steht allerdings noch aus.

Des Weiteren überabeitete die Gruppe den standardisierten Inspektionsplan für die nationalen Zugangsstellen zu Eurodac, der den Datenschutzbehörden als Hilfsmittel für die vorgeschriebenen Kontrollen des Eurodac-Systems auf nationaler Ebene dienen soll.

Zudem befasste sich die Gruppe mit dem Vorschlag der Europäischen Kommission vom 4. Mai 2016 zur Neufassung der Eurodac-Verordnung (KOM(2016) 272 endgültig). In einer Stellungnahme an die Europäische Kommission, den Rat der Europäischen Union und das Europäische Parlament bemängelte sie insbesondere die Ausweitung der Nutzungszwecke, die Möglichkeit der Erhebung von alphanumeri-

schen und biometrischen Daten einschließlich Fotos, die Absenkung der Altersgrenze zur Erhebung biometrischer Daten bei Kindern auf sechs Jahre, die Nutzung personenbezogener Daten zu Testzwecken, den Datenaustausch mit Drittländern zum Zwecke der Rückführung sowie die vorgesehenen Speicherfristen von fünf Jahren. Zudem werden Zweifel an der Notwendigkeit des Abgleichs durch Strafverfolgungsbehörden geäußert, da diese Möglichkeit bisher kaum genutzt wurde (vgl. o. Nr. 10.3.3).

12. 25. TB Nr. 5.17 **Europäisches Visa-Informationssystem**

Die mehrjährige Phase des „Roll-Out" des europäischen Visa-Informationssystems (VIS) wurde im Berichtszeitraum abgeschlossen, nachdem Ende 2015 auch die Auslandsvertretungen der EU-Staaten in der Ukraine und der Russische Föderation miteinbezogen wurden. Begonnen hatte der Roll-Out im Oktober 2011 mit der Region Persischer Golf.

Als gemeinsame europäische Datenbank verfolgt das VIS den Zweck, Doppel-Vergaben von Kurzzeitvisa zu vermeiden und die Zusammenarbeit der teilnehmenden Staaten im Rahmen der gemeinsamen Visa-Politik zu erleichtern. Ähnlich wie andere europäische Datenbanken, z. B. Eurodac (vgl. Nr. 22.11), besteht das VIS aus einer zentralen Einheit, die von der Europäischen Agentur für IT-Großsysteme (euLISA) in Tallinn betrieben wird, und aus den nationalen Komponenten der Teilnehmerstaaten. Zum Ende des Berichtszeitraums nehmen die EU-Staaten (außer Großbritannien, Irland, Bulgarien, Rumänien, Kroatien und Zypern) sowie Norwegen, Liechtenstein, Island und die Schweiz an dem europäischen VIS als Teilbereich des „Schengen-Acquis", dem Bestand der Rechtsvorschriften für den Schengen-Raum, teil.

Die Datenschutzaufsicht über das VIS folgt dem Modell der koordinierten Kontrolle: 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 die Anwendung des VIS verantwortlich sind. Um die Arbeit und die Kontrollschwerpunkte in den Mitgliedstaaten aufeinander abzustimmen, existiert eine gemeinsame Kontrollaufsichtsgruppe - derzeit unter Vorsitz Italiens -, die sich mindestens zweimal jährlich trifft und an deren Beratungen und Aktivitäten ich regelmäßig teilnehme. Neben einem Informationsbesuch bei der euLISA hat die Datenschutzgruppe im Berichtszeitraum die Anwendung der Betroffenenrechte in den VIS-Teilnehmerstaaten ausgewertet und weiterhin die Problematik des Einsatzes externer Dienstleister bei der Visumvergabe an den Auslandsvertretungen untersucht. Letzteres war auch Gegenstand meines Kontrollbesuches an den deutschen Auslandsvertretungen in Dubai und in Abu Dhabi in den Vereinigten Arabischen Emiraten (vgl. o. Nr. 4.2). In Bezug auf die zentrale technische Einheit des VIS hat der EDPS im Sommer 2016 einen Kontrollbesuch durchgeführt.

Zudem wurde ich im Berichtszeitraum in die Schengen-Evaluierung Deutschlands miteinbezogen, die durch Vertreter der europäischen Kommission im Sommer 2015 vorgenommen worden ist (vgl. Nr. 2.3.3). Gegenstand der Evaluierung war dabei auch die Einhaltung der Vorschriften der Verordnung über das europäische VIS. In diesem Zusammenhang habe ich über meine Kontrollen und Erfahrungen hinsichtlich der Gewährleistung des Datenschutzes durch die Anwenderbehörden des VIS in Deutschland sowie durch die deutschen Auslandsvertretungen berichtet.

13. 25. TB Nr. 14.6 **E-Call - Leben retten dank personenbezogener Daten**

Der Einbau des sog. E-Call-Systems ist aufgrund einer Änderung der EU-Typgenehmigungsvorschriften ab dem 31. März 2018 verpflichtend für alle neu entwickelten PKW und leichten Nutzfahrzeuge.

Die entsprechende EU-Verordnung wurde im April 2015 durch das Europäische Parlament beschlossen. Im Verlauf des Verordnungsverfahrens wurden die datenschutzrechtlichen Regelungen verschärft, damit die Fahrzeuge aufgrund der E-Call-Technologie nicht ständig verfolgbar sind und die Bildung von Bewegungsprofilen ausgeschlossen ist. Daher wird nur im Falle eines tatsächlichen Unfalls ausschließlich ein Minimaldatensatz übermittelt, der lediglich Informationen zum Fahrzeugtyp, der Art des Treibstoffs, dem Unfallzeitpunkt, der Fahrzeugposition und zur Anzahl der Insassen enthalten darf. Dies begrüße ich nachdrücklich.

Die Hersteller müssen gewährleisten, dass die E-Call-Technologie die vollständige und dauerhafte Löschung aller Daten erlaubt. Der übermittelte Datensatz darf von den Notdiensten und ihren Dienstleistern ohne ausdrückliche vorherige Genehmigung der betroffenen Person nicht an Dritte weitergegeben werden.

Der Aufbau der E-Call-Infrastruktur liegt in der Verantwortung der Bundesländer und soll bis zum 1. Oktober 2017 abgeschlossen sein.

Anlage 1

Übersicht über die durchgeführten Beratungs- und Kontrollbesuche

Auswärtiges Amt
- Zentrale
- Auslandsvertretungen

Bundeskanzleramt
- Bundesnachrichtendienst (3)

Bundesministerium des Innern
- Bundesverwaltungsamt (2) (Begleitung bei Termin mit Fr. BfDI und Infobesuch AZR)
- Fachliche Leitstelle Nationales Waffenregister
- Bundesamt für Migration und Flüchtlinge (2) (Zentrale und Bearbeitungsstraße Freilassing)
- Technisches Hilfswerk
- Bundeszentrale für politische Bildung
- Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
- Statistisches Bundesamt
- Bundesamt für Verfassungsschutz (2)
- Bundeskriminalamt (4)
- Bundespolizei (2)

Bundesministerium für Verkehr und digitale Infrastruktur
- Der Deutsche Wetterdienst (DWD)
- Kraftfahrt-Bundesamt
- Bundesamt für Güterverkehr
- Bundesanstalt für Straßenwesen

Bundesministerium für Ernährung und Landwirtschaft
- Bundesamt für Risikobewertung

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit
- Ministerium
- Bundesamt für Strahlenschutz

Bundesministerium der Finanzen
- Bundesanstalt für Immobilienaufgaben
- Bundesfinanzdirektion Südwest
- Hauptzollamt Darmstadt (Organisation Kontrolle Mindestlohn)
- Bundesamt für zentrale Dienste und offene Vermögensfragen
- Deutsche Bundesbank
- Zollkriminalamt (1)

Bundesministerium der Verteidigung
- Kommando Sanitätsdienst der Bundeswehr
- Bundesamt für das Personalmanagement der Bundeswehr
- Institut für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr
- Bundeswehr
- Militärischer Abschirmdienst (1)

Bundesministerium für Arbeit und Soziales
- 11 Jobcenter (Landkreis Starnberg, Frankfurt am Main, Merzig-Wadern, Mannheim, Stormarn, Düsseldorf, Ulm, Stadt Kassel, Region Hannover, Leipzig, Landkreis Ahrweiler)
- Bundesagentur für Arbeit (Zentrale - Verfahren APOLLO)
- Bundesagentur für Arbeit (Regionaldirektion Hessen)
- Bundesagentur für Arbeit (Agentur für Arbeit Saarland einschließlich Service Center Ludwigshafen am Standort Saarlouis)
- Bundesagentur für Arbeit (Servicecenter Mönchengladbach)

Bundesministerium für Gesundheit
- GKV Spitzenverband
- Bundesversicherungsamt
- Gemeinsamer Bundesausschuss
- Deutsches Institut für Medizinische Dokumentation und Information (DIMDI)
- Zentralinstitut für die kassenärztliche Versorgung in Deutschland (ZI)

Bundesministerium für Justiz und Verbraucherschutz
- Bundesverwaltungsgericht
- Deutsches Patent- und Markenamt

Bundesministerium für Familie, Senioren, Frauen und Jugend
- Bundesamt für Familie und gesamtgesellschaftliche Aufgaben
- Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs (UBSKM)
- Conterganstiftung für behinderte Menschen

Beauftragte der Bundesregierung für Kultur und Medien
- Behörde des Bundesbeauftragten für die Stasi-Unterlagen
- Bundesarchiv

Telekommunikationsunternehmen
- Telefónica Germany GmbH & Co. OHG
- Simyo (Telefónica Germany GmbH & Co. OHG)
- Global Star Communications GmbH
- KEVAG Telekom GmbH

- sipgate GmbH
- yourfone AG
- 1&1 Telecom GmbH
- Deutsche Telekom AG
- Turkcell Europe (Telekom Deutschland Multibrand GmbH)
- Fonic GmbH (Telefónica Germany GmbH & Co. OHG)
- Tele Columbus AG
- mobilcom-debitel GmbH
- 1&1 Internet AG
- NetCologne Gesellschaft für Telekommunikation mbH
- Tchibo Mobilfunk GmbH & Co. KG
- 3M Services GmbH
- Unitymedia GmbH
- R-KOM GmbH & Co. KG, R-KOM Regensburger Telekommunikationsgesellschaft mbH & Co. KG
- Mentana-Claimsoft GmbH
- bn:t Blatzheim Networks Telecom GmbH
- Posteo e.K.

Postdienstunternehmen
- Deutsche Post AG
- PIN Mail AG
- MAILCATS oHG
- Hermes Germany GmbH
- DPD Dynamic Parcel Distribution GmbH & Co. KG
- General Logistic Systems Germany GmbH & Co. OHG

Sonstige Behörden
- GKV-Spitzenverband
- BKK actimoda (Aachen)
- HKK (Handelskrankenkasse) Bremen
- VIACTIV BKK (Oberhausen/Bochum)
- IKK gesund plus
- Fa. Bitmark GmbH
- Knappschaft-Bahn-See
- Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG)
- Berufsgenossenschaft Nahrungsmittelung Gastgewerbe (BGN)
- Deutsche Rentenversicherung Bund
- Nationale Kohorte e. V.
- NAKO Biorepositorium bei Helmholtz-Zentrum München
- Studienzentrum im Helmholtz-Zentrum Augsburg
- ein Hauptzollamt in Süddeutschland (Beschäftigtendatenschutz 2015)
- Auswärtiges Amt (Beschäftigtendatenschutz 2015)

Anlage 2

Übersicht über Beanstandungen nach § 25 BDSG

Auswärtiges Amt

Beanstandung gegenüber dem Auswärtigen Amt wegen fehlender Verfahrensverzeichnisse gem. §§ 4d und 4e BDSG (vgl. Nr. 4.2).

Bundeskanzleramt

Bei einer Kontrolle des BND wurden mehrere schwerwiegende Rechtsverstöße festgestellt (vgl. Nr. 10.3.6).

Bundesministerium des Innern

- Bei einer Kontrolle des BfV wurden gemäß § 25 Absatz 1 Satz 1 Bundesdatenschutzgesetz (BDSG) i. V. m. § 24 Absatz 4 Satz 1 BDSG die unzureichende Unterstützung sowie gemäß § 25 Absatz 1 Satz 1 BDSG i. V. m. § 24 Absatz 4 Satz 1 BDSG i. V. m. § 3 Absatz 3 Antiterrordateigesetz Verstöße gegen die gesetzlich vorgeschriebene Kennzeichnungspflicht beanstandet (vgl. Nr. 10.3.5).

- Gegenüber dem Bundesministerium wegen nicht rechtzeitiger Antwort auf eine Bitte um Übersendung von Unterlagen durch die Bundespolizei (gemäß § 25 Abs. 1 BDSG als Verstoß gegen § 24 Abs. 4 Satz 1 und 2 BDSG i. V. m. § 37 BPolG).

Bundesministerium für Arbeit und Soziales

Praxis eines Jobcenters bei der Erhebung und Speicherung von Kontendaten im Rahmen der Leistungsbewilligung nach dem SGB II. Bei Weiterbewilligungsanträgen wurden die vollständigen Kontoauszüge sämtlicher Konten aller Bedarfsgemeinschaftsmitglieder für den vergangenen Bewilligungszeitraum von sechs Monate angefordert. Schon in meinem 24. Tätigkeitsbericht habe ich die Anforderung von Kontoauszügen bei der Beantragung von Leistungen nach dem SGB II regelmäßig für einen zurückliegenden Zeitraum von drei Monaten bei Erst- und Folgeanträgen sowie einmaligen Leistungen für zulässig erklärt (vgl. Urteile des BSG vom 19.09.2008, Az. B 14 AS 45/07 R und 19.02.2009, B 4 AS 10/09 R), (vgl. Nr. 3.3.2).

Die BA hat Vermittlungsvorschläge in Arbeitgeber-Accounts in der JOBBÖRSE nicht gelöscht, obwohl ein Zugriff der Arbeitgeber auf die Kontaktdaten und beruflichen Werdegänge der Bewerber nicht mehr erforderlich war. Darüber hatte ich berichtet (vgl. 25. TB Nr. 9.2.1) und in Aussicht gestellt, die BA würde umgehend für Abhilfe sorgen. Leider hat die BA die notwendigen technischen Änderungen erst im April 2016 umgesetzt, obwohl mir dies für April 2015 zugesagt worden war. Diese nicht gerechtfertigte Verzögerung habe ich nach § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG als Verstoß gegen die Vorschriften §§ 67b Absatz 1, 67c Absatz 1 SGB X beanstandet. Inzwischen wurde der festgestellte Datenschutzverstoß durch die BA beseitigt (vgl. Nr. 22.6).

Bundesministerium der Finanzen

Beim ZKA wurde festgestellt, dass die für Speicherungen notwendigen Negativprognosen nicht dokumentiert wurden (vgl. Nr. 10.3.2) (gemäß § 25 Abs. 1 BDSG als Verstoß gegen §§ 8 Abs. 2, 11 Abs. 2 Satz 3 BKAG).

Telekommunikationsunternehmen

Deutsche Telekom AG

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

Turkcell Europe (Telekom Deutschland Multibrand GmbH)

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

Fonic GmbH (Telefónica Germany GmbH & Co. OHG)

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

TÜRK TELEKOM mobile (Telefónica Germany GmbH & Co. OHG)

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

Tele Columbus AG

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

mobilcom-debitel GmbH

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

1&1 Internet AG

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

NetCologne Gesellschaft für Telekommunikation mbH

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

Tchibo Mobilfunk GmbH & Co. KG

Verstoß gegen §§ 4, 4a BDSG gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG.

Beanstandung wegen nicht-datenschutzkonformer Umsetzung der Einwilligung zur Gesprächsaufzeichnung von Kundengesprächen bei Callcentern (vgl. Nr. 17.3.2).

O2 Shop Bad Hersfeld (Telefónica Germany GmbH & Co. OHG)

Beanstandung gemäß § 115 Abs. 4 Telekommunikationsgesetz i. V. m. § 25 Abs. 1 BDSG (vgl. Nr. 17.3.1).

Martens Deutsche Telekabel GmbH

Beanstandung gemäß § 24 Abs. 4 BDSG i. V. m. § 25 Abs. 1 BDSG wegen mangelnder Unterstützung.

Gesetzliche Krankenkassen

- nach § 81 Abs. 4 SGB X i. V. m. § 25 Abs. 1 BDSG wegen der gleichzeitigen Nutzung von Räumlichkeiten der gesetzlichen Krankenkasse (BARMER GEK) und eines privaten Versicherungsunternehmens (HUK Coburg) der sogenannte „Kostenerstattung aus einer Hand“ wegen Verstoßes gegen § 25 Abs. 1 SGB I sowie § 78a nebst der Anlage hierzu.

- nach § 81 Abs. 4 SGB X i. V. m. § 25 Abs. 1 BDSG wegen der Durchführung von Fallmanagement-Programmen ohne Rechtsgrundlage wegen Verstoßes gegen § 284 Abs. 1 SGB V.

- nach § 81 Abs. 4 SGB X i. V. m. § 25 Abs. 1 BDSG wegen des praktizierten Umschlagverfahrens und die in diesem Zusammenhang stehende Datenerhebung, -verarbeitung und -nutzung wegen Verstoßes gegen § 276 Abs. 2 SGB V.

Gesetzliche Unfallversicherungsträger

- nach § 81 Abs. 4 SGB X i. V. m. § 25 Abs. 1 BDSG wegen der unzulässigen Übermittlung von Versicherungsdaten an private Stellen wegen Verstoßes gegen § 35 Abs. 1 SGB I.

Anlage 3

Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)

Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge

Vorbemerkung

Bereits heute benötigt und produziert das moderne Kraftfahrzeug eine Vielzahl an Daten. Aufgrund der fortschreitenden informationstechnischen Ausstattung der Kraftfahrzeuge und deren Anbindung an das Internet sowie der Vernetzung der Verkehrsteilnehmer untereinander wird sich dieser Trend fortsetzen und in den kommenden Jahren zu weitreichenden Veränderungen im Straßenverkehr führen. Darüber hinaus entstehen zahlreiche neue Fahrzeugfunktionen und Verkehrstelematikanwendungen, z. B. in den Bereichen Service und Multimedia. Die Digitalisierung und insbesondere die Vernetzung bergen neben den unbestreitbaren Vorteilen für die Verkehrssicherheit und den Komfort zugleich auch Risiken für die Persönlichkeitsrechte der Fahrzeugnutzer. Vor diesem Hintergrund halten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder und der VDA nachfolgende datenschutzrechtliche Aspekte für besonders relevant[1].

1. **Personenbezogenheit:** Bei der Nutzung eines modernen Kraftfahrzeugs wird permanent eine Vielzahl von Informationen erzeugt und verarbeitet. Insbesondere bei Hinzuziehung weiterer Informationen können die anfallenden Daten auf den Halter oder auch auf den Fahrer und Mitfahrer zurückführbar sein und Informationen über persönliche oder sachliche Verhältnisse einer bestimmbaren Person enthalten. Die bei der Kfz-Nutzung anfallenden Daten sind jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes (BDSG), wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.

2. Entscheidend ist der **Zeitpunkt der Datenerhebung** durch eine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Hier ist zu unterscheiden, ob es sich um Kraftfahrzeuge handelt, bei denen eine Datenspeicherung innerhalb des Fahrzeuges stattfindet („offline"), oder ob eine Übermittlung von Daten aus dem Fahrzeug heraus erfolgt („online"), wie etwa bei der Übermittlung und Speicherung von Fahrzeugdaten auf Backend-Servern.

   Bei „Offline"-Autos ist von einer Datenspeicherung ohne vorherige Erhebung auszugehen. Eine Erhebung liegt mangels Erfüllung des Tatbestandes des § 3 Abs. 3 BDSG nicht vor; gleichwohl fallen anlässlich der Kfz-Nutzung Daten an, die im Fahrzeug abgelegt werden. Diese Daten müssen geschützt werden und machen - vergleichbar der Regelung in § 6c BDSG (Mobile personenbezogene Speicher- und Verarbeitungsmedien) - auch eine Sicherung des Rechts auf informationelle Selbstbestimmung erforderlich. Erst wenn die im Fahrzeug abgelegten Daten z. B. von einer Werkstatt für Reparaturzwecke ausgelesen werden, kommt es zu einer Erhebung durch eine verantwortliche Stelle nach § 3 Abs. 3 BDSG.

   Bei „Online"-Autos findet bereits im Zeitpunkt der Datenkommunikation aus dem Fahrzeug heraus eine Erhebung durch eine verantwortliche Stelle im Sinne des § 3 Abs. 3 BDSG statt.

3. **Verantwortliche Stelle:** Auch für die Identifikation der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ist zwischen „Offline"- und „Online"-Autos zu differenzieren.

[1] Datenschutzrechtliche Fragestellungen, die sich bei der Besitzüberlassung eines Kfz z. B. im Rahmen eines Dienst- oder Arbeitsverhältnisses oder einer Vermietung ergeben, sind nicht Gegenstand des vorliegenden Papiers.

Bei „Offline“-Autos wird derjenige, der personenbezogene Fahrzeugdaten aus dem Fahrzeug ausliest (d. h. erhebt) und anschließend verarbeitet, zur verantwortlichen Stelle. Hierbei wird es sich in der Regel um Werkstätten handeln.

Auch wenn die Hersteller bei „Offline“-Autos regelmäßig mangels Erhebung nicht bereits beim „Entstehen“ der Daten verantwortliche Stelle sind, trifft diese unter anderem nach dem Gedanken „Privacy by Design“ dennoch eine Verantwortung im Hinblick auf den Datenschutz. Dies gilt insbesondere, weil der Hersteller im Rahmen seiner technischen Gestaltungsmöglichkeiten (Art und Umfang von Schnittstellen, Zugriffsmöglichkeiten, Verfolgung der in § 3a BDSG niedergelegten Grundsätze von Datenvermeidung und -sparsamkeit) Einfluss auf die zeitlich nach hinten verlagerte Erhebung und Verarbeitung hat (vergleichbar der Regelung in § 6c BDSG). Sofern es um die technischen Gestaltungsmöglichkeiten geht, sind die Hersteller auch bei dieser Fahrzeugkategorie als Ansprechpartner für die Datenschutzaufsichtsbehörden anzusehen.

Bei „Online“-Autos sind diejenigen als verantwortliche Stellen anzusehen, die personenbezogene Daten erhalten, d. h. in der Regel die Hersteller und gegebenenfalls dritte Dienste-Anbieter. Insbesondere wenn Hersteller Zusatzdienstleistungen für das Kfz anbieten und dabei in ihren Backend-Servern Daten speichern, sind sie verantwortliche Stelle für diese Datenverarbeitung.

4. Die **Zulässigkeit der Datenerhebung und -verarbeitung** kann sich insbesondere aus § 28 Abs. 1 S. 1 Nrn. 1 oder 2 BDSG, §§ 11 ff. Telemediengesetz oder aus einer Einwilligung ergeben, die den Voraussetzungen des § 4a BDSG genügt.

   Wie die Informationen über Datenerhebungs- und -verarbeitungsvorgänge aufbereitet sein müssen, um Teil des Vertrags oder Grundlage für eine ggf. relevante informierte Einwilligung sein zu können (ausführliche Informationen im Sinne eines Verfahrensverzeichnisses oder strukturierte, überblicksartige Informationen), bleibt Frage des Einzelfalls. Der Erstkäufer kann die notwendigen Informationen jedenfalls vom Verkäufer (Hersteller oder herstellergebundener Händler) erhalten.

   Grundsätzlich sind die wichtigsten Informationen zur Datenverarbeitung in allgemein verständlicher Form auch in der Borddokumentation nachlesbar vorzuhalten, die der Hersteller bereitstellt.

5. Gegenüber dem Hersteller besteht ein unentgeltliches **Auskunftsrecht** des Halters über seine durch den Hersteller erhobenen und gespeicherten personenbezogenen Daten nach § 34 BDSG. Darüber hinaus besteht aus § 34 BDSG kein datenschutzrechtliches Auskunftsrecht des Halters gegenüber dem Hersteller allein aufgrund dessen Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme. Die Fahrzeughalter von „Offline“-Autos haben die Möglichkeit des Auslesens von Daten, ggf. mithilfe von Sachverständigen, was nicht zwingend unentgeltlich sein muss. Aufgrund des Transparenzgebots muss der Betroffene sich unentgeltlich und ohne sachverständige Hilfe über die Grundsätze der Datenverarbeitungsvorgänge einschließlich zumindest der Art der verarbeiteten personenbezogenen Daten beim Hersteller informieren können.

6. In Bezug auf die **Datenhoheit** sollen die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können. Die Automobilhersteller streben an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status‘ vorzusehen. Einschränkungen der Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung

sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist. Vom Nutzer eingegebene Informationen (z. B. Komfortdaten wie Sitzeinstellung, bevorzugte Radiosender, Navigationsdaten, E-Mail-/SMS-Kontaktdaten, etc.) muss der Nutzer jederzeit selbst ändern oder zurückstellen können.

Berlin/Schwerin, 26. Januar 2016

Anlage 4

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6./7. April 2016

Wearables und Gesundheits-Apps - Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).

- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.

- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.

- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.

- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

Anlage 5

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie - wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht - moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

   Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
Kühlungsborn, den 10. November 2016

Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf
Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[5] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift" (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.

- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.

- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.

- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt - entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.

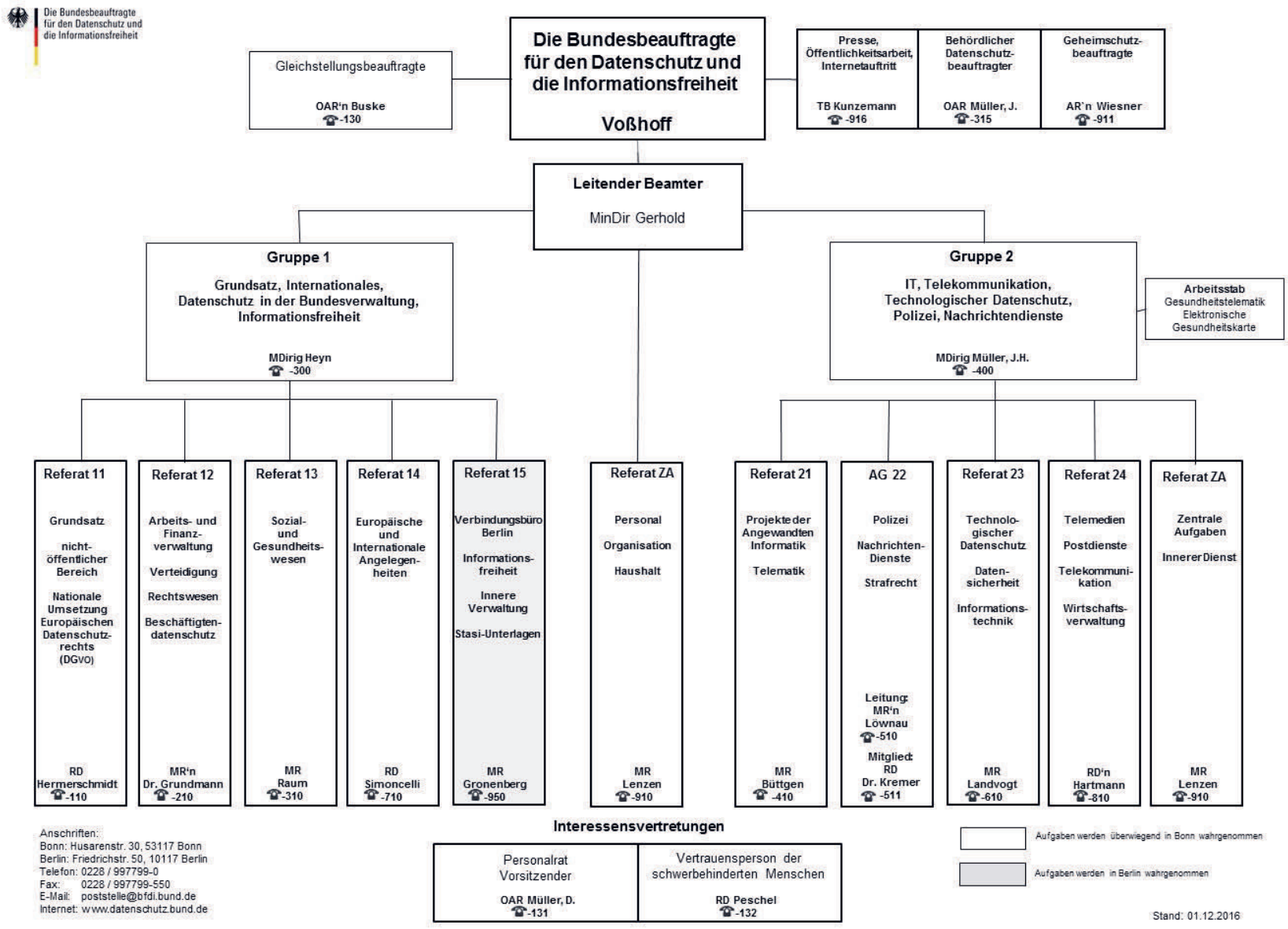
Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.

---

5 bei Enthaltung Hamburg

In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.


Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Gleichstellungsbeauftragte
OAR'n Buske ☎-130
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Voßhoff
Presse, Öffentlichkeitsarbeit, Internetauftritt
TB Kunzemann ☎-916
Behördlicher Datenschutzbeauftragter
OAR Müller, J. ☎-315
Geheimschutzbeauftragte
AR`n Wiesner ☎-911
Leitender Beamter
MinDir Gerhold
Gruppe 1
Grundsatz, Internationales, Datenschutz in der Bundesverwaltung, Informationsfreiheit
MDirig Heyn ☎-300
Gruppe 2
IT, Telekommunikation, Technologischer Datenschutz, Polizei, Nachrichtendienste
MDirig Müller, J.H. ☎-400
Arbeitsstab Gesundheitstelematik Elektronische Gesundheitskarte
Referat 11
Grundsatz
nicht-öffentlicher Bereich
Nationale Umsetzung Europäischen Datenschutzrechts (DGVO)
RD Hermerschmidt ☎-110
Referat 12
Arbeits- und Finanzverwaltung
Verteidigung
Rechtswesen
Beschäftigtendatenschutz
MR'n Dr. Grundmann ☎-210
Referat 13
Sozial- und Gesundheitswesen
MR Raum ☎-310
Referat 14
Europäische und Internationale Angelegenheiten
RD Simoncelli ☎-710
Referat 15
Verbindungsbüro Berlin
Informationsfreiheit
Innere Verwaltung
Stasi-Unterlagen
MR Gronenberg ☎-950
Referat ZA
Personal
Organisation
Haushalt
MR Lenzen ☎-910
Referat 21
Projekte der Angewandten Informatik
Telematik
MR Büttgen ☎-410
AG 22
Polizei
Nachrichtendienste
Strafrecht
Leitung: MR'n Löwnau ☎-510
Mitglied: RD Dr. Kremer ☎-511
Referat 23
Technologischer Datenschutz
Datensicherheit
Informationstechnik
MR Landvogt ☎-610
Referat 24
Telemedien
Postdienste
Telekommunikation
Wirtschaftsverwaltung
RD'n Hartmann ☎-810
Referat ZA
Zentrale Aufgaben
Innerer Dienst
MR Lenzen ☎-910
Interessensvertretungen
Personalrat Vorsitzender
OAR Müller, D. ☎-131
Vertrauensperson der schwerbehinderten Menschen
RD Peschel ☎-132
Aufgaben werden überwiegend in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen
Stand: 01.12.2016
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

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
AnaCredit	Analytical Credit Datasets
AND	Andere Nachrichtendienste
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
AOS	Allianz Ortungs Services GmbH
APAK	Abschlussprüferaufsichtskommission
APEC	Asia Pacific Economic Cooperation
APOK	Anwenderportal Onlinekanal

APOLLO	Antragsportal Leistungen Online
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
BADV	Bundesamt für zentrale Dienste und offene Vermögensfragen
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAföG	Bundesausbildungsförderungsgesetz
BAFzA	Bundesamt für Familie und zivilgesellschaftliche Aufgaben
BAG	Bundesamt für Güterverkehr
BAköV	Bundesakademie für öffentliche Verwaltung
BAMF	Bundesamt für Migration und Flüchtlinge
BAPersBw	Bundesamt für das Personalmanagement der Bundeswehr
BArchG	Bundesarchivgesetz
BASt	Bundesanstalt für Straßenwesen
BAZ	Bundesamt für den Zivildienst

BBG	Bundesbeamtengesetz
BBk	Deutsche Bundesbank
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
BfR	Bundesinstitut für Risikobewertung
BfS	Bundesamt für Strahlenschutz
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BImA	Bundesanstalt für Immobilienaufgaben
BISp	Bundesinstitut für Sportwissenschaft

BIT	Bundesstelle für Informationstechnik des Bundesverwaltungsamts
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
BKM	Beauftragte der Bundesregierung für Kultur und Medien
Bluetooth	Standard für die drahtlose Übermitlung von Sprache und Daten im Nahbereich
BMAS	Bundesministerium für Arbeit und Soziales
BMBF	Bundesministerium für Bildung und Forschung
BMEL	Bundesministerium für Ernährung und Landwirtschaft
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesmeldegesetz
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
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BPolG	Bundespolizeigesetz
BR	Bundesrat
BR-Drs.	Bundesratsdrucksache
BSG	Bundessozialgericht

BSH	Bundesamt für Seeschifffahrt und Hydrographie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BStatG	Bundesstatistikgesetz
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT	Bundestag
BT-Drs.	Bundestagsdrucksache
BTLE	Border, Travel, Law Enforcement
Bufdis	Bundesfreiwilligendienstleistende
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
CAHDATA	Ad-hoc Committee on Data Protection
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
DFIS	Dokumentenfundstelleninformationssystem
DGUV	Deutsche Gesetzliche Unfallversicherung
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
DSAnpUG-EU	Datenschutz-Anpassungs- und Umsetzungs-Gesetz EU
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSL	Digital Subscriber Line
DSGVO	Datenschutz-Grundverordnung

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
EES	Ein- und Ausreiseregister
EETS / EEMD	Europäischer Elektronischer Mautdienst
EG	Europäische Gemeinschaft(en)
eGK	elektronische Gesundheitskarte
EG-ZIS	Europäisches Zollinformationssystem
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EGovG	Gesetz zur Förderung der elektronischen Verwaltung
E-Health-Gesetz	Gesetz für sichere digitale Kommunikation im Gesundheitswesen
EHUG	Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
EHW	ermittlungsunterstützende Hinweise
eID-Funktion	elektronischer Identitätsnachweis, elektronische Identitätsfunktion
EIS	Europäisches Informationssystem
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
ESF	Europäischer Sozialfonds
EStA	Register der Entscheidungen in Staatsangehörigkeitsangelegenheiten
EstG	Einkommensteuergesetz
etc.	ecetera
ETIAS	Reiseinformations- und -genehmigungssystem
eTIN	Lohnsteuerliches Ordnungsmerkmal
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
eu-LISA	europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht
Eurodac	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
Europol	Europäisches Polizeiamt
EUV	Vertrag über die Europäische Union
EVA	Elektronische Verwaltungsakte
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft

EWR	Europäischer Wirtschaftsraum
EZB	Europäische Zentralbank
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
GewO	Gewerbeordnung
GDV	Gesamtverband der Deutschen Versicherungswirtschaft

GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
GewO	Gewerbeordnung
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
GR-J	Berichterstattergruppe Justizielle Zusammenarbeit
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
IT-Sicherheitsgesetz	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
ITZBund	Informationstechnikzentrum Bund
IVBB	Informationsverbund Berlin-Bonn
JI-Rat	Rat der Innen- und Justizminister der Europäischen Union
JI-Richtlinie	Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
KarrC Bw	Karrierecenter der Bundeswehr
KBA	Kraftfahrt-Bundesamt
KdU	**K**osten **d**er **U**nterkunft und Heizung
KEV	Kontrolleinheit Verkehrswege
KDAV	Kundendatenauskunftsverordnung
KFU	Krebsfrüherkennungsrichtlinien
Kfz	Kraftfahrzeug
KGSG	Gesetz zur Neuregelung des Kulturgutschutzrechts
KIWI	Kindergeld-Windows-Implementierung
KOM	Europäische Kommission
KRITIS	Kritische Infrastrukturen
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
NAKO	Nationale Kohorte
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

PGP	Pretty Good Privacy
PHW	personengebundene Hinweise
PIA	Privacy Impact Assessment
PIAV	Polizeilicher Informations- und Analyseverbund
PIN	Persönliche Identifikationsnummer
PIPC	Personal Information Protection Commission
PKGr	Parlamentarisches Kontrollgremium
PMK-Links-Z	Zentraldatei „Politisch motivierte Kriminalität-links“
PNR	Passenger Name Record
Protection Profile	Schutzprofil
PVS	Personalverwaltungssystem
PY	PVS-Komponente Payment
Ratsdok.	Ratskokument (EU)
RatSWD	Rat für Sozial- und Wirtschaftsdaten
RAVPV	Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer
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

s.	siehe
s.o.	siehe oben
s.u.	siehe unten
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuFV	Schuldnerverzeichnisführungsverordnung
SchwarzArbG	Schwarzarbeitsbekämpfungsgesetz
SDM	Standard-Datenschutzmodell
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
SPersAV	Verordnung über die Führung der Personalakten der Soldaten und der ehemaligen Soldaten
STADA	Staatsangehörigkeitsdatei
StAG	Staatsangehörigkeitsgesetz
Stasi	Staatssicherheitsdienst der ehemaligen DDR
StDAV	Steuerdaten-Abruf-Verordnung
StDÜV	Steuerdatenübermittlungsverordnung
STEP	Stammdatenerfassungssystem und Stammdatenpflegesystem
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
TCDP	Trusted Cloud Datenschutz Profil
TFG	Transfusionsgesetz
TFTP	Terrorist Finance Tracking Program
THW	Bundesanstalt Technisches Hilfswerk
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation
TMG	Telemediengesetz
TNB	Teilnehmernetzbetreiber
TOP	Tagesordnungspunkt
TPG	Transplantationsgesetz
TR	Technische Richtlinie
TR TKÜV	Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten
TS	Technology Subgroup
TTIP	Transatlantic Trade and Investment Partnership
u. a.	unter anderem
u. ä.	und ähnliches
UAS	Unmanned Aerial Systems
UBSKM	Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs
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
VBL	Versorgungsanstalt des Bundes und der Länder
VBM	vorläufiges Bearbeitungsmerkmal
VDA	Verband der Automobilindustrie
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
VfB	Vergabestelle für Berechtigungszertifikate
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
VUDat-DV	Verkehrsunternehmensdatei-Durchführungsverordnung
W3C	World Wide Web Consortium
WADA	Welt-Anti-Doping-Agentur
WAP	Wireless Application Protocol
WehrRÄndG	Wehrrechtsänderungsgesetz 2011

WehrMedStatInstBw	Institut für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr
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
ZensVorbG2021	Zensusvorbereitungsgesetz 2021
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
25.	2013 - 2014	18/5300

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 2017

Druck:
Silber Druck oHG
Am Waldstrauch 1
34266 Niestetal

18/12500