Tätigkeitsbericht 2017 – 2018

27. Tätigkeitsbericht

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

27. Tätigkeitsbericht

Dieser Bericht wurde am 8. Mai 2019 dem Präsidenten des Deutschen Bundestages, Herrn Dr. Wolfgang Schäuble, überreicht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Ulrich Kelber

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht 2017 und 2018 zum Datenschutz
– 27. Tätigkeitsbericht –

Inhaltsverzeichnis

Einführung

Der 27. Tätigkeitsbericht umfasst mit den Jahren 2017 und 2018 einen Zeitraum, in dem meine Vorgängerin, Frau Andrea Voßhoff, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit war. Ich möchte mich bei Frau Voßhoff herzlich für ihre wichtige Arbeit bedanken.

Beide Jahre waren in meiner Behörde selbst, bei den Behörden des Bundes, sowie den von mir beaufsichtigten Unternehmen und sonstigen Behörden geprägt von den Vorbereitungen auf die im Mai 2018 wirksam gewordene Datenschutz-Grundverordnung (DSGVO) und den ersten Schritten unter neuem Recht. Schon jetzt wird deutlich, dass sich die DSGVO in kurzer Zeit zu einem Standard entwickelt hat, an dem sich auch andere Weltregionen orientieren, wie die Entwicklungen in Kalifornien, Japan, aber auch das hohe Interesse weiterer Staaten in Lateinamerika und Asien zeigen.

Jetzt geht es darum, die DSGVO in der Praxis um- und durchzusetzen, möglichst einheitlich in Deutschland und in Europa. Staatliche Stellen müssen beim Datenschutz Vorbild sein. Sie dürfen nicht kurzsichtig das Grundrecht der Bürgerinnen und Bürger auf Privatsphäre, informationelle Selbstbestimmung und das Gefühl der Unbeobachtetheit neuen Möglichkeiten zur Erhebung, Verarbeitung und Verknüpfen von Daten unterordnen, weder im Bereich der inneren Sicherheit, noch bei der Erbringung staatlicher Dienstleistungen und auch nicht zur Steuerung von Infrastrukturplanung oder statistischen Zwecken.

Gänzlich erfolgreich wird die DSGVO erst dann zu nennen sein, wenn Gesellschaft und unabhängige Datenschutzaufsichtsbehörden es auf ihrer Grundlage schaffen, den Appetit vor allem der großen Internetgiganten auf die Daten der europäischen Bürgerinnen und Bürger auf das erlaubte, zur Durchführung der angebotenen Dienstleistungen benötigte Maß zu reduzieren. 2017 und 2018 wurde immer deutlicher, in welchem Ausmaß Konzerne wie Facebook gegen europäisches Recht verstoßen und in welchem Maß sie Daten europäischer Bürgerinnen und Bürger auch aus Quellen sammeln, für die sie niemals eine Einwilligung der Betroffenen erhalten haben.

Meine Behörde und ich werden unsere eigenen Kompetenzen in der Aufsicht nutzen, um die Ziele der DSGVO zu erreichen. Wir arbeiten außerdem in der Datenschutzkonferenz mit den Datenschutzaufsichtsbehörden der Bundesländer und im Europäischen Datenschutzausschuss (EDSA) mit den entsprechenden Behörden der anderen EU- und EWR-Staaten eng zusammen. Gerade im EDSA wünsche ich mir dabei eine erhebliche Beschleunigung der Unterbindung und Sanktionierung großer Datenschutzverstöße.

Aktuell hat bereits eine Debatte über eine Novelle der DSGVO begonnen. Aus meiner Sicht muss diese Novelle Lücken beim Datenschutz schließen, z. B. durch klare Vorgaben beim Profiling und beim Scoring, die die Grundlage der Datenverarbeitung darstellen. Ich bin überzeugt, dass man den Aufwand für Bürgerinnen und Bürger, Vereine, sowie kleinere Unternehmen beim Datenschutz durch Veränderung bei den Informations- und Dokumentationspflichten deutlich reduzieren kann, ohne das Datenschutzniveau damit zu senken. Die EU muss außerdem endlich eine ambitionierte E-Privacy-Verordnung zum Schutz der besonders sensiblen Kommunikationsdaten beschließen.

Auch in Deutschland bedarf es weiterer Verbesserungen beim Datenschutz: Wir brauchen ein umfassendes Gesetz zum Schutz der Daten von Beschäftigten sowie Bewerberinnen und Bewerbern. Außerdem benötigt meine Behörde Sanktionsmöglichkeiten bei der Datenschutzaufsicht über die gesetzlichen Krankenkassen (Bußgelder) und die Sicherheitsbehörden (Anordnungen).

Datenschutz dient nicht dem Schutz von Daten, er dient dem Schutz der Grundrechte der Bürgerinnen und Bürger in unserer freiheitlichen Demokratie. Und deswegen gibt es Geschäftsmodelle, die wegen der damit verbundenen Verletzungen der Prinzipien des Datenschutzes in Europa nicht möglich sind und nicht möglich werden dürfen. In der Regel ist Datenschutz

aber nicht Hemmschuh, sondern eher Innovationsquelle, Beschleuniger und Alleinstellungsmerkmal für Produkte und Dienstleistungen. Wenn wir mit „privacy by default“ und „privacy by design“ in Europa und Deutschland Spitzenreiter bei datenschutzkonformen Dienstleistungen und Produkten werden, dann dient das nicht nur unseren Bürgerinnen und Bürgern, sondern ist auch ein wirtschaftlicher Vorteil. Unsere Firmen haben dann in Ländern mit ähnlichen Gesetzen und vor allem in Ländern, wo Bürgerinnen und Bürger solche Gesetze herbeisehnen, aber zunächst nur auf vertrauenswürdige Produkte und Dienstleistungen setzen können, einen großen Wettbewerbsvorsprung.

Bei der Bundesregierung, insbesondere dem Bundesministerium der Finanzen, sowie beim Bundestag, vor allem den berichterstattenden Abgeordneten im Haushaltsausschuss zu meinem Einzelplan 21 möchte ich mich für die deutliche personelle Stärkung des BfDI in den Haushalten 2017, 2018 und 2019 herzlich bedanken. Die zusätzlichen Pflichtkontrollen bei Sicherheitsbehörden, neue gesetzliche Aufgaben für den BfDI, die durch die DSGVO deutlich erhöhte Zahl von Meldungen und Beschwerden, neue und datenschutzrelevante Technologien, sowie die Digitalisierung im Gesundheitssektor, dem Verkehr und bei staatlichen Dienstleistungen machen allerdings auch in den Folgejahren einen weiteren personellen Aufwuchs notwendig.

Ein herzlicher Dank geht an meine Mitarbeiterinnen und Mitarbeiter für ihr großes Engagement und die dabei gezeigte hohe Fachkompetenz. Dieser Tätigkeitsbericht gibt einen Überblick über die Breite der Aufgaben, für die meine Behörde zuständig ist: bei Kontrollen, Beratungen, Information sowie Zusammenarbeit in einer hohen Zahl von Arbeitsgruppen, Kommissionen, Ausschüssen und Organisationen auf nationaler, europäischer und internationaler Ebene.

Zuletzt und besonders herzlich bedanke ich mich bei allen Bürgerinnen und Bürgern, die durch Eingaben und Anfragen mein Haus in die Pflicht genommen haben. Nur wenn Sie Datenschutz für wichtig halten und das auch öffentlich zum Ausdruck bringen, sind wir stark genug, diesen Datenschutz im Alltag durchzusetzen.

Ulrich Kelber

Die Arbeit des BfDI in Zahlen

Allgemeines: Die Arbeit des BfDI in Zahlen

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat vielfältige Aufgaben zu erfüllen. Das Aufgabenspektrum lässt sich auch mit Zahlen verdeutlichen.

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. Aufgrund der durch die DSGVO veränderten Rechtslage sind die statistischen Angaben – nach einem allgemeinen Teil – in zwei Zeiträume aufgeteilt: A. Zeitraum vom 01.01.2017 – 24.05.2018 und B. Zeitraum vom 25.05.2018 – 31.12.2018.

Wen kontrolliere ich?

Zu meinen Aufgaben gehört u. a. die datenschutzrechtliche Kontrolle der öffentlichen Stellen des Bundes, d. h., neben den 28 Obersten Bundesbehörden mit ihren Behörden und Einrichtungen des Geschäftsbereichs (die detaillierte Behördenübersicht finden Sie unter www.bund.de) auch 228 Auslandsvertretungen des Auswärtigen Amtes. Weiter unterstehen meiner Kontrolle 149 bundesunmittelbare Sozialversicherungsträger und deren Spitzenverbände sowie 303 gemeinsame Einrichtungen gemäß § 50 Absatz 2 SGB II (Jobcenter). Seit dem 25. Mai 2018 obliegt mir auch die datenschutzrechtliche Aufsicht über die 26 Landesfinanzbehörden einschließlich der 535 Finanzämter und über Teile der 11.000 kommunalen Steuerämter. Zudem unterliegen in den Bereichen Sabotageschutz und Geheimschutz alle öffentlichen Stellen des Bundes und die Unternehmen, die dem Sicherheitsüberprüfungsgesetz unterfallen, meiner Kontrolle.

Darüber hinaus kontrolliere ich auch die Einhaltung der datenschutzrechtlichen Bestimmungen bei den Anbietern von Post- und Telekommunikationsdienstleistungen. Dies umfasste bis zum Anwendungsbeginn der DSGVO ca. 3.500 Telekommunikations- und ca. 1.000 Postdienstleister. Seit dem 25. Mai 2018 bin ich darüber hinaus auch für die Kontrolle der nicht lizensierten Postdienstleister zuständig, so dass die Gesamtsumme ca. 61.000 beträgt. (vgl. hierzu auch unter Nr. 25.1.4).

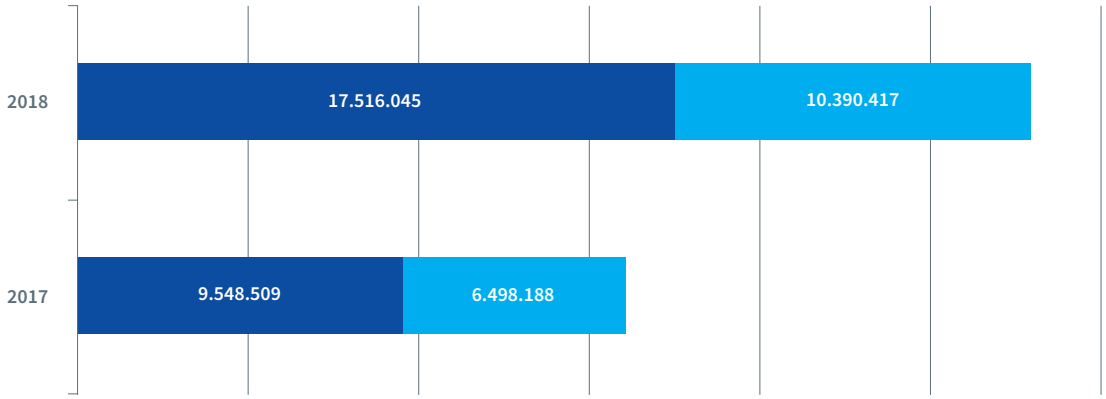
Datenschutzrechtliche Kontrollzuständigkeit des BfDI	
28	Oberste Bundesbehörden
228	Auslandsvertretungen Auswärtiges Amt
149	Sozialversicherungsträger
303	Jobcenter
26	Landesfinanzbehörden
535	Finanzämter
11.000	Kommunale Steuerämter
61.180	Postdienstleister
3.500	Telekommunikationsdienstleister

Zugriffs-/Nutzerzahlen meiner Homepage

Nutzerzahlen

Internet-Browser	Jahr 2017	Jahr 2018
Seitenaufrufe (gesehener Traffic)	9.548.509	17.516.045
Seitenaufrufe (nicht gesehener Traffic)*	6.498.188	10.390.417
Seitenaufrufe gesamt	16.046.697	27.906.462

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



A. Zeitraum vom 01.01.2017 – 24.05.2018 (Rechtsgrundlage BDSG(alt))

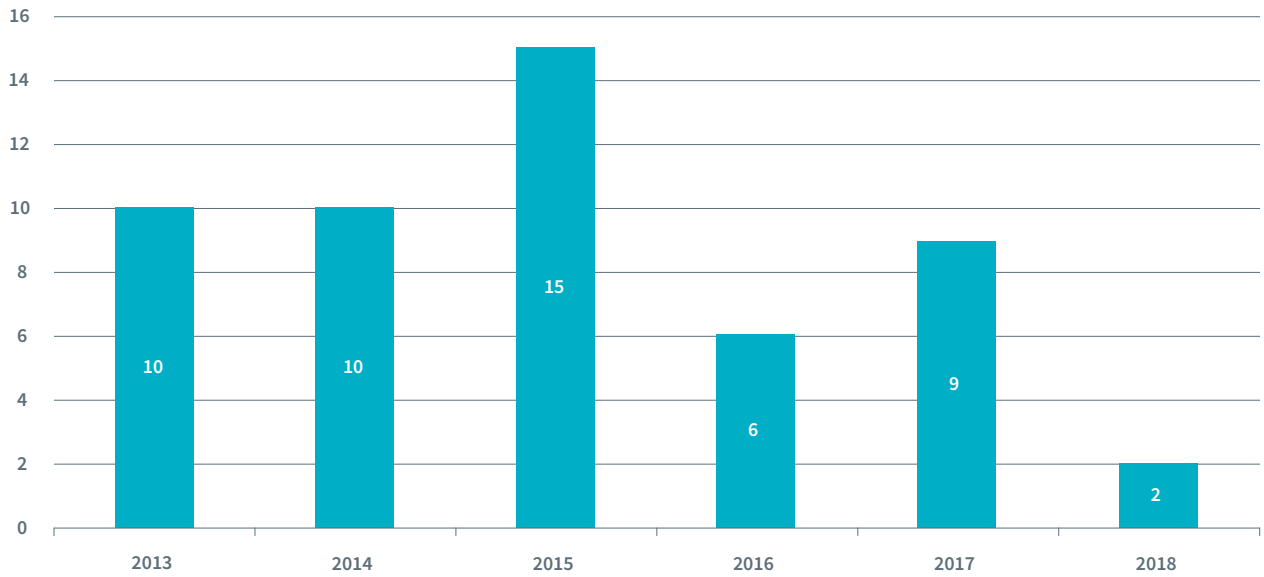
Anzahl der Informations-, Beratungs- und Kontrollbesuche

Im Berichtszeitraum haben meine Mitarbeiterinnen und Mitarbeiter bis zum Anwendungsbeginn der DSGVO 105 Kontrollen bei Behörden und Unternehmen in oft mehrtägigen Besuchen umfassend oder in bestimmten Bereichen beraten und geprüft. Dabei habe ich elfmal erhebliche Mängel festgestellt, die ich förmlich beanstandet habe. Meine Mitarbeiterinnen und Mitarbeiter haben bei Kontrollen das Recht auf Zutritt zu allen Diensträumen sowie das Recht auf Auskunft und auf Einsichtnahme in Unterlagen und gespeicherte Daten und Datenverarbeitungsprogramme.

Berichtszeitraum	Informations-, Beratungs- und Kontrollbesuche
01.01.2018 – 24.05.2018	21
2017	84
2016	97
2015	102
2014	60
2013	59

Berichtszeitraum	Beanstandungen
01.01.2018 – 24.05.2018	2
2017	9
2016	6
2015	15
2014	10
2013	10

Beanstandungen 2013 – 2018



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, jeden gemeldeten Fall zu überprüfen, und gegebenenfalls weitergehende Maßnahmen einzuleiten.

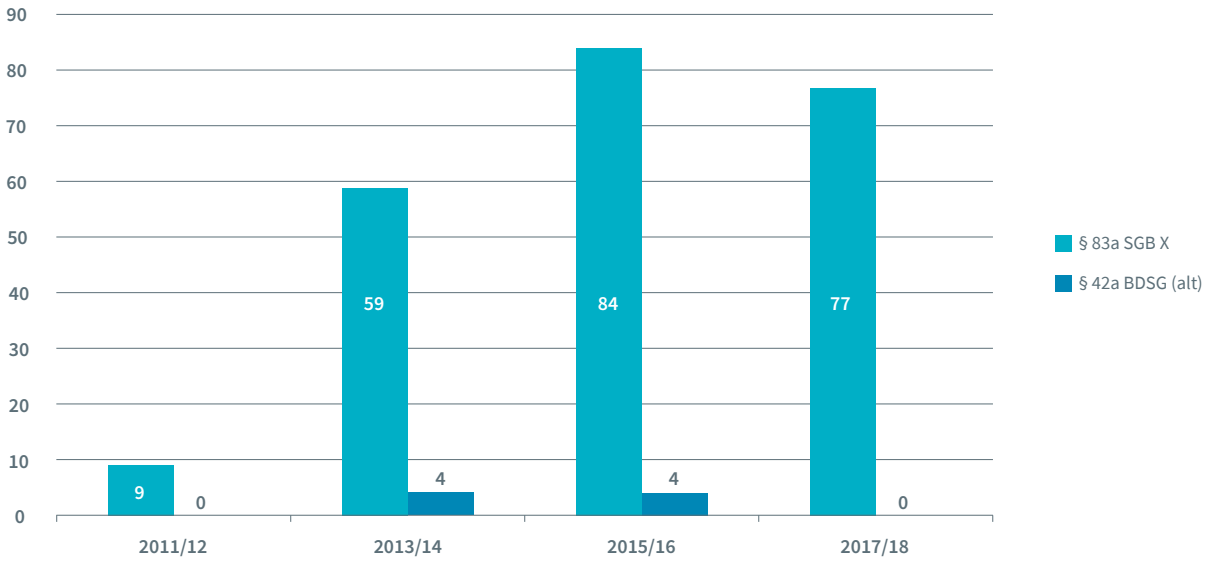
Sozialleistungsträger sind nach § 83a SGB X verpflichtet, mir eine Datenschutzverletzung innerhalb ihrer Organisationseinheiten mitzuteilen, wenn sie feststellen, dass dort gespeicherte besondere Arten personenbezogener Daten (vgl. § 67 Abs. 12 SGB X) unrechtmäßig übermittelt oder auf sonstige Weise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

der Betroffenen drohen. Insgesamt haben mich im Berichtszeitraum 77 Meldungen erreicht.

(Angaben zu Mitteilungen aufgrund § 42a BDSG (alt) bzw. § 83a SGB X seit 2012 – siehe Grafik)

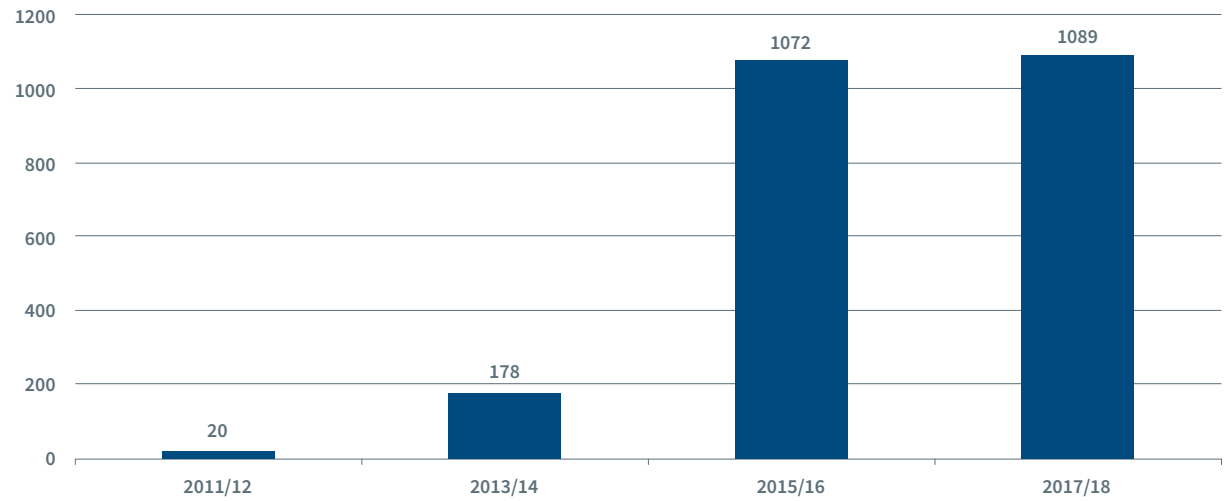
Im Berichtszeitraum haben mich keine Meldungen anderer öffentlicher Stellen erreicht, die nach § 42a BDSG (alt) zur Information verpflichtet waren (vgl. u. Nr. 6.2.2, 15.2.4).

Meldungen nach § 83a SGB X und § 42a BDSG (alt)



Weiter wurden mir im Berichtszeitraum 1.089 Datenschutzverstöße von Telekommunikationsanbietern gemeldet (vgl. Nr. 15.2.4). Gemäß § 109a Telekommunikationsgesetz (TKG) sind diese verpflichtet, die Bundesnetzagentur und mich sowie unter bestimmten Umständen auch die Betroffenen zu benachrichtigen, wenn der Schutz personenbezogener Daten verletzt worden ist.

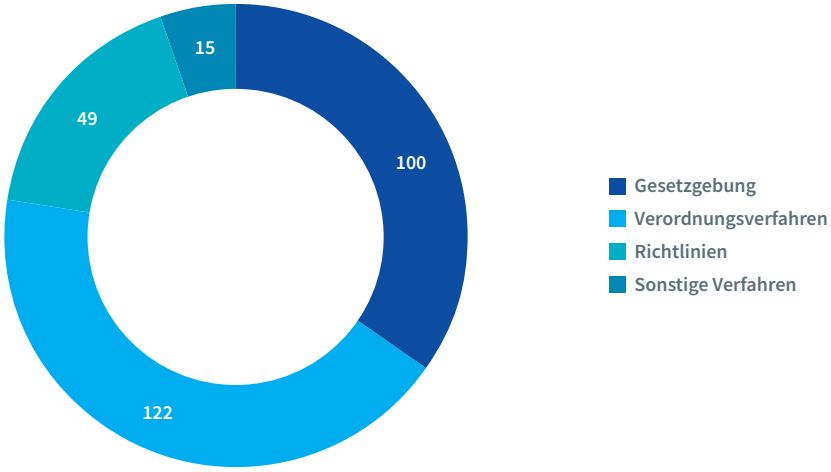
Meldungen nach § 109a TKG



Begleitung von Rechtsetzungsvorhaben

Gemäß § 45 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) hat das federführende Bundesministerium mich bei der Erstellung von Gesetzesvorlagen frühzeitig zu beteiligen, soweit dadurch meine Aufgaben berührt werden. Im Berichtszeitraum habe ich 100 Gesetzgebungsverfahren, 122 Verordnungsverfahren und 49 Richtlinien sowie 15 übrige Vorhaben, bei denen ich nach § 21 GGO einzubinden war, geprüft und begleitet.

Beteiligungen nach § 12 GGO

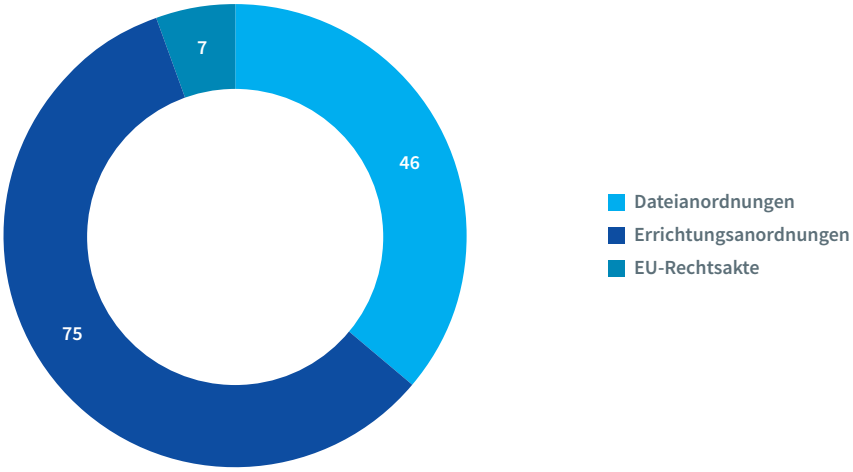


Darüber hinaus habe ich sieben Entwürfe von EU-Gesetzgebungs- und Rechtsakten geprüft.

Zudem wurden mir im Bereich der Sicherheitsbehörden 75 Errichtungsanordnungen (EAO) und 66 Dateianordnungen (DAO) zur Prüfung vorgelegt. Das Bundeskriminalamt (BKA) hat für jede bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten eine EAO zu erlassen. Hier werden unter anderem die Rechtsgrundlage und der Zweck der Datei festgelegt, 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. Vor Erlass der EAO bin ich anzuhören und prüfe dabei die Rechtsmäßigkeit der Datenverarbeitung, soweit sie sich aus der EAO ergibt. Seit Inkrafttreten des neuen Bundeskriminalamtgesetzes Ende Mai 2018 hat das BKA weder die Verpflichtung noch die Möglichkeit, weiterhin EAO zu erstellen.

Das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der Militärische Nachrichtendienst haben für jede automatisierte Datei, in denen sie personenbezogene Daten verarbeiten, DAO zu erstellen und dort Details zur Datenverarbeitung festzulegen. Auch hier bin ich vor Erlass der DAO anzuhören und prüfe dann die Rechtmäßigkeit der Datenverarbeitung, soweit sie sich aus der DAO ergibt.

Sonstige Beteiligungen der BfDI



Neue Aufgaben

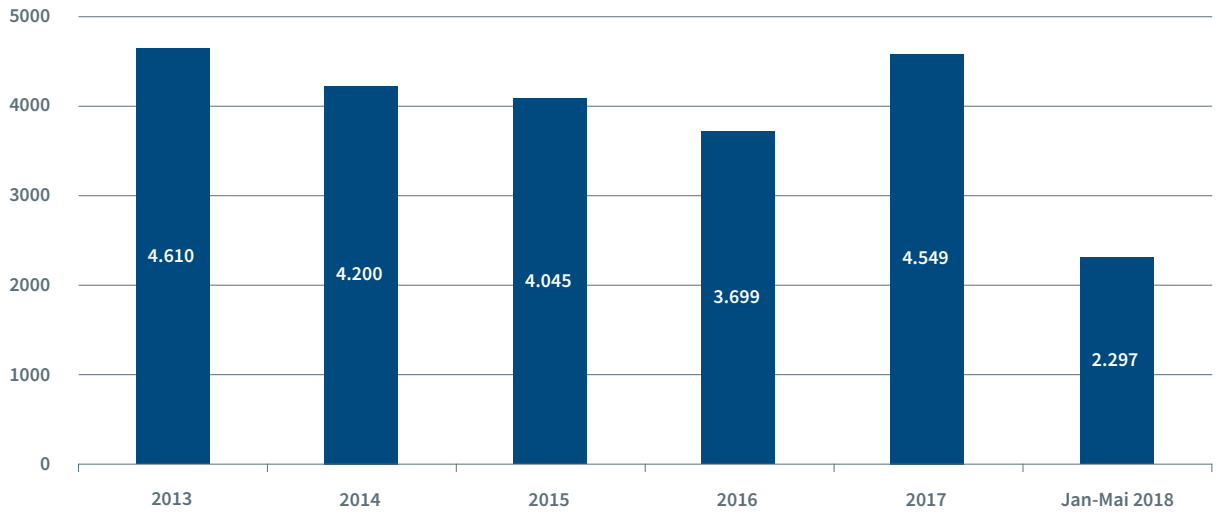
Im Berichtszeitraum wurden mir durch Gesetze oder Verordnungen zahlreiche neue Aufgaben übertragen.

Gesetz	Neue Aufgabe	Verweis auf Beitrag im TB
Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG, BGBl. 2017 I S. 1484))	Berichtspflicht und Kontrollpflicht	1.3
Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BGBl. 2017 I S. 1354)	Pflichtkontrollen	9.1.3
Telekommunikationsgesetz (TKG, BGBl. 2017 I S. 1963)	Entgegennahme von Berichten	15.1.3
Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) Datenschutz-Anpass-UmsetzG vom 30.06.2017 (BGBl. I 2017 S. 2097 ff) – Art. 4 (§ 32a Nr. 1 Buchstabe b BNDG-neu)	Vorgabe neuer Verfahrensabläufe im Zusammenhang mit der datenschutzrechtlichen Aufsicht über den BND	1.2.1
Gesetz zur Änderung des Soldatengesetzes und weiterer soldatenrechtlicher Vorschriften vom 27. März 2017 (BGBl. I 2017 S. 562 ff)	Neue/erweiterte Kontrollaufgabe des BfDI im Zusammenhang mit der Einführung allgemeiner Sicherheitsüberprüfungen von Soldatinnen und Soldaten	

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 Eingaben über Datenschutzverstöße. Im Zeitraum bis 24.05.2018 erreichten mich 6.846 schriftliche Eingaben.

Schriftliche Eingaben 2013 – 24.05.2018



Sonstiges

Im Berichtszeitraum habe ich an zehn öffentlichen Anhörungen von Ausschüssen des Deutschen Bundestages als Sachverständiger teilgenommen.

Ich habe vier Stellungnahmen gegenüber dem Bundesverfassungsgericht abgegeben.

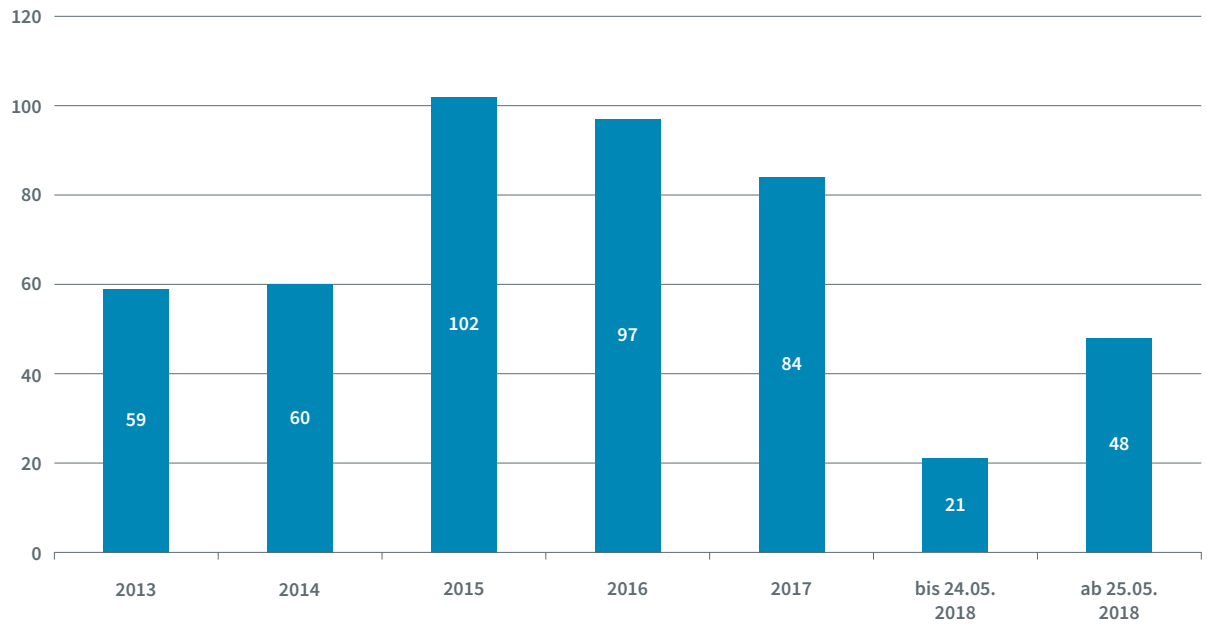
Im Berichtszeitraum habe ich und – auf meine Veranlassung hin – meine Mitarbeiterinnen und Mitarbeitern (auch als „Mitherausgeber“) drei Beiträge in der Fachliteratur veröffentlicht. Zudem haben meine Mitarbeiterinnen und Mitarbeiter und ich 67 Vorträge gehalten und an Podiumsdiskussionen teilgenommen.

B. Zeitraum vom 25.05.2018 – 31.12.2018 (Rechtsgrundlage DSGVO, BDSG)

Anzahl der Informations-, Beratungs- und Kontrollbesuche

Im Berichtszeitraum haben meine Mitarbeiterinnen und Mitarbeiter nach dem Inkrafttreten der DSGVO 48 Kontrollen bei Behörden und Unternehmen in oft mehrtägigen Besuchen umfassend oder in bestimmten Bereichen beraten. Zudem wurde überprüft, ob die Regelungen der DSGVO, des BDSG und sonstige Vorschriften über den Datenschutz eingehalten wurden.

Informations-, Beratungs- und Kontrollbesuche 2013–2018 (Gesamtjahre)



Meldungen von Datenschutzverstößen

Die DSGVO normiert im Unterschied zur alten Rechtslage nunmehr Meldepflichten für sämtliche in ihren Anwendungsbereich fallende öffentliche und nicht-öffentliche Stellen gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DSGVO). Im Berichtszeitraum haben mich 7.293 Meldungen über Datenschutzverstöße erreicht. Diese umfassen auch Meldungen von Telekommunikationsunternehmen. Soweit Unternehmen personenbezogene Daten für die geschäftsmäßige Erbringung von Telekommunikationsdiensten verarbeiten, liegt die Zuständigkeit für Meldungen nach Art. 33 DSGVO ausschließlich bei mir (§ 115 Absatz 4 Satz 1 TKG vgl. u. Nr. 15.2.4).

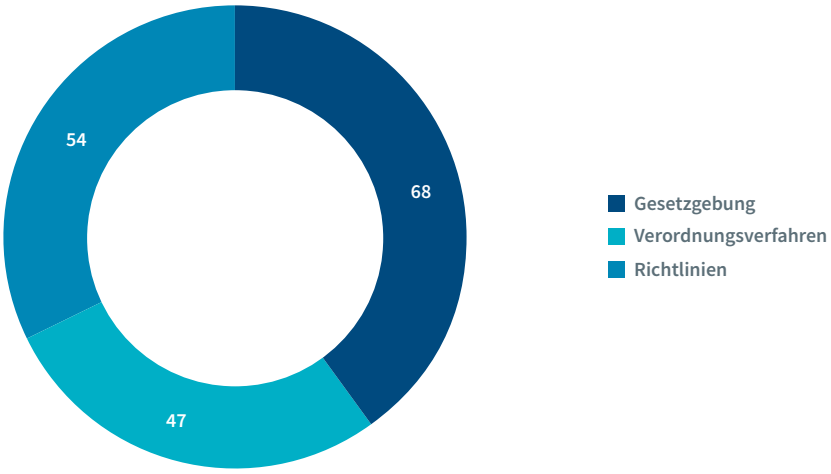
Daneben haben mich 17 Meldungen nach § 109a TKG erreicht. Gemäß § 109a TKG sind die Telekommunikationsdiensteanbieter verpflichtet, die Bundesnetzagentur und mich sowie unter bestimmten Umständen auch die Betroffenen zu benachrichtigen, wenn der Schutz personenbezogener Daten verletzt worden ist (vgl. u. Nr. 15.2.4).

Meldungen von Datenschutzverstößen	25.05.2018 – 31.12.2018
Art. 33 DSGVO	7.293
§ 65 BDSG	0
§ 109 Absatz 1 TKG	17

Begleitung von Rechtssetzungsvorhaben

Seit dem 25. Mai 2018 habe ich 68 Gesetzgebungs-, 47 Verordnungsverfahren und 54 Richtlinien sowie sieben übrige Vorhaben, bei denen ich nach § 21 GGO beteiligt wurde, geprüft und begleitet.

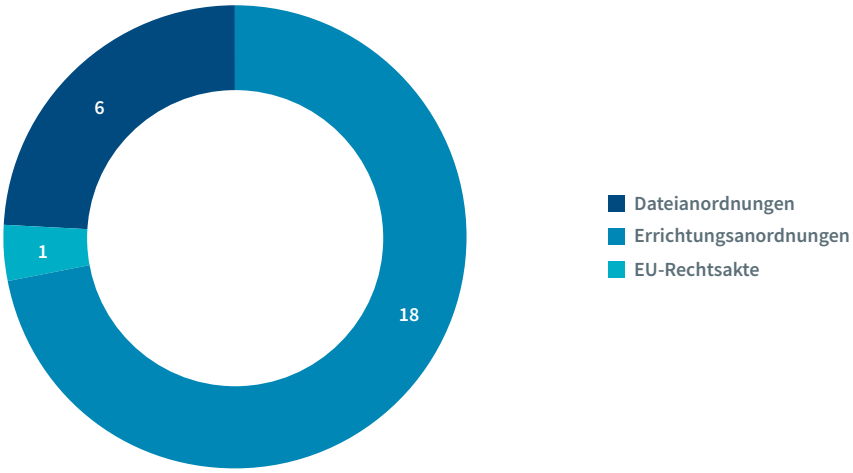
Beteiligungen nach § 21 GGO



Im Berichtszeitraum habe ich sechs Entwürfe von EU-Gesetzgebungs- und Rechtsakten geprüft.

Zudem wurden mir im Bereich der Sicherheitsbehörden eine Errichtungsanordnung und 18 Dateianordnungen zur Prüfung vorgelegt.

Sonstige Beteiligungen der BfDI



Neue Aufgaben

Im Berichtszeitraum wurden mir folgende neue Aufgaben durch Gesetze oder Verordnungen übertragen.

Gesetz	Neue Aufgabe	Verweis auf Beitrag im TB
§ 32 h Abgabenordnung (AO – BGBl. I 2017 S. 2541)	§ 32 h AO regelt die datenschutzrechtliche Aufsicht über die Finanzbehörden im Anwendungsbereich der AO neu. Für die Finanzbehörden ist nunmehr nur der oder die BfDI zuständig und nicht mehr die datenschutzrechtlichen Aufsichtsbehörden der Länder. Darüber hinaus wird den Ländern die Befugnis eingeräumt (§ 32 h Absatz 3 AO) weitere datenschutzrechtliche Zuständigkeiten auf den oder die BfDI zu übertragen.	6.1.1
Hamburgisches Datenschutzgesetz (HmbDSG – HmbGVBL 2018 S. 145))	Für die Aufsicht über die Verarbeitung personenbezogener Daten im Rahmen der Verwaltung landesrechtlich geregelter Steuern ist die oder der BfDI zuständig, soweit die Datenverarbeitung auf bundesgesetzlich geregelten Besteuerungsgrundlagen oder auf bundeseinheitlichen Festlegungen beruht.	6.1.1
Wegfall §§ 41, 42 BDSG (alt) (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017, BGBl. I S. 2097)	Datenschutzkontrolle über die Deutsche Welle	10.1.1
Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017, BGBl. I S. 2097) – Art. 1: § 1 Abs. 8 BDSG	DSGVO und Teile 1 und 2 BDSG gelten für das Militärische Nachrichtenwesen der Bundeswehr (MilNW) entsprechend. – D. h.: Neue/erweiterte Aufgaben der BfDI gegenüber MilNW	1.2.1
Art. 66 Abs. 4 VO (EU) 2018/1240 (Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, ABl 2019/236 S. 54)	Pflichtkontrollen ab Inbetriebnahme ETIAS	1.3

Gesetz	Neue Aufgabe	Verweis auf Beitrag im TB
Akkreditierung von Zertifizierungsstellen, Art. 43 DSGVO (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. EU 2016 L 119/1)	Datenschutzkriterien, Befugniserteilung	15.2.2
Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. EU 2016 L 119/1)	BfDI ist nach Anwendungsbeginn der DSGVO für weitere 60.000 Postdienstleister zuständig	15.1.4

Allgemeine Anfragen und Beschwerden

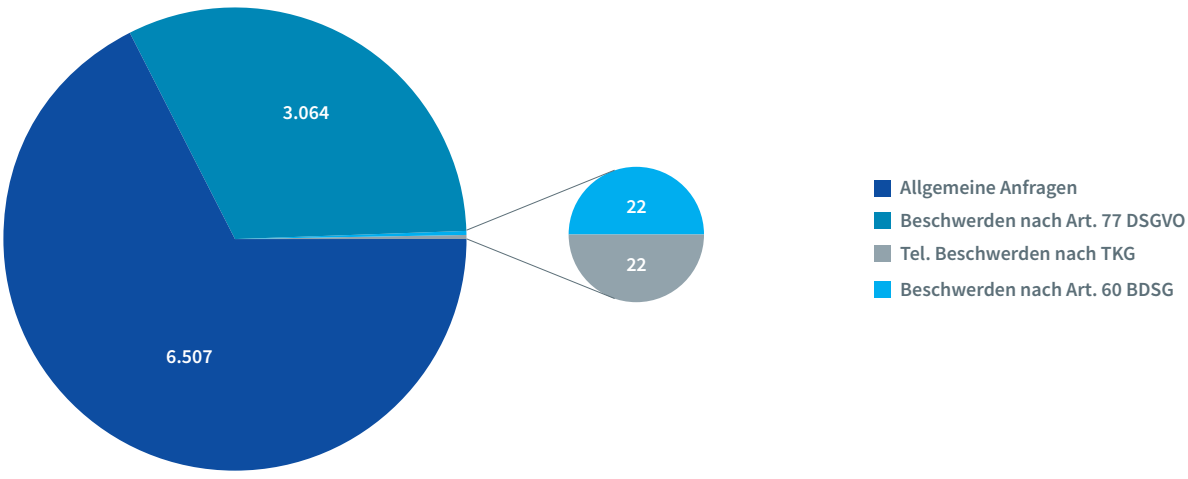
Seit Anwendungsbeginn der DSGVO erfasse ich Beschwerden und allgemeine Anfragen getrennt. Mit einer Beschwerde können sich betroffene Personen an mich wenden, wenn sie annehmen, bei der Erhebung, Verarbeitung oder Nutzung ihrer persönlichen Daten in ihren Rechten verletzt worden zu sein.

Als allgemeine Anfragen erfasse ich sowohl Hinweise auf datenschutzrechtliche Verstöße, die ich von Personen erhalte, die nicht selbst betroffen sind, als auch Anfragen zu datenschutzrechtlichen Themen. Die bis zum 24.05.2018 erfassten Eingaben beinhalteten sowohl Beschwerden als auch allgemeine Anfragen.

Vom 25.05. bis zum 31.12.2018 haben mich 6.507 allgemeine Anfragen, 3.064 Beschwerden nach Art. 77 DSGVO, 22 Beschwerden nach § 60 BDSG sowie 22 telefonische Beschwerden nach dem Telekommunikationsgesetz erreicht. Das sind in einem Zeitraum von nur gut sieben Monaten mit 9.615 zusammengerechnet mehr als doppelt so viele wie im gesamten Jahr 2017. Dies zeigt einerseits den gestiegenen Beratungsbedarf und andererseits, dass die Bürgerinnen und Bürger ihre Rechte seit Einführung der DSGVO stärker einfordern.

Betroffene haben im Berichtszeitraum gegen meine Entscheidungen keine Rechtsmittel eingelegt.

Anfragen und Beschwerden seit 25. Mai 2018



Verfahren

Im Berichtszeitraum habe ich fünfmal Amtshilfe nach Art. 57 Absatz 1 Buchstabe. g) und nach Art. 61 DSGVO i. V. m § 14 Absatz 1 Nummer 7 BDSG geleistet. In drei Fällen fanden – gestartet von der Zentralen Anlaufstelle (ZASt) – interne Konsultationen mit den deutschen Aufsichtsbehörden statt (vgl. Nr. 27.2 f.)

Ich habe eine vorherige Konsultation gem. Art. 36 DSGVO, § 69 BDSG durchgeführt.

Seit Anwendungsbeginn der DSGVO gab es mit meiner Beteiligung

- ein Kooperationsverfahren nach Art. 60 DSGVO,
- keine gemeinsame Maßnahmen nach Art. 62 DSGVO,
- 26 Kohärenzverfahren nach Art. 63 DSGVO.

Ich habe 67 Verfahren nach Art. 56 DSGVO selbst initiiert, während elfmal das Verfahren von anderen Behörden gestartet wurde.

Sonstiges

Im Berichtszeitraum habe ich an sechs öffentlichen Anhörungen von Ausschüssen des Deutschen Bundestages als Sachverständiger teilgenommen.

Im Berichtszeitraum habe ich und – auf meine Veranlassung hin – meine Mitarbeiterinnen und Mitarbeitern (auch als „Mitherausgeber“) zwei Beiträge in der Fachliteratur veröffentlicht. Zudem haben meine Mitarbeiterinnen und Mitarbeiter und ich 42 Vorträge gehalten sowie an Podiumsdiskussionen teilgenommen.

Zusammenfassung der Empfehlungen

Ich empfehle dem Gesetzgeber, Abhilfebefugnisse für den BfDI ins neue BPolG aufzunehmen. Diese sollten zumindest den bereits im neuen BKAG enthaltenen Befugnissen entsprechen (Nr. 1.2).

Ich empfehle dem Gesetzgeber, Sanktionsbefugnisse für den BfDI auch im Bereich der Nachrichtendienste einzuführen (Nr. 1.2.1).

Ich empfehle dem Gesetzgeber klarzustellen, dass auch gegenüber den gesetzlichen Krankenkassen bei Verstößen gegen die DSGVO Geldbußen verhängt werden können, soweit diese als Wirtschaftsunternehmen tätig werden (Nr. 1.1).

Ich empfehle, dass die Jobcenter ausreichend personell ausgestattet werden, um ihre Datenschutzbeauftragten von anderen Aufgaben freizustellen, damit diese ihre gesetzlich vorgeschriebenen Aufgaben erfüllen können (Nr. 3.2.1).

Ich empfehle der Bundesregierung, im Hinblick auf die Vorgaben des EuGH zu PNR Kanada das FlugDG zu überarbeiten und sich in Brüssel für eine Überarbeitung der Richtlinie (EU) 2016/681 einzusetzen (Nr. 1.3).

Ich empfehle dem Gesetzgeber, eine klare Zuständigkeitsregelung für die Kontrolltätigkeit von BfDI und G-10-Kommission zu schaffen, die auch die Kooperation zwischen diesen beiden Aufsichtsbehörden umfasst. Ich empfehle außerdem, die Kontrollbefugnis des BfDI umfassend auch beim Führen gemeinsamer Dateien des BfV mit ausländischen Nachrichtendiensten anzuerkennen und diese ggf. gesetzlich klarstellend zu regeln (Nr. 9.1.5).

Ich empfehle, in der gesamten Bundesverwaltung bei Verträgen zur Auftragsverarbeitung das neu entwickelte Vertragsmuster zur Auftragsverarbeitung zu verwenden. Die Mustervereinbarung ist in meinem Internetangebot veröffentlicht (Nr. 9.2.6).

Ich empfehle, bei Zugriffen auf Eurodac und auf das VIS-Informationssystem durch Polizeibehörden auf eine aussagekräftige Dokumentation zu achten (Nr. 9.3.5).

Ich empfehle dem Gesetzgeber angesichts des festgestellten geringen Nutzwerts von Antiterrordatei und Rechtsextremismus-Datei, diese abzuschaffen (Nr. 9.3.5).

Ich empfehle, die Strafprozessordnung zu überarbeiten. Insbesondere sind die Erhebung und Nutzung von Daten, die von V-Leuten aus polizeilichen oder nachrichtendienstlichen Zusammenhängen ermittelt wurden, im Strafprozess nicht normenklar geregelt. Die Zusammenarbeit mit Verfassungsschutzbehörden bedarf ohnehin einer engeren und präziseren Regelung. Die Rechtsprechung des Bundesverfassungsgerichts ist insoweit umzusetzen (Nr. 11.1.2).

Ich rate dringend, die E-Privacy-Verordnung schnellstmöglich zu verabschieden. Die aktuelle Anwendung der auf der Grundlage der Richtlinie 2002/58/EG erlassenen nationalen Vorschriften trägt den gegenwärtigen Entwicklungen nicht mehr angemessen Rechnung und schafft Rechtsunsicherheit für alle Beteiligten. Dies betrifft insbesondere das Verhältnis zwischen dem deutschen Telekommunikationsgesetz und der DSGVO (Nr. 15.1.2)

Ich rate den öffentlichen Stellen des Bundes dazu, die Erforderlichkeit des Einsatzes Sozialer Medien kritisch zu hinterfragen. Wichtige Informationen sollten nicht ausschließlich über Soziale Medien bereitgestellt werden. Sensible personenbezogene Daten haben in Sozialen Medien nichts zu suchen; weder sollten öffentlichen Stellen selbst solche Daten einstellen, noch sollten sie Bürger dazu ermuntern, diese dort preiszugeben. Für die vertrauliche Kommunikation gibt es geeignete sichere Kommunikationskanäle, auf die verwiesen werden sollte, etwa SSL-verschlüsselte Formulare, verschlüsselte E-Mails oder De-Mail (Nr. 15.2.7).

Ich empfehle den Bundesbehörden, die eine Fanpage betreiben, zu prüfen, ob der Betrieb einer Facebook-Fanpage zur Erfüllung ihrer Aufgaben unbedingt erforderlich ist oder sie sich nicht – zumindest bis zur rechtlichen Klärung der Situation – datenschutzfreundlichere Kommunikationskanäle nutzen können (Nr. 15.2.8).

Empfehlungen im 26. Tätigkeitsbericht – Stand der Umsetzung

	Empfehlung im 26. TB	Stand der Umsetzung
🟡	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 zur gewährleisten (Nr. 1.1, 1.2 ff. im 26. TB).	Mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung des Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) sowie der damit verbundenen Schaffung eines neuen Bundesdatenschutzgesetzes ist meiner Empfehlung in Teilen entsprochen worden. Einige Regelungen des BDSG beurteile ich jedoch dabei kritisch (vgl. Nr. 1.1). Mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU sollen nun auch größere Teile des bereichsspezifischen Datenschutzrechts des Bundes an die DSGVO angepasst werden. Auch dieses Gesetzgebungsverfahren begleite ich und habe im Rahmen meiner Stellungnahme bereits auf entsprechenden Nachbesserungsbedarf hingewiesen (vgl. Nr. 1.1).
🔴	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 im 26. TB).	Zwar hat der Gesetzgeber im Rahmen der Neuregelung des Bundesdatenschutzgesetzes in § 26 BDSG einige Regelungen zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses getroffen. Im Wesentlichen wurden damit allerdings nur die bestehenden Regelungen übernommen. Nach wie vor fehlen umfassende spezifische Regelungen, so dass ich dem Gesetzgeber abermals empfehle, spezifische nationale Regelungen zum Beschäftigtendatenschutz zu erlassen (vgl. Nr. 3.1.3).
🟡	Ich empfehle dem Gesetzgeber die Prüfung, bei Regelungen zur Datenverarbeitung besondere Vorschriften zum Schutz von Kindern zu ergreifen (Nr. 7.1 im 26. TB).	Der Gesetzgeber hat durch den neuen § 14 Absatz 1 Nr. 2 BDSG mir die Aufgabe übertragen, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder besondere Beachtung finden sollen. Die im Entwurf des Zweiten Datenschutz- Anpassungs- und Umsetzungsgesetz EU angepassten und ergänzten Vorschriften erhalten nur rudimentäre Regelungen zum Schutz Minderjähriger bei der Verarbeitung personenbezogener Daten. Ich würde es sehr begrüßen, wenn der Gesetzgeber gerade hinsichtlich der Nutzung von sozialen Medien und Messenger Diensten Regelungen zum Schutz Minderjähriger treffen würde.

	Empfehlung im 26. TB	Stand der Umsetzung
	Ich empfehle dem Gesetzgeber, die nach der DSGVO von Mitgliedstaten 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 im 26. TB).	Ich begrüße es, dass der Gesetzgeber diese Empfehlung schnell und ausreichend umgesetzt hat.
	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 im 26. TB).	Mit dem Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541) hat der Gesetzgeber die Grundregelungen zum Sozialdatenschutz im 2. Kapitel des Zehnten Buches Sozialgesetzbuch (SGB X) der Datenschutz-Grundverordnung angepasst. Dabei wurde aber versäumt, unter Beachtung der DSGVO im Sinne der Versicherten, aber auch der Sozialverwaltung und der Forschung bessere Regelungen zu schaffen (vgl. Nr. 7.1.1). Mit dem Zweiten Datenschutz- Anpassungs- und Umsetzungsgesetz EU sollen auch die bereichsspezifischen Sozialgesetzbücher den Vorgaben der DSGVO angepasst werden. Dabei sind lediglich redaktionelle Anpassungen vorgesehen. Für eine Erhaltung des sorgfältig aufeinander abgestimmten Gefüges der bereichsspezifischen datenschutzrechtlichen Vorschriften im Bereich der gesetzlichen Krankenkassen ist dies jedoch noch zu wenig.
	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 im 26. TB).	Meine Empfehlung wurde leider bislang nur im BKAG umgesetzt, so dass es mir nur in diesem begrenzten Bereich möglich ist, geeignete Maßnahmen anzuordnen, wenn dies zur Beseitigung eines erheblichen Datenschutzverstoßes erforderlich ist.
	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 im 26. TB).	Im Gesetzgebungsverfahren zum BKAG ist der Mehrbedarf an Personalmitteln und Sachkosten der BfDI explizit herausgestellt worden (BT-Drs. 18/11163, S. 3). Allerdings ist das BKAG nur eines von zahlreichen, in der letzten Legislaturperiode verabschiedeten Gesetzen, mit denen die Aufgaben und Befugnisse – und damit verbunden auch die Personal- und Sachmittel – der Sicherheitsbehörden weiter erheblich ausgebaut worden sind. Auf Seiten der Kontrollbehörden hat der Gesetzgeber dagegen nur vereinzelt eine entsprechende Entwicklung nachvollzogen Neben dem BKAG betrifft diese positive Ausnahme z. B. das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des BND. Die Bundesregierung sollte in Zukunft die vom BfDI im Bereich der Nachrichtendienste zur Erfüllung ihrer verfassungsgerichtlich zugewiesenen Kompensationsfunktion benötigten – und bis dato nur teilweise gewährten – Personal- und Sachmittel berücksichtigen.

	Empfehlung im 26. TB	Stand der Umsetzung
		Dies gilt insbesondere vor dem Hintergrund, dass aufgrund des seit dem Jahr 2001 vollzogenen Befugnis- und Personalaufwuchses bei den Sicherheitsbehörden ein deutliches Ungleichgewicht zwischen meinem Haus und den von mir kontrollierten Stellen besteht. Ich schlage daher vor, im Rahmen von Gesetzgebungsverfahren künftig eine Proporz-Regelung dergestalt einzuführen, dass immer dann, wenn Sicherheitsbehörden per Gesetz neue Aufgaben oder Befugnisse – und damit ein entsprechender Personalbedarf – zugestanden wird, dem BfDI bzw. den zuständigen Kontrollorganen proportional ebenfalls entsprechende Stellen zugebilligt werden.
🟡	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 im 26. TB).	Der Gesetzgeber hat diese Empfehlung teilweise umgesetzt. Er hat die Gesetzesbegründung zu § 26a Absatz 2 BVerfSchG angepasst, sie enthält jetzt entsprechende Ausführungen, die ich begrüße. Es fehlt jedoch weiterhin eine ausdrückliche Normierung, die aus meiner Sicht auch konkrete Aussagen zur Kooperationspflicht der Kontrollinstanzen beinhalten muss (vgl. auch Nr. 9.1.5 und 9.1.6).
🔴	Ich empfehle dem Gesetzgeber, die Rechtsgrundlagen für die Eingriffsbefugnisse der Sicherheitsbehörden und der Nachrichtendienste entsprechend des Vorgaben des Bundesverfassungsgerichtes zum BKAG verfassungskonform auszugestalten, d. h. auch geltende Regelungen entsprechend zu ändern (Nr. 1.3 im 26. TB).	Dies betrifft Eingriffsschwellen und betroffene Personenkreise, Zweckbindung und Übermittlungsregelungen, Auslandsübermittlungen sowie Verfahrensabsicherungen inklusive Weisungsbefugnissen gegenüber den Nachrichtendiensten. In weiten Teilen fehlen diese Umsetzungen noch immer, und sie werden auch in aktuellen Gesetzgebungsverfahren überwiegend nicht beachtet.
🟢	Ich empfehle dem Gesetzgeber, den datenschutzrechtlichen Auskunftsanspruch im Besteuerungsverfahren zeitnah gesetzlich zu regeln (Nr. 8.2.3 im 26. TB).	Mit dem zum 25. Mai 2018 in Kraft getretenen »Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften« vom 17. Juli 2017 (BGBl. I 2017 S. 2541) ist der Gesetzgeber meiner Empfehlung gefolgt und hat den datenschutzrechtlichen Auskunftsanspruch im Besteuerungsverfahren geregelt (vgl. Nr. 6.1.1).
🔴	Ich empfehle dem Gesetzgeber, gesetzliche Regelungen für das Einführen von Mortalitätsregistern für Forschungszwecke zu schaffen (Nr. 9.2.3 im 26. TB).	Bedauerlicherweise ist der Gesetzgeber hier nicht tätig geworden.
🔴	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 im 26. TB).	Der Entwurf eines IT-Sicherheitsgesetzes 2.0 steht immer noch aus. Ich erhoffe mir von dem Gesetz, dass es einen wesentlichen Beitrag leistet und bisher noch nicht berücksichtigte Punkte, die die Sicherheit in Deutschland erhöhen, aufgreift.

1 Schwerpunktthemen – national

1.1 Umsetzung der Datenschutz-Grundverordnung

Meine Tätigkeit war in den Jahren 2017 und 2018 ganz wesentlich geprägt von der Umsetzung der Datenschutz-Grundverordnung. Mit deren Wirksamwerden zum 25. Mai 2018 wurde das europäische und auch das deutsche Datenschutzrecht auf eine vollkommen neue rechtliche Grundlage gestellt und damit eine Zeitenwende im Datenschutz eingeleitet. Dies stellte mein Haus vor große Herausforderungen.

Einleitung

Neben der Begleitung der entsprechenden Anpassungsgesetzgebung des Bundesgesetzgebers waren sowohl auf nationaler Ebene im Kreis der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes- und der Länder (DSK), als auch auf europäischer Ebene durch die Artikel-29-Gruppe bzw. den Europäischen Datenschutzausschuss (EDSA- dazu Nr. 2.1) Auslegungshilfen für die Anwendungspraxis zu erarbeiten bzw. bestehende Dokumente zu überarbeiten. Die DSK hat u. a. fast zwanzig sog. Kurzpapiere zu bestimmten Fragen der DSGVO erstellt, in denen unter den deutschen Aufsichtsbehörden abgestimmte einheitliche Sichtweisen zu verschiedenen Kernthemen der DSGVO wiedergegeben werden (abrufbar unter www.datenschutz.bund.de, vgl. auch unter Nr. 17.9). In der Artikel-29-Gruppe bzw. nach dem 25. Mai 2018 im EDSA war mein Haus maßgeblich an der Erarbeitung verschiedener Leitlinien zur DSGVO beteiligt, unter anderem zu Schwerpunktthemen wie der Einwilligung oder der Akkreditierung von datenschutzspezifischen Zertifizierungsstellen.

Besonders gefordert war auch meine Presse- und Öffentlichkeitsarbeit. Unter anderem war nahezu das gesamte Informationsmaterial, das ich als Broschüren, Flyer oder in Beiträgen auf meiner Internetseite zur Verfügung stelle, zu überarbeiten (vgl. u. Nr. 17.9). Auch Anfragen und Beschwerden von Bürgerinnen und Bürgern sowie die Meldung von Datenschutzverstößen sind seit dem 25. Mai 2018 sprunghaft gestiegen (vgl. o. Die Arbeit des BfDI in Zahlen). Hierin zeigt sich ein immenser Beratungs- und Informationsbedarf bei Verantwortlichen sowie Bürgerinnen und Bürgern gleichermaßen.

Letztendlich war die DSGVO auch in meinem Haus in seiner Funktion als Aufsichtsbehörde umzusetzen, was organisatorische und inhaltliche Neuerungen mit sich brachte (vgl. u. Nr. 17.1). Da meine Behörde auch selbst personenbezogene Daten verarbeitet, hatte ich die DSGVO auch in meiner Rolle als datenschutzrechtlich Verantwortlicher umzusetzen.

Die Anpassungsgesetzgebung

Der deutsche Gesetzgeber hat die Anpassung des nationalen Datenschutzrechts an die DSGVO und die Umsetzung der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie, vgl. auch u. Nr. 1.2) zum Gegenstand von zwei größeren Gesetzgebungsverfahren gemacht.

Mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) wurde insbesondere das Bundesdatenschutzgesetz neu konzipiert. Dieses ergänzt seit dem 25. Mai 2018 die unmittelbar geltende DSGVO in den Bereichen, in denen die DSGVO den Mitgliedstaaten Gestaltungsspielräume belässt oder Regelungsaufträge erteilt. Daneben werden mit dem BDSG wesentliche Teile der o. g. Richtlinie 2016/680 umgesetzt. Das neue BDSG gilt – wie zuvor das BDSG (alt) – für öffentliche Stellen des Bundes sowie für nicht-öffentliche Stellen. Für öffentliche Stellen der Länder gilt es nur in Bereichen, soweit es keine landesrechtlichen Regelungen gibt. Um eine möglichst einheitliche Entwicklung des allgemeinen Datenschutzrechts zu fördern, findet das BDSG auch Anwendung auf die Verarbeitung personenbezogener Daten durch Tätigkeiten von öffentlichen Stellen des Bundes, die nicht in den Anwendungsbereich des Unionsrechts fallen (z. B. Nachrichtendienste, Bundeswehr).

Durch meine Initiative konnten in dem Gesetz einige Verbesserungen gegenüber den Vorentwürfen erreicht werden, u. a. beim zentralen Grundsatz der Zweckbindung

im öffentlichen Bereich. Andere Regelungen des neuen BDSG sehe ich nach wie vor kritisch. Dies gilt beispielsweise für die in § 29 geregelten beschränkten Befugnisse der Aufsichtsbehörden gegenüber Geheimnisträgern wie beispielsweise Rechtsanwälten. Gleiches gilt für meine eingeschränkten Aufsichtsbefugnisse im Bereich Polizei und Justiz und außerhalb des Geltungsbereichs des EU-Rechts. Gerade für heimliche Datenerhebungen ist eine unabhängige Kontrolle zwingend notwendig. Anstatt jedoch das Vertrauen der Bürger in die staatliche Datenerhebung in diesem Bereich zu verbessern, habe ich hier keinerlei wirksame Durchsetzungsbefugnisse; möglich sind mir nur nicht-bindende Beanstandungen. Ich sehe hier einen Verstoß gegen die verfassungs- und europarechtlichen Grundsätze einer starken und unabhängigen Datenschutzaufsicht (vgl. Nr. 1.2 f.).

Auch im Sozial- und Steuerverfahrensrecht wurden grundlegende Anpassungen an die DSGVO zum 25. Mai 2018 vorgenommen (vgl. Nr. 3.1.1, Nr. 6.1.1).

Mit dem „Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“ (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) sollen nunmehr auch größere Teile des übrigen bereichsspezifischen Datenschutzrechts des Bundes an die DSGVO angepasst werden. Der von der Bundesregierung eingebrachte Gesetzesentwurf (BT-Drs. 19/4674) sieht Änderungen in 154 Fachgesetzen fast aller Ressorts vor. Zu den Regelungsschwerpunkten zählen etwa Anpassungen von Begriffsbestimmungen und von Rechtsgrundlagen für die Datenverarbeitung sowie Regelungen zu den Betroffenenrechten. Im Rahmen meiner Stellungnahme habe ich auf Nachbesserungsbedarf, u. a. bei den vorgesehenen Änderungen des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS-Gesetz), hingewiesen. Des Weiteren habe ich gefordert, dass durch eine entsprechende Formulierung im Fünften Buch Sozialgesetzbuch geregelt wird, dass auch gegenüber den gesetzlichen Krankenkassen bei Verstößen gegen die DSGVO Geldbußen verhängt werden können. Einen durchgreifenden Grund, die sich verstärkt als Wirtschaftsunternehmen verstehenden gesetzlichen Krankenkassen mit einem Ausgabevolumen von zum Teil mehr als 25 Mrd. Euro gegenüber einem Handwerks- oder kleinen Industrieunternehmen zu privilegieren, erkenne ich nicht. Besonders kritisch sehe ich, dass die zwingend notwendigen Anpassungen des Telekommunikationsgesetzes auch mit diesem Gesetz nicht angegangen werden. Dies erschwert die Anwendung und Durchsetzung des Datenschutzrechts im Telekommunikationsbereich und führt zu erheblicher Rechtsunsicherheit (vgl. unter Nr. 15.1.1).

Der Bundestag hat am 12. Oktober 2018 den Entwurf der Bundesregierung nach erster Lesung zur federführenden Beratung an den Innenausschuss überwiesen. Das parlamentarische Verfahren soll Anfang 2019 fortgesetzt werden.

Umsetzung in Unternehmen und Behörden

Leider haben viele Beteiligte die zweijährige Übergangsphase vor dem Wirksamwerden der DSGVO nicht hinreichend genutzt, um sich auf die Neuregelungen angemessen vorzubereiten. Diese Defizite verdeutlicht eine repräsentative Erhebung des Branchenverbands Bitkom bei 505 Unternehmen kurz vor Ablauf der zweijährigen Übergangsfrist am 25. Mai 2018. Lediglich ein Viertel (24 Prozent) der befragten Unternehmen in Deutschland gab an, die neuen Regelungen zum Stichtag nahezu vollständig umgesetzt zu haben. Ein weiteres Drittel meinte, dieses Ziel zumindest teilweise erreichen zu können. Vier Prozent der Unternehmen standen erst am Anfang ihrer Bemühungen und zwei Prozent der befragten Unternehmen mussten einräumen, dass sie es bis zum Stichtag nicht schaffen würden, erste Schritte bei der Umsetzung zu gehen.

Vier Monate nach Fristablauf sah die Welt dann doch etwas besser aus.

Einer weiteren repräsentativen Befragung zufolge hadern auch nach dem Stichtag noch viele der 502 befragten Unternehmen mit der Umsetzung. Beklagt wurden u. a. die erweiterten Dokumentations- und Informationspflichten. Noch immer hatte erst ein Viertel (24 Prozent) der Unternehmen in Deutschland die DSGVO vollständig umgesetzt. Immerhin hatten aber weitere 40 Prozent die Regeln größtenteils umgesetzt; und 30 Prozent zumindest teilweise. Gerade erst begonnen mit den Anpassungen hatten nur fünf Prozent der Unternehmen. Insgesamt zeigt sich, dass nach wie vor Anstrengungen der Aufsichtsbehörden notwendig sind, um die Unternehmen für die Anforderungen der DSGVO zu sensibilisieren. Was die Umsetzung der DSGVO in den meiner Kontrolle unterliegenden Bundesbehörden angeht, so lässt sich festhalten, dass zwar ein großer Bedarf an Information und Beratung bestanden hat, insgesamt aber die Neuregelungen konsequent umgesetzt wurden. Unterstützt habe ich diesen Prozess u. a. durch meine Broschüre „Die DSGVO in der Bundesverwaltung“ (abrufbar unter www.datenschutz.bund.de).

Auswirkungen der DSGVO im Alltag

Es ist nicht überraschend, dass ein komplett neues Recht in einer so wichtigen Querschnittsmaterie wie dem Datenschutz nicht völlig reibungslos und ohne jede Diskussion eingeführt werden kann. In der Medienberichterstattung zur DSGVO und der Debatte über die DSGVO

standen leider nicht immer die Vorteile und Chancen eines harmonisierten europäischen Datenschutzrechts im Vordergrund, sondern – verständlicherweise – einzelne Fragen zur konkreten Umsetzung. Das hat zu einer starken Verunsicherung geführt. Dabei zeigte sich häufig, dass Fehlinformationen verbreitet oder Regelungen mit Verweis auf die neue DSGVO behauptet wurden, die es unter dem alten Recht schon seit Jahrzehnten gab (vgl. hierzu auch nebenstehender Informationskasten zu Nr. 1.1). Dies hat der Akzeptanz der gesetzlichen Neuregelungen in der Öffentlichkeit geschadet. Viele Berichte betrafen mutmaßliche oder tatsächlich Alltagsgeschichten wie beispielsweise Fotografien im Kindergarten, das Anbringen von Klingelschildern oder die allfällige Angst vor Abmahnungen:

→ Umgang mit Fotografien

Im Sommer 2018 erreichten mich zahlreiche Bürgeranfragen, nachdem eine Reihe von Presseartikeln eine erhebliche Verunsicherung angerichtet hatte. Bereits in den ersten Tagen nach Geltungsbeginn der DSGVO gab es eine breite öffentliche Diskussion über den datenschutzgerechten Umgang mit Fotografien, sei es im Sportbereich, in Kindergärten oder durch Journalisten. Allerdings hat sich hier durch die DSGVO nichts Wesentliches gegenüber den bereits zuvor bestehenden rechtlichen Anforderungen geändert. Es gilt weiterhin: Werden die Bilder durch natürliche Personen im Rahmen ausschließlich familiärer oder persönlicher Tätigkeiten erstellt, gilt das Datenschutzrecht von vornherein nicht. Dies trifft beispielsweise immer dann zu, wenn ein Familienmitglied auf einer privaten Familienfeier Fotografien oder Videos anfertigt und diese nicht veröffentlicht. Ist das Datenschutzrecht doch anzuwenden, können Fotos – wie bisher – in vielen Fällen auf der Grundlage einer Interessenabwägung aufgenommen und weiterverarbeitet werden. Dabei gilt die Faustformel: Je geringer der Eingriff in das Persönlichkeitsrecht (bspw. bei Überblicksaufnahmen, Aufnahmen in Stadien oder bei öffentlichen Veranstaltungen usw.), umso eher fällt diese Interessenabwägung zu Gunsten des Fotografierenden aus. Dies kann auch bei besonders Schutzbedürftigen wie Kindern gelten, soweit damit nicht nur eigene Interessen, sondern zum Beispiel gleichzeitig die des Kindes selbst und anderer Kinder verfolgt werden – wie im Fall von Fotoalben als Abschlussgeschenk im Kindergarten. Das ist alles nicht neu und mit der bisherigen Rechtslage weitgehend identisch. Eine Einwilligung ist hingegen – wie bisher – nur in wenigen Fällen notwendig, vor allem dann, wenn die Interessen des Betroffenen nicht aufgenommen zu werden, überwiegen. Eine Einwilligung kann also unter anderem notwendig sein, wenn es sich um Porträtaufnahmen handelt oder die Aufnahme eine nicht sozialadäquate Situation wiedergibt. Für

die Veröffentlichung von Bildern im Internet gilt, wie inzwischen auch gerichtlich bestätigt wurde, weiterhin das Kunsturhebergesetz, mit dem das Recht am eigenen Bild geschützt wird. Dieses Gesetz erlaubt, Bilder von Versammlungen oder Aufzügen wie Volksfesten, Festumzügen usw. ohne Einwilligung zu veröffentlichen. Diese Rechtslage gilt seit Jahrzehnten und hat sich durch die DSGVO nicht geändert.

→ Klingelschilder

Ein besonders bizarres Beispiel war die Frage, ob an Mehrfamilienhäusern künftig Klingelschilder mit Namen verboten seien oder nicht. Hier habe ich – ebenso wie viele meiner Kolleginnen und Kollegen in den Ländern – deutlich gemacht, dass das Datenschutzrecht gar nicht anwendbar ist. Die DSGVO gilt nämlich nur für automatisierte Datenverarbeitungen oder Verarbeitungen in Dateisystemen.

→ Abmahnungen

In dunklen Farben wurde vor dem Geltungsbeginn der DSGVO eine Abmahnwelle heraufbeschworen, deren volle Wucht vor allem kleine und mittlere Unternehmen oder Vereine treffe. Von dieser vorhergesagten Abmahnwelle sind in meinem Haus bis Ende 2018 weniger als fünf Beschwerden über Abmahnungen übrig geblieben.

Sonderfälle der Anwendung der DSGVO

Bei der Umsetzung und Anwendung der DSGVO innerhalb Deutschlands ist den bestehenden verfassungsrechtlichen Vorgaben Rechnung zu tragen. Im Bereich der legislativen Tätigkeit des Deutschen Bundestages darf ich beispielsweise nur beratend tätig werden (vgl. u. Nr. 14.1.1).

Für die Verarbeitung personenbezogener Daten durch die Rundfunk- und Medienanstalten sind die Bestimmungen der DSGVO nur eingeschränkt anwendbar. Dies folgt aus der verfassungsrechtlich garantierten Freiheit der Presse- und Rundfunkberichterstattung (Art. 5 Abs. 1 GG), einem diesbezüglichen Regelungsauftrag aus Art. 85 DSGVO sowie den hierzu getroffenen Bestimmungen im Rundfunkstaatsvertrag. An Stelle der datenschutzrechtlichen Vorschriften treten hier überwiegend rundfunkspezifische Datenschutzvorschriften (§ 9c und § 57 Rundfunkstaatsvertrag). Was die Kirchen oder religiöse Vereinigungen angeht, enthält Artikel 91 Absatz 1 DSGVO eine Bestandsschutzregelung. Danach können diese, wenn sie zum Zeitpunkt des Inkrafttretens der DSGVO eigene umfangreiche Regelungen zum Datenschutz anwenden, diese Regeln weiterhin anwenden, sofern sie mit der DSGVO in Einklang gebracht werden. Für Kirchen und religiöse Vereinigungen, die im Zeitpunkt des Inkrafttretens der DSGVO nicht über ein umfangreiches Datenschutzregelungswerk verfügen, gilt hingegen die DSGVO i. V. m. dem BDSG.

Für die Bereiche Rundfunk und Medien sowie Kirchen und Religionsgemeinschaften können eigenständige Aufsichtsbehörden errichtet werden (Art. 85 Abs. 2, Art. 91 Abs. 2 DSGVO). In Deutschland haben die Medienunternehmen, die Rundfunkanstalten sowie

Eine besonders skurrile Berufung auf den Datenschutz der DSGVO ereignete sich in Berlin. Dort beklagte sich eine Kundin darüber, dass sie beim Einkauf von einer Metzgerei-Verkäuferin mit ihrem Namen angesprochen wurde. Eine derartige persönliche Ansprache sei nach der DSGVO unzulässig (Berliner Morgenpost, Online-Ausgabe vom 11.12.2018). Eine solche Zurückweisung einer freundlichen Begrüßung befremdet ebenso wie die diesbezügliche Berufung auf den Datenschutz. Die DSGVO befasst sich ausschließlich mit der ganz oder teilweise automatisierten Verarbeitung personenbezogener Daten sowie der nicht-automatischen Speicherung personenbezogener Daten in einem Dateisystem. Das gute Namensgedächtnis einer Verkäuferin ist aber ganz gewiss kein Dateisystem im Sinne der DSGVO.

die Katholischen Bistümer und die EKD jeweils eigene Datenschutzbeauftragte benannt bzw. eigene Datenschutzbehörden eingerichtet (zur Deutschen Welle vgl. u. Nr. 10.1.1). Da jeder Mitgliedstaat unabhängig von der Zahl der eingerichteten Datenschutzbehörden im EDSA mit nur einer Stimme sprechen kann, haben in Deutschland entsprechende Abstimmungen unter den Aufsichtsbehörden voranzugehen (vgl. u. Nr. 17.3). Bei diesen Abstimmungen haben die allgemeinen Datenschutzaufsichtsbehörden des Bundes und der Länder auch die nach Art. 85 und 91 DSGVO eingerichteten spezifischen Aufsichtsbehörden zu beteiligen, soweit diese betroffen sind (§ 18 Abs. 1 S. 4 BDSG). Zu dieser Thematik haben in meinem Haus mehrere konstruktive Gesprächsrunden mit Vertreterinnen und Vertretern der Datenschutzbehörden der Kirchen, Religionsgemeinschaften sowie von Medien und Rundfunk stattgefunden, bei denen auch der DSK-Vorsitz einbezogen wurde.

Ich empfehle dem Gesetzgeber klarzustellen, dass auch gegenüber den gesetzlichen Krankenkassen bei Verstößen gegen die DSGVO Geldbußen verhängt werden können, soweit diese als Wirtschaftsunternehmen tätig werden.

1.2 Umsetzung der Richtlinie (EU) 2016/680

Für die Datenverarbeitung bei Polizei und Justiz müssen seit dem 6. Mai 2018 einheitliche Mindeststandards in allen Mitgliedstaaten umgesetzt sein.

In meinem letzten Tätigkeitsbericht hatte ich über die Pflicht zur Umsetzung der Mindestvorgaben aus der Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 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) berichtet (vgl. 26. TB Nr. 1.2.2). Inzwischen ist die Umsetzungsfrist abgelaufen und der Bundesgesetzgeber hat mit dem neuen Bundesdatenschutzgesetz die Vorgaben der Richtlinie allgemein in nationales Recht umgesetzt. Der wesentliche Teil dieser Regelungen ist im dritten Teil des Gesetzes zusammengefasst, einige finden sich im ersten Teil mit den gemeinsamen Regelungen für alle Bereiche.

Auch verschiedene Fachgesetze mussten und müssen noch sukzessive angepasst werden. Den Auftakt hat der Bundesgesetzgeber mit dem neuen Bundeskriminalamtgesetz (BKAG) gemacht (vgl. u. Nr. 9.1.3). Für das Zollfahndungsdienstgesetz (ZfDG) und die Strafprozessordnung liegen Gesetzentwürfe zur Umsetzung der JI-Richtlinie vor (vgl. u. Nr. 9.1.4 und Nr. 11.1.2). Ein Entwurf zur Anpassung des Bundespolizeigesetzes steht noch aus.

Zu den Spezifika der Richtlinie gehören die Protokollierungspflichten und Vorgaben zur Gestaltung von Datenbanken, die besondere Kontrollfunktion der Aufsichtsbehörden bei der Einschränkung von Betroffenenrechten (sogenannter indirekter Zugang) und die nur ihrer Art nach geregelten Befugnisse der Aufsichtsbehörden.

Meiner Empfehlung, die Befugnisse der Aufsichtsbehörden analog der DSGVO zu regeln (vgl. 26. TB Nr. 1.2.2), ist der Gesetzgeber auf Bundesebene nicht gefolgt. So habe ich zwar umfassende Informations- und Untersuchungsbefugnisse, bei der Abhilfe bleibe ich jedoch wie früher auf das Mittel der Beanstandung beschränkt. Das neue BKAG sieht immerhin eine Anordnungsbefugnis nach Beanstandung erheblicher Datenschutzverstöße vor. Auch der Entwurf für ein neues ZfDG enthält einen entsprechenden Vorschlag und ich gehe davon aus, dass auch im Bundespolizeigesetz eine entsprechende Regelung geschaffen werden muss. Denn die Beanstandung alleine reicht nicht aus, um die Vorgaben der Richtlinie zu erfüllen, wonach die Aufsichtsbehörden in die Lage versetzt werden müssen, wirksam Abhilfe zu schaffen.

Als insgesamt ungünstige Entwicklung sehe ich einen uneinheitlichen Anwendungsbereich bei der Umsetzung der Richtlinie. Der Anwendungsbereich knüpft an den Begriff der Straftat an, der in der Richtlinie nicht abschließend definiert ist. Hierdurch besteht Umsetzungsspielraum insbesondere im Bereich der Verfolgung und Abwehr von Ordnungswidrigkeiten. Sowohl innerhalb Deutschlands als auch EU-weit wird dieser Raum unterschiedlich ausgefüllt. Dies reicht von der vollständigen Einbeziehung der Verfolgung von Ordnungswidrigkeiten (so auf Bundesebene in Deutschland) bis hin zur Beschränkung auf formale Straftaten nach nationalem Recht (so in verschiedenen anderen Mitgliedstaaten). Bedingt durch die unscharfe Vorgabe konnte hier eine Mindestharmonisierung leider nicht erreicht werden.

In den nächsten Jahren wird sich zeigen, wie sich die neuen Regelungen in der Praxis bewähren. Noch sind viele Einzelfragen zu beantworten, wie etwa zur Ausgestaltung der obligatorischen Verfahrensverzeichnisse, zur Durchführung von Datenschutzfolgenabschätzungen, zu den Melde- und Informationspflichten bei Datenschutzverstößen oder zum Umfang der Protokollierung.

Ich empfehle dem Gesetzgeber, Abhilfebefugnisse für den BfDI ins neue BPolG aufzunehmen. Diese sollten zumindest den bereits im neuen BKAG enthaltenen Befugnissen entsprechen.

1.2.1 „DSGVO-freie Räume“ im Bereich der Nachrichtendienste

Die Regelungen der DSGVO betreffen weder die Arbeit des Bundesnachrichtendienstes (BND) noch die Aufgabenwahrnehmung durch das Bundesamt für Verfassungsschutz (BfV) bzw. den Militärischen Abschirmdienst (MAD). Einige grundlegende Vorschriften gelten allerdings für das Militärische Nachrichtenwesen.

Die Auswirkungen der DSGVO sowie der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) sind im Bereich der Nachrichtendienste bzw. beim Sicherheitsüberprüfungsrecht vergleichsweise gering. Weder die DSGVO noch die JI-Richtlinie finden Anwendung auf das Recht der Nachrichtendienste im engeren Sinne oder den Bereich des Sicherheitsüberprüfungsgesetzes (SÜG). Die Nachrichtendienste müssen die DSGVO lediglich im Bereich der allgemeinen Behördenverwaltung anwenden. Der nationale Gesetzgeber hat einzelne Begrifflichkeiten sowie einige Normen, die er in Ergänzung der DSGVO bzw. in Umsetzung der JI-Richtlinie erlassen hat, für (entsprechend) auf die nachrichtendienstlichen Aufgabenbereiche des BND, des BfV und des MAD sowie im SÜG anwendbar erklärt. Im Wesentlichen bleibt hier allerdings alles so, wie es war.

Eine Ausnahme bildet das Militärische Nachrichtenwesen (MilNw): Dieser Bereich der Bundeswehr ist, wie der Name schon sagt, ähnlich wie die Nachrichtendienste, auf Nachrichten- und Informationsgewinnung angelegt, die auch die Erhebung und Verarbeitung personenbezogener Daten betreffen können. Die dazu eingesetzten Mittel ähneln im Einzelfall denen, die man aus dem nachrichtendienstlichen Bereich kennt. Ich habe daher schon immer vertreten, dass auch hier eine spezialgesetzliche Grundlage erforderlich ist. Diese fehlt bislang. Das Bundesministerium der Verteidigung (BMVg) ist anderer Auffassung. Es sieht Artikel 87 a und Artikel 24 Absatz 2 GG als ausreichende verfassungsrechtliche Grundlage für das Tätigwerden der Bundeswehr im Rahmen des MilNW und für die Verarbeitung personenbezogener Daten in diesem Zusammenhang.

Unabhängig davon arbeitet das BMVg derzeit an einem Erlass, wie Vorgaben des BDSG für das MilNW umgesetzt werden können. Dies betrifft u. a. die Vorschriften über die Meldung von Datenschutzverstößen sowie die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung. Ich bin mit dem BMVg hierzu im Gespräch.

Im Zuge der Umsetzung der DSGVO sowie der JI-Richtlinie hat der Gesetzgeber auch das Bundesnachrichtendienstgesetz, das Bundesverfassungsschutzgesetz sowie das Gesetz über den militärischen Abschirmdienst geändert. Anders als im Anwendungsbereich der DSGVO und der JI-Richtlinie verfüge ich gegenüber den Nachrichtendiensten weiter über keinerlei Sanktionsbefugnisse, wenn ich der Auffassung bin, dass eine Verarbeitung personenbezogener Daten rechtswidrig ist. Die Einstellung rechtswidriger Tätigkeiten der Nachrichtendienste kann daher weiterhin letztlich nur gerichtlich durch Klagen einzelner Betroffener erzwungen werden, was bei den ohnehin eingeschränkten Rechtsschutzmöglichkeiten der Betroffenen faktisch aber nur sehr schwierig erreichbar ist.

Ich empfehle daher dem Gesetzgeber, Sanktionsbefugnisse für meine Behörde auch im Bereich der Nachrichtendienste einzuführen.

1.3 Neue Entwicklungen im Bereich Grenzkontrollen und Fluggastdaten

Daten zu Reisebewegungen stehen verstärkt im Fokus der Sicherheitsbehörden. Die bestehenden Informationssysteme werden in den nächsten Jahren mit Daten angereichert, neue Systeme kommen hinzu und alle Systeme werden nach einem gerade verhandelten Verordnungsentwurf unter dem Dach der Interoperabilität miteinander verflochten. So soll dem Identitätsbetrug und damit verbundenen Sicherheitsrisiken Einhalt geboten werden. Die Datenschutzaufsichtsbehörden wird dieses Projekt vor enorme Herausforderungen stellen.

In meinen vergangenen Tätigkeitsberichten habe ich sowohl die unter dem Schlagwort „Smart Borders“ verfolgten Projekte (vgl. 24. TB Nr. 2.5.3.4; 25. TB Nr. 3.3; 26. TB Nr. 2.3.1) als auch alle Projekte rund um die Verwendung von Fluggastdaten für den Sicherheitsbereich (vgl. 22. TB Nr. 13.5.5; 26. TB Nr. 2.3.2) kritisch beleuchtet. Inzwischen ist hier überall ein neues Stadium erreicht worden.

Der Startschuss für die erste neue Großdatenbank erfolgte bereits Ende Dezember 2017 mit der Verordnung (EU) 2017/2226 über ein Einreise-/Ausreisesystem (Entry Exit System, EES). Auf dieser Grundlage wird eine Datenbank errichtet, in der künftig alle Grenzübertritte von Drittstaatsangehörigen an den Schengen-Außengrenzen erfasst und für mindestens drei Jahre ab Ausreise gespeichert werden. Zum Datensatz gehören Lichtbilder und Fingerabdrücke. Wenn zwischen Ausreise und nächster Einreise weniger als drei Jahre liegen, werden außerdem alle vorhandenen Daten weiter gespeichert. Durch diese Mitziehautomatik können umfassende Reisehistorien entstehen.

Die zweite neue Datenbank soll das Visa-Informationssystem (VIS) ergänzen. Die Rechtsgrundlagen für

das neue Europäische Reiseinformations- und -genehmigungsportal (European Travel Information and Authorisation System, ETIAS) sind mit der Verordnung (EU) 2018/1240 Ende Oktober 2018 in Kraft getreten. Über dieses System müssen künftig alle visumbefreit einreisenden Drittstaatsangehörigen vorab eine Einreisegenehmigung beantragen. Ihre Daten werden einer vorgezogenen automatisierten Überprüfung auf Sicherheits-, Migrations- und Gesundheitsrisiken unterzogen und bleiben im Regelfall drei Jahre, bei Ablehnung sogar fünf Jahre gespeichert.

Der Aufbau neuer Datenbanken wird begleitet von einer intensiven Anreicherung und Ausweitung der bestehenden Datenbanken. So sollen in VIS künftig auch Langzeitvisa und Aufenthaltserlaubnisse erfasst werden (vgl. Nr. 2.2). Im Asylsystem Eurodac sollen künftig auch Drittstaatsangehörige registriert werden, die bei einem illegalen Aufenthalt oder einer illegalen Grenzüberquerung angetroffen werden. Das Schengener Informationssystem der zweiten Generation (SIS II) wird um neue Ausschreibungstatbestände (u. a. zur verdeckten Untersuchung/Befragung) und Datenkategorien (u. a. Handabdrücke) ergänzt und insgesamt für eine Abwicklung der Rückführung von sich illegal aufhaltenden Drittstaatsangehörigen nutzbar gemacht. Die neuen Regelungen waren zum Zeitpunkt des Redaktionsschlusses bereits beschlossen, aber noch nicht unterzeichnet und verkündet.

Zwei weitere Verordnungsvorschläge zur sogenannten Interoperabilität werden derzeit noch beraten und sollen die oben genannten Datenbanken mit Hilfe einer gemeinsamen Suchmaske (European Search Portal, ESP) und drei neuer Datenbanken miteinander verknüpfen, um Identitätsbetrug aufzudecken und zu verhindern. Hierzu sollen alle vorhandenen biometrischen Identifizierungsdaten in sogenannte Templates (mathematische Abbilder) umgerechnet und in einem gemeinsamen Biometrischen Identifikationsdienst (shared Biometric Matching Service, sBMS) für einen schnellen Abgleich hinterlegt werden. Die Fachanwendungen VIS, Eurodac, EES und ETIAS sollen darüber hinaus ein gemeinsames Identitätsregister (Common Identity Repository, CIR) erhalten, in dem alle Identitätsdaten einschließlich der biometrischen Originale hinterlegt werden. Nur die SIS-Daten bleiben – aus technischen Gründen – außerhalb des CIR. Bei jeder Eingabe oder Aktualisierung von Daten in den Fachanwendungen soll dann künftig im ersten Schritt über den sBMS und das ESP (im SIS und im CIR) ein Abgleich stattfinden. Hierbei erzielte Treffer werden den zuständigen Stellen zur Bearbeitung gemeldet und zugleich im sogenannten Multiple Identity Detector (MID) nach verschiedenen Kategorien abgespeichert.

Zu allen Rechtsakten haben sich sowohl die Datenschutzbehörden der Mitgliedstaaten als auch der Europäische Datenschutzbeauftragte kritisch positioniert und verschiedene Bedenken vorgetragen, jedoch wenig Gehör gefunden. Die gezielte Erweiterung bestehender Informationssysteme zusammen mit dem Aufbau neuer Datenbanken und dem vorgeschlagenen komplexen System der Interoperabilität sind höchst besorgniserregend. Insbesondere der Grundsatz der Zweckbindung erhobener Daten droht hierbei immer weiter aufzuweichen. Die Identifizierung von Drittstaatsangehörigen mit Hilfe eines umfassenden biometrischen und alphanumerischen Identitätsregisters wird hier zum fachübergreifenden Selbstzweck.

Weiter verdichtet werden die verfügbaren Daten noch durch die inzwischen in verschiedenen Staaten umgesetzte Fluggastdaten-Richtlinie. In Deutschland gilt seit Juni 2017 das Fluggastdatengesetz (FlugDaG), wonach alle Luftfahrtunternehmen verpflichtet sind, die von ihnen zum Zwecke der Flugdienstleistung erhobenen Fluggastdaten (sogenannte Passenger Name Records, PNR) an eine dafür beim Bundeskriminalamt (BKA) eingerichtete Fluggastdatenzentrale (Passenger Information Unit, PIU) zu übermitteln, soweit es sich nicht um innerdeutsche Flüge handelt. Vergleichbares muss in allen Mitgliedstaaten erfolgen. In Deutschland hat die PIU Ende August 2018 ihren Wirkbetrieb aufgenommen. Die eingehenden Fluggastdaten dürfen sowohl mit Fahndungsdatenbanken als auch mit abstrakten Gefährdungsmustern abgeglichen werden. Infolge eines solchen Abgleiches können Fluggäste in das Visier polizeilicher Maßnahmen geraten, ohne hierfür selbst einen konkreten Anlass gegeben zu haben, nur weil Ähnlichkeiten zum Verhalten von straffälligen Personen bestehen. Schon dies ist höchst bedenklich. Hinzu kommt die fünfjährige Speicherdauer für alle Fluggastdaten, die eine rückwirkende Recherche zur Verhütung und Verfolgung terroristischer oder sonstiger schwerer Straftaten ermöglicht. Hier erwächst bei einer Polizeibehörde eine langzeitverfügbare Datenbank über Personen, die außer einer Flugreise mehrheitlich keinerlei konkreten Anlass für einen Eintrag in einer polizeilichen Vorsorgedatenbank gegeben haben. Auch dies halte ich für extrem bedenklich, zumal inzwischen der Europäische Gerichtshof in einem Gutachten zum geplanten Fluggastdatenabkommen der EU mit Kanada gerade die langfristige anlasslose Speicherung als unvereinbar mit der Europäischen Grundrechtecharta gerügt hat.

Ich empfehle der Bundesregierung, im Hinblick auf die Vorgaben des EuGH zu PNR Kanada, das FlugDaG zu überarbeiten und sich in Brüssel für eine Überarbeitung der Richtlinie (EU) 2016/681 einzusetzen.

Datenethikkommission – DEK

Die DEK wurde von der Bundesregierung im Herbst 2018 ins Leben gerufen. Aufgabe der DEK ist es, bis Herbst 2019 Handlungsempfehlungen für die künftige Datenpolitik der Bundesrepublik zu entwickeln. Die DEK soll Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstandes im Informationszeitalter entwickeln. Zudem sollen Handlungsempfehlungen ausgesprochen werden, wie diese ethischen Leitlinien entwickelt, beachtet, implementiert und beaufsichtigt werden können.

Die DEK gibt es seit

Herbst 2018

Die DEK hat neben mir 15 weitere Mitglieder. Bei den Mitgliedern handelt es sich um Datenschutzaufsichtsbehörden, Professorinnen und Professoren verschiedener Fachrichtungen, Vertreter des Verbraucherschutzes und der Industrie. Weitere Informationen sind auf dem Internetauftritt der DEK unter https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html abrufbar.

1.4 Künstliche Intelligenz

Das Bundeskabinett hat am 15. November 2018 die von den Bundesministerien für Wirtschaft und Energie, für Bildung und Forschung sowie für Arbeit und Soziales gemeinsam vorgelegte Strategie Künstliche Intelligenz (KI) verabschiedet. Mit der Strategie Künstliche Intelligenz verfolgt die Bundesregierung das Ziel, Deutschland und Europa zu einem führenden Standort für Innovationen und die Anwendung von KI-Technologien zu entwickeln und dadurch die Wettbewerbsfähigkeit Deutschlands zu sichern.

Bandbreite und Einsatzmöglichkeiten der KI sind schon heute enorm. Sie reichen vom einfachen Errechnen von Wegerouten über Bild- und Spracherkennung bis hin zu überaus komplexen Entscheidungs- und Vorhersageumgebungen. Selbstlernende Algorithmen überprüfen kontinuierlich ihre eigenen Rechenabläufe und schreiben sie fort. Zu erwarten ist die Entwicklung immer selbstständigerer und umfassenderer Anwendungen, die immer mehr menschliches Verhalten in immer breiteren Handlungsfeldern automatisieren und teilweise ersetzen sollen. Dabei wird eine zunehmende Menge personenbezogener Daten verarbeitet werden. Gleichzeitig werden die Verarbeitungswege für die betroffenen Personen immer schwerer nachvollziehbar. Ebenso komplex wie die Einsatzmöglichkeiten sind deshalb die mit KI-Technologien einhergehenden Risiken für die informationelle Selbstbestimmung einzelner Betroffener.

Deshalb habe ich die Entstehung der KI-Strategie begleitet und mich dafür eingesetzt, den Schutz der Privatsphäre als essentiellen Bestandteil der Förderung von Innovation zu verstehen und die Vorgaben der DSGVO von Beginn an als Qualitätsmerkmale für eine verantwortungsvolle und gemeinwohlorientierte Entwicklung und Nutzung von KI zu verstehen. In der Datenethikkommission (DEK – vgl. nebenstehender Informationskasten) haben wir Anfang September 2018 das Eckpunktepapier der Bundesregierung diskutiert und datenschutzrechtliche Empfehlungen für die KI-Strategie erarbeitet.

Auf dieser Grundlage konnte ich wichtige datenschutzrechtliche Aspekte beim Forum „Arbeitswelt und Arbeitsmarkt“ des Bundesministeriums für Arbeit und Soziales Mitte September 2018 einbringen, dessen Ergebnisse wiederum in die KI-Strategie eingeflossen sind.

Wichtige Punkte, wie der Beschäftigtendatenschutz im Bereich von KI-Anwendungen, die Nutzung moderner Pseudonymisierungs- und Anonymisierungsverfahren, die Notwendigkeit von Technikfolgenabschätzungen oder die datenschutzkonforme Erschließung großer Datenmengen, werden an mehreren Stellen innerhalb der

KI-Strategie berücksichtigt. Die Empfehlungen der DEK sind mehrfach erwähnt. Außerdem wird die Einrichtung eines Runden Tisches mit Datenschutzaufsichtsbehörden und Wirtschaftsverbänden angekündigt, um gemeinsame Leitlinien für eine datenschutzrechtskonforme Entwicklung und Anwendung von KI-Systemen zu erarbeiten und Best-Practice-Anwendungsbeispiele aufzubereiten. Insgesamt lässt sich festhalten, dass die Perspektive des Datenschutzes an erfreulich vielen Stellen in der KI-Strategie Erwähnung findet. Ob und inwieweit diese dann auch bei der weiteren Umsetzung der Strategie berücksichtigt werden, muss sich erst zeigen. Ich werde die weitere Ausarbeitung und Umsetzung der KI-Strategie kritisch begleiten.

Auch die Datenschutzkonferenz, das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, wird sich 2019 mit Datenschutzfragen beim Einsatz von Künstlicher Intelligenz befassen.

Die Internationale Datenschutzkonferenz hat im Oktober 2018 eine Erklärung zu Ethik und Datenschutz bei KI abgestimmt. In dieser Resolution werden u. a. sechs Prinzipien formuliert, die bei der Anwendung von Künstlicher Intelligenz stets beachtet werden sollten:

- Fairness,
- Nachverfolgbarkeit,
- Transparenz,
- Privacy by design,
- starke Betroffenenrechte und
- das Vermeiden von eingebauten Vorurteilen bzw. Diskriminierungen.

Ich unterstütze diese Resolution ausdrücklich und erachte es als sinnvoll und hilfreich, wenn die internationale Datenschutzgemeinschaft bestimmte Leitprinzipien für die Entwicklung und Anwendung von Systemen mit Künstlicher Intelligenz formuliert. Dies betrifft beispielsweise Einsatzgebiete von Künstlicher Intelligenz bei Handschrift-, Bild-, Gesichtserkennung, selbstfahrenden Kraftfahrzeugen, Suchmaschinen, Diagnostik und Marketing, ebenso wie die weiteren Entwicklungsmöglichkeiten.

1.4.1 Blockchain – ohne Datenschutz?

Die Bundesregierung plant, bis Mitte 2019 eine Blockchain-Strategie vorzulegen. Die Federführung für diese Strategie liegt beim Bundesministerium für Wirtschaft und Energie und beim Bundesministerium der Finanzen. Mithilfe eines Konsultationsprozesses soll sichergestellt werden, dass Hinweise und Empfehlungen von Marktakteuren, Wissenschaft und anderen Stakeholdern zum politischen Handlungsbedarf berücksichtigt werden.

Unter Blockchain versteht man im Allgemeinen eine kontinuierlich erweiterbare Liste von Datensätzen, genannt Blöcke, die mittels kryptografischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise den Hashwert des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten. So sind Existenz und Inhalt einzelner Blöcke später nicht mehr veränderbar, ohne dass dies in allen hierauf aufbauenden Blöcken zu Unregelmäßigkeiten führt. Der große Vorteil der Blockchain liegt in der Unverfälschbarkeit der Datenkette und bietet sich für Finanztransaktionen an. Insofern ist der Begriff der Blockchain verbunden mit der Distributed-Ledger-Technologie. Das „Distributed Ledger-Konzept“ bezeichnet ein öffentliches, dezentrales Kontobuch und ist die technologische Grundlage virtueller Währungen.

Die Bundesregierung fördert Blockchain-Pilotprojekte in den Bereichen Elektromobilität, Stromhandel und Migration. Den möglichen Einsatz der Blockchain-Technologie beim Bundesamt für Migration und Flüchtlinge habe ich insbesondere im Hinblick auf die datenschutzgerechte Konzeptionierung und Implementierung überprüft (vgl. u. Nr. 9.3.1).

Die zentralen Herausforderungen beim datenschutzkonformen Einsatz der Blockchain-Technologie betreffen die Rechte des Betroffenen auf Löschen, Korrektur und „Vergessenwerden“.

1.5 Datensouveränität und Dateneigentum

Ein viel diskutiertes Thema der letzten zwei Jahre war die sogenannte Datensouveränität, die als eine Art Gegenentwurf oder zumindest Weiterentwicklung zum bisherigen Datenschutz dargestellt wurde.

Die erste größere Aufmerksamkeit fand der Begriff auf dem Nationalen IT-Gipfel im Jahr 2016. Der damalige Bundesminister für Wirtschaft und Energie, Sigmar Gabriel, meinte, man müsse sich endgültig vom klassischen Datenschutzbegriff verabschieden, da dieser mit seinem „Datenminimierungsgedanken“ modernen Anwendungen wie „Big Data“ im Weg stünde. Dem Bürger solle stattdessen sowohl physische als auch rechtliche Souveränität im Umgang mit Daten gegeben werden. Dem pflichtete Bundeskanzlerin Angela Merkel zumindest insofern bei, indem sie davon sprach, das Prinzip der Datensparsamkeit könne nicht mehr die Richtschnur für neuartige Produkte sein.

Genauere Ausführungen, was Datensouveränität nun im Einzelnen bedeute, blieben beide in der Veranstaltung schuldig. Ein Blick in das „Grünbuch – Digitale Plattformen“ des Wirtschaftsministeriums offenbart, dass Datensouveränität einer digitalen Privatautonomie gleichkommen soll, die durch weitgehende Transparenzvorschriften der Informationsasymmetrie, die aktuell zwischen Verarbeiter und Verbraucher häufig vorliege, vorbeugen soll. Gleichzeitig soll Datensouveränität eine Kommerzialisierung von Daten ermöglichen.

Im Großen und Ganzen zeigt die nähere Beschreibung der vorgestellten Datensouveränität allerdings lediglich Aspekte, die entweder bereits durch das bestehende Datenschutzrecht (u. a. die DSGVO) geregelt sind oder keinen unmittelbaren Bezug zum Datenschutz haben. Neue Transparenzvorschriften, Datenportabilität, Zugriffsbeschränkung für Dritte, Privacy by Design und Default sind Gegenstand der DSGVO. Ausführungen im Grünbuch zu „neuen Formen der Einwilligung“ oder zu einem „ausdifferenzierten Identity Managements“ bleiben im Ungefähren. Letzteres geht zwar auf Möglichkeiten zur Einstellung verschiedener Sphären der eigenen Daten ein, aber eine in diesem Zusammenhang vorgeschlagene zentrale Identifikationsdatenbank, bei der der Betroffene eben jene Einstellungen gegenüber Unternehmen und Dritten bezüglich der Offenlegung seiner Daten vornehmen kann, birgt ganz eigene Risiken. Eine solche zentrale Datenbank wäre ein herausgestellter Angriffspunkt, bei dem im Zweifel alle personenbezogenen Daten eines Betroffenen, wenn nicht gar aller, die dort eingetragen sind, kompromittiert werden könnten. Zudem wäre diese zentralisierte Ansammlung personenbezogener Daten verfassungsrechtlich fragwürdig.

An Fahrt gewann die Diskussion über den Begriff der Datensouveränität dann erst wieder Mitte 2017, als das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) eine Studie zum Thema „Eigentumsordnung spezifischer Mobilitätsdaten“ vorstellte. Einige Ansätze dieser Studie wurden auch Teil eines Strategiepapiers des Ministeriums zur Digitalen Souveränität. Auch an dieser Stelle sollte der Ansatz der Datensparsamkeit aufgegeben werden. Stattdessen sollten die personenbezogenen Daten wirtschaftlich besser nutzbar gemacht werden können, sowohl für die Unternehmen als auch für den Einzelnen. Hierfür müssten neue Wertschöpfungsmöglichkeiten geschaffen werden. Beispielsweise solle der Bürger die Möglichkeit erhalten, sich frei zu entscheiden, ob er Daten als Gegenleistung preisgibt oder stattdessen eine reguläre Bezahlmöglichkeit wahrnehmen möchte. Personenbezogene Daten müssten hierfür eigentumsfähig und zuordenbar gemacht werden. Die anschließende Nutzung dürfte allerdings nur anonymisiert und pseudonymisiert erfolgen. Im speziellen Umfeld moderner Fahrzeuge könnte Transparenz durch einen Datenpass hergestellt werden.

Für die konkrete Umsetzung einer Eigentumsfähigkeit, die notwendigerweise ein ausschließliches Verfügungsrecht umfassen muss, schlagen die Autoren der Studie mehrere Ansätze vor:

1. Ein datenspezifischer Ansatz, bei dem ähnlich dem bisherigen Datenschutzrecht das Ausschließlichkeitsrecht zunächst beim Betroffenen liegt.

2. Ein gegenständlicher Ansatz, bei dem das Ausschließlichkeitsrecht dem Eigentum an der Anlage zur Datenerhebung folgt (Beispiel: Monitoringanlage als Teil eines Kfz gehört dem Fahrzeugeigentümer, der so auch das Ausschließlichkeitsrecht über die Daten erhält).

3. Zuletzt ein handlungsbezogener Ansatz, bei dem der für die ursprüngliche Datenerhebung Verantwortliche das ausschließliche Verfügungsrecht erhält.

Die Autoren neigten dabei am ehesten dem handlungsbezogenen Ansatz zu, während das BMVI selbst in seinem Strategiepapier eher den datenspezifischen Ansatz verfolgte und Parallelen zum Urheberrecht zog. Der Bürger könnte also statt Eigentum an seinen Daten eine Art Nutzungslizenz für diese übertragen.

Beide Vorschläge sind allerdings nicht nur im Hinblick auf das bestehende Datenschutzrecht kritisch zu bewerten, sondern bereits aus Sicht des verfassungsrechtlich garantierten informationellen Selbstbestimmungsrechts.

Gerade beim Beispiel der Mobilität wären hiernach häufig Dritte Dateneigentümer, ganz gleich, ob der Betroffene selbst fährt oder das Fahrzeug verleiht oder vermietet, da der Betroffene selbst für die Datenerhebung eben meist nicht verantwortlich ist. Dieser hat im Zweifel ja auch gar kein Interesse an der Erhebung. Stattdessen würden die Fahrzeughersteller oder spezialisierte Firmen Dateneigentümer. In diesem Falle würde auf übertriebene Weise die Sichtweise auf Daten als Rohstoff verinnerlicht. Im übertragenen Sinn wäre der jeweilige Schürfer auch der Eigentümer am Datengold.

Personenbezogene Daten sind aber kein beliebiges Handelsobjekt, sondern stets Teil einer bestimmten natürlichen Person, deren Menschenwürde unveräußerlich ist. Unter anderem aus dieser Menschenwürde leitet sich auch das Recht auf informationelle Selbstbestimmung ab. Beim handlungsgezogenen Ansatz würden diese Teile der Person dem Schutz der Würde entzogen und zum reinen Handelsobjekt herabgestuft. Der Gedanke vom Menschen als Rohstoff ist mit unserer gesellschaftlichen Ordnung jedoch nicht vereinbar. Nicht umsonst war

„Humankapital“ bereits das Unwort des Jahres 2004 und „Menschenmaterial“ das Unwort des 20. Jahrhunderts.

Ein ausschließliches Verfügungsrecht als notwendiger Baustein des Dateneigentums könnte durch den Rahmen, den das Recht auf informationelle Selbstbestimmung setzt, aktuell auch gar nicht gesetzlich umgesetzt werden. Der Betroffene hat stets eigene Rechte bezüglich der ihn betreffenden Daten, die so lange fortbestehen, wie er durch diese Daten identifizierbar ist. Wer auch immer Dateneigentümer ist, könnte nicht unbeschränkt über diese Daten verfügen. Der Sinn und Zweck des Eigentums wäre verfehlt. Dieser Widerspruch zeigt sich besonders deutlich, wenn man dem Dateneigentum konkrete Regelungen der DSGVO gegenüberstellt. Ein Beispiel hierfür ist Art. 7 Absatz 3 DSGVO, nach dem der Betroffene seine Einwilligung jederzeit widerrufen kann. Hängt die Rechtmäßigkeit der Verarbeitung von eben jener Einwilligung ab, kann ab dann keine rechtmäßige Verfügung mehr über diese ggf. im Eigentum eines Dritten befindlichen Daten getroffen werden. Die effektive Verfügungsmöglichkeit des „Eigentümers“ wäre mit einem Schlag auf null reduziert. Diese Problematiken gelten dabei nicht nur für den handlungsbezogenen Ansatz, sondern auch für den datenspezifischen, ans Urheberrecht angelehnten. Auch bei der Vergabe einer Nutzungslizenz durch den Betroffenen wären Möglichkeiten zum Widerruf oder zur Auskunft gegeben.

Die These vom Dateneigentum als einer besonderen Ausprägung der Souveränität offenbart ebenfalls Schwächen. Daten sind zwar der Rohstoff der Informationsgesellschaft, aber eben nur begrenzt vergleichbar mit dem vielfach erwähnten Gold oder Öl. Während Eigentum an diesen Ressourcen vollständig möglich ist, ohne die Rechte anderer einzuschränken, ist dies bei Daten häufig nicht der Fall. Personenbezogenen Daten ist es inhärent, dass hinter jedem Datum ein Mensch steht, dessen grundlegendes Interesse, frei von Beobachtung zu sein, beim Umgang mit diesen Daten stets eine Rolle spielt. Dieses grundlegende Interesse lässt sich zwar in Einklang bringen mit ebenfalls schützenswerten wirtschaftlichen Interessen, kann aber durch Letztere nicht ersetzt werden. Ein ausschließliches Recht an personenbezogenen Daten würde letztlich den Boden eines verhältnismäßigen Ausgleichs zwischen diesen beiden Interessen verlassen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder kommt in ihrer 2017 verabschiedeten Göttinger Erklärung zum Wert des Datenschutzes in der digitalen Gesellschaft zum gleichen Schluss: Verstanden als eigentumsähnliche Verwertungshoheit kann „Datensouveränität“ nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen. Auch im digitalen Zeitalter bleibt die Menschenwürde und die freie Entfaltung der Persönlichkeit der Maßstab, an dem sich staatliches wie wirtschaftliches Handeln zu orientieren hat.

Insgesamt zeigt sich, dass die Diskussion über Datensouveränität zwar einige interessante Gedanken enthält, aber eben kein großer Wurf weg vom „klassischen“ Datenschutzrecht ist. Eine Erkenntnis, die im Grunde schon im Begriff „Souveränität“ selbst liegt, da dieser ohnehin nichts anderes bedeutet, als Selbstbestimmungsmöglichkeit, den Kern des Datenschutzrechts.

1.6 Digitalisierung in Fahrzeugen nicht ohne ausreichenden Schutz der Privatsphäre

Das Thema „Datenschutz im Kraftfahrzeug“ beschäftigt die Medien, seit immer mehr Fahrzeuge auf den Markt kommen, die Online-Dienste anbieten. Dabei zeigt sich das Bemühen der Hersteller, den Fahrzeugnutzern auch Möglichkeiten für eine datenschutzfreundliche Anwendung zu geben.

Meine Kolleginnen und Kollegen in den Ländern und ich haben uns in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder wiederholt zur datenschutzgerechten Nutzung von Fahrzeugdaten geäußert. Aus unserer Sicht sind die folgenden zentralen Punkte zu beachten:

- Alle beim Betrieb von Fahrzeugen anfallenden Daten werden durch den individuellen Gebrauch des Fahrzeugs beeinflusst und sind deshalb personenbezogen. Somit gibt es keine Daten, die von vornherein datenschutzrechtlich irrelevant sind.
- Die Automobilindustrie ist verantwortlich 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 müssen die im Fahrzeug ablaufenden Datenerhebungs- und -verarbeitungsvorgänge umfassend transparent gemacht 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 Ergebnis geführt (abrufbar unter www.datenschutz.bund.de). 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 Transparenzpflichten 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. Der Dialog wird fortgesetzt, damit den mit dem Einzug der Digitalisierung im Mobilitätssektor neu entstehenden Herausforderungen für den Schutz der Privatsphäre frühzeitig begegnet werden kann.

Automatisiertes und Vernetztes Fahren

Mit der Digitalisierung im Automobil- und Verkehrssektor werden Cybersicherheit und Datenschutz auch in diesem Bereich zu wichtigen Themen. So habe ich im Berichtszeitraum das BMVI bei der Novellierung des Straßenverkehrsgesetzes beraten, die mit dem Ziel durchgeführt wurde, automatisierte Fahrfunktionen für den Straßenverkehr in Deutschland zuzulassen. Auf mein Betreiben hin wurde dabei insbesondere der im Auto zu Beweiszwecken im Fall eines Unfalls zu speichernde Datenumfang auf das notwendige Maß beschränkt. Gespeichert werden dürfen nur Ort und Zeitpunkt der Übernahme bzw. Abgabe der Fahrzeugführung durch eine automatisierte Fahrfunktion und Ort und Zeitpunkt des Auftretens einer Fehlfunktion. Bei dem Erlass der Verordnung zur Regelung der technischen Details werde ich darauf achten, dass cybersichere und die Privatsphäre schützende technische Anforderungen einen Datenschutz auf dem Stand der Technik gewährleisten.

Darüber hinaus berate ich den vom BMVI eingerichteten „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 technischer 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. 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 festgelegten Mindestanforderungen an die Cybersicherheit und den Datenschutz erfüllen.

Auf meine Einladung haben am 1. Juni 2017 rund 130 Gäste in Berlin über Datenschutzaspekte der automatisierten und vernetzten Mobilität diskutiert. In einem zum Symposium veröffentlichten Positionspapier habe ich 13 Empfehlungen für den Datenschutz im vernetzten und automatisierten Fahrzeug und in digitalisierten Verkehrssystemen formuliert (abrufbar unter www.datenschutz.bund.de). So ist etwa für den reinen Fahrbetrieb in der Regel keine Datenspeicherung erforderlich. Müssen Daten zwischen Fahrzeugen ausgetauscht werden, sollten sie wirksam verschlüsselt und vor unbefugter Nutzung geschützt werden. Auch sollte es Nutzerinnen und Nutzern möglich sein, personenbezogene Daten zu löschen, soweit die Speicherung nicht gesetzlich notwendig ist. Diese Empfehlungen haben Eingang in einen Beschluss der Internationalen Datenschutzkonferenz gefunden, den diese auf ihrer 39. Tagung vom 25. bis 29. September 2017 in Hongkong auf meine Veranlassung hin gefasst hat (vgl. hierzu auch Nr. 2.5).

Car-to-Car-Kommunikation

In diesem Zusammenhang befasse ich mich auch mit der sogenannten Car-to-Car-Kommunikation. Es handelt sich 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. Gemeinsam mit meinen europäischen Kollegen habe ich deshalb an die Europäische Kommission appelliert, bei der Regulierung intelligenter Verkehrssysteme den Anforderungen der Datenschutz-Grundverordnung gebührend Rechnung zu tragen.

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 im Hinblick auf ein Mehr an Verkehrssicherheit von Vorteil für die auf Mobilität angewiesene Gesellschaft. Das erlaubt es der Industrie aber nicht, ihre datenschutzrechtliche Verantwortung für die von ihr verbauten Systeme zu vernachlässigen. Wichtig sind Transparenz, Datensparsamkeit und weitestgehende Erhaltung der Datenherrschaft beim Betroffenen.

Ich freue mich deshalb, dass in vielen neu zugelassenen Fahrzeugtypen mit Online-Diensten meine datenschutzrechtlichen Empfehlungen umgesetzt werden. Fahrzeugnutzer können datenschutzfreundliche Einstellungen vornehmen, ohne dazu eine Werkstatt aufsuchen zu müssen. Ich bin zuversichtlich und werde mich dafür einsetzen, dass auch die Cybersicherheit der online-fähigen Fahrzeuge überprüfbar gewährleistet wird. Kunden werden nach meiner Überzeugung beim Kauf neuer Fahrzeuge auf deren Cybersicherheit sowie die Möglichkeiten für einen aktiven Datenschutz achten und den Grad ihres Vertrauens in die Hersteller daran messen.

1.7 Datenschutz für Kinder stärker in den Fokus nehmen

„Ich sehe Daten, die du nicht siehst …“
Unter diesem Motto stand eine Konferenz, die ich Anfang Juli 2018 in Zusammenarbeit mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V., Deutschland sicher im Netz (DsiN) e. V. und dem Institut für Medienforschung und Medienpädagogik der Technischen Hochschule Köln in der Landesvertretung Niedersachsen in Berlin für Kinder und Medienexperten ausgerichtet habe.

Im Mittelpunkt dieser Veranstaltung, an der rund 130 Experten aus den Bereichen der Medienbildung, Pädagogik, Datenschutz und Politik sowie 70 Kinder und Jugendliche im Alter ab zwölf Jahren teilgenommen haben, stand die Frage, wie junge Heranwachsende in Anbetracht der täglich von ihnen genutzten Medienangebote selbst über das Thema Datenschutz denken, was ihnen wichtig ist und wo aus ihrer Sicht noch Verbesserungen möglich wären.

Zwei von den Partnern DsiN und BvD jeweils unterstützte Berliner Grundschulklassen hatten sich kurz vor den Sommerferien intensiv mit diesem Thema beschäftigt und die Ergebnisse ihrer Workshops in der Konferenz kompetent und selbstbewusst präsentiert. Im anschließenden unmittelbaren Dialog mit den Experten gelang es, zentrale Fragen des Umgangs von Minderjährigen mit den häufig gezielt auf diesen Nutzerkreis zugeschnittenen Medienangeboten unter dem Blickwinkel des Datenschutzes näher zu beleuchten und die damit einhergehenden Probleme aufzuzeigen. Mir war es wichtig, die Gedanken, Sorgen und Ideen der Kinder zum Datenschutz im Zusammenhang mit modernen Medien einmal aus erster Hand zu erfahren und ihnen gleichzeitig ein Forum zu bieten, sich darüber mit Experten auszutauschen. Dieses Angebot ist bereitwillig aufgegriffen worden und es war beeindruckend zu erleben, mit welchem Selbstverständnis, aber auch wie kritisch und mitunter selbstkritisch die Schülerinnen und Schüler über das Thema Datenschutz in ihrem eigenen Lebensumfeld diskutieren. Das dazu gewählte und für meine Behörde neue Format einer Dialogkonferenz hat sich bewährt und bietet sich für vergleichbare Veranstaltungen, insbesondere wenn es um die gezielte Ansprache und Einbeziehung von Kindern geht, auch für die Zukunft an.

Als wichtige Erkenntnis aus dieser Konferenz nehme ich mit, dass das Thema Datenschutz bei der Vermittlung digitaler Kompetenzen in der Ausbildung von Heranwachsenden noch stärker in den Mittelpunkt gerückt werden sollte. Das kann aber nicht allein in die Verantwortung der Schulen gelegt werden – auch das private Erziehungsumfeld von Kindern und Jugendlichen ist gezielt einzubinden. Es bedarf noch mehr Aufklärung darüber, welchen Beitrag z. B. die Eltern oder Verantwortliche in Vereinen leisten können, um Kinder auf die in der neuen digitalen Welt lauernden Risiken vorzubereiten und sie sowohl für den Schutz der eigenen Persönlichkeit, aber auch den Respekt vor der Persönlichkeit des

anderen zu sensibilisieren. In diesem Zusammenhang habe ich einige Empfehlungen für einen kindgerechten Datenschutz im Umgang mit digitalen Medien formuliert (vgl. nebenstehende Empfehlungen).

Die für die Einhaltung der Datenschutzvorschriften verantwortlichen Aufsichtsbehörden des Bundes und der Länder sehen sich hier ebenfalls in der Pflicht. Sie sind nach der DSGVO dazu angehalten, die Öffentlichkeit u.a. für die Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und darüber aufzuklären. Hierbei sollen auch spezifische Maßnahmen für Kinder vorgesehen werden. Mit der seit Jahren gemeinsam und mit Erfolg betriebenen Internetseite „youngdata“ (https://www.youngdata.de) und den dort speziell für Kinder und Jugendliche aufbereiteten Beiträgen und weiterführenden Hinweisen zum Thema Datenschutz haben die Aufsichtsbehörden insoweit bereits ein wegweisendes Projekt etabliert. Die Bedeutung dieses Themas hat auch der deutsche Gesetzgeber erkannt und mir in § 14 Absatz 1 Nummer 2 BDSG ausdrücklich die Aufgabe der öffentlichen Sensibilisierung und Information im Hinblick auf die datenschutzrechtlichen Belange von Kindern und Jugendlichen zugewiesen. Die Durchführung der Dialogkonferenz Datenschutz für Kinder war ein erster Schritt, dem weitere spezifische Beratungs- und Aufklärungsangebote für Kinder und junge Erwachsene folgen sollen.

Empfehlungen

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
für einen kindgerechten Datenschutz im Umgang mit digitalen Medienangeboten

Empfehlung 1:
Anbieter digitaler Medien und Dienste, die insbesondere auch Minderjährige ansprechen, sind aufgefordert, die Datenschutzbelange dieser Zielgruppe in besonderem Maße zu berücksichtigen.

Empfehlung 2:
Der besonderen Schutzbedürftigkeit Minderjähriger ist durch eine entsprechende Gestaltung von Produkten und Dienstleistungen besonders Rechnung zu tragen. Informationspflichten sind kindgerecht verständlich darzustellen.

Empfehlung 3:
Medienanbieter und -dienste, die sich entweder gezielt an Minderjährige wenden oder jedenfalls nicht ausschließen können, dass ihr Angebot auch von Kindern und Jugendlichen unter 16 Jahren in Anspruch genommen wird, sind verpflichtet, für eine umfassende Transparenz und Sicherheit der Datenverarbeitung zu sorgen.

Empfehlung 4:
Datenschutzhinweise einschließlich Informationen zu den erforderlichen Einwilligungen sind in einfacher und für Minderjährige leicht verständlicher Sprache abzufassen und an exponierter Stelle zu platzieren.

Empfehlung 5:
Erziehungsberechtigte, Lehrkräfte und alle sonstigen in die Betreuung von Kindern und Jugendlichen eingebundenen gesellschaftliche Kräfte sind aufgerufen, gerade in Zeiten
der durch die Digitalisierung ermöglichten Freiheiten sowohl für den besonderen Wert personenbezogener Informationen als auch für das Risiko der hohen Verletzbarkeit der eigenen Persönlichkeit zu sensibilisieren.

Empfehlung 6:
Insbesondere staatlichen Institutionen obliegt es, Kinder und Jugendliche altersgerecht und umfassend auf die digitale Welt und die datenschutzrechtlichen Risiken vorzubereiten und ihnen Chancen und Risiken einer selbstbewusst-kritischen Teilhabe an den vielfältigen medialen Angeboten zu vermitteln.

Empfehlung 7:
Auf Bundes- und Landesebene sollten Informations- und Aufklärungskampagnen von Verbänden und Institutionen für kindgerechten Datenschutz initiiert und stärker unterstützt werden. Hierzu gehören auch die verschiedenen Initiativen der Landesdatenschutzbehörden.

Empfehlung 8:
Der Umgang mit digitalen Medien und die Vermittlung entsprechender Kompetenzen im Bereich des Datenschutzes sollte fester Bestandteil des schulischen Bildungsangebots sein.

Empfehlung 9:
Eltern sollten durch Informationsinitiativen dabei unterstützt werden, ihren Kindern insbesondere bei der Ersterkundung digitaler Medien die notwendige Hilfestellung auch im Bereich des Datenschutzes zu geben.

2 Schwerpunktthemen – europäisch und international

2.1 Der Europäische Datenschutzausschuss

Mit der Datenschutz-Grundverordnung wurde ein Europäischer Datenschutzausschuss geschaffen, der die bisherige sog. Artikel-29-Gruppe ersetzt. Sein Ziel ist es, die einheitliche Anwendung der Datenschutz-Grundverordnung und der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) sicherzustellen. Dazu hat er bereits mehrere Leitlinien beschlossen sowie einheitliche Stellungnahmen abgegeben.

Eine der wesentlichen institutionellen Neuerungen der seit 25. Mai 2018 geltenden Datenschutz-Grundverordnung besteht in der Einführung des sogenannten Europäischen Datenschutzausschusses (EDSA). Der EDSA ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Der Ausschuss nimmt seine Aufgaben und Befugnisse unabhängig wahr und unterliegt keinen Weisungen. Wie bereits der Vorgänger des EDSA, die sogenannte Artikel-29-Gruppe, setzt sich das Gremium aus den Leiterinnen und Leitern der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten zusammen. Die Aufsichtsbehörden der EWR-Staaten sind im Hinblick auf Angelegenheiten mit Bezug zur DSGVO ebenfalls Mitglied, allerdings ohne Stimmrecht und ohne das Recht, zum Vorsitzenden oder zu stellvertretenden Vorsitzenden gewählt werden zu können. Die Europäische Kommission ist berechtigt, an den Ausschusssitzungen ohne Stimmrecht teilzunehmen. Der Ausschuss wird von einem für die Dauer von fünf Jahren gewählten Vorsitz vertreten. Zur ersten Vorsitzenden des Ausschusses wurde am 25. Mai 2018 die Leiterin der österreichischen Datenschutzbehörde, Dr. Andrea Jelinek, gewählt. Sitz des Ausschusses ist Brüssel.

EU-Mitgliedstaaten wie Deutschland, die über mehrere nationale Aufsichtsbehörden verfügen, müssen einen „Gemeinsamen Vertreter“ für den EDSA benennen. Die Funktion des Gemeinsamen Vertreters wird vom Bundesdatenschutzgesetz (BDSG) dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) übertragen. Zugleich fungiert er als „Zentrale Anlaufstelle“, die es den Aufsichtsbehörden der anderen Mitgliedstaaten, dem EDSA und der EU-Kommission ermöglicht, ohne Kenntnis der innerstaatlichen Zuständigkeitsverteilung effektiv mit den deutschen Aufsichtsbehörden zu kommunizieren. Als Stellvertreter des gemeinsamen Vertreters wählt der Bundesrat einen Leiter der Datenschutzaufsichtsbehörde eines Landes.

Der EDSA soll die einheitliche Anwendung der DSGVO und der JI-Richtlinie innerhalb der EU sicherstellen. Hierzu weisen ihm DSGVO und JI-Richtlinie ein umfangreiches Aufgabenspektrum zu. Beraten soll der EDSA zu datenschutzpolitischen und datenschutzrechtlichen Fragestellungen auf EU-Ebene, insbesondere zu Legislativvorschlägen der Europäischen Kommission. Ferner kann der Ausschuss Leitlinien, Empfehlungen und bewährte Verfahren zu datenschutzspezifischen Fragestellungen erarbeiten, beispielsweise zu Datenverarbeitungen im Zusammenhang mit Profiling, zu Zertifizierungsverfahren und Datenschutzsiegeln oder zu Datenübermittlungen in Drittstaaten. Eine besondere Aufgabe kommt dem EDSA im Rahmen des sogenannten Kohärenzverfahrens (Art. 63ff. DSGVO) zu. Dieses Verfahren soll die Rechtsanwendung und Aufsichtspraxis der Datenschutzbehörden der Mitgliedstaaten vereinheitlichen. Innerhalb dieses Verfahrens kann der Ausschuss beispielsweise Stellung nehmen, wenn eine nationale Behörde verbindliche Datenschutzvorschriften für internationale Datenübermittlungen innerhalb einer Unternehmensgruppe genehmigen will (sog. Binding Corporate Rules, vgl. u. Nr. 17.8.1). Zudem fasst er rechtsverbindliche Beschlüsse zur Frage, ob ein Verstoß gegen die DSGVO vorliegt, wenn sich die betroffenen Datenschutzbehörden der Mitgliedstaaten nicht auf eine einheitliche Linie einigen können. Zu einem derartigen Streitbeilegungsverfahren ist es innerhalb des Berichtszeitraums indes noch nicht gekommen.

Wie schon die Artikel-29-Gruppe verfügt auch der EDSA über Expertengruppen, die themenbezogen die Stellungnahmen und Entscheidungen des Ausschusses vorbereiten.

Die Arbeiten des Ausschusses werden in administrativer Sicht von einem Sekretariat unterstützt, dessen Personal vom Europäischen Datenschutzbeauftragten (EDPS) und Experten der nationalen Aufsichtsbehörden gestellt wird. Das Personal des Sekretariats unterliegt ausschließlich den Weisungen des Vorsitzes des EDSA und ist insoweit organisatorisch vom EDPS getrennt. Neben der administrativen Unterstützung des Ausschusses erstellt das Sekretariat nach den Weisungen des Vorsitzes auch Entwürfe von Stellungnahmen und sonstigen Dokumenten des EDSA, einschließlich der Entwürfe für verbindliche Beschlüsse innerhalb des Kohärenzverfahrens.

Innerhalb des Berichtszeitraums seit Inkrafttreten der DSGVO hat der EDSA Leitlinien zum räumlichen Anwendungsbereich der DSGVO (Art. 3 DSGVO), zur Zertifizierung (Art. 42 DSGVO) und Akkreditierung (Art. 43 DSGVO) sowie zu Ausnahmen für Datenübermittlungen in Drittstaaten (Art. 49 DSGVO) angenommen. Zudem hat er im Verfahren nach Artikel 64 DSGVO einheitliche Stellungnahmen abgegeben zu Listen von Datenverarbeitungen, für welche gemäß Artikel 35 DSGVO Datenschutzfolgeabschätzungen vorzunehmen sind. Ferner hat er verschiedene Leitlinien mit Bezug zur DSGVO bestätigt, die noch von dem Vorgängergremium, der Artikel-29-Gruppe, erarbeitet wurden, unter anderem zur federführenden Aufsichtsbehörde, zur Einwilligung (Art. 6 DSGVO), zum Recht auf Datenübertragbarkeit (Art. 20 DSGVO), zum Datenschutzbeauftragten (Art. 37 DSGVO), zu Datenschutzfolgeabschätzungen (Art. 35 DSGVO) sowie zum Profiling (Art. 22 DSGVO). Schließlich hat der EDSA eine Stellungnahme zum Entwurf eines Angemessenheitsbeschlusses der Europäischen Kommission zu Japan angenommen (vgl. Nr. 2.1.1).

Die vom EDSA angenommenen Leitlinien und sonstigen Dokumente sind abrufbar unter www.datenschutz.bund.de.

2.1.1 Internationaler Datenverkehr

Die Diskussionen zum internationalen Datenverkehr waren auch im Berichtszeitraum von Angemessenheitsbeschlüssen geprägt, die die Europäische Kommission erlassen hat.

Angemessenheitsbeschluss zu Japan

Wie bereits unter der europäische Datenschutzrichtlinie 95/46/EG kann die Europäische Kommission nach Art. 45 DSGVO beschließen, dass ein Land, das nicht an die in der EU geltenden datenschutzrechtlichen Vorgaben gebunden ist, ein angemessenes Schutzniveau bietet. Personenbezogene Daten aus der EU dürfen dann ohne weitere Schutzmaßnahmen in dieses Land übermittelt werden. Im September 2018 hat die Europäische Kommission den Entwurf eines solchen Angemessenheitsbeschlusses zu Japan vorgelegt und ihn am 23. Januar 2019 endgültig beschlossen. Der EDSA hat am 5. Dezember 2018 seine Stellungnahme nach Art. 70 Absatz 1 Buchstabe s DSGVO zu diesem Entwurf abgegeben, an deren Erarbeitung ich maßgeblich mitgewirkt habe. Der EDSA sieht nach der Reform des japanischen Datenschutzrechts in Schlüsselbereichen große Ähnlichkeiten mit dem europäischen Datenschutzregime und erkennt an, dass die für aus der EU übermittelte Daten erlassenen ergänzenden Regelungen erheblich zum Schutz der Betroffenen beitragen. Die Europäische Kommission hat ihren Entwurf des Angemessenheitsbeschlusses im Hinblick auf die Anregungen des EDSA zwar angepasst und verbessert, dennoch fordert der EDSA, bestimmte Bereiche in der Praxis verstärkt zu überwachen. Im Fokus stehen dabei insbesondere Fragen zur Informiertheit der Einwilligung, die im japanischen Recht eine zentrale Rechtsgrundlage der Datenverarbeitung ist, zur Weiterübermittlung europäischer Daten in Drittländer und zum Zugriff der Sicherheitsbehörden auf die auf der Grundlage des Angemessenheitsbeschlusses aus der EU nach Japan übermittelten Daten. Auch die bestehenden Möglichkeiten für EU-Bürger, bei Datenschutzverstößen japanischer Verantwortlicher Abhilfe zu erlangen, sollten aus Sicht des EDSA weiter verbessert werden.

EU-US Privacy Shield

Wie in meinem 26. Tätigkeitsbericht (Nr. 2.1) dargestellt, steht seit dem 12. Juli 2016 mit dem „EU-US Privacy Shield“ (Privacy Shield) eine Rechtsgrundlage für Datenübermittlungen in die USA in Form eines Angemessenheitsbeschlusses zur Verfügung, der allerdings weiterhin auf Bedenken der europäischen Datenschutzbehörden trifft. Das Privacy Shield wurde im Berichtszeitraum zwei gemeinsamen Überprüfungen unterzogen, an denen ich intensiv mitgewirkt habe. Die deutliche Kritik der Artikel-29-Gruppe im Vorfeld und auch nach der ersten gemeinsamen Überprüfung, die der EDSA im Juli 2018 bestätigte, hat zu Verbesserungen des Privacy Shields geführt. Als im Oktober 2018 die zweite gemeinsame Überprüfung stattfand, konnte festgestellt werden, dass das Zertifizierungsverfahren und die Verfahren zur Durchsetzung des Privacy Shields verstärkt wurden: Die fehlenden Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB), das die US-Sicherheitsbehörden überwacht, wurden ernannt und ein zuvor klassifizierter Bericht dieses Gremiums wurde veröffentlicht. Dennoch hat der EDSA weiterhin Bedenken, insbesondere im Hinblick auf die Ombudsperson. Dieser Posten ist seit Beginn der Trump-Administration noch nicht dau-

erhaft besetzt worden. Inzwischen hat die US-Regierung zwar eine Ombudsperson nominiert, aber sie wurde noch nicht vom Kongress bestätigt. Auch die Frage, ob die Ombudsperson tatsächlich einen wirksamen Rechtsschutz im Sinne von Artikel 47 der EU-Grundrechtecharta gewährleisten kann, ist weiterhin offen und liegt dem Europäischen Gerichtshof zur Klärung vor. Dieses Verfahren und ein weiteres, beim Europäischen Gericht anhängiges Verfahren gegen das Privacy Shield, werden weiteren Aufschluss über die Rahmenbedingungen für den transatlantischen Datenverkehr und Datenübermittlungen in andere Drittstaaten geben.

2.2 Mitarbeit in Datenschutzaufsichtsgruppen

Europäisches Visa-Informationssystem

Seit Oktober 2011 wird das europäische Visa-Informationssystem (VIS) angewandt und von einer auf EU-Ebene bestehenden Datenschutzaufsichtsgruppe gemeinschaftlich überwacht. Zum Entwurf der Europäischen Kommission für eine neue VIS-Verordnung hat die Gruppe eine kritische Stellungnahme abgegeben.

Als gemeinsame europäische Datenbank verfolgt das VIS den Zweck, Doppelvergaben von Kurzzeitvisa zu vermeiden und die Zusammenarbeit der teilnehmenden Staaten im Rahmen der gemeinsamen Visa-Politik zu erleichtern. Entsprechend der bewährten Architektur großer europäischer Datenbanken besteht das VIS aus einer zentralen Einheit, die von der europäischen Agentur für große IT-Systeme (euLISA) in Tallinn betrieben wird, und aus den nationalen Komponenten der Teilnehmerstaaten. Zum Ende des Berichtszeitraums nehmen die EU-Staaten, ausgenommen Großbritannien, Irland, Bulgarien, Rumänien, Kroatien und Zypern, jedoch ergänzt um Norwegen, Liechtenstein, Island und die Schweiz, an dem europäischen VIS als Teilbereich des „Schengen-Acquis“ teil.

Die Datenschutzaufsicht über das VIS folgt dem Modell der koordinierten Kontrolle: Der Europäische Datenschutzbeauftragte 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 Datenschutzaufsichtsgruppe – derzeit unter Vorsitz der Schweiz –, die sich mindestens zweimal jährlich trifft, und an deren Beratungen und Aktivitäten ich regelmäßig teilnehme.

Im Berichtszeitraum hat diese Gruppe Verfahrensgrundsätze erarbeitet, wie die Aufsichtstätigkeit der nationalen Kontrollbehörden nach Artikel 41 der europäischen Verordnung 767/2008 (VIS-Verordnung) auszuüben ist. Zudem hat sie ein Positionspapier zum Einsatz externer Dienstleister bei der Bearbeitung von Visumanträgen an den Auslandsvertretungen der Mitgliedstaaten beschlossen.

Im Hinblick auf das von der Europäischen Kommission und dem Rat angestrebte Konzept der engeren Verknüpfung vorhandener und neu zu schaffender Datenbanken der Europäischen Union (sog. Interoperability), beschloss die Gruppe mit den entsprechenden Aufsichtsgruppen von Eurodac (s. u.) sowie des Schengener Informationssystems eine gemeinsame Stellungnahme.

Bis zum Ende des Berichtszeitraums war die Revision der VIS-Verordnung noch nicht abgeschlossen. Der von der Europäischen Kommission vorgelegte Entwurf sieht u. a. eine Absenkung des Mindestalters von Kindern, deren Fingerabdrücke erfasst werden, von 14 auf sechs Jahre vor. Ferner sollen die Sicherheitsbehörden einen erweiterten Zugriff auf die in VIS gespeicherten Daten erhalten. Generell soll der Anwendungsbereich der VIS-Datenbank erweitert werden, indem auch Visa für einen längeren Aufenthalt (mehr als 90 Tage) und Aufenthaltserlaubnisse erfasst werden. Zu diesen und anderen Aspekten hat die Datenschutzaufsichtsgruppe eine kritische Stellungnahme an die Europäische Kommission, den Rat und das Parlament versandt, weil die Notwendigkeit für diese erweiterten Eingriffe in das Recht auf informationelle Selbstbestimmung der Betroffenen nach Ansicht der Gruppe nicht hinreichend dargelegt wurde.

Die Stellungnahmen zum Vorhaben der Interoperabilität von Eurodac, Schengen und VIS sowie zum Entwurf der Europäischen Kommission für eine neue VIS-Verordnung sind auf meiner Internetseite unter www.datenschutz.bund.de abrufbar.

Eurodac

Fingerabdrücke von Asylbewerbern werden in der europäischen Datenbank „Eurodac“ gespeichert. Die zuständige Datenschutzaufsichtsgruppe führte u. a. Untersuchungen zu den Rechten der Betroffenen durch.

Mit dem Namen „Eurodac“ wird eine gemeinsame Datenbank für Fingerabdrücke von Asylbewerbern und in der EU aufgegriffenen illegalen Einwanderern bezeichnet. Die Datenbank unterstützt die effektive Anwendung des Dubliner Übereinkommens über die Bearbeitung von Asylanträgen. Eurodac ist auf der Grundlage einer Verordnung des Rates der EU eingerichtet worden, die auch Regelungen zur Garantie des Datenschutzes für die betroffenen Personen einschließt. Die Datenbank ging

am 15. Januar 2003 in Betrieb und wird derzeit von den 28 Mitgliedstaaten der EU sowie von Island, Norwegen, Liechtenstein und der Schweiz genutzt.

Der Europäische Datenschutzbeauftragte (EDPS) überwacht die Verarbeitung personenbezogener Daten im Zentralsystem der Datenbank einschließlich der Übermittlung von Daten daraus an die Mitgliedstaaten. Die Datenschutzbehörden der Mitgliedstaaten überwachen die Verarbeitung von Daten durch die einzelstaatlichen Behörden sowie die Übermittlung dieser Daten an das Zentralsystem. Um einen gemeinsamen Ansatz bei der Datenschutzkontrolle zu gewährleisten, versammeln sich Vertreter des EDPS und der Aufsichtsbehörden aus den Anwenderstaaten mindestens zweimal pro Jahr in der Eurodac-Datenschutzaufsichtsgruppe, derzeit unter dem Vorsitz Schwedens. An den Beratungen und Tätigkeiten dieser Gruppe nehme ich regelmäßig teil.

Im Berichtszeitraum führte die gemeinsame Gruppe eine u. a. koordinierte Untersuchung dahingehend durch, wie in den Eurodac-Anwenderländern die Wahrnehmung der Rechte der Betroffenen sichergestellt wird. Ein Bericht hierzu mit Empfehlungen wird voraussichtlich 2019 veröffentlicht. Ferner setzte die Gruppe ihre Arbeiten zur vorzeitigen Löschung von Fingerabdrücken in Eurodac (Art. 13 der europäischen Verordnung 603/2013) fort, so dass der diesbezügliche Bericht ebenfalls 2019 erscheinen dürfte.

2.3 Abschluss 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 hat 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 befasst. Das Änderungsprotokoll wurde durch den Ministerrat des Europarats am 18. Mai 2018 angenommen.

Die Konvention 108 des Europarats stammt aus dem Jahr 1981 und war das erste rechtsverbindliche zwischenstaatliche Übereinkommen zum Datenschutz. Sie enthält die wichtigsten Grundsätze des Datenschutzrechts und ist sowohl auf den privaten als auch auf den öffentlichen Sektor anwendbar. Angesichts der gewaltigen technologischen Entwicklungen war eine Modernisierung der Konvention 108 einschließlich ihres Zusatzprotokolls aus dem Jahr 2001 erforderlich. Der über mehrere Jahre dauernde Prozess konnte durch Verabschiedung des Protokolls zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Mai 2018 erfolgreich abgeschlossen werden. Während der Erarbeitung habe ich an den Sitzungen des Beratenden Ausschusses als Beobachter teilgenommen (Artikel 18 der Konvention). Neben den 47 Mitgliedstaaten des Europarats, zu denen alle EU-Mitgliedstaaten sowie eine Reihe weiterer Staaten wie etwa die Russische Föderation, die Türkei, die Schweiz und Norwegen gehören, haben bereits Uruguay, Mauritius, Senegal, Tunesien, Kap Verde und jüngst Mexiko die Konvention 108 ratifiziert. Die Konvention 108 hat damit – weit über Europa hinaus – Bedeutung für die globale Entwicklung des Datenschutzrechts.

Durch das Änderungsprotokoll wurde die Konvention 108 mit den datenschutzrechtlichen Grundprinzipien, den Betroffenenrechten und Pflichten der verantwortlichen Stelle an die Grundsätze der Datenschutz-Grundverordnung angepasst, so dass die notwendige Kohärenz zwischen der Konvention und dem neuen EU-Rechtsrahmen erreicht werden konnte. Insbesondere werden die Unterzeichnerstaaten verpflichtet, die Betroffenenrechte zu stärken. Diese sollen z. B. das Recht erhalten, Kenntnis von der Art und Weise der Datenverarbeitung zu erlangen und dieser widersprechen zu können.

Ferner ist eine Meldepflicht für Verantwortliche bei Verletzungen des Datenschutzes an die Aufsichtsbehörde einzuführen. Auch die Schaffung von unabhängigen Aufsichtsbehörden, die über Kontroll- und Sanktionsbefugnisse bei Datenschutzverstößen verfügen und zu Zwecken der Umsetzung der Konvention miteinander kooperieren, ist für alle Konventionsstaaten verpflichtend.

2.4 Europäische Datenschutzkonferenz

Die jährliche Frühjahrskonferenz („Spring Conference") der europäischen Datenschutzbeauftragten befasste sich in den Jahren 2017 und 2018 vor allem mit den Entwicklungen zur Umsetzung der europäischen Datenschutz-Grundverordnung und der Modernisierung der Konvention 108 sowie mit den aufsichtsrechtlichen Befugnissen der Datenschutzbehörden.

Die europäische Datenschutzkonferenz dient dem Gedanken- und Erfahrungsaustausch von Vertretern aller Datenschutzaufsichtsbehörden aus Europa, der Europäischen Kommission, des Europarats sowie der OECD.

Bei der Frühjahrskonferenz 2017 in Limassol (Zypern) wurde neben Umsetzungsfragen zur DSGVO vor allem die Frage diskutiert, wie Bürger und Unternehmen für einen effektiven Schutz personenbezogener Daten sensibilisiert werden können. Unter anderem wurden eine Beteiligung von Verbraucherschutzverbänden als

Multiplikatoren sowie die Rolle der betrieblichen Datenschutzbeauftragten erörtert. Ferner wurde im Rahmen einer Diskussion zum Thema Cloud Computing über Transparenzpflichten und Verantwortlichkeit seitens der Betreiber gesprochen.

Die Frühjahrskonferenz 2018 fand unter dem Titel „Data Protection – Better Together" vom 2. bis 4. Mai 2018 in Tirana (Albanien) statt. Verschiedene Foren befassten sich u. a. mit der Umsetzung der DSGVO, der Modernisierung der Konvention zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (Konvention 108, vgl. o. Nr. 2.3) und deren Einfluss auf den Datenschutz weltweit.

Anlässlich des Falles „Cambridge Analytica – Facebook" wurde über Herausforderungen und Möglichkeiten im Umgang mit Datenschutzverstößen auf Social-Media-Plattformen beraten. Im Rahmen der Diskussion über die Befugnisse der jeweiligen Aufsichtsbehörden wurde ersichtlich, dass es zwischen den Mitgliedern noch teils erhebliche Unterschiede gibt. Des Weiteren diskutierte die Konferenz die Frage einer ethisch vertretbaren Nutzung von Künstlicher Intelligenz im Bereich des polizeilichen und justiziellen Sektors einschließlich der Überwachung der Nutzung einer solchen Technik in diesem Bereich (vgl. hierzu auch Nr. 1.4 f.).

Die Entschließungstexte der Frühjahrskonferenzen 2017 und 2018 sind auf meiner Internetseite unter www.datenschutz.bund.de abrufbar.

2.5 Internationale Datenschutzkonferenz

Die Internationale Datenschutzkonferenz diskutierte wichtige Zukunftsthemen. Sie fasste Beschlüsse zum vernetzten Fahren sowie zu den Herausforderungen für den Datenschutz, die sich durch die Entwicklung und den Einsatz von künstlicher Intelligenz ergeben können.

Die 39. Internationale Datenschutzkonferenz (IDSK) in Hongkong (25. bis 29. 09.2017) stand unter dem Motto „**WE** – Connecting **W**est with **E**ast in Protecting and Respecting Data Privacy". Dieses Motto sollte zum Ausdruck bringen, dass der Schutz personenbezogener Daten ein Regionen übergreifendes Anliegen sein muss. Im Rahmen dieser Konferenz wurden drei Entschließungen verabschiedet. Neben zwei Entschließungen zur internen Kooperation der IDSK-Mitglieder sowie zur Zusammenarbeit mit Behörden des Konsumentenschutzes ist die Entschließung über den „Schutz personenbezogener Daten in automatisierten und vernetzten Fahrzeugen" hervorzuheben, die ich zusammen mit den Datenschutzaufsichtsbehörden aus Belgien, Frankreich, Italien, Hongkong, Mexiko, Neuseeland, Slowenien sowie aus der Schweiz und dem Vereinigten Königreich in die Konferenz einbringen konnte. Die Entschließung fordert alle beteiligten Parteien, namentlich Normungsgremien, Behörden, Fahrzeug- und Ausrüstungshersteller, Unternehmen für Privattransporte und Mietwagenanbieter sowie Anbieter von datengetriebenen Dienstleistungen, wie z. B. Spracherkennung, Navigation, Fernwartung oder Telematikdienste für Kfz-Versicherungen, dazu auf, die Grundrechte der Nutzer auf Schutz ihrer personenbezogenen Daten und ihrer Privatsphäre in vollem Umfang zu achten und diesen Grundrechten in jeder Phase der Herstellung und Entwicklung neuer Geräte oder Dienstleistungen hinreichend Rechnung zu tragen. Zu diesem Zweck werden in der Entschließung anschließend 16 konkrete Anforderungen formuliert (vgl. hierzu auch Nr. 1.6).

Die 40. IDSK in Brüssel und Sofia (21. bis 25.10.2018) trug das Motto **„Debating Ethics: Dignity and Respect in a Data Driven Life"** und wurde vom Europäischen Datenschutzbeauftragten zusammen mit der bulgarischen Datenschutzbehörde organisiert. Im Zentrum der Diskussionen standen die Herausforderungen, welche die aktuellen Entwicklungen bestimmter Zukunftstechnologien für den Persönlichkeitsschutz des Einzelnen und für die Gewährleistung des Datenschutzes mit sich bringen. Wegen der besonders gravierenden Auswirkungen, die Anwendungen der künstlichen Intelligenz (vgl. o. Nr. 1.4 f.) zur Folge haben können, hat die IDSK eine „Erklärung zu Datenschutz und Ethik im Bereich der künstlichen Intelligenz" beschlossen. Darin bringt sie ihre Auffassung zum Ausdruck, dass die Schaffung, Entwicklung und Nutzung von Systemen der künstlichen Intelligenz die Menschenrechte, insbesondere das Recht auf den Schutz personenbezogener Daten und auf den Schutz der Privatsphäre, sowie die Menschenwürde, das Diskriminierungsverbot und die Grundwerte uneingeschränkt achten müssen und stets Lösungen bieten sollen, die es dem Einzelnen ermöglichen, die Kontrolle über die Systeme der künstlichen Intelligenz zu bewahren und diese Systeme zu verstehen. Zu diesem Zweck beschloss die Konferenz sechs Leitprinzipien: (1) Grundsatz der Fairness, (2) kontinuierliche Aufmerksamkeit und Wachsamkeit, (3) Transparenz und Verständlichkeit, (4) „privacy by design" und „privacy by default", (5) Befähigung des Einzelnen, (6) Vermeidung von Voreingenommenheit und Diskriminierung. Entsprechend ihrem Motto hat die 40. IDSK zudem darüber debattiert, ob und inwieweit ethische und moralische Werte als Grundlage für die Sicherstellung des Datenschutzes auch unter den Bedingungen des digitalen Zeitalters fungieren können und ob diese Werte als Instrumentarium geeignet sind für die Bewältigung der Herausforderungen, die sich

für den Datenschutz durch neue Wege der Interaktion von Mensch und Maschine – wie z. B. bei Anwendungen der künstlichen Intelligenz – und durch den immer rascheren technologischen Fortschritt ergeben. In den wenigen Tagen der Konferenz konnte die Debatte naturgemäß nur angestoßen werden. Es wird aber Aufgabe künftiger Tagungen der IDSK sein, diese Diskussion fortzuführen und das „Rüstzeug“ der Datenschützer um universell anwendbare ethisch-moralische Grundsätze für den Umgang mit Zukunftstechnologien zu erweitern.

Die Entschließungen der Internationalen Datenschutzkonferenzen stehen in englischer Sprache auf meiner Internetseite (www.datenschutz.bund.de), zum Abruf bereit; dort finden sich auch Arbeitsübersetzungen der Entschließungen in deutscher Sprache.

Die 41. IDSK wird vom 21. bis 25. Oktober 2019 in Tirana, Albanien, stattfinden.

3 Ausschuss für Arbeit und Soziales

3.1 Aus den Gesetzgebungsvorhaben

3.1.1 Die Umsetzung der DSGVO im Sozialrecht

Das Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541) passt die Grundregelungen zum Sozialdatenschutz im 2. Kapitel des Zehnten Buches Sozialgesetzbuch (SGB X) der Datenschutz-Grundverordnung an.

Bei den Beratungen zur Anpassung des BDSG im Rahmen des Datenschutz-Anpassungs- und Umsetzungsgesetz EU ließ sich die Bundesregierung noch die erforderliche Zeit.

Dem gegenüber gestaltete sich die Gesetzgebung zur Anpassung der Grundregelungen des Sozialdatenschutzes im 2. Kapitel SGB X eher ungewöhnlich, denn diese wurde nicht im Rahmen eines eigenständigen Gesetzgebungsverfahrens erarbeitet, sondern im Wege sog. Formulierungsvorschläge für Abgeordnete des Deutschen Bundestages an ein bereits in der parlamentarischen Beratung befindliches Gesetz „angeflanscht". Dieser Weg ist zwar im Grundsatz nicht unüblich, wird aber in der Regel eher für kurzfristige Korrekturen oder vergessene Regelungen genutzt. Dass derart bedeutende gesetzliche Regelungen auf diesem Weg ohne eine vorherige ausreichende Beratung der durch die Bundesministerien und die übrigen vorgesehenen Stellen (wie meine Behörde) in die parlamentarische Beratung kommen, ist allerdings höchst ungewöhnlich. Ein solches Verfahren tut der Qualität der Gesetze nicht gut.

Meine in der Kürze der Zeit vorgetragenen Bedenken, insbesondere zu der hier ebenfalls vorgesehenen Neufassung der Forschungsregelung in § 75 SGB X (vgl. hierzu Nr. 7.1.1), wurden weitgehend ignoriert. Aber auch die neuen Vorschriften über den Ausschluss der sofortigen Vollziehung in § 81a und die Einschränkung in § 81c SGB X n.F. widersprechen den Regelungen in Art. 58 Absatz 2 und 5 DSGVO. Im Bereich des Sozialdatenschutzes sind Fälle nicht ausgeschlossen, in denen die Anordnung der sofortigen Vollziehung erforderlich ist, um die Rechte der Betroffenen zu wahren. Angesichts der Dauer sozialgerichtlicher Verfahren ist diese Möglichkeit in dringenden Eilfällen unverzichtbar. Ordnet der BfDI bspw. die Beseitigung einer Sicherheitslücke in einem IT-System eines Sozialleistungsträgers an, darf eine hiergegen gerichtete Klage des Sozialleistungsträgers nicht dazu führen, dass wegen der aufschiebenden Wirkung dieser Zustand längere Zeit nicht beseitigt wird. Ich hatte bereits gegenüber dem BMAS darauf hingewiesen, dass bei einer Anordnung der sofortigen Vollziehung einer Maßnahme nach Artikel 58 Absatz 2 DSGVO den Sozialleistungsträgern keine Rechte genommen würden. Wie jeder andere Adressat aufsichtsbehördlicher Maßnahmen hätten sie die Möglichkeit, nach § 80 Absatz 5 VwGO oder nach § 86b Sozialgerichtsgesetz die Wiederherstellung der aufschiebenden Wirkung zu beantragen.

Auch die Beschränkungen des Auskunftsrechts nach § 83 SGB X und des Rechts auf Löschung in § 84 SGB X stehen nicht in Einklang mit den Vorgaben der DSGVO.

3.1.2 Europäischer Sozialfonds

Die EU-Verordnung über den Europäischen Sozialfonds Plus (ESF+-Verordnung) ist das Ergebnis der Verschmelzung des Europäischen Sozialfonds (ESF), der Beschäftigungsinitiative für junge Menschen, des Europäischen Hilfsfonds für die am stärksten benachteiligten Personen, des Programms für Beschäftigung und soziale Innovation (EaSI) und des EU-Gesundheitsprogramms. Die geplante Verordnung wird den Anforderungen der DSGVO nicht gerecht.

Bereits in meinem 25. Tätigkeitsbericht habe ich über den ESF, die Vielzahl der an den Förderprojekten beteiligten Stellen und die damit verbundene Datenverarbeitung berichtet (vgl. Nr. 9.4).

Aktuell finden auf der Ebene der Europäischen Union Gespräche zur Vorbereitung der nächsten Förderperiode 2021 bis 2027 für Projekte statt, die mit Mitteln des ESF+ unterstützt werden sollen. Der Verordnungsentwurf sieht vor, künftig personenbezogene Daten für Nachweiszwecke primär aus Registern, vergleichbaren Quellen oder durch „fundierte Schätzung“ („informed estimation“) zu erheben.

Die geplante Ausgestaltung des Verfahrens halte ich für nicht datenschutzgerecht. Die Art und Weise der Datenverarbeitung widerspricht der Zweckbestimmung der originären in Registern vorgehaltenen Daten. Sie erschwert darüber hinaus den an ESF geförderten Projekten teilnehmenden Personen die Wahrnehmung ihrer Rechte als Betroffene.

Ich unterstütze daher das Bundesministerium für Arbeit und Soziales bei seinem Vorhaben, auf eine datenschutzgerechte Ausgestaltung des Verfahrens gegenüber der EU-Kommission zu drängen.

3.1.3 Beschäftigtendatenschutzgesetz – leider noch immer eine Wunschvorstellung!

Obwohl die DSGVO dem nationalen Gesetzgeber einen Gestaltungsspielraum im Beschäftigtendatenschutz eingeräumt hat, fehlt es auch weiterhin an spezifischen nationalen Regelungen.

Bereits vor Jahren haben die Datenschutzbeauftragten des Bundes und der Länder ein eigenes Gesetz zur rechtssicheren Ausgestaltung des Beschäftigtendatenschutzes gefordert – bislang leider vergeblich (vgl. hierzu Entschließung der DSK zum Beschäftigtendatenschutzgesetz aus dem Jahr 2014; 26. TB Nr. 3.2.1; 25. TB Nr. 9.3.1). Angesichts der fortschreitenden Digitalisierung in der Arbeitswelt ist ein Beschäftigtendatenschutzgesetz wichtiger denn je.

Dabei sehe ich einen Regelungsbedarf 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

Die Bundesregierung wollte beim Beschäftigtendatenschutz zunächst die Reform des europäischen Datenschutzrechts abwarten. Die nunmehr seit Mai 2018 geltende DSGVO sieht in Artikel 88 jedoch nur eine pauschale Regelung vor und legt den groben Handlungsrahmen für die Mitgliedsstaaten fest. So sollen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz getroffen werden. Die genaue Ausgestaltung bleibt dem nationalen Gesetzgeber überlassen. Eine solche nationale Regelung enthält § 26 BDSG. Dieser ist mit seinen acht Absätzen zwar umfangreicher als die vorherige Regelung des § 32 BDSG (alt), lässt aber nach wie vor viele praxisrelevante Einzelfragen zu einem angemessenen Ausgleich zwischen berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers offen. Eine Streitklärung für die Betroffenen bleibt daher auch weiterhin der Datenschutzaufsicht und den Gerichten überlassen.

Bereits im 26. Tätigkeitsbericht hatte ich ausgeführt, dass auch das federführende BMAS im Rahmen seines Konsultationsprozesses zum Thema „Arbeiten 4.0“ explizite Regelungen zum Beschäftigtendatenschutz für erforderlich hält. Das Ministerium hatte angekündigt, einen interdisziplinär besetzten Beirat einzusetzen, der anhand eines verbindlichen Zeitplans entsprechende Regelungen erarbeiten sollte. Bislang gibt es einen solchen Beirat, in dem ich gerne mitarbeiten würde, nicht.

Ich halte auch weiterhin die Verabschiedung eines Beschäftigtendatenschutzgesetzes für dringend erforderlich.

3.2 Einzelthemen

3.2.1 Vorbereitung auf die DSGVO: Abfrage zur Stellung der behördlichen Datenschutzbeauftragten in den Jobcentern

Die Aufgaben der behördlichen Datenschutzbeauftragten sind anspruchsvoll und zeitintensiv. Dem wird in

vielen Fällen leider nicht durch ausreichende Entlastung von anderen Aufgaben Rechnung getragen.

Die behördlichen Datenschutzbeauftragten spielen bei der Einhaltung der datenschutzrechtlichen Regelungen in der Verwaltung eine zentrale Rolle. Ihre Aufgaben sind vielfältig: Sie reichen von der Beratung von Mitarbeiterinnen und Mitarbeitern, Bürgerinnen und Bürgern und der Behördenleitung über Schulungsaufgaben bis hin zu eigenen Kontrollrechten. Um diese Aufgaben wahrnehmen zu können, benötigen die Datenschutzbeauftragten vor allem Zeit. Eine ausreichende Freistellung von anderen Aufgaben ist deshalb Grundvoraussetzung für eine gesetzeskonforme Wahrnehmung ihrer Aufgaben.

Im Berichtszeitraum habe ich eine Abfrage zur Freistellung der behördlichen Datenschutzbeauftragten in allen gemeinsamen Einrichtungen (Jobcentern) durchgeführt. Dabei stellte sich heraus, dass nur etwa jedes zehnte Jobcenter seine/seinen behördliche(n) Datenschutzbeauftragte(n) ausreichend von anderen Aufgaben freistellt. In den anderen Fällen wird die Aufgabe zumeist als „Rucksackaufgabe“ ohne oder mit nur geringer Freistellung wahrgenommen. Dies geht nicht nur zu Lasten der Datenschutzbeauftragten, sondern vor allem auch zu Lasten der gesetzlich vorgeschriebenen Aufgaben.

Die Jobcenter berichteten mir, dass sie mit sehr knappen Personalressourcen arbeiten müssen. Eine Freistellung der behördlichen Datenschutzbeauftragten gehe daher zwangsläufig mit einer Belastung anderer Bereiche einher. Aus diesem Grund kann ich nur an die verantwortlichen Aufsichtsbehörden von Bund und Ländern appellieren, eine gemeinsame Lösung zur personellen Ausstattung der Jobcenter zu finden, die eine Freistellung der behördlichen Datenschutzbeauftragten sicherstellt, ohne an anderer Stelle Lücken zu reißen.

Spätestens mit Anwendungsbeginn der DSGVO ist ein kompetenter Ansprechpartner für den Datenschutz für jede Behörde von unschätzbarem Wert. Die datenschutzrechtlichen Anforderungen an die Behörden sind gestiegen. Zugleich werden den betroffenen Personen neue Klagerechte und Schadensersatzansprüche zur Verfügung gestellt. Gut geschulte und ausreichend freigestellte behördliche Datenschutzbeauftragte können dazu beitragen, dass die Behörde die gesetzlichen Anforderungen erfüllt.

Im Rahmen eines datenschutzrechtlichen Beratungs- und Kontrollbesuchs bei der Bundesagentur für Arbeit (BA) habe ich auch festgestellt, dass sowohl die Datenschutzorganisation als auch die Ausstattung des behördlichen Datenschutzbeauftragten verbessert werden musste. Die BA hat auf meine Hinweise bereits reagiert und erste Maßnahmen ergriffen.

Ich empfehle, dass die Jobcenter ausreichend personell ausgestattet werden, um ihre Datenschutzbeauftragten von anderen Aufgaben freizustellen, damit diese ihre gesetzlich vorgeschriebenen Aufgaben erfüllen können.

3.2.2 Weiterhin fehlende Löschkonzepte bei den gesetzlichen Sozialleistungsträgern

Trotz klarer gesetzlicher Regelungen verfügen Sozialleistungsträger noch immer über keine Löschkonzepte – oder haben diese nicht umgesetzt.

Eines der datenschutzrechtlich wichtigsten Rechte ist das Recht auf Löschung und das ebenfalls in Art. 17 DSGVO neu geschaffene „Recht auf Vergessenwerden“. Nach der Rechtsprechung des Europäischen Gerichtshofs handelt es sich hierbei um eine spezielle Ausprägung der Grundrechte auf Achtung des Privat- und Familienlebens und auf Schutz personenbezogener Daten. So sind personenbezogene Daten vom Verantwortlichen insbesondere dann zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf andere Weise verarbeitet worden, nicht mehr erforderlich sind.

Ich habe eine Vielzahl von Beratungs- und Kontrollbesuchen bei Sozialleistungsträgern (Berufsgenossenschaften, gesetzliche Krankenkassen und (Reha)Kliniken in meinem Zuständigkeitsbereich) durchgeführt, wo ich feststellen musste, dass viele dieser Sozialleistungsträger weiterhin über keinerlei Löschkonzepte verfügen oder diese über ein Entwurfsstadium nicht hinausgehen. Bei Stichproben konnte ich beispielsweise Datensätze einzelner Personen in IT-Systemen aufrufen, deren Geburtstage bis in das 19. Jahrhundert zurückreichen und/oder Personen betreffen, die bereits vor mehr als 70 Jahren verstorben sind. Dass diese Daten für die Aufgabenerledigung nicht mehr erforderlich sein können, ist selbsterklärend.

Personenbezogene Daten nicht löschen zu können, stellte bereits vor dem 25. Mai 2018 einen Rechtsverstoß dar. Mit einem Rundschreiben hatte ich dem Spitzenverband der Gesetzlichen Krankenversicherung bereits im Jahr 2014 mitgeteilt, dass ich fehlende Löschmöglichkeiten bzw. das Fehlen von Löschkonzepten bei den gesetzlichen Krankenkassen nicht mehr akzeptiere. Damals konnte ich derartige Datenschutzverstöße (aufgrund des alten Datenschutzrechts) nur beanstanden.

Art. 58 Absatz 2 DSGVO gibt mir nunmehr erweiterte Befugnisse gegenüber den Verantwortlichen, noch energischer darauf einzuwirken, dass Löschkonzepte nicht nur zeitnah erstellt oder finalisiert, sondern IT-seitig auch umgesetzt werden. Diese Rechte werde ich zukünftig in Anspruch nehmen.

3.3 Aus Kontrolle und Beratung

3.3.1 Beanstandungen nach einem Beratungs- und Kontrollbesuch

Und wieder einmal der Datenmüll.

Im Berichtszeitraum habe ich bei einem Beratungs- und Kontrollbesuch in einem Jobcenter festgestellt, dass der Datenmüll des Jobcenters, der Agentur für Arbeit und des Ärztlichen Dienstes in einem großen abschließbaren Container entsorgt wurde. Dieser Container war jedoch defekt, sodass ein Zugriff auf die darin enthaltenen sensiblen Daten für Dritte möglich war.

Aufgrund des großen Umfangs und der hohen Sensibilität der vorgefundenen Daten habe ich Beanstandungen gegenüber dem Jobcenter und der Bundesagentur für Arbeit ausgesprochen. Diese haben den defekten Container umgehend ersetzt. Das Jobcenter hat seine Papierentsorgung inzwischen vollständig auf das bewährte System mit Datenschutzmülltonnen umgestellt.

3.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

4 Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

4.1 Aus Kontrolle und Beratung

4.1.1 Langzeit-Forschung zu Bildungsprozessen und -verläufen in Deutschland

Bei einem Informations- und Beratungsbesuch beim Leibniz-Institut für Bildungsverläufe e. V. (LIfBi) im Frühjahr 2018 habe ich mich über Inhalte und Abläufe des Nationalen Bildungspanels (NEPS) informiert.

Mit dem NEPS sollen Längsschnittdaten zu Kompetenzentwicklungen, Bildungsprozessen, Bildungsentscheidungen und Bildungsrenditen über die gesamte Lebensspanne erhoben werden. Das 2009 gestartete Projekt wird seit 2014 vom LIfBi an der Otto-Friedrich-Universität in Bamberg durchgeführt. Mit rund 60.000 regelmäßig befragten Zielpersonen handelt es sich um die größte Bildungsstudie zur Erforschung von Bildungsverläufen in Deutschland. Beteiligt ist ein Netzwerk von rund 200 Wissenschaftlern an 29 Institutionen, darunter Universitäten und Forschungseinrichtungen der Bereiche Pädagogik, Psychologie, Soziologie und Ökonomie.

Die Geschäftsführung des Instituts ist 2017 an mich herangetreten und hat um eine datenschutzrechtliche Beratung gebeten. Dabei standen die Verantwortung im Umgang mit den Kontaktdaten der Studienteilnehmenden und konkrete Fragen der Wirksamkeit der Einwilligungen, der Anonymisierung der Erhebungsdaten sowie einer Datenweitergabe an Partner des NEPS-Netzwerks im Vordergrund. Im Informations- und Beratungstermin vor Ort haben sich meine Mitarbeiter außerdem die Arbeitsweise des institutseigenen Forschungsdatenzentrums demonstrieren lassen. Sie konnten mir von einem durchweg positiven Gesamteindruck und einem hohen Datenschutzniveau in der Aufgabenwahrnehmung des Leibniz-Instituts berichten. Die Beratung stieß bei den Verantwortlichen auf großes Interesse, so etwa meine Hinweise zur konkreten Gestaltung der vom Institut zur Legitimation der Verarbeitung personenbezogener Daten eingeholten Einwilligung der Teilnehmenden und zu den Anforderungen an die Informiertheit der Betroffenen. Die erkennbare Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Datenschutzfragen war sehr erfreulich.

Dem nachvollziehbar dargelegten Wunsch des Instituts nach größerer Flexibilität auch im Umgang mit den Kontaktdaten der Studienteilnehmenden stehe ich grundsätzlich offen gegenüber, solange die dazu erforderlichen organisatorischen und verfahrenstechnischen Veränderungen den vorgefundenen Datenschutzstandard nicht beeinträchtigen.

4.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

5 Ausschuss für Familie, Senioren, Frauen und Jugend

5.1 Einzelthemen

5.1.1 Das Portal „ElterngeldDigital“

Für E-Government-Anwendungen wie „ElterngeldDigital“, in denen Sozialleistungen der Länder digital mit Unterstützung des Bundes beantragt werden können, ist die Schaffung von Rechtsgrundlagen erforderlich, die eine Bund-Länder-Zusammenarbeit ermöglichen. Das Datenschutzniveau bei der digitalen Beantragung von Elterngeld sollte dabei genauso hoch sein wie bei der schriftlichen Antragstellung.

Im Rahmen der Gesetzgebung zum Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) soll mit § 24b eine neue Regelung im Bundeselterngeld- und Elternzeitgesetz (BEEG) eingefügt werden, die es dem Bund erlaubt, die Elterngeldstellen der Länder bei der elektronischen Elterngeldbeantragung zu unterstützen. Diese Neuregelung war erforderlich, da der Bund das Portal „ElterngeldDigital“ nur dann als datenschutzrechtlich verantwortliche Stelle betreiben kann, wenn ihm die Aufgabe der elektronischen Unterstützung der Länder bei der Elterngeldbeantragung gesetzlich übertragen wird. Das Online-Portal soll das elektronische Ausfüllen der Antragsformulare der Länder sowie die Übermittlung der Daten aus dem Antragsformular an die nach dem BEEG für das Elterngeld zuständigen Elterngeldstellen der Länder ermöglichen.

Die Rechtsgrundlage für eine Datenverarbeitung durch den Bund - hier das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) - sieht eine datenschutzrechtliche Einwilligung der Nutzer des Portals gegenüber dem BMFSFJ vor. Die elektronische Antragstellung über das Bundesportal ist freiwillig und die Nutzer können ihre Einwilligung jederzeit widerrufen. Alternativ gibt es stets die Möglichkeit, den Elterngeldantrag unmittelbar bei der zuständigen Elterngeldstelle einzureichen. Nach Beendigung der Nutzung des Internetportals sollen die Elterngelddaten unverzüglich gelöscht werden.

Der Antrag auf Elterngeld enthält eine Reihe sensibler Daten, wie z. B. Angaben zu einer eventuellen Behinderung des Kindes bzw. der Kinder, die Geburtsbescheinigung, eventuelle Adoptionsverfahren, den Familienstand, die Steuer-Identifikationsnummer, das Einkommen der Eltern, Informationen zum Bezug von Kranken- oder Arbeitslosengeld, Einzelheiten zu Geschwistern etc.

Bei den im Rahmen der Beantragung von Elterngeld erhobenen Daten handelt es sich um Sozialdaten, die durch das Sozialgeheimnis besonders geschützt sind.

Ich hatte im Gesetzgebungsverfahren empfohlen, die neue Vorschrift im Ersten-, Zweiten- oder Dritten Abschnitt des BEEG einzufügen, um sicherzustellen, dass nach § 26 BEEG, § 68 Nummer 15 SGB I das Sozialgesetzbuch auch bei einer elektronischen Elterngeldbeantragung anwendbar ist. Das hohe Datenschutzniveau des Sozialgesetzbuches sollte nicht nur bei Papieranträgen gelten, sondern auch bei der elektronischen Verarbeitung der für die Elterngeldbeantragung erforderlichen Daten durch das BMFSFJ und deren Weiterleitung an die zuständigen Elterngeldstellen der Länder. Meinem Vorschlag wurde leider nicht gefolgt, sodass für die elektronische Antragstellung beim BMFSFJ – im Gegensatz zur Papierantragstellung bei den Elterngeldstellen – nicht das Sozialgesetzbuch gelten soll. Da die Nutzung des Online-Portals freiwillig ist, können die Nutzer selbst entscheiden, welchen Weg sie für ihre Antragstellung wählen.

Das Portal „ElterngeldDigital“ ist grundsätzlich ein gelungenes Beispiel für die Institutionalisierung der Datenverarbeitungen bei E-Government-Projekten im Rahmen einer Bund-Länder-Zusammenarbeit. Im Sozialleistungsbereich muss jedoch in Zukunft verstärkt darauf geachtet werden, dass das hohe Datenschutzniveau des Sozialgesetzbuches durchgängig gilt. Das ist insbesondere dann notwendig, wenn digitale Angebote verpflichtend sind und den Bürgern keine Alternativen zur Verfügung stehen.

5.A Zudem von besonderem Interesse

1.1, 1.7, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

6 Finanzausschuss

6.1 Aus der Gesetzgebung

Im Berichtszeitraum wurde ich bei einer Vielzahl von Gesetzgebungsvorhaben durch das Bundesministerium der Finanzen beteiligt. Teilweise wurde ich dabei mit meinen datenschutzrechtlichen Bedenken gehört und habe so Verbesserungen im Bereich des Datenschutzes durchsetzen können.

Zwei wichtige Gesetzgebungsvorhaben möchte ich herausgreifen. Zum einen das Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften, das mir die Aufsicht über Landesfinanzbehörden zuwies (vgl. u. Nr. 6.1.1) und zum anderen die Umsetzung der Vierten Geldwäscherichtlinie und die damit verbundenen Regelungen zum Transparenzregister (vgl. u. Nr. 6.1.2).

6.1.1 Neue Aufgabe für den BfDI

Seit dem 25. Mai 2018 obliegt mir die datenschutzrechtliche Aufsicht auch über die Landesfinanzbehörden einschließlich der Finanzämter und über Teile der kommunalen Steuerämter.

Mit dem zum 25. Mai 2018 in Kraft getretenen „Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften“ vom 17. Juli 2017 (BGBl. I 2017 S. 2541) wurde mir gemäß § 32h Absatz 1 Abgabenordnung (AO) die datenschutzrechtliche Aufsicht über die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich der AO übertragen. Soweit den Gemeinden die Verwaltung der Realsteuern – also die Gewerbe- und Grundsteuer übertragen wurde, bekam ich über den Verweis in § 1 Absatz 2 Nr. 1 AO auch die datenschutzrechtliche Aufsicht für die kommunalen Steuerämter. Schließlich kann nach Maßgabe des § 32h Absatz 3 AO durch Landesrecht bestimmt werden, mir die Aufsicht über die Verarbeitung personenbezogener Daten im Rahmen landesrechtlicher oder kommunaler Steuergesetze zu übertragen, soweit die Datenverarbeitung auf bundesgesetzlich geregelten Besteuerungsgrundlagen oder auf bundeseinheitlichen Festlegungen beruht. Als erstes Bundesland hat die Freie und Hansestadt Hamburg von dieser Möglichkeit Gebrauch gemacht.

Bereits vor dem Inkrafttreten der neuen Regelungen habe ich auf administrativer Ebene intensiv darauf hingewirkt, diesen Übergang der Zuständigkeiten von den Landesdatenschutzaufsichtsbehörden auf mich reibungslos zu gestalten. Unter anderem habe ich den jeweiligen Arbeitsgruppen und Arbeitskreisen des Bundesministeriums der Finanzen und der obersten Landesfinanzbehörden in zahlreichen Gesprächen und Abstimmungsrunden beratend zur Seite gestanden. Diese Beratungstätigkeit betraf sowohl meine neue Aufsichtszuständigkeit als auch die Umsetzung der Anforderungen durch die DSGVO bei den Finanzbehörden.

Beratung

Im Berichtszeitraum habe ich einen ersten Informationsbesuch bei einer obersten Landesfinanzbehörde und in zwei Finanzämtern absolviert. Dabei wurden zahlreiche operative Fragen geklärt, aber auch Fragen im Zusammenhang mit der erforderlichen Benennung eines oder einer Datenschutzbeauftragten. Bei meinen Besuchen in den beiden Finanzämtern konnte ich mich davon überzeugen, dass diese sorgsam und datenschutzkonform mit den Steuerdaten der Bürgerinnen und Bürger umgehen. Zudem haben mich schon in der kurzen Zeit meiner neuen Aufsichtszuständigkeit zahlreiche Anfragen von Bürgerinnen und Bürgern erreicht, denen ich nachgegangen bin.

Darüber hinaus haben mich sowohl das Bundesministerium der Finanzen als auch oberste Finanzbehörden um Beratung zu Einzelfragen gebeten. Dabei konnte u. a. geklärt werden, dass Lohnsteuerhilfevereine als nichtöffentliche Stellen der datenschutzrechtlichen Aufsicht meiner Landeskolleginnen und –kollegen unterstehen. Gleiches gilt für Steuerberaterinnen und Steuerberater.

6.1.2 Umsetzung der Vierten Geldwäscherichtlinie und die damit verbundenen Regelungen zum Transparenzregister

Das Gesetz zur Umsetzung der Vierten Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen trat am 26. Juni 2017, die Änderungen im Geldwäschegesetz traten am 25. Mai 2018 in Kraft. Mit diesem Gesetzgebungsvorhaben wurde das Transparenzregister eingeführt.

Mit dem Umsetzungsgesetz wurde u. a. ein zentrales elektronisch geführtes Register (sog. Transparenzregister) über die wirtschaftlich Berechtigten von juristischen Personen des Privatrechts, eingetragenen Personengesellschaften, Trusts und Rechtsgestaltungen , die in ihrer Struktur und Funktion Trusts ähneln, geschaffen. Diese sind nun verpflichtet, aktuelle Angaben zu ihren wirtschaftlich Berechtigten an das Transparenzregister zu melden. Sind die Daten bereits im Handels-, Partnerschafts-, Genossenschafts-, Vereins- oder Unternehmensregister vorhanden, so entfällt die Meldepflicht, da diese Register mit dem Transparenzregister verknüpft sind.

Als wirtschaftlich Berechtigte definiert § 3 Absatz 1 Geldwäschegesetz(GwG) natürliche Personen, in deren Eigentum oder unter deren Kontrolle der Vertragspartner letztlich steht. Wirtschaftlich Berechtigte sind darüber hinaus natürliche Personen, auf deren Veranlassung eine Transaktion letztlich durchgeführt oder eine Geschäftsbeziehung letztlich begründet wird. Bei Stiftungen und ähnlichen Rechtsgestaltungen sind wirtschaftlich Berechtigte die Vorstandsmitglieder der Stiftung, Treugeber, Verwalter oder Protektoren sowie begünstigte natürliche Personen. Wirtschaftlich Berechtigter ist darüber hinaus auch eine Person, die auf sonstige Weise Einfluss auf die Vermögensverwaltung oder Ertragsverwaltung ausübt. Der wirtschaftlich Berechtigte ist verpflichtet, dem Meldepflichtigen die Informationen zur Verfügung zu stellen.

In das Transparenzregister werden Vor- und Nachname, Geburtstag und Wohnort, Art und Umfang des wirtschaftlichen Interesses des wirtschaftlich Berechtigten eingetragen sowie die in § 22 Absatz. 1 GwG aufgeführten Informationen. Unter welchen Voraussetzungen in das Transparenzregister online Einsicht genommen werden kann, regelt die Transparenzregistereinsichtnahmeverordnung (TrEinV). Neben einsichtsberechtigten Behörden und den Verpflichteten im Sinne des GWG dürfen danach auch sonstige Personen in das Transparenzregister Einsicht nehmen, sofern sie ein berechtigtes Interesse darlegen. Von einem berechtigten Interesse geht die TrEinV aus bei

- Nichtregierungsorganisationen, deren Satzungszweck der Kampf gegen Geldwäsche und entsprechende Vortaten ist,
- Journalisten mit Journalistenausweis, wenn sie die getätigten oder geplanten Recherchen im Bereich der Geldwäsche und Terrorismusfinanzierung darstellen oder
- eine Darstellung bereits getätigter oder geplanter Aktivitäten im Zusammenhang mit Geldwäschebekämpfung.

Personen mit nachgewiesenem berechtigtem Interesse erhalten über die Einsicht Kenntnis über Vor- und Nachname, Geburtsmonat und –Jahr, Wohnsitzland und die Art und den Umfang des wirtschaftlichen Interesses. Sind weitere Daten in einem anderen öffentlichen Register zugänglich, so sind diese darüber hinaus auch im Transparenzregister für Dritte mit berechtigtem Interesse ersichtlich. Sofern der wirtschaftlich Berechtigte im Einzelfall überwiegende schutzwürdige Interessen darlegt, kann auf seinen Antrag hin die Einsichtnahme für Dritte gesperrt werden. Dies ist zum einen dann der Fall, wenn er Opfer bestimmter Straftaten werden könnte, wie etwa Betrug, Erpressung oder Mord, und zum anderen, wenn er minderjährig oder geschäftsunfähig ist. Eine etwaige Beschränkung der Einsichtnahme gilt nicht gegenüber Behörden und einigen anderen im Gesetz aufgeführten Personen wie Notaren.

Den Umsetzungsprozess der Vierten Geldwäscherichtlinie in nationales Recht habe ich aus datenschutzrechtlicher Sicht kritisch begleitet. U.a. sehe ich die hier vorgesehene Verknüpfung mit anderen Registern kritisch, da die Daten aus diesen Registern ursprünglich für andere Zwecke erhoben wurden. Zudem habe ich Bedenken hinsichtlich des Identifizierungsprozesses bei der Eröffnung eines Nutzerkontos. Hierfür genügt bereits die Vorlage einer einfachen Kopie eines amtlichen Lichtbildausweises, die heute mit allgemein verfügbarer Technik sehr einfach hergestellt werden kann und nicht mehr oder kaum von einer echten Kopie zu unterscheiden ist. Folglich besteht die Gefahr, dass sich eine nicht berechtigte Person registriert, um in das Transparenzregister Einsicht nehmen zu können.

Der EU-Gesetzgeber hat bereits die Fünfte Geldwäscherichtlinie verabschiedet. Diese ist bis zum 10. Januar 2020 in nationales Recht umzusetzen. Somit bleibt das Geldwäscherecht mein steter Begleiter.

6.2 Einzelthemen

6.2.1 Zum Internationalen Steuerdatenaustausch

Am 29. Oktober 2014 unterzeichneten 51 Staaten in Berlin ein Abkommen über den automatischen Informationsaustausch in Steuersachen, den sog. OECD-Standard. Mittlerweile sind 104 Staaten dem Abkommen beigetreten. Im September 2017 fand der erste Datenaustausch zwischen den ursprünglichen 51 Unterzeichnerstaaten statt.

Auf Ebene der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) wurde gemeinsam mit den G-20-Staaten und in enger Kooperation mit der EU ein Modell für den globalen Standard zum Austausch von Informationen zu Finanzkonten entwickelt. Dieses sieht vor, dass die zuständigen staatlichen Stellen von den Finanzinstituten die erforderlichen Informationen erhalten und diese einmal jährlich automatisch mit anderen Staaten austauschen. Am 29. Oktober 2014 unterzeichneten 51 Staaten eine multilaterale Vereinbarung über diesen Standard. Im Rahmen der nationalen Umsetzung habe ich versucht, auf eine datenschutzkonforme Lösung hinzuwirken, mir wurde aber nicht in allen Punkten gefolgt (vgl. 25. TB Nr. 7.9; 26. TB Nr. 8.2.4).

Im September 2017 fand der erste Informationsaustausch zwischen den 51 „Early Adopters“ statt.

Ich habe das Thema im Rahmen der Artikel-29-Gruppe und des Europäischen Datenschutzausschusses (EDSA) begleitet und bin über die Financial Matters Subgroup des EDSA mit der OECD im Dialog. Um bei den nationalen Finanzministerien den Stand der Umsetzung des OECD-Standards in den Mitgliedstaaten zu erheben und die Erfahrungen mit dem ersten Datenaustausch vom September 2017 abzufragen, hatte der EDSA einen Fragebogen erarbeitet. Aus den Antworten ergab sich erfreulicherweise, dass bisher keine schwerwiegenden Datenschutzverletzungen aufgetreten sind.

6.2.2 Meldungen von Datenschutzverstößen aus den Finanzbehörden

Im Berichtszeitraum haben mich auch mehrere Tausend Meldungen von Datenschutzverstößen aus den Finanzbehörden erreicht.

Häufig handelte es sich dabei um Fehlversendungen aufgrund eines individuellen Bearbeitungsfehlers. Da die Finanzbehörden pro Jahr Millionen von Postsendungen in Auftrag geben, zeigt mir die Anzahl der Meldungen, dass es sich nicht um ein systemisches Problem innerhalb der Finanzverwaltung handelt und sich die Finanzverwaltung insoweit im Fehlertoleranzbereich bewegt, den ich von anderen Behörden kenne. Es ist aber noch zu früh, um abschätzen zu können, ob auch systemische Fehlerquellen zu Datenschutzverstößen führen. Die gemeldeten Datenschutzverstöße werde ich bei meinen künftigen Kontrollen zum Kontrollgegenstand machen.

Administrativ stellt mich die Vielzahl dieser Meldungen allerdings vor große Herausforderungen. Während nach dem bisherigen § 42a BDSG (alt) nur gesetzlich bestimmte besondere Datenschutzverletzungen gemeldet werden mussten, unterfallen der Meldeverpflichtung nach Art. 33 DSGVO alle öffentlichen und nicht-öffentlichen Stellen im Anwendungsbereich der DSGVO. Die Meldungen von Datenschutzverletzungen sind seit dem 25. Mai 2018 daher auch exorbitant angestiegen. Im Rahmen meiner Zuständigkeit bin ich von Amts wegen gehalten, diese Meldungen zu prüfen und – soweit im Einzelfall erforderlich – von meinen datenschutzaufsichtsbehördlichen Untersuchungs- und Abhilfebefugnissen Gebrauch zu machen.

6.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

7 Ausschuss für Gesundheit

7.1 Einzelthemen

7.1.1 Datenschutz-Grundverordnung in der medizinischen Forschung und im Gesundheitswesen

Der Gesetzgeber muss den erforderlichen Schutz von Gesundheits- und genetischen Daten auch im Rahmen der Forschung mit diesen Daten garantieren.

In meinem 26. Tätigkeitsbericht hatte ich bereits darauf hingewiesen, dass die Digitalisierung des Gesundheitswesens und die rasche technologische Entwicklung neue Chancen für die Forschung mit Gesundheits- und genetischen Daten versprechen, für die die DSGVO nun die Rahmenbedingungen setzt (vgl. dort Nr. 9.1). Seit Geltung der DSGVO liegen zwar noch keine aussagekräftigen Erfahrungen im Bereich der medizinischen Forschung vor, allerdings ist eine gewisse Verunsicherung über die rechtlichen Grundlagen für die Forschungstätigkeit festzustellen. Die Vorgaben des Artikel 89 DSGVO sind vor dem Hintergrund der generellen Haltung der EU zum Wissenschaftsbereich und dem in Artikel 179 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) festgelegten Zieles der Schaffung eines Europäischen Forschungsraumes dabei als eher forschungsfreundlich zu interpretieren. Gleichwohl darf gerade bei sensiblen Gesundheits- und genetischen Daten der Schutz der betroffenen Person(en) nicht aus dem Auge verloren werden.

Besondere Bedeutung bei der Anpassung der Regelungen zum Sozialdatenschutz im Zehnten Buch Sozialgesetzbuch (vgl. Nr. 3.1.1) kommt dabei der Neufassung des § 75 SGB X zu. Hier wird die Berechtigung der Sozialleistungsträger geregelt, Sozialdaten für die wissenschaftliche Forschung zur Verfügung zu stellen (vgl. auch 25. TB Nr. 9.5). Diese Daten bestehen zwar nicht nur, aber doch zu einem großen Teil aus Gesundheitsdaten. Die bisherigen Regelungen über die Genehmigungspflicht der Bereitstellung von Sozialdaten für die wissenschaftliche Forschung sowie die Einschränkungen bei der Verarbeitung dieser Daten für bestimmte Forschungsvorhaben im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung wurden grundsätzlich beibehalten. Ich begrüße es auch ausdrücklich, dass der antragstellende Sozialleistungsträger für das Forschungsprojekt ein Datenschutzkonzept vorzulegen hat. Dies erleichtert sowohl der Genehmigungs-, aber auch der Datenschutzaufsichtsbehörde die Prüfung des Forschungsprojektes und sorgt letztlich für einen besseren Schutz sensibler Sozialdaten.

Neu eingefügt wurde in Absatz 2 allerdings eine Regelung für Folgeforschungen. Danach kann die Frist, die den Wissenschaftlern zur Verarbeitung der Sozialdaten für Forschungszwecke gegeben wurde, entweder verlängert oder ganz neu bestimmt werden und es können weitere Sozialdaten übermittelt werden, wenn sich bei der wissenschaftlichen Forschung eine weitere Forschungsfrage ergibt, die in einem inhaltlichen Zusammenhang mit der ursprünglichen Forschungsfrage steht. Für die Weiternutzung der aufgrund der ursprünglichen Genehmigung übermittelten Sozialdaten für andere, aber noch in einem weiteren Sinn mit der ursprünglichen Forschungsfrage in Zusammenhang stehende neue Forschungsfragen, findet danach auch ein erleichtertes Genehmigungsverfahren statt. Die Regelung lässt Spielraum für missverständliche Interpretationen und man wird in der Praxis beobachten müssen, wie die Genehmigungsbehörden die Norm auslegen.

Besonders kritisch sehe ich § 75 Absatz 4 Satz 6 SGB X, in dem zwei unterschiedliche Regelungen in einem Satz zusammengefasst wurden. Die zehnjährige Speicherfrist aus dem ersten Teil des Satzes dient dazu, Forschungsergebnisse reproduzieren zu können. Dies ist ein Ergebnis der Forderung der Deutschen Forschungsgemeinschaft und eine Reaktion auf betrügerische wissenschaftliche Veröffentlichungen in den 1990er Jahren. Gegen diese Regelung bestehen keine datenschutzrechtlichen Bedenken. Es muss allerdings betont werden, dass der Zweck der Regelung notwendigerweise bedingt, dass die Rohdaten, die den wissenschaftlichen Forschungsergebnissen zugrunde liegen, nicht verändert werden, um Manipulationen zu verhindern. Dem widerspricht jedoch die Regelung im zweiten Teil des Satzes, wonach diese

Daten, die ausschließlich für Zwecke der Nachprüfung der Forschungsergebnisse verwendet werden sollen, für weitere Forschungen zur Verfügung stehen. § 75 Absatz 4 Satz 6 SGB X erweckt damit den Eindruck, sensible Daten unabhängig von einem konkreten Forschungszweck der Forschung zur freien Verfügung überlassen zu wollen. Dies geht weit darüber hinaus, was selbst nach dem sog. „broad consent" aus Erwägungsgrund 33 der DSGVO zulässig wäre. Maßstab muss auch hier der Grundsatz der Erforderlichkeit sein.

Ich bin besorgt darüber, dass die DSGVO trotz aller Privilegierung der wissenschaftlichen Forschung im Grundsatz von der informierten Einwilligung der betroffenen Person bei der Bereitstellung ihrer Daten für die wissenschaftlichen Forschung ausgeht, aber Regelungen wie in § 75 Absatz 4 Satz 6 SGB X die Nutzung des „broad consent" zur Regel machen. Die Idee eines „broad consent", also einer Einwilligung in zum Zeitpunkt der Einwilligung noch nicht hinreichend feststehende Forschungszwecke, war erst in der allerletzten Spätphase des sog. Trilogs über den späteren Erwägungsgrund 33 in die DSGVO eingefügt worden. Im eigentlichen Normtext finden sich ausschließlich Regelungen zur informierten Einwilligung der betroffenen Person. Auch die Artikel-29-Gruppe hatte in ihrer Stellungnahme zur Einwilligung darauf hingewiesen, „dass in Erwägungsgrund 33 die Verpflichtungen in Bezug auf die Anforderung der Einwilligung für den bestimmten Fall nicht gestrichen werden. Das bedeutet, dass wissenschaftliche Forschungsprojekte personenbezogene Daten grundsätzlich nur auf der Grundlage der Einwilligung mit einbeziehen dürfen, wenn es einen gut beschriebenen Zweck gibt. Für Fälle, in denen die Zwecke für die Datenverarbeitung im Rahmen eines wissenschaftlichen Forschungsprojektes am Anfang nicht angegeben werden können, ermöglicht Erwägungsgrund 33 ausnahmsweise, dass der Zweck allgemeiner beschrieben werden kann." (WP 259rev.01 vom 10.04.2018, S. 34). Beim „broad consent" handelt es sich also um eine Ausnahmeregelung, die nach den allgemein geltenden juristischen Auslegungsregeln daher auch eng auszulegen ist.

Bedauerlicherweise fanden meine Einwände zur Änderung des § 75 SGB X auch im Hinblick auf das von der Bundesregierung gewählte Verfahren, diese in Form von Formulierungshilfen in die parlamentarischen Beratungen zum Gesetz zu Änderung des Bundesversorgungsgesetzes mit einzuführen (vgl. Nr. 3.1.1), keine Berücksichtigung. So sind andere, wesentlich datenschutzfreundlichere Einwilligungsmodelle nicht hinreichend diskutiert worden. Dazu gehört etwa der auch international diskutierte „dynamic consent", bei dem der betroffenen Person die Möglichkeit bleibt, im gesamten Lauf einer wissenschaftlichen Studie zu einzelnen Teilen ihre Einwilligung zu erteilen, zu widerrufen oder zu modifizieren. Bei sozialwissenschaftlichen Studien in den USA sowie Großbritannien wurde dies bereits durch die Nutzung einer entsprechenden App verwirklicht.

Auch außerhalb der Forschung mit Sozialdaten werde ich die Nutzung von personenbezogenen Daten, insbesondere von Gesundheitsdaten, im Auge behalten. Dabei möchte ich betonen, dass ich der wissenschaftlichen Forschung sehr positiv gegenüberstehe. Allerdings darf bei der wissenschaftlichen Auswertung von personenbezogenen Daten nicht vergessen werden, dass sich nicht nur die Wissenschaft auf die Forschungsfreiheit berufen kann. Grundrechtlich verbürgte Rechte haben auch diejenigen, deren Daten für die Wissenschaft genutzt werden. Hier stelle ich auch weiterhin meine Expertise gerne bereit, um bei der Abwägung zwischen Forschungsfreiheit einerseits und Recht auf informationeller Selbstbestimmung andererseits zu angemessenen Ergebnissen zu kommen.

7.1.2 Elektronische Gesundheits- und Patientenakten sowie sog. GesundheitsApps

Ein Begriffswirrwarr kann auch zur Vereinheitlichung führen.

Die Presse berichtet immer wieder über „elektronische Gesundheitsakten" oder „elektronische Patientenakte". Die Krankenkassen sind auf dem Vormarsch, den Versicherten eine Möglichkeit zu bieten, ihre Gesundheitsdaten elektronisch zu speichern und darauf zuzugreifen. Auch das Bundesministerium für Gesundheit (BMG) treibt die Entwicklung im Bereich der Digitalisierung im Gesundheitswesen voran, mit der auch ich mich wegen der damit verbundenen datenschutzrechtlichen Fragen befasse.

In der Öffentlichkeit werden die verschiedenen Lösungen einer Gesundheitsdatensammlung wenig bis gar nicht unterschieden. Die Begriffe „Patientenakte" und „Gesundheitsakte" werden vielmehr synonym verwendet. Es ist jedoch wichtig zu wissen, dass die verschiedenen Lösungen auf verschiedenen gesetzlichen Grundlagen beruhen und unterschiedliche Konsequenzen gerade für die Versicherten haben (vgl. Schaubild zu Nr. 7.1.2).

Elektronische Patientenakte (ePA)

Der Begriff der elektronischen „Patientenakte" wird sowohl im Bürgerlichen Gesetzbuch (BGB) als auch im Sozialgesetzbuch (SGB) verwendet. Gemeinsam ist der elektronischen Patientenakte sowohl nach § 630f BGB als auch nach § 291a SGB V, dass sie von den Leistungserbringern (Ärzte, Psychotherapeuten, Apotheker, Krankenhaus etc.) geführt werden soll. Sie beinhaltet Befunde, Diagnosen, Behandlungsberichte etc. und dokumentiert – wie in der bisherigen in Papierform geführten

Patientenakte – die medizinische Behandlung. Bei der elektronischen Patientenakte im Sinne des § 291a SGB V kommt noch hinzu, dass sie grundsätzlich einrichtungsübergreifend und nicht fallbezogen angelegt ist.

Derzeit ist der rechtliche Rahmen so gestaltet, dass die elektronische Patientenakte nach § 291a SGB V durch die elektronische Gesundheitskarte unterstützt werden soll. Erforderlich für den Zugriff auf die Daten ist ein elektronischer Heilberufeausweis sowie eine elektronische Gesundheitskarte, die das Einverständnis des Versicherten nachweist. Auf die gleiche Weise kann der Versicherte auch bestimmten Leistungserbringern seine Daten zur Verfügung stellen. Die elektronische Patientenakte nach § 630f BGB ist demgegenüber die Umsetzung der ärztlichen Dokumentation der Behandlung, auf die zunächst nur der behandelnde und dokumentierende Arzt Zugriff hat.

Elektronische Gesundheitsakte (eGA)

Eine verbindliche Definition für die elektronische Gesundheitsakte gibt es nicht. Sie hat sich vielmehr aus der in § 68 SGB V normierten Möglichkeit der gesetzlichen Krankenversicherungen heraus entwickelt, ihre Versicherten bei der Nutzung einer „fremden" eGA finanziell zu unterstützen. Im Gegensatz zur ePA, die vom jeweiligen Leistungserbringer zu Dokumentationszwecken geführt wird, wird die eGA von Privatunternehmen bisweilen in enger Zusammenarbeit mit gesetzlichen und privaten Krankenversicherungen entwickelt und im Rahmen einer „GesundheitsApp" angeboten. Wie bei einer ePA im Sinne des § 291a SGB V können darin Gesundheitsdaten des Versicherten erhoben, verarbeitet und gespeichert werden. Allerdings erfolgt dies grundsätzlich unabhängig von der Telematik-Infrastruktur und somit ohne Nutzung der elektronischen Gesundheitskarte.

Gegen eGA oder ePA bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken. Es gibt aber in unterschiedlichen geprüften Projekten im Einzelnen datenschutzrechtlich problematische Punkte. Das gilt beispielsweise im Rahmen des Authentifizierungsverfahrens oder durch Weitergaben von Nutzerdaten durch Trackingdienste. Auch die geplante elektronische Übermittlung von Arbeitsunfähigkeitsbescheinigungen außerhalb des Systems der Telematik-Infrastruktur ist datenschutzrechtlich bedenklich. Außerdem sehe ich die Möglichkeit kritisch, Gesundheitsdaten im Sinne des § 305 SGB V direkt von der Krankenversicherung in eine eGA zu senden. Wegen der engen Auslegung des § 284 SGB V sind die gesetzlichen Krankenversicherungen nicht berechtigt, diese Daten jemand anderem zu übermitteln als an den Versicherten selbst. Das gilt sogar für den Fall der Einwilligung des Betroffenen. Allerdings sieht der zum Redaktionsschluss sich noch in der parlamentarischen Beratung befundene Entwurf eines Terminservice- und Versorgungsgesetzes (TSVG) eine entsprechende gesetzliche Grundlage vor.

Im Rahmen des TSVG ist künftig der Zugriff auf die Daten der ePA auch ohne Heilberufsausweis vorgesehen. Bisher sah das Konzept des Gesetzgebers neben der ePA auch ein elektronisches Patientenfach (ePF) vor, für das andere Zugriffsmodalitäten als für die ePA gelten sollten. Mit Inkrafttreten des TSVG soll nach Plänen des Gesetzgebers das ePF jedoch mit der ePA zusammengeführt und vereinheitlicht werden. Das bisher geplante Patientenfach wird dann entfallen.

Unter Beachtung datenschutzrechtlicher Anforderungen sind für die Nutzung von elektronischen Patienten- und Gesundheitsakten weitere gesetzliche Grundlagen und Rahmenbedingungen notwendig. Besonderer Wert ist in diesem Zusammenhang darauf zu legen, dass die Datenhoheit eindeutig bei dem Versicherten verankert wird. Außerdem ist auf die Freiwilligkeit der Nutzung einer solchen „Gesundheitsdatensammlung" zu achten.

Gesundheits-Apps

Über die datenschutzrechtlichen Probleme bei den sog. Gesundheits-Apps hatte ich in meinem 26. TB (Nr. 1.5 und 9.2.4) berichtet. Leider bestehen diese Probleme nach wie vor. Hinzu kommt, dass auch für den Zugriff auf eGA vermehrt auf sog. Gesundheits-Apps gesetzt wird. So wurde beispielsweise im Sommer/ Herbst 2018 in der Presse sehr ausführlich über die App der Fa. Vivy GmbH berichtet. Die Sicherheit der dazugehörigen App der Fa. Vivy wird von der hierfür zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit geprüft.

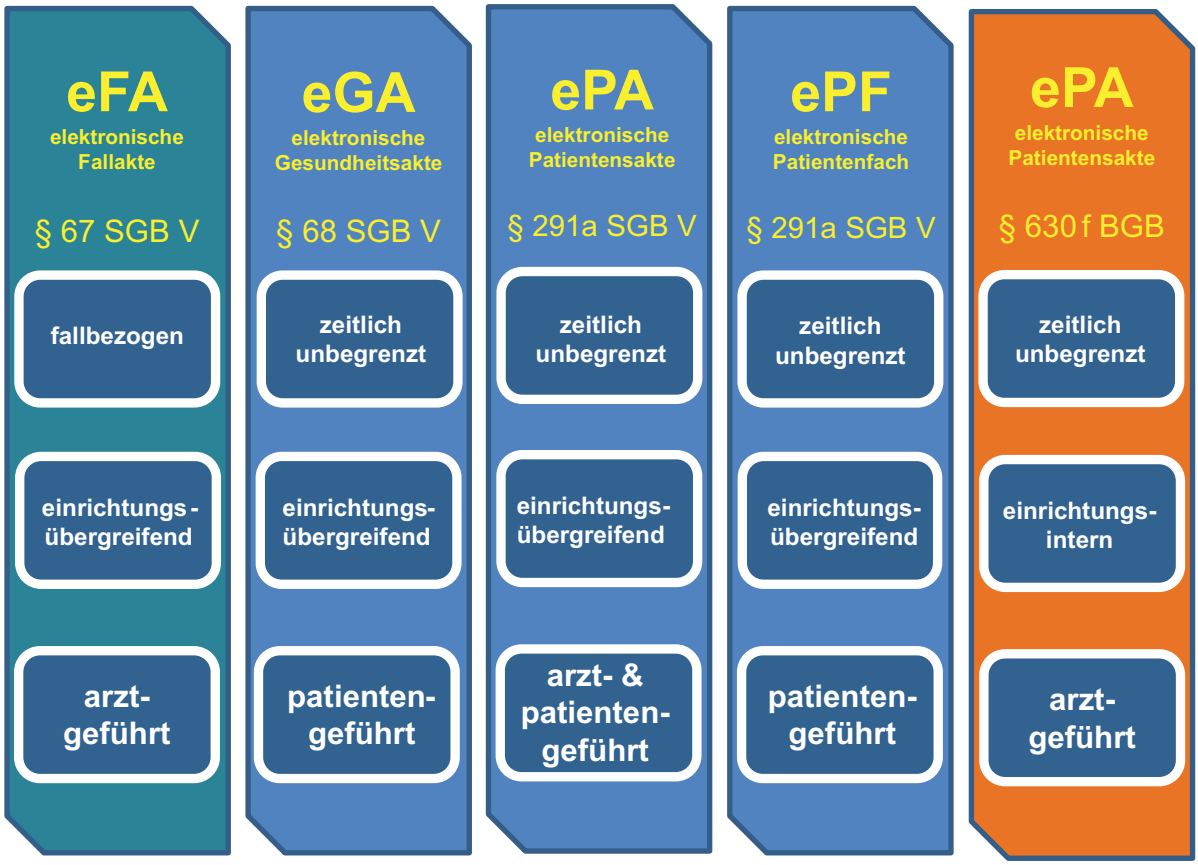
Um die Nutzung von mobilen Anwendungen, u.a. von Gesundheits-Apps im Bereich des Gesundheitswesens, geht es auch in einer vom BMG eingerichteten Arbeitsgemeinschaft, an der ich mich beteilige.

7.1.3 Elektronische Gesundheitskarte – Verfahrensstand einer ewig Unvollendeten

Wie im letzten Tätigkeitsbericht berichtet, hat die Erprobung der elektronischen Gesundheitskarte in der Arztpraxis zwar endlich begonnen, es fehlen aber noch immer die ersten medizinischen Anwendungen. Selbst der Versicherten-Stamm-Datendienst (VDD) ist noch nicht in Betrieb genommen. Die Patientinnen und Patienten müssen weiterhin warten.

In meinem 26. Tätigkeitsbericht habe ich über die geplanten Erprobungsmaßnahmen in den Testregionen Nordwest und Südost berichtet (vgl. Nr. 9.3.2). Die Weiterentwicklung erfolgt allerdings nur sehr schleppend.

Schaubild elektronische Gesundheits- und Patientenakte zu Nr. 7.1.2



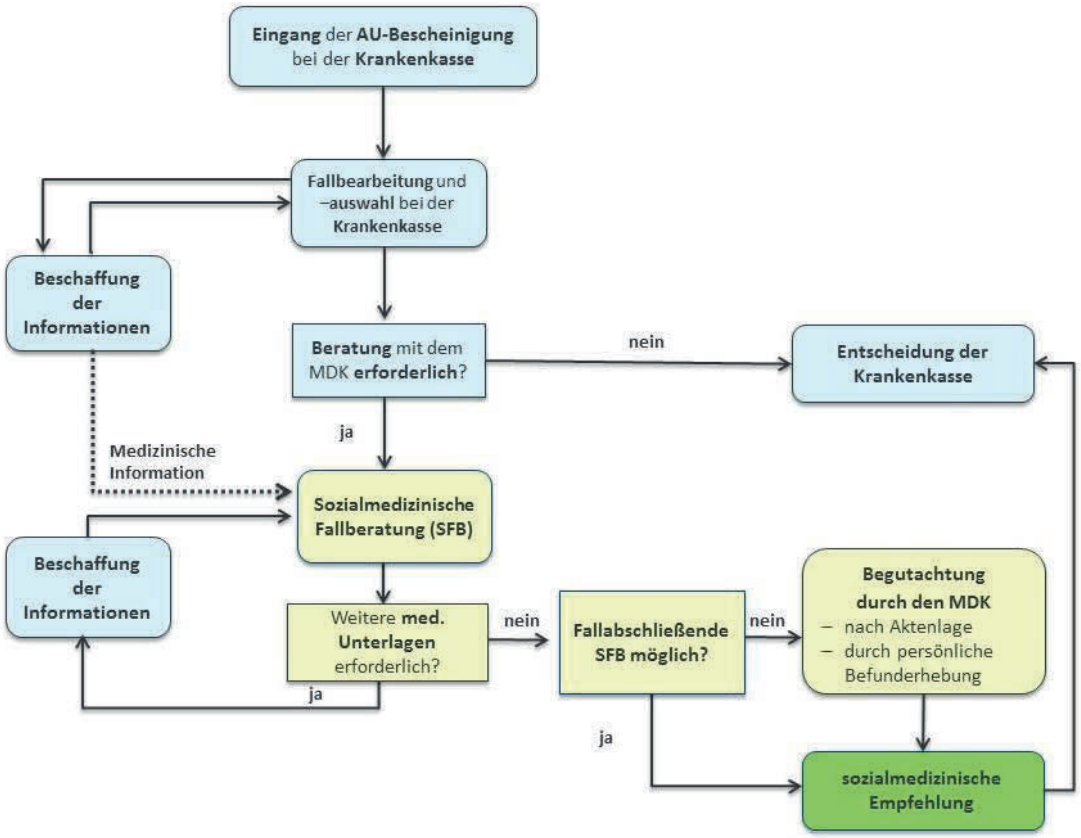
Die spürbare Belebung des Projekts der elektronischen Gesundheitskarte durch das „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz; vgl. 26. TB Nr. 9.2.1) zeigt aber Wirkung. Fachkonzepte für die ersten Anwendungen (Notfalldatenmanagement, elektronische Patientenakte) liegen mittlerweile vor oder sie befinden sich kurz vor der Endabstimmung. Die Androhung von Sanktionen scheint Wirkung zu zeigen.

Im Jahre 2019 soll die elektronische Gesundheitskarte endlich online gehen. Der VDD sowie das Notfalldatenmanagement werden die ersten Anwendungen sein, die dann bis Mitte 2019 durch die elektronische Patientenakte (ePA) ergänzt werden sollen (vgl. hierzu auch Nr. 7.1.2). Die Ausgabe der hierzu notwendigen Heilberufsausweise des Arztes und Institutsausweise ist angelaufen.

Nach dem Anwendungsbeginn der DSGVO im Mai 2018 stellte sich mit Nachdruck die Frage, wer eigentlich Verantwortlicher für die Telematik-Infrastruktur (TI) ist und damit eine Datenschutz-Folgenabschätzung (DSFA) vorzulegen hat (vgl. hierzu auch unter Nr. 15.2.3). Viele Arztpraxen sind ihrer gesetzlichen Verpflichtung zur Erstellung einer DSFA nachgekommen. Sie haben dabei allerdings nicht an der Schwelle ihrer Praxisräume Halt gemacht, sondern vielmehr auch die TI in ihre Betrachtungen mit einbezogen. Die gesetzlich vorgeschriebene DSFA der Arztpraxis ergab dann, dass ein Anschluss an die TI nicht vertretbar sei. Viele Ärzte haben sich deshalb an mich gewandt.

Die Frage, wer der datenschutzrechtliche Verantwortliche im Sinne der DSGVO für die TI ist, konnte bis zum Redaktionsschluss noch nicht endgültig geklärt werden.

Schaubild Arbeitsunfähigkeit zu Nr. 7.1.4



Quelle: GKV-Spitzenverband „Begutachtungsanleitung Arbeitsunfähigkeit“ S. 52

7.1.4 Das Krankengeldfallmanagement

Rund zwei Jahre nach Einführung des § 44 Absatz 4 SGB V als neue gesetzliche Grundlage für das Krankengeldfallmanagement lässt die datenschutzkonforme Umsetzung durch die Krankenkassen noch auf sich warten.

Bei meinen Kontrollen vor Ort und anhand zahlreicher Beschwerden von Versicherten musste ich feststellen, dass die durch § 44 Absatz 4 SGB V vorgesehene Beratung und Unterstützung von Versicherten im Krankengeldbezug weiterhin (vgl. 26. TB Nr. 9.2.5; 25. TB Nr. 13.7.1) nicht datenschutzkonform erfolgt. So wurde beispielsweise der Beratungsprozess mit einer ausführlichen Datenerhebung begonnen, ohne dass zuvor die erforderliche schriftliche Einwilligung der versicherten Person vorgelegen hat. Die Vordrucke wiesen teilweise nicht auf die Freiwilligkeit dieses Beratungsangebots hin. Auch wurden den Versicherten keine ausführlichen „schriftlichen“ Informationen zur Datenverarbeitung zur Verfügung gestellt.

Die individuelle Beratung und Hilfestellung durch die Krankenkassen endet zudem dort, wo im Rahmen des Krankengeldfallmanagements die medizinische Beurteilung durch den Medizinischen Dienstes der Krankenversicherung (MDK) zur Sicherung des Behandlungserfolges erforderlich ist. Hier überschreiten die Krankenkassen zum Teil deutlich die ihnen gesetzlich zugewiesenen Befugnisse.

§§ 275 Absatz 1 und 276 Absatz 2 SGB V regeln in diesem Zusammenhang sowohl die Kompetenzen als auch die Zusammenarbeit der gesetzlichen Krankenkassen und des MDK. Um dem Rechnung zu tragen, hat der Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) seinen gesetzlichen Auftrag nach § 282 Absatz 2 Satz 3 SGB V umgesetzt und die „Begutachtungsanleitung Arbeitsunfähigkeit“ als Richtlinie über die Zusammenarbeit der Krankenkassen mit dem MDK neu gefasst.

Demnach sollen Krankenkassen in einer gemeinsamen „sozialmedizinischen Fallberatung“ mit dem MDK die Fälle bestimmen, die ohne ein Fallmanagement zu einer

Langzeitarbeitsunfähigkeit führen würden. Durch eine umfassende Informationsbeschaffung beim behandelnden ärztlichen Personal oder beim Betrieb soll die Genesung des Versicherten schneller vorangebracht werden.

Eine sozialmedizinische Fallberatung als erster – und häufig einziger Schritt – eines Begutachtungsverfahrens nach § 275 Absatz 1 SGB V steht im Einklang mit den datenschutzrechtlichen Regelungen. Voraussetzung dafür ist aber, dass die Krankenkasse dem MDK einen Gutachtenauftrag erteilt hat. Der MDK stellt dann fest, ob die sozialmedizinische Fallberatung abgeschlossen werden kann oder zusätzliche Unterlagen sowie eine weitere Begutachtung erforderlich sind. Die von mir kontrollierten bzw. befragten Krankenkassen gaben jedoch an, dass in der Praxis eine Anforderung medizinscher Unterlagen bereits vor Erteilung eines Gutachtenauftrags nach § 275 Absatz 1 SGB V an den MDK und vor der sozialmedizinischen Fallberatung erfolge. Entsprechend der o. g. Begutachtungsanleitung ergehe mit der Anforderung medizinischer Unterlagen beim Leistungserbringer zeitgleich eine Benachrichtigung an den MDK; dies stelle auch nach Aussage des GKV-Spitzenverbandes den Auftrag zur Begutachtung dar.

In einem beratenden Gespräch hat der GKV-Spitzenverband meine Bedenken aufgenommen und wird die Begutachtungsanleitung einer Prüfung und Überarbeitung unterziehen.

7.1.5 Nutzung von Messenger-Diensten bei den Sozialversicherungsträgern

Das Angebot verschiedener Sozialversicherungsträger, mit ihren Versicherten mittels Messenger-Dienst in Kontakt zu treten, ist datenschutzrechtlich problematisch.

Das gilt vor allem für den verbreitetsten Messenger WhatsApp, der seine Nutzung als „Einwilligung“ auch für eine undurchsichtige Datenübermittlung an Facebook und regelmäßige Adressbuchuploads betrachtet (allgemein zur datenschutzrechtlichen Problematik von Messenger-Diensten vgl. Nr. 15.2.6). Da im Kontakt mit Sozialversicherungsträgern häufig gesundheitsbezogene Daten betroffen sein können, die zu den besonderen Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 DSGVO zählen und deshalb einen besonders hohen Schutz genießen, habe ich die Sozialversicherungsträger darauf hingewiesen, dass derzeit aufgrund mangelnder Datenschutzkonformität auf alternative Kommunikationsverfahren zurückgegriffen werden sollte.

7.1.6 Neue Register im Bereich des Gesundheitswesens

Neben den schon seit langem existierenden Krebsregistern sind in den letzten Jahren im Gesundheitsbereich weitere Register entstanden, die der besseren Gesundheitsversorgung der betroffenen Patienten, aber auch der medizinischen Forschung dienen sollen.

Transplantationsregister

In meinem 26. Tätigkeitsbericht (Nr. 9.2.2) konnte ich mitteilen, dass im Gesetz zur Errichtung eines Transplantationsregisters dem Schutz der darin verarbeiteten hochsensiblen Daten die erforderliche Bedeutung beigemessen wurde. Die neu eingeführten Vorschriften in §§ 15a bis 15i Transplantationsgesetz (TPG) regeln die verschiedenen Datenflüsse. Neu ist auch die Zwischenschaltung einer Vertrauensstelle, die gewährleistet, dass die medizinischen Daten von Organspendern und Organempfängern ausschließlich pseudonymisiert im Register erfasst werden. Dies schützt die Identität der Beteiligten und ermöglicht gleichzeitig im erforderlichen Fall die konkrete Zuordnung.

Auch die Verfahrensordnung für die Datenübermittlung gemäß §§ 15a bis 15h TPG, zu der es gemäß § 15e Absatz 4 Satz 1 TPG meines Einvernehmens bedurfte, enthält ein hohes Datenschutzniveau.

Derzeit befindet sich die o. g. Vertrauensstelle im Aufbau. Regelungen zu deren Aufgaben sowie zum Verfahren der Pseudonymisierung bedürfen ebenfalls nach § 15c Absatz 3 Satz 2 TPG meines Einvernehmens.

Ich halte die bisherigen Überlegungen für vorbildlich. Sie berücksichtigen umfänglich die Anforderungen an eine unabhängige Vertrauensstelle, die räumlich, technisch, organisatorisch und personell vom Register getrennt ist, werden den besonderen Anforderungen der sensiblen Zusammenhänge im Organspendeverfahren mit den verschiedenen Beteiligten gerecht und tragen so zum Vertrauen in der Bevölkerung bei.

Deutsches Hämophilieregister

Im Berichtszeitraum wurde mir der Entwurf der Verordnung über das Deutsche Hämophilieregister zur Stellungnahme vorgelegt. Die zugrunde liegenden Vorschriften des Transfusionsgesetzes sind ab August 2019 anzuwenden. Das schon länger bestehende Deutsche Hämophilieregister ermöglicht die systematische und umfängliche Erfassung der Behandlungsdaten mit dem Ziel der Qualitätssicherung und Verbesserung der Versorgung. Die Daten werden meist von der behandelnden ärztlichen Person an das Register gemeldet. Die dem Register zugehörige Vertrauensstelle erzeugt für die Meldung ein Pseudonym, so dass die Daten beim Register ausschließlich pseudonymisiert erfasst werden. Falls die Patientin oder der Patient für die pseudonymisierte Meldung nicht die erforderliche Einwilligung erteilt, sehen die Regelungen vor, dass die behandelnde ärztliche Person die Daten anonym und zusammengefasst meldet.

Weitere Gesundheitsregister

Nach mir vorliegenden Informationen ist die Einrichtung weiterer Register mit Gesundheitsdaten vom BMG geplant. Dies ist im Sinne einer besseren Gesundheitsvorsorge und medizinischen Forschung auch im Interesse der betroffenen Patienten. In deren Sinne ist es allerdings auch, hierbei die besondere Sensibilität von Gesundheitsdaten zu beachten. Der europäische Verordnungsgeber hat Gesundheitsdaten nach Artikel 9 Absatz 1 DSGVO unter einen besonderen Schutz gestellt und ihre Verarbeitung grundsätzlich verboten. Nur unter den besonderen Voraussetzung des Artikel 9 Absatz 2 DSGVO ist die Verarbeitung von Gesundheitsdaten erlaubt. Dies bedeutet, dass der Gesetzgeber sich zum einen dieser Regel-Ausnahme-Situation bei der Schaffung von Normen zur Registrierung von Gesundheitsdaten bewusst sein muss. Er ist zum anderen gehalten, hier besondere Maßnahmen zum Schutz dieser besonderen Kategorien von Daten zu ergreifen.

Mein besonderes Augenmerk bei der Einrichtung künftiger Register im Gesundheitsbereich wird auf der Einrichtung von Vertrauensstellen liegen, die von der eigentlichen Registerstelle räumlich, technisch, organisatorisch und personell getrennt sind. Sowohl die Vertrauensstelle als auch die eigentliche Registerstelle haben zudem ein dem Stand der Technik entsprechendes Datensicherheitsniveau nachzuweisen. Dies gilt insbesondere auch für die zu nutzenden Pseudonymisierungsverfahren. Zudem sollte in einem Datenschutzkonzept festgelegt werden, wie die in der DSGVO vorgesehenen Rechte der Betroffenen, insbesondere das Auskunftsrecht, gewährleistet werden.

7.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

8 Haushaltsausschuss

8.1 Einzelthemen

8.1.1 Beratung zum Datenschutz bei der IT-Konsolidierung Bund

Das Projekt „IT-Konsolidierung Bund“ hat zum Ziel, die Arbeitsfähigkeit der Bundesregierung für die nächsten Jahre sicherzustellen und einen effizienten Betrieb zu gewährleisten. Hierzu müssen IT-Netze sowie Rechenzentren konsolidiert und die IT-Beschaffung des Bundes gebündelt werden. Betroffen sind ca. 350.000 Benutzer der Bundesverwaltung. Damit der Datenschutz im Projekt eingehalten wird, bezieht mich die Bundesregierung in beratender Funktion ein, wie im Beschluss des Haushaltsausschusses des Deutschen Bundestags vom 17. Juni 2015 vorgesehen.

Um meiner Beratungsaufgabe im Projekt gerecht zu werden, ist eine intensive Mitarbeit erforderlich, insbesondere im Teilprojekt 6 „Dienstekonsolidierung“. Dieses Teilprojekt beinhaltet mehrere Maßnahmen wie den „Bundesclient“, die „Bundescloud“ und das „Identity and Access Management“, für die jeweils eigene Kernteams gebildet wurden. Diese Kernteams setzen sich aus Vertretern von BSI (Bundesamt für Sicherheit in der Informationstechnik), IT-Dienstleistern des Bundes, BMI und BfDI zusammen. Während die Maßnahme „Identity and Access Management“ gerade erst Fahrt aufnimmt, sind die Maßnahmen „Bundescloud“ und „Bundesclient“ schon weit fortgeschritten.

Die „Bundescloud“ ist definiert als eine standardisierte, skalierbare Plattform für die Basis-, Querschnitts- und Fachverfahren der IT des Bundes. Sie wird als private Cloud in den Rechenzentren des Bundes betrieben. Um in der Bundescloud verschiedene Dienste bereitzustellen, sind mehrere Cloud-Komponenten (Stacks) verschiedener Hersteller erforderlich. Neben Themen wie Mandantentrennung, Monitoring und Logging, Aufbewahrungszeiten sowie generell der Durchsetzbarkeit von Nutzerrechten, ging und geht es aus Datenschutzsicht bei den verschiedenen Produkten um das Auslesen und Übertragen von personenbezogenen Daten zum Hersteller. Da das Auslesen von Daten auch die IT-Sicherheit und den Geheimschutz betrifft, haben die IT-Dienstleister des Bundes diesen Punkt bei den Cloud-Komponenten, die zum Einsatz kommen sollten, im Vorfeld untersucht. Dabei wurde festgestellt, dass die Cloud-Komponente von Microsoft, selbst wenn sie auf eigener Infrastruktur betrieben wird, Daten zum Hersteller in die USA überträgt und sich dies – im Gegensatz zu den Produkten anderer Hersteller – auch nicht verhindern lässt. Deshalb ist ein Einsatz der Cloud-Komponente von Microsoft in der Bundescloud aus Sicherheits-, Geheimschutz- und nicht zuletzt Datenschutzgründen nicht möglich.

Bei der Maßnahme „Bundesclient“ geht es um die Bereitstellung eines bundesweit einheitlichen Arbeitsplatzes bis Ende 2025 mit standardisiertem Betriebssystem sowie Basis- und Querschnittsdiensten, wie z. B. E-Mail und Anwendungen zur Dokumentenbearbeitung.

Die Bundesverwaltung setzt bisher auf Produkte von Microsoft. Nachdem auf den Arbeitsplatzsystemen hauptsächlich Windows 7 installiert ist und der diesbezügliche erweiterte Support am 14. Januar 2020 ausläuft, ist der Wechsel auf ein anderes Betriebssystem unumgänglich. Die als gesetzt angesehene Ablösung durch Windows 10 wurde von mir aus mehreren Gründen in Frage gestellt. Mit Windows 10 lassen sich die im Grobkonzept zur IT-Konsolidierung Bund dargestellten Ziele nicht erreichen. Die Gewährleistung der Informationssicherheit vor dem Hintergrund steigender Komplexität, die dauerhafte Erhaltung der Hoheit und Kontrollfähigkeit über die eigene IT, die Fähigkeit, auf innovative technologische Trends flexibel reagieren zu können sowie die Sicherstellung eines leistungsfähigen, wirtschaftlichen, stabilen und zukunftsfähigen Betriebes betreffen unmittelbar den Datenschutz und sind bei der Bindung an einen Hersteller (Vendor Lock-in) nicht zu erreichen. Darüber hinaus wird zeitgleich mit der geplanten Fertigstellung des Bundesclients im Jahr 2025 der erweiterte Support für Windows 10 und Office 2016 eingestellt. Spätestens dann muss der Wechsel zu einem

datenschutzkonformen, wirtschaftlichem, stabilem und zukunftsfähigem Betriebssystem erfolgt sein.

Des Weiteren führt der Einsatz von Windows 10 aus Datenschutzsicht zu einem größeren Problem: Durch das nicht verhinderbare Auslesen von (auch personenbezogenen) Daten und deren Übertragung zu Microsoft in die USA können Datenschutz, Geheimschutz und IT-Sicherheit nicht gewährleistet werden. Dies wurde durch eine im November 2018 veröffentlichte Studie des BSI mit dem Titel „SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10“ bestätigt. Vom BSI vorgeschlagene Gegenmaßnahmen sind lediglich temporär wirksam und führen nicht zu einem möglichen datenschutzkonformen Einsatz von Windows 10. Aus diesem Grund kann der Einsatz von Windows 10 in der Bundesverwaltung nach wie vor nicht empfohlen werden. Meine Aufgabe war und wird sein, zu dieser Problemstellung weiter zu beraten. Insbesondere bei der durch den Lenkungsausschuss des Teilprojekts 6 beschlossenen „Machbarkeitsstudie zu alternativen Betriebssystemen“ ist eine intensive Mitarbeit erforderlich, um eine langfristige und zukunftsfähige Alternative zu Windows 10 zu eruieren, mit der sich sowohl die Ziele der IT-Konsolidierung Bund erreichen, als auch die Anforderungen an den Datenschutz auf Basis der DSGVO erfüllen lassen.

Alle Maßnahmen des Teilprojekts 6 „Dienstekonsolidierung“ müssen auf Konformität untereinander – insbesondere zur Bundescloud als der grundlegenden Infrastruktur – geprüft werden. Da ich bei allen Maßnahmen umfassend beteiligt werde, können Datenschutzaspekte auch maßnahmenübergreifend bewertet werden, was sich positiv auf die Beratungsqualität auswirkt.

Um die Projektleitung der IT-Konsolidierung Bund langfristig bei den strategischen Entscheidungen zu unterstützen, war eine intensive Mitarbeit in den entsprechenden Gremien, etwa zur Architekturrichtlinie, erforderlich. Darüber hinaus erfolgten ein regelmäßiger Austausch mit der Gesamtprojektleitung und die Teilnahme an Ressortworkshops, um Fragestellungen zum Datenschutz einzubringen und zu beantworten.

Neben den Maßnahmen der Teilprojekte wurde ich zu konkreten Vorhaben wie PVS+ (Personalverwaltungssystem) und E-Akte (elektronische Aktenführung) hinzugezogen. Hierbei ging es u. a. um Themen wie Mandantentrennung, Monitoring und Logging sowie Aufbewahrungszeiten. Im Vorhaben PVS+ wurden meine Empfehlungen bisher nicht umgesetzt. Es erfolgt nach wie vor keine, dem Schutzbedarf der personenbezogenen Daten entsprechende Mandantentrennung bei der Datenhaltung und der Datenverarbeitung. Es wird weder die anwendungsseitig vorhandene Mandantenfähigkeit genutzt, noch erfolgen eine physisch bzw. logisch getrennte Datenhaltung. Der Zugriff wird lediglich über ein Rechte- und Rollenkonzept gesteuert. Hier sehe ich die mandantenspezifische Verschlüsselung als kurzfristiges Mittel der Wahl, auch unter dem Aspekt, dass beim PVS+ Microsoft- und Adobe-Produkte verwendet werden.

Das Vorhaben E-Akte wurde datenschutzkonform umgesetzt. Besonders hervorzuheben sind die browserbasierte Oberfläche und die offenen Schnittstellen, die den Betrieb unabhängig von Betriebssystem und Office-Anwendungen ermöglichen. Dasselbe wäre auch für die behördeneigenen Fachverfahren wünschenswert. Fachverfahren müssen aus Sicherheits-, Stabilitäts- und Datenschutzgründen unabhängig vom Betriebssystem und etwaiger Basisanwendungen betrieben werden können. Obwohl diese Anforderung bereits in den Architekturrichtlinien für die Bundesverwaltung festgeschrieben ist, wurde sie bisher nur in wenigen Behörden als Aufgabe angegangen. Dies ist aber die Voraussetzung für den Einsatz einer alternativen, datenschutzkonformen Plattform.

Zusammenfassend stelle ich fest, dass die Bundesregierung die Aufforderung des Haushaltsausschusses des Deutschen Bundestages zu meiner Einbeziehung ernst nimmt und die Zusammenarbeit mit allen Beteiligten, einschließlich der IT-Dienstleister des Bundes, sehr gut ist. Meiner Verantwortung, auf die Einhaltung des Datenschutzes bei der Umsetzung der IT-Konsolidierung Bund hinzuwirken, werde ich zukünftig nachkommen.

8.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.1, 17.5, 17.9, Die Arbeit des BfDI in Zahlen

9 Ausschuss für Inneres und Heimat

9.1 Aus den Gesetzgebungsvorhaben

9.1.1 Zweites Datenaustauschverbesserungsgesetz

Die fortlaufenden Änderungen des Ausländer- und Asylrechts begegnen – teils erheblichen – Bedenken aus Datenschutzsicht.

Nachdem bereits im Jahr 2016 mit dem Datenaustauschverbesserungsgesetz zahlreiche datenschutzrechtlich bedeutsame Änderungen ausländer- und asylrechtlicher Vorschriften vorgenommen wurden, hat die Bundesregierung im Berichtszeitraum mit dem Entwurf für ein zweites Datenaustauschverbesserungsgesetz ein Gesetzesvorhaben vorgelegt, mit dem erneut tiefgreifende Veränderungen einhergehen.

Mit Sorge sehe ich dabei vor allem die fortschreitende Aufweichung des Verbots der unbeschränkten Nutzung der AZR-Nummer. Aus meiner Sicht wird hierdurch schrittweise ein einheitliches Personenkennzeichen geschaffen.

Bereits in seiner Volkszählungsentscheidung vom 15. Dezember 1983 (BVerfGE 65, 1) hat das Bundesverfassungsgericht die Gefahr einer umfassenden Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner personenbezogener Informationen zur Erstellung von Persönlichkeitsprofilen erkannt und deshalb die Einführung einheitlicher Personenkennzeichen oder sonstiger Ordnungsmerkmale als unzulässig qualifiziert. Auch wenn Stimmen in der Literatur und Praxis eine solche Gefahr im Falle der unbeschränkten Nutzung der AZR-Nummer nicht sehen wollen, können die verfassungsrechtlichen und verfassungsgerichtlichen Vorgaben nicht außer Acht gelassen werden.

Nach den Plänen der Bundesregierung soll das Ausländerzentralregister (AZR) perspektivisch zu einem zentralen Ausländerdateisystem weiterentwickelt werden (vgl. BT-Drs. 19/5791, S. 11). Der Umfang der im AZR gespeicherten personenbezogenen Daten soll ebenso erweitert werden wie die Zugriffsmöglichkeiten im automatisierten Verfahren. Immer mehr Behörden sollen für immer mehr Zwecke Zugriff erhalten. War das AZR zunächst in erster Linie zur Unterstützung ausgewählter Behörden bei der Durchführung ausländer- und asylrechtlicher Vorschriften insbesondere in Fragen der Einreise und des Aufenthalts gedacht, sind bereits jetzt über 14.000 Behörden und Organisationen zum Zugriff auf das Register berechtigt, teils ohne überhaupt ausländer- und asylrechtliche Vorgänge zu bearbeiten. Der weitere Ausbau führt dazu, dass eine letztlich unüberschaubare Menge personenbezogener Daten aus unterschiedlichsten Lebensbereichen von Ausländern in das Register gelangen. Die durch das Bundesverfassungsgericht gesehene Gefahr einer umfassenden Registrierung und Katalogisierung der Persönlichkeit wächst dadurch noch einmal. Die Verknüpfung dieser Daten mit der AZR-Nummer würde zwangsläufig zu einem einheitlichen Personenkennzeichen führen.

Vor diesem Hintergrund halte ich eine weitere Ausdehnung des Kreises der zugriffsberechtigten Behörden, insbesondere die Einführung des automatisierten Abrufs aus dem AZR als Regelfall, für höchst problematisch. Im Gegenteil sollte aufgrund der Vielzahl der gespeicherten Daten und deren Sensibilität insbesondere im Kontext von Asylverfahren der Kreis der Zugriffsberechtigten möglichst klein gehalten werden.

Mit fortschreitendem Ausbau des AZR wird letztlich auch meine Rolle als datenschutzrechtliche Aufsichtsbehörde immer wichtiger. Die zunehmende Komplexität und datenschutzrechtliche Sensibilität des Gesamtsystems führt zu einem deutlich steigenden Personalaufwand bei der gebotenen datenschutzrechtlichen Kontrolle.

Bei Redaktionsschluss zu diesem Tätigkeitsbericht dauerten die Ressortberatungen in der Bundesregierung noch an.

9.1.2 Weitere Rechtssetzungsvorhaben im Ausländer- und Asylrecht

Im Berichtszeitraum gab es in diesem Bereich zahlreiche weitere Regelungsvorhaben, allen voran das Gesetz zur besseren Durchsetzung der Ausreisepflicht, mit dem u. a. die Möglichkeit zur Auswertung von Datenträgern zur Feststellung der Identität und Staatsangehörigkeit im Asylgesetz verankert wurde.

Diese unter dem Begriff der „Handydatenauswertung" bekannt gewordene Befugnis des Bundesamtes für Migration und Flüchtlinge (BAMF) habe ich scharf kritisiert. So habe ich insbesondere darauf hingewiesen, dass die Erforderlichkeit für diesen Grundrechtseingriff nicht ersichtlich und die Maßnahme zudem unverhältnismäßig ist. Die beim Auslesen der Datenträger gewonnenen Informationen lassen keinen verlässlichen Rückschluss auf die tatsächliche Herkunft des Besitzers zu. Die Angaben können somit allenfalls ein schwaches Indiz sein. Die Anhörung des Geflüchteten und die individuelle Entscheidung durch einen Mitarbeiter des BAMF kann hierdurch nicht ersetzt werden. Ob die durch das Auslesen eines Datenträgers gewonnenen Informationen hierbei einen echten Mehrwert darstellen, habe ich bezweifelt. Meine Bedenken wurden letztlich jedoch nicht aufgegriffen. Von der praktischen Umsetzung der Regelung konnte ich mir bei mehreren Kontrollbesuchen beim BAMF ein erstes Bild machen (vgl. u. Nr. 9.3.1). Wegen der unterschiedlichen Auslegung der gesetzlichen Grundlagen zu den Voraussetzungen für die Nutzung der ausgelesenen Daten stehe ich derzeit mit dem BAMF in Kontakt.

9.1.3 Neue Polizeigesetze braucht das Land – aber welche?

Nachdem die Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) im Jahr 2016 in Kraft getreten ist, sind die Gesetzgeber in Bund und Ländern aktiv geworden. Bereits im letzten Tätigkeitsbericht habe ich über das neue Bundeskriminalamtgesetz (BKAG) berichtet, das inzwischen in Kraft getreten ist. Es darf aber nicht in Vergessenheit geraten, dass die Innere Sicherheit eigentlich in der Kompetenz der Bundesländer liegt. Der Bund hat nur eine ergänzende und das Bundeskriminalamt (BKA) nur eine koordinierende Funktion. Das Bundespolizeigesetz (BPolG) wurde geändert, ohne aber die Richtlinie umzusetzen. Ein entsprechender Entwurf dafür wurde für Anfang 2019 angekündigt.

Bundeskriminalamtgesetz – kleine Nachlese

Das neue BKAG ist im Mai 2016 in Kraft getreten (vgl. 26. TB Nr. 10.2.9.1). Es war unter hohem Zeitdruck durchgesetzt worden, weshalb für ausführliche inhaltliche Diskussionen im parlamentarischen Raum wenig Zeit blieb. Gerade das gegen mein Votum geregelte neue Informationssystem – ein zentrales Informationssystem war auch schon nach altem Recht erlaubt – wurde während der Verhandlungen als höchst dringlich dargestellt. Umso mehr verwundert es, wenn es jetzt in der Praxis plötzlich nicht mehr so eilig ist (vgl. dazu Nr. 9.2.4). Aufgenommen wurde immerhin meine Forderung, auf die sog. Mitziehautomatik bei Aussonderungsprüffristen zu verzichten (vgl. auch 26. TB Nr. 10.2.9.1).

Die Polizeibehörden der Länder benötigen das BKA als eine gut funktionierende Zentralstelle. Dazu muss dieses koordinieren und gegebenenfalls auf einen zielgerichteten, effektiven Informationsaustausch zwischen den zuständigen Polizeibehörden hinwirken. Daran ist auch aus Sicht des Datenschutzes nichts zu kritisieren. Es darf aber dabei nicht aus dem Blickfeld geraten: Die Zentralstellenaufgabe ist begrenzt (vgl. dazu auch Nr. 9.3.6 f.). Gefahrenabwehr bleibt Aufgabe der Länder. Deshalb ist es auch aus Datenschutzsicht kritisch zu hinterfragen, wenn immer mehr Aufgaben und Befugnisse Bundesbehörden zugewiesen werden sollen. Dies führt zu mehr Datenverarbeitung an zentraler Stelle. Sicherheit wird aber nicht hauptsächlich im Bund und vor allem nicht durch umfangreiche zentrale Datenbestände produziert. Generell stellt sich die Frage: Führen neue und umfassendere Befugnisse zu mehr Sicherheit? Viel zu wenig wird die Frage gestellt, ob die Polizeibehörden in der Praxis gut aufgestellt sind oder ob Vollzugsdefizite bestehen. Hier hilft gesetzgeberischer Aktionismus nicht.

Bundespolizeigesetz

Für den Bereich der Bundespolizei wurde die JI-Richtlinie noch nicht umgesetzt, so dass die Umsetzungsfrist versäumt wurde. Ein entsprechender Entwurf wurde zwar angekündigt, lag aber zum Redaktionsschluss noch nicht vor.

Geändert wurde das BPolG aber durch das „Gesetz zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Beamtinnen und Beamten der Bundespolizei". Eingeführt wurde damit die sog. Bodycam für die Bundespolizei. Hier wurden einige meiner Anmerkungen in der Ressortberatung berücksichtigt. Mir war zum Beispiel folgender Punkt wichtig: Wenn die Kameras schon eingesetzt werden, dann nicht nur zu Lasten, sondern auch zum Nutzen der Betroffenen. Die erhobenen Daten können nicht nur zur Strafverfolgung eingesetzt werden. Die von Maßnahmen betroffenen Bürger können ebenfalls verlangen, dass die Aufnahmen zur Prüfung der Rechtmäßigkeit von Polizeieinsätzen genutzt werden. Kritisch habe ich auch den von der Bundespolizei genutzten Speicher- und Verarbeitungsort für die Bodycamdaten hinterfragt. Zur Speicherung und Verarbeitung der Daten werden die Cloud-Server

eines US-amerikanischen Konzerns genutzt. In diesem Fall hat die Bundespolizei wegen des amerikanischen Cloud-Acts keine ausschließliche Weisungshoheit an den Auftragnehmer. Es besteht die Möglichkeit des Herausgabeverlangens von amerikanischen Behörden. Diesem kann nur der Cloud-Anbieter widersprechen, nicht die verantwortliche Bundespolizei. Über den Widerspruch entscheiden dann amerikanische Gerichte. Das entspricht nicht den klaren Vorgaben für eine Auftragsverarbeitung nach § 62 BDSG und ist deshalb rechtswidrig. Die Bundespolizei habe ich mehrfach darauf hingewiesen (vgl. auch Nr. 9.3.3).

Ebenfalls neu ist die Kfz-Kennzeichenerfassung. Diese kann unter anderem eingerichtet werden, wenn Straftaten von erheblicher Bedeutung im Bereich der Grenzen zu befürchten sind. Gerade in diesem Bereich habe ich Zweifel angemeldet, ob die Maßnahmen zeitlich hinreichend begrenzt sind. Es besteht insofern die Gefahr, eine dauerhafte Maßnahme zu etablieren. Nicht geklärt ist zudem, mit welchem Fahndungsbestand die Daten abgeglichen werden können. Gerade an dieser Stelle hatte das Bundesverfassungsgericht gesetzliche Klarstellungen eingefordert.

9.1.4 Neues Zollfahndungsdienstgesetz

Für den Zollfahndungsdienst hätten die Vorgaben der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) eigentlich bereits bis zum 6. Mai 2018 umgesetzt sein müssen (vgl. o. Nr. 1.2). Dies betrifft auch die Maßgaben des Bundesverfassungsgerichts zum Umgang von Ermittlungsbehörden mit Daten aus heimlichen Ermittlungsmaßnahmen (dazu 26. TB Nr. 1.3). Der bislang vorliegende Gesetzentwurf entspricht dem nur zum Teil.

Zunächst hält der Entwurf an der bisher wenig differenzierten Aufgabenverteilung zwischen allgemeiner Zollverwaltung und Zollfahndungsdienst fest. Die Aufgabenzuweisung an den Zollfahndungsdienst beschränkt sich nicht auf die Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten sowie die Aufdeckung unbekannter Straftaten und die Vorsorge für künftige Strafverfahren im Zuständigkeitsbereich der Zollverwaltung. Sie umfasst zusätzlich diverse Unterstützungs- und Mitwirkungsaufgaben zugunsten der Behörden der allgemeinen Zollverwaltung. Die Befugnisse sind nicht ausreichend klar voneinander abgegrenzt.

Das Zollkriminalamt (ZKA) als Zentralstelle erhält zudem den Auftrag eines umfassenden Risikomanagements für sämtliche Aufgaben der Zollverwaltung einschließlich der Zollfahndung. Diese Aufgabe ist weit im Vorfeld angesiedelt und mit ihr korrespondieren niedrigschwellige Datenverarbeitungsbefugnisse, so etwa schon bei einer Teilnahme am grenzüberschreitenden Warenverkehr. Es fehlt eine differenzierte Regelung, die zwischen Erhebung und weiterer Verwendung für die diversen Aufgabenfelder der Zollfahndung unterscheidet und hierfür gegebenenfalls eigene Schwellen setzt. Im Rahmen des Risikomanagements verarbeitete Daten dürfen nicht automatisch und ohne zusätzliche Anforderungen auch für Zwecke der Gefahren- und Strafverfolgungsvorsorge weiter verwendet werden.

Die fehlende Differenzierung zwischen der Erhebung und der weiteren Verwendung von Daten zieht sich durch den gesamten Gesetzentwurf. Die vom Bundesverfassungsgericht aufgestellten Grundsätze zur Zweckbindung bei der weiteren Verwendung von Daten können so nicht ausreichend abgebildet werden. Die JI-Richtlinie steht einer weiteren Ausdifferenzierung nicht im Wege, denn sie setzt nur einen Mindeststandard und lässt höhere nationale Schutzstandards ohne weiteres zu.

Für unverhältnismäßig halte ich die Regelung zur Bestandsdatenauskunft und Zuordnung von IP-Adressen. Diese wird ermöglicht, wann immer dies für die Aufgaben des Zollfahndungsdienstes erforderlich ist. Im Ergebnis können diese Informationen permanent abgerufen und fortlaufend für die gesamte Speicherdauer hinzugespeichert werden.

Auch die sogenannten Prüffalldateien halte ich für unzulässig. Hier werden Daten zu Personen in Vorsorgedateien gespeichert und weiter verarbeitet, gegen die rechtlich im Zeitpunkt der Speicherung keine Negativprognose festgestellt werden kann. Die Speicherung ermöglicht eine anschließende „Anreicherung“ der Daten mit dem Ziel, im weiteren Verlauf eine Negativprognose begründen zu können. Die Daten werden hier zur Verdachtsgenerierung auf Vorrat gespeichert. Eine bloße Befristung der Speicherung löst das Problem nicht.

Nicht hinreichend begründet ist die Erforderlichkeit der neuen Befugnis zum Einsatz verdeckter Ermittler.

Immerhin konnten im Laufe der Abstimmungen zum Gesetzentwurf schon einige Verbesserungen erreicht werden, die ich ausdrücklich begrüße. So wurde eine Regelung über Errichtungsanordnungen in den Entwurf aufgenommen, die Prognoseanforderungen in den Vorschriften zur Telekommunikationsüberwachung, zur Erhebung von Verkehrs- und Nutzerdaten sowie zur Identifizierung und Lokalisierung von Mobilfunkkarten und Telekommunikationsendgeräten wurden konkretisiert und die bei den Aussonderungsprüffristen zunächst vorgesehene Mitziehautomatik wurde wieder gestrichen.

9.1.5 Kontrollfreie Räume im Bereich der Nachrichtendienste und Kooperation mit anderen Aufsichtsbehörden

Leider gibt es immer noch Bereiche, in denen ich die Verarbeitung personenbezogener Daten nicht vollumfänglich prüfen kann. Ich versuche, dies durch eine enge Zusammenarbeit mit anderen Kontrollorganen zu kompensieren, wie es das Bundesverfassungsgericht auch vorgibt.

Das Bundesverfassungsgericht verpflichtet die Aufsichtsbehörden über die Nachrichtendienste zur Zusammenarbeit – ein Aspekt zum Ausgleich des schwachen Individualrechtsschutzes gegen entsprechende heimliche Maßnahmen. Die Verwirklichung dieser Pflicht wird aber immer wieder vor neue Herausforderungen gestellt.

Die Zusammenarbeit mit den Gremien des Deutschen Bundestages und die Vorgaben des Bundesverfassungsgerichts zur Zusammenarbeit der Kontrollorgane habe ich bereits in meinem letzten Tätigkeitsbericht dargestellt (vgl. 26. TB Nr. 10.2.10.2 und 10.3.5). Auch im aktuellen Berichtszeitraum habe ich umfänglich mit der G-10-Kommission zusammen gearbeitet. So wurden mehrere Kontrollen sowie Informationsbesuche gemeinsam und erfolgreich durchgeführt, auf deren Inhalt ich aus Gründen des Geheimschutzes hier nicht weiter eingehen kann.

Darüber hinaus bestehen Kontakte zum neu ernannten Bevollmächtigten des Parlamentarischen Kontrollgremiums. Ich möchte die Zusammenarbeit mit dem Parlamentarischen Kontrollgremium selbst weiterentwickeln sowie künftig auch den Kontakt zu dem beim Bundesgerichtshof zur Kontrolle der Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes eingerichteten Unabhängigen Gremium aufnehmen.

Kontrollfreie Räume können auf unterschiedlichen Ursachen beruhen. Entweder gibt es mehrere Kontrollorgane, deren Zuständigkeit nicht eindeutig geklärt ist bzw. die zumindest in der Praxis nicht so zusammen arbeiten (können), dass Datenverarbeitungen lückenlos geprüft werden können. Oder der Gesetzgeber sieht von vorneherein für bestimmte Bereiche keine umfängliche Datenschutzkontrolle vor.

Die Verarbeitung personenbezogener Daten durch die Nachrichtendienste des Bundes wird sowohl von mir als auch von der G-10-Kommission kontrolliert. Letztere kontrolliert die Datenverarbeitung jedoch ausschließlich im Rahmen von Beschränkungen gegen das Brief-, Post- oder Fernmeldegeheimnis nach dem G-10-Gesetz, so dass deren Kontrollkompetenz inhaltlich beschränkt ist. Betroffen sind Anträge der Nachrichtendienste, die Telekommunikation von Personen zu überwachen, bei denen die gesetzlichen Voraussetzungen nach § 3 G-10-Gesetz vorliegen. Zur Abgrenzung meiner Zuständigkeit von der der G-10-Kommission habe ich schon ausführlich im 24. Tätigkeitsbericht (Nr. 7.7.2) Stellung genommen und seitdem den Gesetzgeber aufgefordert, eine Klarstellung vorzunehmen (24. TB Nr. 7.7.2 sowie 26. TB Nr. 10.2.10.3). Eine solche Klarstellung auf gesetzlicher Ebene fehlt bislang. Allerdings hat der Gesetzgeber eine solche zumindest in der Begründung zu § 26a Bundesverfassungsschutzgesetz (BVerfSchG) (eingefügt durch Art. 2 des Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) vom 30. Juni 2017 – vgl. hierzu unter Nr. 1.1) ansatzweise vorgenommen. Seit Inkrafttreten dieser Norm habe ich zwei gemeinsame Kontrollen mit der G-10-Kommission durchgeführt (vgl. auch Nr. 9.3.5). Bei der Kontrolle beim Bundesamt für Verfassungsschutz (BfV) gab es in dieser Hinsicht keinerlei Probleme. Bei der Kontrolle beim Bundesnachrichtendienst (BND) wurde der G-10-Kommission kein umfassender Einblick in alle Daten gewährt mit der Begründung, dass es sich bei den fraglichen Daten nicht um „G-10-Daten“ handele. Ich bin mit BND, Bundeskanzleramt und G-10-Kommission im Gespräch, wie eine verfassungskonforme gemeinsame Kontrolle in diesen Fällen sichergestellt werden kann. Diese Problematik ist im Übrigen auch Gegenstand einer Verfassungsbeschwerde (vgl. auch Nr. 9.1.6).

Das Phänomen kontrollfreier Räume durch fehlende Vorgaben des Gesetzgebers begegnet mir im Bereich der internationalen Kooperation der Nachrichtendienste. Der BND und das BfV haben 2016 gesetzliche Befugnisse erhalten, sich an gemeinsamen Dateien mit ausländischen Nachrichtendiensten (AND) zu beteiligen sowie selbst in eigener Verantwortung solche Dateien zu führen. Wie schon im 26. Tätigkeitsbericht ausgeführt, sprechen mir das Bundesministerium des Innern, für Bau und Heimat sowie das Bundeskanzleramt die Befugnis ab, die Daten deutscher Dienste in einer von einem AND geführten Datei durch Einsichtnahme vor Ort zu kontrollieren (vgl. 26. TB Nr. 10.2.10.1). Sie begründen dies mit der Formulierung der entsprechenden Vorschriften im BVerfSchG sowie im Gesetz über den Bundesnachrichtendienst, wonach die Vorschriften über die unabhängige Datenschutzkontrolle durch die BfDI bei Fällen der Errichtung gemeinsamer Dateien mit AND nur für die vom jeweiligen Nachrichtendienst eingegebenen Daten und dessen Abrufe gilt. Bei der Teilnahme an gemeinsamen Dateien mit AND fehlt ein Verweis auf die Vorschriften über die unabhängige Datenschutzkontrolle. Seit meinem letzten Tätigkeitsbericht hat sich hier leider nichts getan.

Ich empfehle daher dem Gesetzgeber, eine klare Zuständigkeitsregelung für BfDI und G-10-Kommission zu

schaffen und dort auch die Kooperation zwischen diesen Aufsichtsbehörden zu regeln. Außerdem sollte die Kontrollbefugnis der BfDI umfassend auch beim Führen gemeinsamer Dateien des BfV mit AND anerkannt und ggf. klarstellend geregelt werden.

Ich empfehle dem Gesetzgeber, eine klare Zuständigkeitsregelung für die Kontrolltätigkeit von BfDI und G-10-Kommission zu schaffen, die auch die Kooperation zwischen diesen beiden Aufsichtsbehörden umfasst. Ich empfehle außerdem, die Kontrollbefugnis der BfDI umfassend auch beim Führen gemeinsamer Dateien des BfV mit ausländischen Nachrichtendiensten anzuerkennen und diese ggf. gesetzlich klarstellend zu regeln.

9.1.6 Aktuelle Verfassungsbeschwerden im Bereich der Nachrichtendienste

Im Berichtszeitraum habe ich zu zwei Verfassungsbeschwerden Stellung genommen, die den Bereich des BND betreffen. Die Entscheidungen werden mit Spannung erwartet. In einem weiteren Fall habe ich mich durch Beantwortung eines Fragenkatalogs am laufenden Verfahren beteiligt.

Stellungnahme zur Verfassungsbeschwerde gegen das G-10-Gesetz und das BDSG

Aktuell ist eine Verfassungsbeschwerde beim Bundesverfassungsgericht anhängig, die u. a. auch das Verhältnis zwischen G-10-Kommission und BfDI im Hinblick auf deren Kontrolltätigkeit thematisiert. § 26a Bundesverfassungsschutzgesetz (BVerfSchG) – der über Verweisungen sowohl für das Bundesamt für Verfassungsschutz (BfV), den Militärischen Abschirmdienst (MAD) als auch für den Bundesnachrichtendienst (BND) gilt – und § 15 Absatz 5 Satz 2 G-10-Gesetz sollen verfassungswidrig sein, da die Aufspaltung der Kontrollaufgabe keine ordnungsgemäße aufsichtliche Kontrolle strategischer Fernmeldeüberwachungen gewährleiste. Die G-10-Kommission entscheidet über die Zulässigkeit und Notwendigkeit von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses. Ihre Kontrollbefugnis erstreckt sich auf die gesamte Verarbeitung der nach diesem Gesetz erlangten personenbezogenen Daten durch die Nachrichtendienste des Bundes einschließlich der Entscheidung über die Mitteilung an Betroffene. Nach § 26a BVerfSchG i. V. m. § 32 Bundesnachrichtendienstgesetz (BNDG) kontrolliere ich die Einhaltung der Vorschriften über den Datenschutz beim BND. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G-10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch mich, es sei denn, die G-10-Kommission ersucht mich, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

Ich habe zu dieser Verfassungsbeschwerde Stellung genommen und dargelegt, dass ich mir seit langem eine klarere gesetzliche Regelung wünsche. Dies betrifft insbesondere die Ausgestaltung der Kooperationspflicht sowie die Abgrenzung der Zuständigkeiten. Wenn die Kooperationspflicht von Kontrollorganen wie von kontrollierten Behörden und deren Fachaufsichten ernst genommen wird, könnte man die Regelungen möglicherweise verfassungskonform auslegen. Welcher Auffassung das Gericht folgen wird, bleibt abzuwarten.

Stellungnahme zur Verfassungsbeschwerde gegen das Bundesnachrichtendienstgesetz (BNDG) in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung vom 23. Dezember 2016

Die Klage gegen das im Januar 2017 in Kraft getretene Gesetz wurde von Reporters sans frontières sowie einer Anzahl in Deutschland sowie im europäischen und außereuropäischen Ausland ansässigen Journalisten erhoben. Gegenstand der Verfassungsbeschwerde ist die Frage der Verfassungskonformität der getroffenen Regelungen zur strategischen Ausland-Ausland-Fernmeldeaufklärung hinsichtlich der territorialen und persönlichen Geltung des Grundrechtsschutzes sowie zur Kooperation des BND mit ausländischen Stellen.

Kennzeichen der strategischen Ausland-Ausland-Fernmeldeaufklärung ist ein breit angelegtes, auf die Erlangung von Daten aus Kommunikationsnetzen für die Erfüllung des gesetzlichen Auftrags des BND gerichtetes Vorgehen. Dabei dürfen zum Zweck der Auftragserfüllung personenbezogene Daten aus den aufzuklärenden Netzen erfasst und einer Analyse anhand von sog. Selektoren zugeführt werden. Selektoren können vereinfacht gesagt als Suchbegriffe bezeichnet werden. Diese können z. B. Rufnummernbereiche oder Domain-Namen sein.

Im Fall der Ausland-Ausland-Fernmeldeaufklärung handelt es sich, je nach Konstellation, um vom Inland oder vom Ausland aus erfasste Kommunikationsdaten von Ausländern. Einen konkreten Anlass für die Erfassung der personenbezogenen Daten von Ausländern aus dem Ausland heraus setzt das Gesetz nicht voraus. Damit steht das Prinzip der strategischen Fernmeldeaufklärung im Gegensatz zu dem Prinzip der Einzelaufklärung, das stets einen konkreten Verdacht sowie eine richterliche Genehmigung hinsichtlich der betroffenen Einzelperson fordert und auf diese Weise eine anlasslose und pauschale Erfassung von persönlichen Daten durch den Staat unterbindet. Das Prinzip der Einzelaufklärung gilt uneingeschränkt im Inland.

Der Umstand, dass ein konkreter Anlass bei der strategischen Ausland-Ausland-Fernmeldeaufklärung nicht vorliegen muss, bedeutet, dass der besondere Schutz, den ein Kommunikationsteilnehmer im Inland im Verhältnis zum deutschen Staat genießt, insbesondere auch als Mitglied einer Gruppe von Personen, die aus beruflichen Gründen Geheimnisträger sind (Anwälte, Ärzte, Journalisten) und deren Kommunikation mit Mandanten, Patienten, Augenzeugen besonders schutzbedürftig ist, nicht gewährt wird. Dieser im Verhältnis zur Gesetzlage im Inland verkürzte Schutz setzt sich bei der Weitergabe von Daten an beispielsweise ausländische Nachrichtendienste fort. Innerhalb solcher Kooperationen erfolgt die Weitergabe personenbezogener Daten teilweise automatisiert.

Die klagenden Journalisten vertreten die Auffassung, die Vorgaben zur Kooperation mit ausländischen Nachrichtendiensten hätten zur Konsequenz, dass sensible Informationen über die Kommunikation mit journalistischen Quellen undifferenziert weitergegeben würden. In Abhängigkeit davon, welche Daten in welchem Kooperationsverhältnis weitergegeben werden, führe dies zu gravierenden Gefährdungen für die Journalisten und ihre Quellen. In Folge dessen sei zudem eine freie journalistische Tätigkeit signifikant eingeschränkt.

Ich habe zu diesem Sachverhalt unter datenschutzrechtlichen Gesichtspunkten vor dem Hintergrund der verfassungsgerichtlichen Rechtsprechung und der gegenwärtigen Diskussion über die tatsächlichen Möglichkeiten differenzierender Erfassung von Telekommunikationsdaten Stellung genommen. Ein Schwerpunkt der Stellungnahme befasst sich damit, dass angesichts der notwendig heimlichen Grundrechtseingriffe durch den BND den Kontrollorganen vom Bundesverfassungsgericht eine Kompensationsfunktion (BVerfG 1 BvR 1215/07, Rn. 207, 1 BvR 966/09, Rn. 14) zum Schutz der Grundrechte der Betroffenen zugewiesen wurde. Deren Umsetzung obliegt Behörden und Gesetzgeber gemeinsam. Diese Anforderung ist aber für den Bereich der Nachrichtendienste noch nicht umfassend realisiert. Ein weiterer Schwerpunkt betrifft die Darlegung der wachsenden Bedeutung des Rechts auf informationelle Selbstbestimmung auf dem Gebiet der nachrichtendienstlichen Tätigkeit im Verhältnis zu den weiteren einschlägigen Freiheitsrechten im Lichte der Verschiedenartigkeit der von der Ausland-Ausland-Fernmeldeaufklärung erfassten Daten. Abschließend habe ich meine in der Praxis gewonnene Einschätzung zu den Kooperationsanforderungen an die Kontrollorgane dargestellt, auf die die Aufsicht über den BND aufgeteilt ist. Hier erscheint es erforderlich, eine schon bestehende Zusammenarbeit auf einer stetigen Basis zu etablieren, um auf diese Weise die verfassungsgerichtlich geforderte umfassende und wirksame Kontrolle der Nachrichtendienste durch die Kontrollorgane gewährleisten zu können.

Stellungnahme zur Verfassungsbeschwerde gegen § 6a Antiterrordateigesetz (ATDG)

Im Rahmen einer Verfassungsbeschwerde gegen § 6a ATDG hat mir das Bundesverfassungsgericht die Gelegenheit zur Stellungnahme gegeben und einen Fragenkatalog zu für das Verfahren relevanten Sachverhalten übersandt. § 6a ATDG regelt die erweiterte projektbezogene Datennutzung der in der Antiterrordatei (ATD) gespeicherten Daten. Voraussetzung dafür ist, dass dies im Rahmen eines bestimmten einzelfallbezogenen Projekts zur Sammlung und Auswertung von Informationen über eine internationale terroristische Bestrebung, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass Straftaten des internationalen Terrorismus nach den §§ 129a, 129b und 211 des Strafgesetzbuchs begangen werden sollen und dadurch Gefahren für Leib, Leben oder Freiheit von Personen drohen, im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären.

Die Vorschrift wurde bei der Novellierung des ATDG im Jahr 2014 mit der Begründung in das Gesetz eingefügt, dass die Notwendigkeit bestehe, auch komplexe Abfragen über den Datenbestand der ATD durchzuführen. Nach meiner Kenntnis ist die Regelung in der Praxis bis heute aufgrund fehlender technischer Parameter nicht umgesetzt worden, d. h. eine solche Nutzung hat noch nicht stattgefunden. Unabhängig von verfassungsrechtlichen Bedenken sollte diese Tatsache allein Grund genug dafür sein, die Vorschrift wieder abzuschaffen, da sie sich als überflüssig erwiesen hat.

9.1.7 Änderung des BDBOS-Gesetzes

Nicht in allen Fällen dient das 2. DSAnpUG-EU ausschließlich der Anpassung an die DSGVO, sondern kann – wie im Fall des BDBOS-Gesetzes – ganz nebenbei sogar zur Ausweitung von Datenverarbeitungen führen.

Der Entwurf des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU) sieht in Artikel 8 auch eine Änderung des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS-Gesetz) vor. Anders als es der Gesetzestitel zunächst nahelegt, geht es hierbei nicht um eine Anpassung des deutschen Datenschutzrechts an das europäische Datenschutzrecht. Vielmehr wird für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), der bisher dem Datenschutzrecht des Telekommunikationsgesetzes (TKG) unterlag, ein eigenes Datenschutzregime geschaffen. Danach sind Datenverarbeitungen in weiterem Umfang und unter er-

leichterten Voraussetzungen zugelassen, als dies bislang nach dem TKG der Fall war.

In dem Gesetzgebungsverfahren habe ich mich wiederholt dafür ausgesprochen, für den BOS-Funk das Datenschutzrecht des TKG beizubehalten. Dieses hat sich bewährt und bietet einen ausgewogeneren Kompromiss zwischen dem Fernmeldegeheimnis einerseits und berechtigten Datenverarbeitungszwecken andererseits. Aus meiner Sicht ist es nicht sachgerecht, Verkehrsdaten beim BOS-Funk weniger zu schützen als beim gewöhnlichen Mobilfunk. Für besonders bedenklich halte ich es, wenn nun für den BOS-Funk eine anlasslose Speicherung von Verkehrsdaten für 75 Tage eingeführt werden soll, wohlwissend, dass eine vergleichbare Regelung im TKG für europarechtswidrig befunden wurde (vgl. o. Nr. 9.2.7)

9.2 Einzelthemen

9.2.1 Zensus 2021 in Sichtweite

Seit Inkrafttreten des Zensusvorbereitungsgesetzes 2021 (ZensVorbG 2021) im März 2017 laufen die Vorbereitungen für die nächste Volkszählung im Jahr 2021. Eine Ergänzung dieses Gesetzes um eine Regelung zur Durchführung eines Testlaufs zum Zensus sowie die Arbeiten am Zensusgesetz 2021 haben mich im laufenden Jahr intensiv beschäftigt.

Der neu in das ZensVorbG 2021 aufgenommene § 9a regelt die Übermittlung bestimmter Daten sämtlicher in den Meldebehörden Deutschlands zum angegebenen Stichtag registrierter Personen über die jeweiligen Statistischen Ämter der Länder an das Statistische Bundesamt. Hiermit sollen die Übermittlungswege und die Qualität der übermittelten Datensätze sowie die Programme zur Durchführung des Zensus 2021 überprüft und weiter entwickelt werden. § 9a Absatz 6 ZensVorbG 2021 sieht vor, spätestens nach Abschluss der auf längstens zwei Jahre angesetzten Testphase alle zu diesem Zweck verarbeiteten Datensätze wieder zu löschen.

Ich habe kritisiert, dass der Testlauf anhand von Klardaten der Meldebehörden erfolgt und diese für den gesamten Zeitraum der Überprüfungen vorgehalten werden sollen. Meine Bitte, den Testlauf – zumindest zeitweise – auf der Basis pseudonymisierter Datensätze durchzuführen und ihre Löschung sukzessive zum Abschluss der jeweiligen Elemente der Überprüfungen vorzusehen, wurde vom Gesetzgeber nicht aufgegriffen. Auf mein Betreiben enthält die Gesetzesbegründung immerhin die Klarstellung, dass die Vorbereitungen zum Zensus 2021 nach dem ZensVorbG 2021 und damit ausdrücklich auch der Testlauf nach § 9a ZensVorbG 2021 bereits Teil der Bundesstatistik Zensus 2021 sind und insoweit die Vorgaben des Bundesstatistikgesetzes (BStG), etwa zur Geheimhaltung nach § 16 BStG und zur elektronischen Datenübermittlung nach § 11a BStG, zur Anwendung kommen. Da meine Bedenken im Gesetzgebungsverfahren nicht vollständig ausgeräumt werden konnten, werde ich den Testlauf für den Zensus 2021 als die für das Statistische Bundesamt zuständige Datenschutzaufsichtsbehörde eng begleiten.

Kurz vor Ende des Berichtszeitraums ist mir im Rahmen der Ressortabstimmung der Entwurf eines Gesetzes zur Durchführung des Zensus im Jahr 2021 (ZensG 2021) vorgelegt worden. Auch diese Zählung wird wie der letzte Zensus 2011 registergestützt durchgeführt und eine Bevölkerungszählung, eine Gebäude- und Wohnungszählung, eine Haushaltebefragung auf Stichprobenbasis sowie Erhebungen an Anschriften mit Sonderbereichen umfassen.

9.2.2 Bürgerportale und digitale Verwaltung

Die Bundesregierung hat mit dem Gesetz zur Verbesserung des Online-Zugangs zu Verwaltungsleistungen (Online-Zugangsgesetz) die Voraussetzungen für eine Vernetzung der Verwaltungsportale des Bundes, der Länder und Kommunen geschaffen. Bürgerinnen und Bürger sollen bei einem Verwaltungsportal ihrer Wahl Zugang zu allen online angebotenen Verwaltungsleistungen erhalten, ohne sich dazu mehr als einmal identifizieren zu müssen. Das damit einhergehende Versprechen, auch weitere Angaben immer nur einmal machen zu müssen, ist so umzusetzen, dass dadurch keine Risiken für die Privatsphäre der Betroffenen entstehen.

Wenn der Zugang zu allen elektronisch angebotenen Verwaltungsleistungen von nur einem Zugangspunkt aus erfolgen soll (Single Point of Contact), setzt dies voraus, dass sich Nutzerinnen und Nutzer für den elektronischen Zugang zu Verwaltungsleistungen in nur einem Portal anmelden müssen, um dann bundesweit Verwaltungsleistungen in Anspruch nehmen zu können. Die einzelnen Verwaltungsleistungen werden weiterhin von den jeweils zuständigen Behörden in deren eigener datenschutzrechtlicher Verantwortung angeboten. Portalbetreiber erhalten lediglich das Recht, die zur Identifizierung erforderlichen Daten an die für eine bestimmte Verwaltungsleistung zuständige Behörde zu übermitteln. Bei dieser Regelung begrüße ich, dass der Aufbau eines zentralen Datenbestandes zur Bedienung aller Verwaltungsleistungen nicht vorgesehen ist, zur Identifizierung an einem Portal nicht notwendig der Personalausweis genutzt werden muss und Verwaltungsleistungen auch ohne Einrichtung eines dauerhaften Servicekontos online genutzt werden können. Der im Zusammenhang mit Bürgerportalen gelegentlich diskutierte „Kerndatensatz“ ist durch das Online-Zugangsgesetz auf die zur Identifizierung erforderlichen Daten beschränkt.

Im Berichtszeitraum wurde auch der Ansatz eines bereichsspezifischen Personenkennzeichens verfolgt, das im Ergebnis eine abgemilderte Variante einer lebenslang gültigen bereichsübergreifenden Personenkennziffer darstellt. Die Personenkennziffer soll für eine eindeutige Zuordnung und zuverlässige Wiederauffindbarkeit sorgen. Damit wird aber auch eine Zusammenführung von Datenbeständen einzelner Behörden zu – isoliert betrachtet – nachvollziehbaren Zwecken erheblich erleichtert bzw. erst ermöglicht. Allein mit dieser realen Nutzungsmöglichkeit steigt das Risiko eines Missbrauchs. Das sich hieraus ergebende Gefahrenpotenzial für das Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht im Jahr 1983 dazu bewogen, die Schaffung eines Systems von Personenkennzeichen als verfassungswidrig einzustufen. Dieser höchstrichterlich ausgestaltete Rechtsrahmen hat bis heute Bestand und ist Maßstab für die verfassungsrechtliche Bewertung jedweder Art von Personenkennzeichen.

Dieser Gefahr für das Recht auf informationelle Selbstbestimmung durch die Möglichkeit einer Katalogisierung kann nur durch die Herstellung einer Art „Waffengleichheit“ begegnet werden. Bei der Umsetzung des Online-Zugangsgesetzes ist daher darauf zu achten, dass für die Bürgerinnen und Bürger jederzeit und vollständig transparent ist, welche Daten sie zu welchem Zweck wem überlassen. Insbesondere müssen Betroffene einwilligen, wenn im Rahmen etwa einer Antragsbearbeitung Daten von anderer Stelle automatisiert eingeholt werden, die sie sonst selbst hätten beibringen müssen. Beispielsweise dürfen die Angaben zur Wohnadresse für die Ausstellung eines Anwohnerparkausweises nur nach Einwilligung durch den Antragsteller mit einer automatisierten Abfrage beim Einwohnermelderegister überprüft werden. Bei der nun anstehenden Umsetzung des Online-Zugangsgesetzes auf Bundesebene mit der Errichtung eines Bundesportals werde ich darauf achten, dass diese Regeln eingehalten werden.

9.2.3 Eine neue Rechtsgrundlage für Europol

Europol ist auf eine neue Rechtsgrundlage gestellt worden. Diese beinhaltet auch eine neue datenschutzrechtliche Aufsicht und damit eine neue Rolle für mich.

Europol hat das Ziel, die EU-Mitgliedstaaten sowie deren Zusammenarbeit bei der Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerwiegender Kriminalität zu unterstützen, wenn mindestens zwei Mitgliedstaaten betroffen sind. Dies soll insbesondere durch die Förderung des Informationsaustauschs zwischen den EU-Mitgliedstaaten und die Analyse kriminalpolizeilicher Erkenntnisse erreicht werden.

Der rechtliche Rahmen für die Wahrnehmung dieser Aufgaben hat sich in den vergangenen knapp 20 Jahren erheblich verändert, zuletzt durch eine neue Verordnung, die am 1. Mai 2017 in Kraft getreten ist (Verordnung (EU) 2016/794 vom 11.05.2016).

Die neue Verordnung bedeutet auch eine Änderung der datenschutzrechtlichen Aufsicht von Europol. Während diese Aufgabe bislang der sog. Gemeinsamen Kontrollinstanz oblag, die mit Vertretern der Datenschutzbehörden der EU-Mitgliedstaaten besetzt war, liegt die Aufsicht nun bei dem Europäischen Datenschutzbeauftragten (EDPS), der für die Erfüllung dieser Aufgaben sowohl mit mehr Ressourcen als auch mit mehr Befugnissen ausgestattet ist.

Aufgrund der neuen Aufsichtsstruktur ergibt sich für mich auch eine neue Aufgabe. Neben der Aufsicht über die nationale Zentralstelle, die in Deutschland das Bundeskriminalamt wahrnimmt, sitze ich nunmehr gemeinsam mit den anderen nationalen Kontrollstellen und dem EDPS in dem neu gegründeten „Beirat für die Zusammenarbeit“. Dieser befasst sich sowohl mit allgemeinen Fragestellungen zur Auslegung der Europol-Verordnung als auch mit konkreten Fällen, die durch nationale Kontrollstellen oder den EDPS herangetragen wurden. Die stellvertretende Leitung des Beirats wird durch meine Behörde ausgeübt.

9.2.4 Maschinelles Lernen will gelernt sein

Auch Polizei und Nachrichtendienste wollen am Stand der Technik moderner elektronischer Datenverarbeitung teilhaben. Machine Learning hält deshalb auf vielen Wegen Einzug in deren IT-Landschaften. Dies stellt alle Beteiligten vor neue Herausforderungen.

Es muss nicht eine große Umwälzung der IT-Systeme sein, die die Analysemöglichkeiten vorhandener Daten weiter vorantreibt. Mitunter sind es auch lediglich technische Fortentwicklungen wie bei der Videoüberwachung von der konventionellen Überwachungstechnik hin zur „smarten“ Videoanalyse mittels Einsatz von Machine Learning (ML). Gemeint sind Verfahren, bei denen – im Gegensatz zu einer „festverdrahteten“ Programmierung – das innere Datenverarbeitungsmodell im Rahmen der Entwicklung durch ausgewählte und bekannte Datensätze trainiert wird.

Die sinnvolle Nutzung von ML-Techniken im Sicherheitsbereich setzt die Verfügbarkeit großer Datenmengen notwendigerweise voraus. Um hier eine effektive Datenschutzkontrolle gewährleisten zu können, ist neben der Transparenz der individuellen Verarbeitungsschritte auch die Bewertung der Wirkung und damit der Verhältnismäßigkeit von Grundrechtseingriffen im Rahmen der

Datenverarbeitung durch die dazu befugten Behörden unerlässlich. Die Wirkung von aktuellen ML-Verfahren wird definitionsgemäß wesentlich bestimmt durch Qualität und Systematik der Trainingsdaten in der Entwicklungsphase des jeweiligen Softwareprodukts.

Insbesondere die Verwendung von Trainingsdaten für die Entwicklung ist für den Datenschutz ein Problem: Das Trainieren von ML-Modellen mit Echtdaten kann je nach Inhalt schon eine Verarbeitung personenbezogener Daten sein. Gleichzeitig könnte je nach angewandter Methode auch im späteren Wirkbetrieb eine Rückschau auf die unter Umständen lange zurückliegende Trainingsphase zum Verständnis und zur Beurteilung des IT-Systems notwendig werden. Wie in einem solchen Fall die Dokumentation der Entwicklungsprozesse und der Arbeitsweise der einzelnen Systeme auszugestalten ist, um datenschutzkonform zu sein und die geforderte effektive Datenschutzkontrolle zu ermöglichen, muss in einem frühen Stadium des jeweiligen Projekts definiert werden.

Bis heute hat mich noch keine der hier tätigen Behörden über die Verarbeitung personenbezogener Daten im Rahmen der Entwicklung neuer IT-Systeme zum Zweck des Trainings von ML-Modellen informiert oder beteiligt. Zukünftig wird bei derartigen technischen Systemen aber ein Augenmerk des Datenschutzes auf der Herkunft der Trainingsdaten liegen müssen. Bei diversen Beratungs- und Informationsbesuchen im Berichtszeitraum klang dieses Thema in verschiedenen Zusammenhängen bereits an. Bei Tests im Rahmen von Entwicklungen und Produktabnahmen von IT-Systemen unterliegt die Nutzung von Echtdaten aufgrund ihrer engen Zweckbegrenzung strengen Vorgaben. Ich habe in Gesprächen wiederholt darauf hingewiesen, dass dies genauso beim Training von ML-Modellen gelten muss. Ein möglicher Weg wäre etwa die Bereitstellung synthetischer Daten, die aus vielen Gründen für die Entwicklung und den Test konventioneller und ML-basierter IT die beste Wahl sind. Diese technologisch sicherlich anspruchsvolle Aufgabe würde tatsächlich nachhaltig und von Beginn an die Probleme bei der Einführung zukünftiger auf ML basierender IT-Verfahren vermeiden helfen.

9.2.5 Effektiver Datenschutz nach dem „Stand der Technik“

Ziel der DSGVO ist es, die Rechte des Betroffenen bestmöglich zu schützen. Wichtiger Baustein hierfür ist eine datenschutz- und datensicherheitskonforme Technikgestaltung. Die DSGVO fordert hierfür – neben weiteren Vorgaben – u. a. den „Stand der Technik“ zu berücksichtigen. Wie ist dieser „Stand der Technik“ definiert?

Gleich an mehreren Stellen der DSGVO findet sich der Verweis auf den „Stand der Technik“, so etwa im Zusammenhang mit der zentralen Pflicht zur Gewährleistung von Datensicherheit in Artikel 32 DSGVO. Verantwortliche und Auftragsverarbeiter im Sinne der DSGVO müssen geeignete technische und organisatorische Maßnahmen treffen, um einen Schutz etwa vor unbefugter Kenntnisnahme, unrechtmäßiger Verarbeitung oder dem unbeabsichtigten Verlust der Daten zu gewährleisten. Der Stand der Technik ist aber auch nach Art. 25 Absatz 1 DSGVO zu berücksichtigen, der sich dem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen widmet. Auch in den Erwägungsgründen 78 und 83 wird Bezug auf den Stand der Technik genommen: Die Hersteller von Produkten, Diensten und Anwendungen sollen ermutigt werden, das Recht auf Datenschutz und den Stand der Technik gebührend zu berücksichtigen. Maßnahmen, wie etwa Verschlüsselungsverfahren, sollen unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Durch die Klausel „Stand der Technik“ soll in all diesen Fällen sichergestellt werden, dass die in der Praxis beste verfügbare Technik zum Einsatz kommt. Gemeint sind Erfolgsmodelle, die auf gesicherten Erkenntnissen beruhen und ausreichend zur Verfügung stehen, um angemessen umgesetzt zu werden. Hierbei sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch andere Vorgehensweisen, die in der Praxis bereits erprobt wurden. Die Verpflichtung schließt also die Möglichkeit eines neuen bzw. anderen Vorgehens nicht aus, wenn hierbei ein ebenso effektiver Schutz gewährleistet wird.

Die nationalen und europäischen Datenschutzaufsichtsbehörden müssen zusammenarbeiten, um zu klären, welche technisch-organisatorische Maßnahmen dem Stand der Technik entsprechen und um einheitliche Vorgaben für Wirtschaft und öffentliche Verwaltung zu gewährleisten. Nur so kann ein einheitliches europäisches Datenschutzniveau für die in der Regel weltweit verfügbaren Produkte, Dienste und Anwendungen sichergestellt werden.

9.2.6 Vorgaben für die Auftragsverarbeitung bei den IT-Dienstleistern des Bundes

Mit dem Wirksamwerden der DSGVO zum 25. Mai 2018 haben sich auch die Anforderungen an Dienstleister verändert, die personenbezogene Daten für einen Verantwortlichen im Auftrag verarbeiten. Die zentrale Vorschrift für Auftragsverarbeiter ist Artikel 28 DSGVO. Im Hinblick auf die geänderten Anforderungen hat der

Datenschutzbeauftragte des Bundesministeriums des Innern, für Bau und Heimat ein neues Vertragsmuster zur Auftragsverarbeitung entwickelt.

Die geänderte Rechtslage bei der Auftragsverarbeitung wirkt sich insbesondere auf die laufende IT-Konsolidierung der Bundesverwaltung aus. In Zukunft wird es zwei zentrale IT-Dienstleister geben. Das sind die BWI GmbH und das Informationstechnikzentrum Bund, das aus dem Zentrum für Informationsverarbeitung und Informationstechnik des BMF, der Bundesstelle für Informationstechnik des BMI und dem Dienstleistungszentrum IT des BMVI hervorgegangen ist. Sie werden den Großteil der IT-Verfahren der Bundesverwaltung betreiben und außerdem ein einheitliches Client-System für die Bundesverwaltung bereitstellen. Bei Verfahren, die bereits seit längerem von einer verantwortlichen Stelle in Zusammenarbeit mit einer der Vorgängerorganisationen der beiden IT-Dienstleister betrieben wurden, ist neben der Anpassung der Vereinbarungen an die neue organisatorische Situation auch eine Anpassung an die neue Rechtslage notwendig. Hierbei sollte die neue Mustervereinbarung zu Grunde gelegt werden, in die meine Empfehlungen aufgenommen wurden. Ich empfehle, diese Mustervereinbarung künftig in der gesamten Bundesverwaltung zu verwenden. Sie ist in meinem Internetangebot veröffentlicht.

Ich werde bei Kontrollen im Bereich der Bundesverwaltung in der nächsten Zeit verstärkt darauf achten, ob bei bestehenden Verfahren die Vereinbarungen tatsächlich angepasst wurden. Gleichzeitig werde ich die verantwortlichen Behörden als auch die IT-Dienstleister gegebenenfalls dabei unterstützen, die notwendige Zusammenarbeit im Bereich Datenschutz möglichst effizient zu gestalten.

Ich empfehle, in der gesamten Bundesverwaltung bei Verträgen zur Auftragsverarbeitung das neu entwickelte Vertragsmuster zur Auftragsverarbeitung zu verwenden. Die Mustervereinbarung ist in meinem Internetangebot veröffentlicht.

9.2.7 Aktuelles zur Vorratsdatenspeicherung

Der Einführung einer Pflicht zur Vorratsspeicherung von Verkehrsdaten sind sehr enge verfassungs- und europarechtliche Grenzen gesetzt. Darüber ist das letzte Urteil aber noch nicht gesprochen.

Die Thematik der sogenannten Vorratsdatenspeicherung habe ich von Anfang an kritisch begleitet und darüber in meinen Tätigkeitsberichten ausführlich berichtet.

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 ist der bislang letzte Vorstoß der Bundesregierung, eine Verpflichtung von Telekommunikationsunternehmen zur Speicherung und Übermittlung von Telekommunikationsverkehrsdaten auf Vorrat einzuführen. Meine verfassungs- und europarechtlichen Bedenken habe ich schon im Rahmen des Gesetzgebungsverfahrens mehrfach geäußert (vgl. 26. TB Nr. 12.2.2).

Im Berichtszeitraum wurden erneut Stimmen laut, die die Notwendigkeit der Vorratsdatenspeicherung für die Verfolgung bestimmter Straftaten beteuern. Die Argumentation gründet jedoch auf Einzelfällen. Stichhaltige empirische Belege für die Notwendigkeit der Vorratsdatenspeicherung fehlen nach wie vor.

Gerichte werden entscheiden

Die Bundesregierung ist bislang trotz mehrfacher Kritik nicht bereit, das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten zu revidieren. Nun müssen die Gerichte darüber entscheiden.

Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hat in einem Verfahren des vorläufigen Rechtsschutzes die unterschiedslose Erfassung nahezu sämtlicher Nutzer der von § 113 b Telekommunikationsgesetz (TKG) erfassten Telekommunikationsmittel am 22. Juni 2017 als mit dem Europarecht unvereinbar angesehen (Az.: 13 B 238/17). Wenige Tage später teilte die Bundesnetzagentur mit, von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der Speicherfristen gegenüber Telekommunikationsanbietern vorerst abzusehen. Vor diesem Hintergrund haben die meisten Telekommunikationsdiensteanbieter auf die Speicherung von Verkehrsdaten verzichtet. Allerdings haben zwei Unternehmen, bei denen ich im Berichtszeitraum auch Beratungs- und Kontrollbesuche durchgeführt habe (vgl. u. Nr. 15.3.4), die Vorratsdatenspeicherung umgesetzt.

Mit Urteilen vom 20. April 2018 hat sich das Verwaltungsgericht Köln der Ansicht des Oberverwaltungsgerichts Nordrhein-Westfalen hinsichtlich der Europarechtswidrigkeit der telekommunikationsgesetzlichen Speicherpflicht angeschlossen (Az.: 9 K 3859/16 und 9 K 7417/17). Das Verwaltungsgericht hat festgestellt, dass die klagenden Unternehmen nicht verpflichtet sind, die Telekommunikationsverkehrsdaten ihrer Kunden zu speichern. Gegen die Urteile des Verwaltungsgerichts Köln hat die Bundesrepublik Deutschland, vertreten durch die Bundesnetzagentur, Revision eingelegt und ein Vorabentscheidungsersuchen zum Europäischen Gerichtshof angeregt.

Die maßgeblichen Gesetzesvorschriften sind außerdem Gegenstand von Verfassungsbeschwerden, die derzeit

dem Bundesverfassungsgericht vorliegen. Im März 2017 hat das Bundesverfassungsgericht den Erlass einstweiliger Anordnungen abgelehnt und die Entscheidung dem Hauptsacheverfahren vorbehalten. Im Oktober 2017 habe ich gegenüber dem Bundesverfassungsgericht eine Stellungnahme abgegeben und auf die aus meiner Sicht bestehenden verfassungs- und europarechtlichen Probleme hingewiesen. Die Entscheidung des Bundesverfassungsgerichts in der Hauptsache steht noch aus.

9.3 Aus Kontrolle und Beratung

9.3.1 Beratungs- und Kontrollbesuche beim Bundesamt für Migration und Flüchtlinge (BAMF) sowie seinen Außenstellen

Defizite bei den datenschutzrechtlichen Anforderungen im Bereich der Asylverfahren erkannt und gebannt, Blockchain-Technologie in der Bundesverwaltung umstritten.

Im März 2017 habe ich einen umfangreichen Beratungs- und Kontrollbesuch in der Zentrale des BAMF in Nürnberg durchgeführt.

Hierbei ergab eine stichprobenhafte Überprüfung der Archivierung und Löschung von Asylverfahrensakten teils deutliche Überschreitungen der Löschfristen. Dies war u. a. auf die angespannte personelle Situation im Bereich der Bearbeitung der Asylverfahren und die Priorisierung dieser Aufgabe zurückzuführen. Die Priorisierung der Sachbearbeitung darf jedoch nicht zu einer Aushebelung der datenschutzrechtlichen Grundsätze führen. Daher habe ich das BAMF aufgefordert, ein Konzept zur zeitnahen Bereinigung der Rückstände und künftigen Gewährleistung der Löschfristen zu erarbeiten.

Meine Empfehlungen hat das BAMF aufgegriffen und inzwischen eine automatische Löschung von Asylverfahrensakten umgesetzt, so dass eine Überschreitung der gesetzlich vorgeschriebenen Löschfristen im § 7 Absatz 3 Asylgesetz (AsylG) nicht mehr erfolgen kann. Der festgestellte Rückstand konnte bereits ein halbes Jahr nach dem Kontrollbesuch signifikant gesenkt werden.

Die Überprüfung des Datenbanksystems MARiS, in dem die Daten von Asylbewerbern erfasst sind, brachte Defizite insbesondere bei den Zugriffsrechten, der Protokollierung von lesenden Zugriffen sowie der Sperrung besonders sensibler, beispielsweise medizinischer Daten zu Tage. Meine Empfehlungen hat das BAMF umgehend aufgegriffen und die Zugriffsmöglichkeiten auf MARiS-Akten grundlegend überarbeitet, differenzierte Zugriffsbeschränkungen festgelegt und elektronisch gestützte Freigabeverfahren eingerichtet, bei denen besonders schützenswerte Daten zusätzlichen Einschränkungen unterliegen. Darüber hinaus ist eine Beschränkung der elektronischen Freigabe auf bestimmte Personengruppen im Gespräch. Ende 2018 befindet sich dieser MARiS-„Umbau“ in der Endphase.

Überprüft habe ich auch die Zusammenarbeit des BAMF mit den Nachrichtendiensten des Bundes. Dabei habe ich festgestellt, dass die Übermittlung einer bestimmten Datenart an das Bundesamt für Verfassungsschutz ohne Rechtsgrundlage erfolgte. Meine Forderung, diese Übermittlungen unmittelbar einzustellen, hat das BAMF sofort umgesetzt, sodass ich von einer Beanstandung absehen konnte.

Im Juli 2017 habe ich einen Beratungs- und Kontrollbesuch bei der Außenstelle sowie dem Ankunftszentrums des BAMF in Berlin durchgeführt, im August 2018 folgte die Außenstelle des BAMF in Chemnitz. Bei beiden Kontrollbesuchen konnte ich mich davon überzeugen, dass die Abläufe im Aufgabenbereich Asylverfahren datenschutzkonform umgesetzt wurden.

Aufgrund der Errichtung der AnkER-Zentren beim BAMF als gemeinsame Einrichtungen von Bund und Land, die als konzeptionelles Herzstück eine Bündelung von Funktionen und Zuständigkeiten vorsah, habe ich im November 2018 einen Beratungs- und Kontrollbesuch im AnkER-Zentrum Dresden durchgeführt. „AnkER“ steht hier für Ankunft, Entscheidung und Rückführung. Der Fokus lag auf der Zusammenarbeit und dem Datenaustausch der am Asylverfahren beteiligten Stellen. Ich konnte mich vor Ort davon überzeugen, dass die Zusammenarbeit der Behörden durch die Verantwortlichen des BAMF in diesem AnkER-Zentrum datenschutzkonform erfolgt.

Im AnkER-Zentrum Dresden wird ein Pilotprojekt zum Einsatz von Blockchain-Technologie im Asylverfahren durchgeführt. Am Beispiel eines vereinfachten Asylprozesses wird erprobt, ob mit der Entwicklung einer individuellen Blockchain-Architektur die behördenübergreifende Zusammenarbeit in verschiedenen Phasen des Asylprozesses verbessert werden kann. Die Pilotierungsphase wird gemeinsam mit der Ausländerbehörde im AnkER-Zentrum Dresden durchgeführt. Die Technologie soll es möglich machen, Teile des behördlichen Prozessmanagements zu vernetzen. Der unmittelbare, medienbruchfreie Informationsaustausch soll die Verfahrensdauer minimieren. Allerdings ergeben sich mit der Anwendung von Blockchain datenschutzrechtliche Fragestellungen, die einer grundlegenden Prüfung bedürfen und vor Ort nicht abschließend geklärt werden konnten.

Aufgrund der Unveränderbarkeit der Blockchain können z. B. gespeicherte Daten nicht wieder gelöscht werden. Es wird nur eine sogenannte Löschtransaktion gespei-

chert. Vergleichbares gilt auch für die Berichtigung von fehlerhaften Daten. Diese können auf der Blockchain zwar korrigiert, aber nachträglich nicht geändert werden (vgl. hierzu auch Nr. 1.4.1). Ich habe um Übermittlung weiterer Informationen und Unterlagen gebeten, die mir zwischenzeitlich zur Prüfung vorliegen. Das Ergebnis lag bei Redaktionsschluss zu diesem Tätigkeitsbericht noch nicht vor.

9.3.2 Beratungs- und Kontrollbesuch bei der Bundesanstalt Technisches Hilfswerk (THW)

Eine erste Kontrolle der Datenbank „THWin" als zentrales Speicherinstrument und ihre Anwendung in den Dienststellen ist der Auftakt für nachfolgende dezentrale Kontrollmaßnahmen

Das THW nutzt als zentrales Instrument die Anwendung „THWin". Diese besteht aus einzelnen Datenbanken, die in jeder Dienststelle des THW genutzt werden. In "THWin" werden gemäß § 2 Absatz 3 THW-Gesetz die personenbezogenen Daten von rund 80.000 Ehrenamtlichen verarbeitet.

Das Rechte- und Rollenkonzept ist grundsätzlich nicht zu beanstanden, befindet sich derzeit allerdings in der Überarbeitung, sodass es bei künftigen Kontrollmaßnahmen ergänzend zu prüfen ist.

Nach Art. 30 DSGVO ist ein Verzeichnis über die Verarbeitungstätigkeiten zu erstellen und zu führen. Dies war zum Zeitpunkt der Kontrollmaßnahme noch nicht erfolgt. Das THW hat zwischenzeitlich die ersten Maßnahmen zur Einführung und Umsetzung eingeleitet.

9.3.3 Projekte der Bundespolizei

Die Bundespolizei startete im Berichtszeitraum zwei datenschutzrechtlich umstrittene Projekte: den Test von Gesichtserkennungssoftware am Bahnhof Südkreuz in Berlin und den Test von Bodycams. Ich wurde zu spät und unzureichend beteiligt.

Im August 2017 startete die Bundespolizei das Pilotprojekt am **Bahnhof Südkreuz**, zunächst mit dem Test von Gesichtserkennungssoftware. Dabei wurden drei verschiedene Softwareprodukte zur Gesichtserkennung im Live-Betrieb auf die Tauglichkeit zur Anwendung in der polizeilichen Praxis getestet. Die Aufnahmen von ausgewählten Kameras des videoüberwachten Bahnhofes wurden dabei mit einem Testfahndungsbestand abgeglichen. Dieser wurde aus Lichtbildern von freiwilligen Testteilnehmern erstellt. Die Verarbeitung erfolgte in einem separaten und abgeschotteten Netzwerk. Ein Abgleich mit polizeilichen Datenbanken erfolgte nicht. Es wurde die Wiedererkennungsrate der Testpersonen ausgewertet.

Zwar wurde ich schon im Vorfeld des Testbetriebs über das Projekt unterrichtet. Die Kommunikation blieb aber leider nicht auf Dauer so gut. So erfuhr ich z. B. von dem Einsatz aktiv sendender Transponder erst aus der Presse und konnte darauf nur reagieren, statt mich im Vorfeld proaktiv einzubringen. Auch der Abschlussbericht der ersten Testphase wurde mir nicht, wie sonst üblich, vor der Veröffentlichung zur Kenntnis gegeben, obwohl ich mehrmals darum gebeten hatte.

Derzeit wird die zweite Testphase geplant, bei der verschiedene Szenarien erprobt werden sollen, wie das Betreten festgelegter Bereiche und das Erkennen von liegenden Personen. Die Planungen dazu wurden mir bisher in mehreren Informationsveranstaltungen mitgeteilt.

Wenngleich ich sehe, dass Videoüberwachung mit Gesichtserkennung im polizeilichen Alltag ein gutes Hilfsmittel sein kann, halte ich den Einsatz dieser neuen, über die herkömmliche Videoüberwachung hinausgehenden Technik im polizeilichen Alltag nach derzeitiger Rechtslage für rechtswidrig. Gesichtserkennung

stellt eine eingriffsintensive Maßnahme dar, die eine Vielzahl von Menschen betrifft. Dieser Eingriff bedarf einer hinreichend bestimmten Rechtsgrundlage, die es derzeit nicht gibt. Ob die hohen verfassungsrechtlichen Anforderungen an entsprechend tiefgehende Grundrechtseingriffe überhaupt erfüllt werden können, ist zweifelhaft.

Der Test und die geplante Einführung von **Bodycams** ist ein weiteres bedeutendes Projekt der Bundespolizei. Bodycams sind tragbare Videoaufzeichnungsgeräte, die die Beamten an ihrer Kleidung befestigen und nach Bedarf ein- und ausschalten können. Sie sollen zur besseren Eigensicherung der Beamten und zur besseren Dokumentation von Konfliktsituationen beitragen. Die Aufzeichnungen dürfen nur im öffentlichen Raum nach vorheriger Ankündigung erstellt werden. Bei den ersten Tests stellte die Bundespolizei eine deutlich deeskalierende Wirkung fest. Die Rechtsgrundlage für den Einsatz findet sich in § 27a Bundespolizeigesetz (vgl. o. Nr. 9.1.3). Derzeit diskutiere ich mit der Bundespolizei die Frage, wo die Videodaten verarbeitet und gespeichert werden sollen. Hierzu gibt es zwischen der Bundespolizei und mir gegensätzliche Auffassungen. Nachdem auch hier die Information über die geplante Speicherart erst sehr spät, nämlich ohne vorherigen Hinweis mit der Vorlage des geänderten Entwurfs der Errichtungsanordnung zur Bodycam, erfolgte, hoffe ich auf eine künftig frühere Information.

9.3.4 Projekte des Bundeskriminalamts

Mit dem Programm „Polizei 2020“ steht die IT-Landschaft der deutschen Polizei vor einer grundlegenden Neuausrichtung. Dabei zeigt sich auch, dass das Bundeskriminalamt (BKA) sich stärker als ein zentraler IT-Dienstleister für die Polizei positioniert, wie beispielsweise beim einheitlichen Fallbearbeitungssystem (eFBS) und einer neuen Anlage zur Telekommunikationsüberwachung (TKÜ).

Die bisherigen Verbunddateien des bundesweiten polizeilichen Informationssystems (INPOL) sollen abgeschafft und durch einen neuen Informationsverbund im Rahmen des Programms „Polizei 2020“ ersetzt werden. Grundlage hierfür ist das geänderte Bundeskriminalamtgesetz (vgl. hierzu unter Nr. 9.1.3). Zu dem Gesetzesentwurf hatte ich ausführlich kritisch Stellung genommen (vgl. 26. TB Nr. 10.2.9.1).

Anders als bislang, soll der polizeiliche Datenverbund nicht mehr in verschiedene logisch getrennte Dateien unterteilt werden. Vielmehr beabsichtigen das Bundesministerium des Innern, für Bau und Heimat (BMI) und das BKA die Schaffung eines „gemeinsamen Datenhauses“. In diesem Haus sollen die polizeilichen Daten zukünftig für die Polizeien des Bundes und der Länder vorgehalten werden. Die Regelung des Zugriffs auf diese Daten ist aber noch nicht hinreichend geklärt. Insbesondere ist derzeit noch offen, nach welchen Kriterien die Zugriffsrechte für die einzelnen Benutzer vergeben werden sollen. Natürlich ergeben sich in diesem Zusammenhang auch noch weitere grundlegende datenschutzrechtliche Fragestellungen. Zunächst ist allerdings festzustellen, dass weder BMI noch BKA mir bislang detaillierte und aussagekräftige Unterlagen für die geplante neue IT-Struktur der deutschen Polizei vorgelegt haben. Lediglich Einzelheiten sind mir bekannt. Für eine ausführliche datenschutzrechtliche Bewertung fehlen daher derzeit die Grundlagen.

Bei „Polizei 2020“ handelt es sich um ein auf mehrere Jahre angelegtes Programm. Wann die neue IT-Landschaft eingeführt wird, ist derzeit noch offen. Die bisherigen Dateien bleiben aber aufgrund einer Übergangsregelung gleichzeitig erhalten. Aus heutiger Sicht ist kaum zu erwarten, dass die Einführung trotz des ambitionierten Projektnamens schon im Jahr 2020 erfolgen wird.

In den neuen Informationsverbund sollen zudem bereits laufende Projekte und Verfahren integriert werden, wie z. B. die Bereitstellung und der Betrieb eines **eFBS** (einheitliches Fallbearbeitungssystem) durch das BKA. Das eFBS befindet sich noch im Aufbau. Ziel ist die Konsolidierung der dezentralen Fallbearbeitungssysteme der Polizeien hin zu einem einheitlichen Bearbeitungssystem.

Unabhängig vom Programm „Polizei 2020“ hat mir das BKA sein Projekt PHOENIX zur Realisierung einer TKÜ-Anlage der nächsten Generation vorgestellt (TKÜ-NG). Ziel des Projektes ist der Aufbau einer TKÜ-NG-Anlage als zentrales Serviceangebot für die gemeinsame Nutzung verschiedener Behörden. Das Projekt befindet sich noch in der Anfangsphase. Aktuell wird das Pflichtenheft erstellt. Da der Bereich der TKÜ regelmäßig eine hohe datenschutzrechtliche Komponente mit sich bringt, werde ich das Projekt datenschutzrechtlich begleiten.

Welche Problemlagen sich im neuen Informationsverbund stellen können, zeigen auch Erfahrungen aus Kontrollen, die ich in der Vergangenheit durchgeführt habe, so etwa zur Verarbeitung erkennungsdienstlicher Daten oder zur Falldatei Rauschgift.

Über die Verarbeitung von erkennungsdienstlichen Unterlagen habe ich schon in der Vergangenheit mehrfach berichtet (21. TB Nr. 5.2.4.1; 22. TB Nr. 16.21; 24. TB Nr. 7.4.3). Zuletzt hatte ich darauf hingewiesen, dass erkennungsdienstliche Daten (ed-Daten) ein gesondertes Aussonderungsprüfdatum erhalten müssen, damit sie stärker von anderen Daten zur Person getrennt sind und eine auf ed-Daten beschränkte Löschung erfolgen kann.

Außerdem musste das BKA sicherstellen, dass es nur solche ed-Daten speichert, denen eigene Erkenntnisse zugrunde liegen. Inzwischen wurden sowohl die Verantwortlichkeiten als auch die Löschung neu geregelt. Das von mir bemängelte Konstrukt der Mitverantwortung wird nicht mehr weiter verfolgt. Im Zuge dieser Umstellung wurde zudem eine umfassende Datenbereinigung im Bereich der ed-Daten angestoßen, die noch andauert. Bisher wurden schon ca. 2,1 Millionen Akten bzw. Einträge gelöscht, hunderttausende von Akten wurden entsprechend der neuen Regeln neu angelegt und mit eigenen Aussonderungsprüffristen versehen. Der Prozess dauert voraussichtlich noch bis 2023 an.

Die Kontrolle der Falldatei Rauschgift ist ebenfalls sehr erfolgreich verlaufen (26. TB Nr. 10.3.2). Inzwischen konnte ich erfreulicherweise eine deutliche Reduzierung der gespeicherten Fälle feststellen. So wurde allein für den Bereich der Zollfahndung erreicht, dass von den ursprünglich gespeicherten 54 543 Personen (Stichtag 30. Juni 2015) nach der mit der Migration in eine neue Datei verbundenen Bereinigung nur noch 11 091 Personen in dem neuen Verbundsystem gespeichert sind. Damit wurden alleine im Bereich des Bundes 43 452 unnötig gespeicherte Personendatensätze gelöscht. Auch im Bereich der Länderspeicherungen gab es deutliche, wenn auch sehr unterschiedliche Reduzierungen.

9.3.5 Pflichtkontrollen im Bereich Innere Sicherheit

Immer häufiger sehen sowohl nationale Gesetze als auch EU-Recht datenschutzrechtliche Kontrollen bestimmter Dateien oder Ermittlungsmaßnahmen vor, die turnusmäßig durchzuführen sind. Erste Erfahrungen mit den verschiedenen Pflichtkontrollen liegen inzwischen vor.

Nationale Pflichtkontrollen „ungeliebter Dateien“

Nach nationalem Recht muss ich mindestens alle zwei Jahre bei den einspeichernden Behörden die datenschutzkonforme Nutzung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) überprüfen. Während sich diese Kontrollen mittlerweile eingespielt haben, bleiben die beiden Dateien bei den betreffenden Behörden eher „Stiefkinder“. Daher stellt sich die Frage nach deren Sinnhaftigkeit.

Im aktuellen Berichtszeitraum habe ich folgende Kontrollen durchgeführt:

ATD:
Bundespolizei (BPol) (2017), Zollkriminalamt (ZKA) (2017), Bundesamt für Verfassungsschutz (BfV) (2017), Bundesamt für den Militärischen Abschirmdienst (MAD) (2018), Bundesnachrichtendienst (BND) (2018).

RED:
BKA (2018), BPol (2017), BfV (2017), MAD (2017).

Bei keiner Kontrolle werde ich voraussichtlich eine Beanstandung aussprechen müssen – einige Kontrollen waren bei Redaktionsschluss noch nicht abgeschlossen.

Bei den Polizeibehörden konnte ich einen der Sensibilität der Dateien angemessenen Umgang mit den Daten feststellen. Die Speichervoraussetzungen wurden gründlich geprüft und waren meist gut nachvollziehbar. Die Systeme unterliegen strengen Sicherheitsvorkehrungen und strikten Berechtigungskonzepten. Ich musste hier bisher nur kleinere Empfehlungen für den Umgang mit den Dateien geben.

Die Kontrollen der ATD beim BfV und beim BND erfolgten als gemeinsame Kontrollen mit der G-10-Kommission des Deutschen Bundestages (vgl. Nr. 9.1.5).

Bei der Kontrolle der ATD beim MAD wurden meine Mitarbeiter von einem Mitarbeiter des Sekretariats der G-10-Kommission begleitet. Der MAD hatte zwar im Vorfeld der Kontrolle mitgeteilt, dass er in der ATD keine „G-10-Daten“ gespeichert habe, so dass eine Teilnahme der G-10-Kommission als nicht erforderlich angesehen wurde. Um gegebenenfalls während der Kontrolle gleichwohl existierende „G-10-Daten“ prüfen zu können, kamen die Beteiligten überein, dass ich die G-10-Kommission um Begleitung bitte. Diese Vorgehensweise hat sich als praktikabel erwiesen.

Das BfV hat Verfahrensweisen und Fehler, die ich in der Vergangenheit beanstanden musste (vgl. 26. TB Nr. 10.3.5) mittlerweile abgestellt. So wurden etwa die zuständigen Mitarbeiter geschult und technische Probleme auf Seiten der einspeichernden Behörden abgestellt oder minimiert.

Allerdings habe ich bei all diesen Kontrollen festgestellt, dass der Nutzwert beider Dateien zur Terrorabwehr und Extremismusbekämpfung in den geprüften Behörden als eher gering eingeschätzt wird. Insgesamt habe ich außerdem den Eindruck gewonnen, dass auch der Zweck der Dateien, ein Kontaktanbahnungsinstrument für die beteiligten Behörden zu schaffen, nicht erreicht wird.

Für den polizeilichen Alltag ist die Konzeption beider Dateien offenbar nicht flexibel genug. Die für die Terrorismusabwehr und Extremismusbekämpfung wesentlichen Informationen werden in der Praxis in den gemeinsamen Zentren der Behörden – Gemeinsames Extremismus- und Terrorismusabwehrzentrum (GETZ) und Gemeinsames Terrorismusabwehrzentrum (GTAZ) – ausgetauscht. Die Arbeit dort wurde mir als zielführender geschildert als der Betrieb der Dateien RED und ATD. Dies entspricht auch der Einschätzung bei den Nachrichtendiensten. Im Verhältnis zum Nutzen müssen die zuständigen Mitarbeiter der Behörden einen enorm hohen Aufwand betreiben, um die entsprechenden Daten

einzupflegen, aktuell zu halten und gesetzeskonform zu löschen. Hinzu kommen die bereits in den vergangenen Tätigkeitsberichten angesprochenen technischen Probleme, die die Nutzung der ATD und der RED zusätzlich erschweren (vgl. 26. TB Nr. 10.2.10.1 und Nr. 10.3.5).

Ich habe daher begonnen, diese Thematik mit dem BKA als dateiführender Stelle und dem Bundesministerium des Innern, für Bau und Heimat als seiner Fachaufsicht zu besprechen (vgl. 9.3.11).

Pflichtkontrollen über die Verwendung europäischer Systeme

Nach EU-Vorgaben sind in drei Bereichen turnusmäßige Pflichtkontrollen durchzuführen. Dabei handelt es sich um die nationale Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) sowie um die in Einzelfällen zugelassenen Recherchen der Sicherheitsbehörden im Visa-Informationssystem (VIS) und in der europäischen Datenbank Eurodac (vgl. Nr. 2.2).

Im aktuellen Berichtszeitraum sind erstmalig solche Kontrollen erfolgt:

SIS II:

BKA (2017), BPol (2018).

VIS-Abfragen:

BPol (2017), ZKA (2018), BND (2018).

Eurodac-Abfragen:

BKA (2017), BPol (2018).

Seit April 2013 nutzen die Polizei- und Grenzkontrollbehörden des Schengen-Raums das SIS II für zentrale Personenausschreibungen zum Zwecke der Einreise- und Aufenthaltsverweigerung nach der Verordnung (EG)1987/2006 vom 20. Dezember 2006 sowie für zentrale Personen- und Sachfahndungen zu Zwecken der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf der Grundlage des Ratsbeschlusses 2007/533/JI vom 12. Juni 2007 (vgl. Nr. 1.3). Die datenschutzkonforme Nutzung des Systems ist von mir regelmäßig zu überprüfen, die Sicherheitsstandards mindestens alle vier Jahre.

Im Berichtszeitraum habe ich beim BKA die vorhandenen Sicherheitsvorkehrungen für die nationalen Komponenten des Systems sowie den Umfang der Protokollierungen von Speicherungen und Abrufen überprüft und stichprobenartig den Bestand der vom BKA und der BPol initiierten Personenausschreibungen überprüft. Beim BKA waren in allen geprüften Fällen die Voraussetzungen für die Ausschreibung im SIS II gegeben.
Bei der BPol habe ich bei den geprüften Ausschreibungen zum Zwecke der Einreise- und Aufenthaltsverweigerung Defizite bei der Dokumentation der Speichervoraussetzungen festgestellt und entsprechende Empfehlungen ausgesprochen. Dies betraf insbesondere die erforderlichen Prognoseentscheidungen bei präventiven Ausschreibungen zur Aufenthalts- und Einreiseverweigerung. Bei den Ausschreibungen im Bereich der polizeilichen Zusammenarbeit gab es hingegen nichts zu bemängeln.

Seit 2013 dürfen die Polizeibehörden und Nachrichtendienste unter bestimmten Voraussetzungen Datenabfragen im Visa-Informationssystem durchführen. Die durchgeführten Kontrollen ergaben keinen Anlass zur Beanstandung. In den geprüften Fällen erfolgten die Abfragen jeweils zur Abwehr oder Verfolgung ausreichend schwerwiegender Straftaten in einem konkreten Gefahrenabwehr- oder Ermittlungsvorgang und erschienen auch geeignet, das Ziel der Abfrage zu fördern. Beim ZKA gab es nichts zu bemängeln. Die Dokumentation war vollständig und gut nachvollziehbar.
Gegenüber der BPol habe ich eine Empfehlung zur Verbesserung der Dokumentation ausgesprochen, weil die Erforderlichkeit der Abfragen nicht in allen Fällen unmittelbar aus dem Aktenrückhalt rekonstruierbar waren. Die Kontrolle beim BND war zum Redaktionsschluss noch nicht abgeschlossen.

Seit 2015 dürfen die Polizeibehörden unter bestimmten Voraussetzungen Fingerabdrücke mit Daten von Asylantragstellern in Eurodac abgleichen. Bisher wird von dieser Möglichkeit wenig Gebrauch gemacht, wohl ebenso aufgrund der restriktiven Zugangsvoraussetzungen als auch aufgrund des bislang recht kleinen Datenumfangs (z. B. keine Lichtbilder). Zusätzliche Zugangsvoraussetzung – ansonsten sind diese wie beim VIS gestaltet – ist hier die sogenannte Abfragekaskade, d. h. bestimmte andere Datenbanken sind vorrangig abzufragen und dies hat in nachvollziehbarer zeitlicher Nähe zu geschehen (z. B. nicht drei Jahre vor der Eurodac-Abfrage wie in einem der geprüften Fälle). Im Ergebnis habe ich gegenüber dem BKA eine Empfehlung zur Verbesserung der Dokumentation ausgesprochen. Die Kontrolle bei der BPol war zum Redaktionsschluss noch nicht abgeschlossen. Auch hier zeichnen sich aber bereits Dokumentationsdefizite ab.

Ich empfehle, bei Zugriffen auf Eurodac und auf das VIS-Informationssystem durch Polizeibehörden auf eine aussagekräftige Dokumentation zu achten.

Ich empfehle dem Gesetzgeber angesichts des festgestellten geringen Nutzwerts von Antiterrordatei und Rechtsextremismus-Datei, diese abzuschaffen.

9.3.6 Das Bundeskriminalamt als Zentralstelle

9.3.6.1 Das BKA als Zentralstelle – allgemeine Datenerhebungen

Die Polizeigesetze regeln, wann die Polizei tätig werden darf. Normalerweise verlangen diese dafür eine konkrete Gefahr für die öffentliche Sicherheit. Besteht diese Gefahr, dann geht die Polizei gegen den Verursacher der Gefahr vor. Nur in Ausnahmefällen kann sie andere Personen in Anspruch nehmen. Man nennt diese dann Notstandsstörer. Im Strafverfahren ist dies ähnlich. Erst wenn sich aus einem konkreten Sachverhalt der Anfangsverdacht einer Straftat ergibt, dürfen Staatsanwaltschaft und Polizei Ermittlungen aufnehmen und dabei Daten über einzelne Personen erheben. Für das Bundeskriminalamt (BKA) regelt das Gesetz dies aber anders.

Das BKA ist die kriminalpolizeiliche Zentralstelle der Polizeibehörden des Bundes und der Länder. Dazu führt es nicht nur zentrale Informationsbestände, sondern erhebt auch selbst Daten aufgrund einer gesetzlichen Generalklausel. Diese setzt keinen Anfangsverdacht oder eine konkrete Gefahr voraus. Es genügt, wenn die Daten „zur Erfüllung seiner Aufgaben als Zentralstelle erforderlich sind". Allerdings darf das BKA die Daten nur zur „Ergänzung vorhandener Sachverhalte" oder „sonst zu Zwecken der Auswertung" erheben. Es liegt auf der Hand, dass dies für die Grundrechte ein sensibler Bereich ist. Denn eigentlich soll nur derjenige Ziel polizeilicher Ermittlungen werden, der Anlass dafür gegeben hat.

Deshalb habe ich mir diese Datenerhebungen stichprobenartig in einer datenschutzrechtlichen Kontrolle angesehen. Vorweg ein Wort zur Stichprobe: Es ist nicht zentral protokolliert oder erfasst, welche Daten nach der Zentralstellengeneralklausel erhoben werden. Das sieht das Gesetz auch nicht vor. Deshalb waren entsprechende Fälle nicht einfach abrufbar und ich habe mir nur Fälle angesehen, die mir das BKA als Beispiel vorgelegt hat. Die Beispielsfälle sollten nach meiner Anforderung einen Querschnitt der Tätigkeit des BKA abbilden, was nach meinem Eindruck so auch der Fall war.

Typische Konstellationen waren etwa Anfragen ausländischer Behörden oder Hinweise von anderen Behörden auf Straftaten, bei denen noch keine Zuordnung zu einem konkreten Tatort möglich war. In diesen Fällen erhob das BKA ergänzende Informationen, um die weitere Bearbeitung koordinieren zu können.

Im Ergebnis habe ich insofern eine weitgehend restriktive Handhabung durch das BKA vorgefunden. Insbesondere in Fällen, in denen ein konkreter Anfangsverdacht vorlag, beschränkte sich das BKA auf die Erhebung solcher Informationen, mit deren Hilfe sich die zuständige Polizeibehörde herausfinden ließ, etwa wenn als Information über Tatort und Verdächtigen nur eine IP-Adresse vorhanden war.

Etwas umfangreicher ermittelt das BKA bei Anfragen ausländischer Polizeibehörden und schaltet zusätzlich die Landespolizeibehörden ein. Hier erhebt das BKA neben Bestandsdaten auch öffentlich zugängliche Daten aus dem Internet. Problematisch war, dass es in einigen Fällen nach dem Maßstab inländischen Rechts unklar war, ob es sich um Straftaten oder um Extremismus unterhalb der Straftatenschwelle handelte. Nur die Unterstützung bei der Verfolgung von Straftaten liegt in der Zuständigkeit des BKA. Von einer Beanstandung habe ich aber abgesehen, weil das BKA in diesen Fällen gegenüber der ausländischen Behörde keine oder nur eine sehr restriktive Auskunft über die Ergebnisse erteilt hat. Das BKA hat mir zudem in einer Stellungnahme mitgeteilt, künftig schon vor der Datenerhebung mit standardisierten Prozessen bei der anfragenden Stelle um Präzisierung der Anfrage zu bitten. Hierbei ist übrigens zu beachten, dass der polizeiliche Datenaustausch keine prozessualen Rechte der Betroffenen beeinträchtigen darf. Insbesondere darf er nicht die Regeln der internationalen Rechtshilfe umgehen. Keine Umgehung dieser Regeln sehe ich allerdings in der Praxis, zunächst mit nicht schwerwiegenden Eingriffen auf eine Sicherung von Beweismitteln hinzuwirken, die dann ggf. nach richterlicher Prüfung nach den Regeln der Rechtshilfe erhoben und ausgetauscht werden.

Kritisiert habe ich die aktenmäßige Dokumentation der Datenerhebungen. Diese ist nicht einheitlich. Jede Organisationseinheit entscheidet selbst, in welcher Weise sie Datenerhebungen dokumentiert. Teilweise wird das Vorgangsbearbeitungssystem genutzt, teilweise nur die Windows-Dateiablage. Dieser Frage bin ich in der weiteren datenschutzrechtlichen Kontrolle zum Vorgangsbearbeitungssystem nachgegangen. Da diese zum Redaktionsschluss noch nicht beendet war, werde ich darüber im nächsten Tätigkeitsbericht berichten.

9.3.6.2 Das BKA als Zentralstelle – Zentralstellendatei Funkzellenabfragen

Bereits im letzten Tätigkeitsbericht hatte ich über eine Datei berichtet, in der das Bundeskriminalamt (BKA) die Daten aus den Funkzellenabfragen aus einer Vielzahl von Verfahren aus verschiedenen Bundesländern speichert (26. TB Nr. 10.2.9.3). Diese Datei habe ich mir nunmehr genauer angesehen und als unzulässig beanstandet.

In der Datei gleicht das BKA personenbezogene Daten ab, die die Strafverfolgungsbehörden in Bund und Ländern im Rahmen von Funkzellenabfragen erhoben haben. Die Datei enthielt zum Zeitpunkt der Kontrolle rund 5,5 Mio Verkehrsdatensätze. Diese betreffen etwa eine halbe Million Mobilfunkteilnehmer, die sich zu bestimmten Zeitpunkten in den jeweiligen Funkzellen aufgehalten haben.

Das Vorgehen ist in dieser Form nicht durch die Generalklausel des § 7 Absatz 1 Bundeskriminalamtgesetz (BKAG) a.F. für die „Zentralstellentätigkeit" des BKA gedeckt. Der Zentralstellentätigkeit kommt nur die Funktion zu, die Tätigkeit der verschiedenen Polizeibehörden in Bund und Ländern informationell zu verzahnen und zu koordinieren. Sie kann nur leichte Grundrechtseingriffe legitimieren, wie etwa die gegenseitige Information über aktuelle Ermittlungsverfahren.

Das Bundesverfassungsgericht fordert für eingriffsintensive Maßnahmen eine normenklare und verhältnismäßige Regelung. Je schwerer der Grundrechtseingriff ist, desto genauer muss der Gesetzgeber die Voraussetzungen und Eingriffsschwellen regeln. Der Sache nach dient die Funkzellendatei einem äußerst umfassenden Datenabgleich.

Die Funkzellenabfragen erfassen eine Vielzahl von Betroffenen. Konkret wird nicht nur durch die Vorratsdatenspeicherung eine Vielzahl von Personen gespeichert, die dafür keinen konkreten Anlass gegeben haben. Mit der Funkzellenabfrage greifen die Ermittlungsbehörden auch auf diese umfangreichen Daten vieler Personen zu. Damit erfassen sie alle Menschen, die sich mit ihrem aktiven Mobiltelefon in einem bestimmten Zeitraum in einer bestimmten Funkzelle aufgehalten haben. Je nach Funkzelle und Zeitraum kann dies tausende oder hunderttausende Menschen betreffen. In das Visier konkreter Ermittlungen kommt dann derjenige, der bei einem „Kreuz- oder Mehrfachtrefferabgleich" auffällig wird (vgl. dazu auch BT-Drs. 17/14794). Mit Pech genügt es also, zur falschen Zeit am falschen Ort zu sein, um schwerwiegende Ermittlungshandlungen erdulden zu müssen. Je mehr Daten abgeglichen werden, desto höher das Risiko. Deshalb kann die Generalklausel die umfangreiche Datei für den Datenabgleich nicht legitimieren.

Hier hätte zunächst geprüft werden müssen, ob eine Rasterfahndung in Betracht kommt. Diese ist in der Strafprozessordnung speziell geregelt. Sie greift ein, wenn die Polizeibehörden Daten aus unterschiedlichen Quellen erheben, um diese dann abzugleichen. Das ist bei der Funkzellenabfrage der Fall. Denn diese Daten werden bei einem Provider mit dem Ziel erhoben, die Daten mit anderen Datenbeständen – ggf. aus einer weiteren Funkzellenabfrage – abzugleichen. Teilweise erlassen die Gerichte deshalb gleichzeitig mit dem Funkzellenbeschluss einen Rasterfahndungsbeschluss. Die Praxis scheint aber uneinheitlich. Sie ist auch deshalb schwer nachzuvollziehen, weil die Beschlüsse der Ermittlungsrichter in der Regel nicht in der Fachpresse veröffentlicht werden.

Den polizeilichen Ansatz konnte ich in der konkreten Datei durchaus nachvollziehen. Es ging zudem darum, besonders schwere Straftaten zu verfolgen. Dies ändert jedoch an der rechtlichen Beurteilung nichts, da sich die polizeiliche Tätigkeit innerhalb der gesetzlichen Grenzen bewegen muss. Für einen übergreifenden Abgleich gibt es ohne Anordnung einer Rasterfahndung keine Rechtsgrundlage.

Bereits im Jahr 2015 hatte ich beim Gesetzentwurf zur Vorratsdatenspeicherung auf das Risiko hingewiesen, dass Funkzellendaten für Strukturermittlungen oder zur Speicherung von Prüffällen gespeichert werden könnten (abrufbar unter www.datenschutz.bund.de; https://www.bfdi.bund.de/DE/Datenschutz/Themen/Telefon_Internet/TelefonArtikel/VoarratsdatenspeicherungReloaded.pdf?__blob=publicationFile&v=3). Der Gesetzgeber hat es jedoch bislang nicht für notwendig erachtet, den Umgang mit Funkzellendaten genauer zu regeln. Konkret wurde ich auf diese Datei aufmerksam, weil nach BKAG a.F. zu jeder Datei eine Errichtungsanordnung erstellt werden musste. Diese Anforderung ist im neuen Recht weggefallen. Ob mir deshalb auch in Zukunft derartige Datensammlungen auffallen, kann ich derzeit noch nicht abschließend beantworten.

9.3.7 Akkreditierungsverfahren beim G-20-Gipfel

Am 6. und 7. Juli 2017 wurde 32 Journalisten, denen die Akkreditierung zur journalistischen Begleitung des in Hamburg durchgeführten G-20-Gipfels zunächst erteilt worden war, diese wieder entzogen. In der Folge wurde der Vorwurf von datenschutzrechtlichen Verstößen im Zusammenhang mit der Durchführung des Akkreditierungsverfahrens und bei der Speicherung personenbezogener Daten in Dateien der Polizeien und der Sicherheitsbehörden erhoben. Dies hat mich veranlasst, sowohl das Akkreditierungsverfahren wie auch den Umgang mit den personenbezogenen Daten der betroffenen Journalisten zu überprüfen.

Das Akkreditierungsverfahren wurde vom Bundeskriminalamt (BKA) durchgeführt. Grundlage der Entscheidungen waren personenbezogene Daten, die von den Polizeibehörden des Bundes, vom Bundesamt für Verfassungsschutz (BfV) und von den Polizei- und Verfassungsschutzbehörden der Länder übermittelt bzw. in die bundesweiten Informationssysteme eingespeist worden waren.

Der Großteil der entscheidungserheblichen Informationen betraf Daten, die in der Verantwortung der Länder gespeichert waren. Meine datenschutzrechtliche Kontrolle und Bewertung musste sich auf Daten der Bundesbehörden beschränken, weil die Länderdaten zuständigkeitshalber durch meine Kolleginnen und Kollegen in den Ländern zu kontrollieren waren.

Im Ergebnis bin ich zu dem Schluss gekommen, dass das Akkreditierungsverfahren zum G-20-Gipfel für den vom BKA selbst zu verantwortenden Teil hinsichtlich der 32 geprüften Fälle von Journalisten dem Grunde nach datenschutzrechtlich nicht zu beanstanden war. Zwar wurde seitens des BKA in diesem Zusammenhang eine Liste mit Namen von Journalisten unberechtigterweise an Beamte der Länderpolizeien herausgegeben. Dies erfolgte nach Auskunft des BKA aber versehentlich. Da es sich dabei zum einen nicht um einen strukturellen Mangel, sondern um ein Versehen handelte und zum anderen das BKA diesen Fehler selbst erkannt hatte und zugesichert hat, dies in künftigen Fällen zu vermeiden, habe ich auch insoweit keine Beanstandung ausgesprochen.

Zu 14 Personen, denen die Akkreditierung entzogen wurde, hatte das BfV in eigener datenschutzrechtlicher Verantwortung Daten gespeichert und diese Informationen an das BKA übermittelt. Sowohl die Speicherung der Daten als auch deren Übermittlung erfolgte im Hinblick auf 13 dieser Personen zu Recht. In einem Fall konnte die Rechtmäßigkeit der Übermittlung aufgrund einer rechtswidrig unterlassenen Einzelfallbearbeitung nicht bewertet werden. Das BfV hatte mir dazu bereits während der Kontrolle mitgeteilt, zu der Auffassung gelangt zu sein, dass der Datensatz für die Aufgabenerfüllung nicht mehr erforderlich sei und gelöscht werden könne. Eine Löschung musste aber zunächst bis zum Abschluss meiner Kontrolle unterbleiben. Nachdem ich die Kontrolle für abgeschlossen erklärt hatte, hat mir das BfV mitgeteilt, dass der Datensatz nunmehr gelöscht sei.

Da nach meiner Auffassung Bedarf bestand, die polizeilichen und nachrichtendienstlichen Datenbestände auch über meine Zuständigkeit hinausgehend auf ihre Qualität zu prüfen, hatte ich die zuständigen Landesdatenschutzbeauftragten auf die im Rahmen meiner Kontrolle bekanntgewordenen Speicherungen der Landesbehörden hingewiesen und die eigenverantwortliche Prüfung anheimgestellt.

Ein abschließender Bericht an den Innenausschuss des Bundestages zu diesem Thema, der auch die Prüfergebnisse der beteiligten LfD berücksichtigt, befindet sich derzeit in der Abstimmung mit diesen.

9.3.8 Passagierdatenübermittlung beim Zoll

Durch eine Eingabe wurde ich auf die Praxis der Passagierlistenübermittlung durch Reedereien an den Zoll aufmerksam. Nach meiner Prüfung und Feststellung der Rechtswidrigkeit der Maßnahme wurde diese Praxis sofort eingestellt. Dies trug wesentlich zum besseren Datenschutz im Bereich des Zolls bei.

Die Reedereien der deutschen Ostseehäfen wurden von Zollfahndungsämtern aufgefordert, sämtliche Passagierlisten ohne jede Einschränkung an den Zoll zu übermitteln. Dies nahm ich zum Anlass einer Kontrolle. Es stellte sich heraus, dass sämtliche Passagierlisten von Reedereien, die Fährlinien zwischen den Ostseehäfen und Skandinavien betreiben, vom Zoll angefordert wurden. Auch die Passagierlisten von Kreuzfahrtschiffen, die in dem Bereich fuhren, waren betroffen. Die Zollbehörden vermuteten diesen Bereich als regelmäßigen Transportweg für Zigaretten- und Drogenschmuggel und versuchten über diese Maßnahme Fahndungserfolge zu erzielen. Dabei beriefen sich die Zollbehörden auf §§ 208 Absatz 1 Nummer. 3, 93 der Abgabenordnung (AO), auf die Generalklausel in §§ 24 Absatz 1, 27 Absatz 1 Zollfahndungsdienstgesetz (ZFDG) sowie hilfsweise auf die Freiwilligkeit der Reedereien zur Übermittlung.

Meine Prüfung ergab, dass es für diesen erheblichen Grundrechtseingriff keine Rechtsgrundlage gab. Für die Rechtsgrundlage der AO fehlte es an einem hinreichenden Ermittlungsanlass. Die Generalklausel des ZFDG ist für eine solch eingriffsintensive Maßnahme, die eine unbestimmte Anzahl unbescholtener Bürger betrifft, nicht ausreichend. Auch mit der Freiwilligkeit der Reedereien hinsichtlich der Übermittlungen konnte nicht argumentiert werden, da es für solch stark eingriffsintensive Maßnahmen immer einer hinreichend bestimmten Rechtsgrundlage bedarf. Von diesem Standpunkt konnte ich den Zoll überzeugen. Die Passagierlistenübermittlung wurde umgehend eingestellt, eine Beanstandung wurde daher nicht ausgesprochen.

9.3.9 Geschützter Grenzfahndungsbestand

Die Bundespolizei führt die Datei „Geschützter Grenzfahndungsbestand“ derzeit auf Basis einer Errichtungsanordnung aus dem Jahre 2008. Als Rechtsgrundlage nennt diese §§ 30, 31 i. V. m. 2 Absatz 2 Nummer 2b Bundespolizeigesetz (BPolG). Eine Rechtsverordnung gemäß §§ 30 Absatz. 1 Satz 2 und 31 Absatz 1 Satz 2 BPolG existiert nicht.

Das Bundesverwaltungsgericht hat im Hinblick auf § 7 Absatz 6 Bundeskriminalamtgesetz (BKAG) a.F. entschieden, dass das BKA personenbezogene Daten nicht ohne die nach § 7 Absatz 6 BKAG a.F. vorgesehene konstitutive

Rechtsverordnung speichern darf (BVerwG NJW 2011, 405). Daraufhin hat das Bundesministerium des Innern, für Bau und Heimat (BMI) eine entsprechende Rechtsverordnung nach dieser Vorschrift erlassen.

Die gleiche Problematik stellt sich auch für Dateien wie dem geschützten Grenzfahndungsbestand, für die nach § 30 Absatz 1 Satz 2 und § 31 Absatz 1 Satz 2 BPolG ebenfalls eine Rechtsverordnung zu erlassen ist. Diese Regelungen entsprechen § 7 Absatz 6 i. V. m. 8 BKAG a.F.. Aufgrund der Entscheidung des Bundesverwaltungsgerichts habe ich mich daher im April 2015 an das BMI gewandt und auf diese Problematik hingewiesen. Im Sommer 2015 kündigte das BMI daraufhin seine Bereitschaft an, eine entsprechende Rechtsverordnung zu erlassen. Nachdem ich in der Folgezeit keinen Erlass einer solchen Rechtsverordnung feststellen konnte, habe ich Anfang 2018 das BMI um Sachstandsmitteilung gebeten. Daraufhin wurde mir mitgeteilt, dass die Rechtsverordnung noch nicht erlassen worden sei und dies auch nicht mehr beabsichtigt sei, da das BPolG novelliert würde und in diesem Zusammenhang auch die §§ 30 und 31 BPolG so neu gefasst werden sollten, dass eine Rechtsverordnung nicht mehr erforderlich sei.

Dieser seit Jahren bestehende erhebliche Verstoß gegen datenschutzrechtliche Vorschriften wurde von mir daraufhin gem. § 25 Absatz 1 BDSG a.F. beanstandet.

9.3.10 Informationsbesuche

Regelmäßig informiere ich mich auch im Sicherheitsbereich über die Planung neuer Projekte und im Test befindliche Verfahren. Im Bundeskriminalamt (BKA) habe ich mich über den Test von 3D-Gesichtserkennungssoftware, über Instrumente zur Gefährdereinschätzung sowie über Anwendungen zum IP-Tracking informiert. Die Bundespolizei (BPol) hat mich über den Test einer „Fahndungsapp" unterrichtet.

Das vom BKA genutzte Gesichtserkennungssystem wird regelmäßig mit anderer marktgängiger Software verglichen, um deren Tauglichkeit auf den Prüfstand zu stellen. In einem Informationstermin wurde mir dargelegt, welche Problemstellungen sich beim Einsatz von Gesichtserkennungssoftware ergeben. Dabei kommt der Bildqualität eine zentrale Bedeutung zu. Zu nennen sind hier die Ausleuchtung der Bilder und das Verdecken von Gesichtern, z. B. durch Brillen, Bärte, Tücher etc. Auch ein guter Ausbildungsstand der Sachbearbeiter im Umgang mit der Software ist für eine erfolgreiche und effektive Nutzung des Bildmaterials erforderlich. Aktuell werden im BKA verschiedene Softwareprodukte miteinander verglichen. Ergebnisse dieser Tests liegen voraussichtlich erst im nächsten Jahr vor.

Von den Anwendungen RADAR-iTE und RISKANT beim BKA habe ich aus der Presse erfahren. Dies habe ich zum Anlass für einen Informationsbesuch genommen. Bei RADAR-iTE handelt es sich um ein Risikobewertungsinstrument basierend auf Word- und Excel-Dateien. Das Verfahren wurde gemeinsam mit der forensisch-psychologischen Abteilung der Universität Konstanz entwickelt. Ziel ist es, mit Unterstützung durch RADAR-iTE Priorisierungen im Bereich von Gefährdern vorzunehmen. Grundlage sind bereits vorhandene polizeiliche Erkenntnisse. In einem Risikobewertungsbogen strukturieren die Bearbeiter die Erkenntnisse. Die hinterlegten Auswertealgorithmen ergeben schließlich den Gefährdungsgrad, der von dem Verdächtigen ausgeht. Im Test konnten mit dem Verfahren alle bekannten Gefährder identifiziert werden. Das BKA hat dieses Instrument den Ländern zur Verfügung gestellt, weil sie im Regelfall die Datenbesitzer sind und deshalb auch die Bewertung durchführen. Die festgestellten Erkenntnisse werden regelmäßig überprüft.

RISKANT ist ein Verfahren, das auf RADAR-iTE aufbaut und dieses weiterentwickeln soll. Aus der statistischen Bewertung von RADRA-iTE soll eine gutachterliche Stellungnahme zum Einzelfall extrahiert werden. Diese Anwendung befindet sich noch in der Entwicklung.

Im BKA werden mehrere marktgängige Tools genutzt um per aktivem IP-Tracking den Standort eines Nutzers anhand seiner IP-Adresse festzustellen. Diese Maßnahmen werden in einer zentralen Applikation gesteuert, welche auch die erlangten Ergebnisse anzeigt. Alle Arbeitsschritte werden protokolliert, Ergebnisse werden den Ländern übermittelt. Es wird hierbei ausschließlich anlassbezogen und auf staatsanwaltschaftliche oder richterliche Anordnung hin gearbeitet. Entsprechend gering ist die Anzahl der jährlich durchgeführten Maßnahmen. Bisher werden die Ergebnisse zehn Jahre im BKA gespeichert. Ich habe eine deutlich frühere Löschung der Daten, nach Möglichkeit schon nach Übermittlung an die Länder, angeregt. Ein Einvernehmen konnte bislang noch nicht hergestellt werden. Die Gespräche dauern noch an.

Die BPol hat mich über den Test einer „Fahndungsapp" informiert. Dabei handelt es sich um eine Smartphone-App, die die Personenkontrolle erheblich erleichtern soll. Mit der App kann ein Personalausweis überprüft werden. Dabei wird parallel zur Echtheitsüberprüfung auch eine Fahndungsabfrage generiert. Das Ergebnis wird direkt auf das Smartphone gesendet. Der Beamte sieht dann auf einen Blick, ob die Person im Fahndungsbestand enthalten ist und ggf. gefährlich sein könnte. Damit wird der sonst übliche Funkkontakt zur Leitstelle, die die Fahndungsabfrage durchführt und der mögli-

cherweise durch andere Personen mitgehört werden kann, überflüssig. Da die App keine Daten speichert und nur einen Zweck erfüllt, ist hier der datenschutzrechtliche Grundsatz der Datensparsamkeit gewahrt.

9.3.11 ATD und RED – Ermüdungserscheinungen

Die Antiterrordatei (ATD) wurde ebenso wie die Rechtsextremismus-Datei (RED) mit großen Erwartungen an eine verbesserte Zusammenarbeit der Sicherheitsbehörden geschaffen. Beide Dateien laufen diesem Anspruch hinterher, ohne die in sie gesetzte Hoffnung zu erfüllen.

Die Datenschutzkontrollen der ATD und der RED sind sehr aufwändig: Neben den Speicherungen in den Dateien selbst müssen die sog. Quelldateien der einspeichernden Behörden geprüft werden. Auch die Überprüfung der Speicherungen anhand von Protokolldaten gestaltet sich schwierig. Es gab erste Gespräche mit dem Bundesministerium des Innern, für Bau und Heimat und dem Bundeskriminalamt, um diese unbefriedigende Situation zu verbessern.

In den Kontrollen war die Stimmungslage bei den Anwendern klar: Die Zuneigung der teilnehmenden Behörden zu beiden Dateien ist schon lange erkaltet. Die in § 7 Rechtsextremismus-Datei-Gesetz (REDG) und § 6a Antiterrordateigesetz (ATDG) jeweils vorgesehene Analysemöglichkeit dieser Dateien wurde bis heute nicht realisiert (vgl. auch Nr. 9.1.6) und ist von Seiten der Sicherheitsbehörden offenbar nicht als zwingend notwendig eingefordert worden. Aufgrund meiner Eindrücke aus der Kontrollpraxis sollte daher überlegt werden, ob die Dateien wegen ihrer geringen fachlichen Bedeutung nicht abgeschafft werden sollten (vgl. dazu auch Nr. 9.3.5).

9.3.12 Best Practice

Typisch für einen Tätigkeitsbericht zum Datenschutz ist die darin oftmals gegenüber den für die Verarbeitung personenbezogener Daten verantwortlichen Stellen geäußerte Kritik. Ich möchte an dieser Stelle aber auch ausdrücklich erwähnen, dass die Zusammenarbeit mit vielen Behörden wieder als sehr positiv zu bewerten ist. Von dem in diesen Fällen praktizierten offenen, ausführlichen und konstruktiven Austausch konnten alle Beteiligten profitieren.

Gemeinsame ATD-Kontrolle beim Bundesamt für Verfassungsschutz (BfV)

In meinem 26. Tätigkeitsbericht (vgl. Nr. 10.2.10.3) habe ich unter der Rubrik „Kontrollfreie Räume“ unter anderem Handlungsbedarf bei den gemeinsamen Pflichtkontrollen von G-10-Kommission und BfDI zur Antiterrordatei (ATD) beim BfV festgestellt. Die erste gemeinsame Pflichtkontrolle im Jahr 2015 offenbarte neben der Klärung rechtlicher Probleme auch erhebliche organisatorische und technische Schwierigkeiten und Unzulänglichkeiten. Die Datenschutzbehörden sind gemäß § 10 Absatz 2 Antiterrordateigesetz (ATDG) verpflichtet, alle zwei Jahre die Einhaltung der datenschutzrechtlichen Vorgaben in der ATD zu kontrollieren. Demgemäß fand die nächste gemeinsame Pflichtkontrolle im Jahr 2017 statt. Die Vorbereitung der Kontrolle erfolgte in enger Abstimmung mit allen an der Kontrolle beteiligten Stellen. Ziel dieser Abstimmungen war, die wiederkehrenden Pflichtkontrollen von den organisatorischen Abläufen und den technischen Anforderungen an die Falldarstellungen her so zu gestalten, dass sie effektiv und umfassend mit dem größtmöglichen Nutzen durchgeführt werden können. Das Datenschutzteam des behördlichen Datenschutzbeauftragten im BfV hat mit seinem außerordentlich engagierten Einsatz in der Vorbereitung und während der Durchführung der Kontrolle zu einem positiven und für alle Beteiligten zufriedenstellenden Kontrollverlauf beigetragen. In Einzelfällen auftretende Fragen konnten überwiegend unmittelbar mit den Bearbeitern besprochen und geklärt werden. Offene Fragen wurden im Nachgang schriftlich geklärt. Die Kontrolle konnte inzwischen abgeschlossen werden. Eine Beanstandung habe ich nicht ausgesprochen. Bei dieser Kontrolle hat sich wieder einmal bestätigt, dass eine gute Kooperation ein Gewinn für alle Beteiligten ist.

Bundesministerium für Wirtschaft und Energie: Sicherheitsüberprüfungsgesetz

Im Berichtszeitraum konnte die Zusammenarbeit mit dem Bundesministerium für Wirtschaft und Energie (BMWi) im Bereich des Sicherheitsüberprüfungsrechts intensiviert und ausgeweitet werden. Das BMWi ist gemäß § 25 Absatz 1 Sicherheitsüberprüfungsgesetz (SÜG) zuständige Stelle für sicherheitsempfindliche Tätigkeiten im nicht-öffentlichen Bereich und zuständig für die Einleitung und Durchführung von Sicherheitsüberprüfungen von Mitarbeitern in geheimschutzbetreuten Unternehmen. Mit den dafür zuständigen Referaten im BMWi stehe ich im regelmäßigen Kontakt und Austausch. Gemeinsam konnten beispielsweise datenschutzrechtliche Problemlagen gelöst werden, die im Zusammenhang mit der Anwendung der DSGVO standen. Aber auch sonstige Fragen, die durch die Sicherheitsbevollmächtigten bei den Unternehmen (SiBe) an das BMWi herangetragen wurden, konnten beantwortet werden. Gleichzeitig freut es mich, dass das BMWi meine Beratungsfunktion bei der Anwendung und Umsetzung des Datenschutzrechts im Bereich der Geheimschutzbetreuung anerkennt und mir eine praxisorientierte Aufgabenwahrnehmung ermöglicht. Dies geschieht beispielsweise im Rahmen

regelmäßiger Termine, in denen rechtliche Entwicklungen im SÜG diskutiert und datenschutzrechtliche Fragen erörtert werden, die sich aus Kontrollen oder aufgrund von Rückfragen aus den Unternehmen ergeben. Mögliche Ergebnisse wurden direkt durch das BMWi an den Fragesteller zurückgespiegelt oder bei allgemeiner Bedeutung auch über die Kontaktmöglichkeiten des BMWi an die geheimschutzbetreuten Stellen mittels Mail-Infos, in den SiBe-Arbeitskreisen oder den Seminaren des BMWi zum SÜG kommuniziert.

Das BMWi führt regelmäßig Sicherheitsseminare zum Thema „Geheimschutzverfahren" für die Unternehmen durch, die sich in der Geheimschutzbetreuung des BMWi befinden. Ich halte diese Fortbildungsmaßnahmen für unabdingbar, um die SiBe ausreichend für ihre Aufgaben in der Geheimschutzbetreuung zu qualifizieren. Erfreulicherweise werden die Schulungsangebote vom BMWi mehrfach im Jahr angeboten und stehen auch erfahrenen SiBe offen, um vorhandene Fachkenntnisse auffrischen zu können. Auch meinem Haus ermöglicht das BMWi die Teilnahme an diesen Seminaren, was im Ergebnis für alle Beteiligten gewinnbringend ist.

Zusammenarbeit mit dem BND

Im letzten Bericht hatte ich bereits hervorgehoben, dass sich meine Zusammenarbeit mit dem Bundesnachrichtendienst (BND) im Zuge der Aufarbeitung des NSA-Skandals verbessert hat. Dies hat etwa zu gemeinsamen datenschutzrechtlichen Schulungen im BND geführt. Ich freue mich, dass diese Zusammenarbeit in Form von kooperativ durchgeführten Datenschutzschulungen auch mit dem aktuellen behördlichen Datenschutzbeauftragten und seinem Team fortgesetzt werden konnte. Es gilt, diesen Ansatz weiter auszubauen, um im unmittelbaren Bezug zum Tagesgeschäft des BND die Möglichkeit zu haben, mit den betroffenen Fachbereichen sowie dem behördlichen Datenschutzbeauftragten und seinem Team datenschutzrechtlich relevante Fragestellungen zu erörtern und – soweit erforderlich – rechtskonforme Lösungsansätze zu erarbeiten. Die Treffen wurden auch dazu genutzt, sich im gemeinsamen Gespräch für die wechselseitigen Perspektiven zu sensibilisieren.

Darüber hinaus hat der behördliche Datenschutzbeauftragte die unter seiner Vorgängerin wahrgenommene Aufgabe, verstärkt hausinterne Kontrollen durchzuführen und in den Fachabteilungen Datenschutzschulungen durchzuführen, fortgesetzt.

Im Berichtszeitraum habe ich beim BND gemeinsam mit der G-10-Kommission einen ausführlichen Beratungs- und Informationsbesuch durchgeführt. In diesem Termin wurden Zweck und Funktionsweise eines IT-Systems vorgestellt und dessen Funktionsweise erläutert. Diese Art der Zusammenarbeit hat sich in mehrfacher Hinsicht als wertvoll erwiesen: Mit der Erarbeitung eines übereinstimmenden Funktionsverständnisses sowie der Gelegenheit zur Diskussion unterschiedlicher Sichtweisen kann eine wertvolle Grundlage für die spätere Durchführung sowohl effizienter als auch effektiver Datenschutzkontrollen gelegt werden. Ich würde es sehr begrüßen, diese Form eines vom Kontrollgeschäft losgelösten Informationsaustausches zu intensivieren.

Zusammenarbeit mit der Bundeswehr

Wie schon in den vergangenen Jahren war auch in diesem Berichtszeitraum die Zusammenarbeit mit der behördlichen Datenschutzbeauftragten des Bundesministeriums der Verteidigung (BMVg) besonders eng. Ein Jour fixe zur regelmäßigen gegenseitigen Information wurde durchgeführt. Im Rahmen dieser gemeinsamen Termine wurden geplante Vorhaben in vorbildlicher Weise proaktiv vorgestellt und mit dem Team der Datenschutzbeauftragten beraten. Auch im Übrigen ergaben sich bei Anhörungen und Kontrollen aufgrund der guten bundeswehrinternen Vorprüfung kaum datenschutzrechtlich problematische Sachverhalte.

Zu Beginn des Jahres 2018 wurden im BMVg aufgrund einer externen Organisationsanalyse Überlegungen zur Neuorganisation des Datenschutzes angestellt. Ich wurde dabei frühzeitig in die Beratungen einbezogen. Ein Teilergebnis ist die Verortung des Datenschutzes in einem neu gegründeten Referat im BMVg. Darüber hinaus setze ich mich dafür ein, dass die behördliche Datenschutzbeauftragte der Bundeswehr (BfDBW) neben der neuen Außenstelle beim Kommando Sanitätsdienst eine weitere Außenstelle für den Bereich Militärisches Nachrichtenwesen erhält.

9.3.13 Personeller Geheimschutz in der Wirtschaft

Die von mir festgestellten Mängel bei der Durchführung von Sicherheitsüberprüfungsverfahren in der Privatwirtschaft spiegeln wider, wie wichtig Datenschutzkontrollen in diesem Bereich sind.

Im Berichtszeitraum habe ich vier Unternehmen kontrolliert, die sich in der Geheimschutzbetreuung des Bundesministeriums für Wirtschaft und Energie (BMWi) befinden. Bei allen kontrollierten Unternehmen zeigten sich Verstöße bei der Führung der Sicherheitsakten. In der Sicherheitsakte sind alle für die Sicherheitsüberprüfung notwendigen und erforderlichen Informationen zu dokumentieren (vgl. § 18 Abs. 1 Sicherheitsüberprüfungsgesetz [SÜG]). Insbesondere die Einleitung, die Durchführung sowie der Abschluss des Sicherheitsüberprüfungsverfahrens sollten sich aus der Sicherheitsakte erschließen. In den von mir überprüften Sicherheitsakten fehlten vielfach erforderliche Informationen wie

etwa Kopien der VS-Ermächtigungsbestätigung, vollständige Belehrungsnachweise oder Kopien der unterschriebenen Zusatzvereinbarungen zum Arbeitsvertrag. In einigen Akten war nicht dokumentiert, ob und in welchem Bereich dem Betroffenen tatsächlich eine sicherheitsempfindliche Tätigkeit übertragen wurde und ob er diese noch immer ausübt. Die Sicherheitsakte muss jedoch lückenlos dokumentieren, wo der Betroffene seiner sicherheitsempfindlichen Tätigkeit nachgeht und ob diese ggf. beendet wurde. Daneben enthielten die Sicherheitsakten unzulässige Informationen, wie nicht notwendige Personalausweis- oder Reisepasskopien. Darüber hinaus befanden sich in den Sicherheitsakten vereinzelt auch Unterlagen der Personalstelle, die für die sicherheitsmäßige Beurteilung des Betroffenen nicht maßgeblich und erforderlich waren. Bei den von mir geprüften Sicherheitsakten wurden die unzulässigen Inhalte auf meine Veranlassung hin durch den jeweiligen Sicherheitsbevollmächtigten (SiBe) der Unternehmen noch unmittelbar vor Ort aus den Sicherheitsakten entfernt. Zudem habe ich die Unternehmen in meinen Abschlussgesprächen aufgefordert, alle Sicherheitsakten hinsichtlich der angesprochenen Mängel zu sichten und zu bereinigen.

Mir ist ebenfalls aufgefallen, dass es teilweise Probleme beim Informationsfluss zwischen dem SiBe und der Personalstelle gibt. Die Personalstelle ist nach §§ 15 a, 29 Absatz 2 SÜG verpflichtet, den SiBe unverzüglich über Veränderungen der persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse eines Betroffenen zu unterrichten. Aus diesen Informationen können sich nämlich für den SiBe potentiell einzuschätzende Sicherheitsrisiken bei einem Betroffenen ergeben. Nicht bei allen von mir geprüften Unternehmen waren dem SiBe und der Personalstelle bekannt, dass diese Verpflichtung besteht. Die betroffenen SiBe haben meine Prüfung zum Anlass genommen, die Kommunikationsstruktur mit der Personalstelle zu erörtern und ein Verfahren zu entwickeln, welches sicherstellt, dass alle für das Sicherheitsüberprüfungsverfahren erforderlichen Informationen weitergeleitet werden.

In einigen Fällen zeigten sich Verstöße bei der Einhaltung von Vernichtungs- und Löschfristen. So wurden etwa Sicherheitsakten von Personen, die aus der sicherheitsempfindlichen Tätigkeit ausgeschieden waren, über die gesetzlichen Aufbewahrungsfristen hinaus verwahrt. Gleichzeitig wurden die damit verbundenen elektronisch gespeicherten Daten ebenfalls dauerhaft vorgehalten. Ich habe die betroffenen SiBe aufgefordert, umgehend die Vernichtungs- und Löschfristen aller Sicherheitsakten im Nachgang meiner Prüfung zu kontrollieren. Da diese Verstöße offenbar aus Unkenntnis erfolgten, habe ich auf das Sicherheitsseminar beim BMWi hingewiesen und einen Besuch empfohlen (vgl. hierzu auch Nr. 9.3.12). Kritisch betrachte ich die Zeitanteile, die dem SiBe durch die Geschäftsführung zur Erledigung seiner Aufgaben nach dem SÜG eingeräumt werden.

Die Vorschriften des Sicherheitsüberprüfungsrechts im nicht-öffentlichen Bereich erlauben ausdrücklich eine vollständige automatisierte Verarbeitung der personenbezogenen Daten aus der Sicherheitsüberprüfung (vgl. § 31 SÜG). Hinsichtlich der Anforderungen an Datensicherheit und Datenschutz sowie zum Zwecke einer effektiven Datenschutzkontrolle halte ich eine Protokollierung, welche die Aktivitäten und Zugriffe der Nutzer dokumentiert, für zwingend notwendig. Meine Prüfungen haben jedoch ergeben, dass auch in diesem Bereich Defizite bei der Umsetzung dieser Anforderungen bestehen. Über die Art und Weise sowie den Umfang einer Protokollierung bin ich mit dem BMWi noch im Gespräch.

Besonders herausstellen möchte ich, dass mit allen geprüften Unternehmen eine konstruktive Zusammenarbeit möglich war. Meine Hinweise vor Ort und meine Bitte, die von mir festgestellten Mängel zukünftig abzustellen, wurden von den SiBe angenommen.

9.3.14 Netze des Bundes – eine Kontrolle beim BSI

Der Informationsverbund Bonn-Berlin (IVBB) ist zahlreichen Cyberangriffen ausgesetzt. Ich habe dies zum Anlass genommen, mir bei einem Kontroll- und Beratungsbesuch beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erneut über das Schadprogrammerkennungssystem (SES) und weitere Verfahren, die bei der Abwehr dieser Angriffe eingesetzt werden, berichten zu lassen.

Das SES wird vom BSI zur Gefahrenabwehr am Übergabepunkt des Behördennetzes IVBB zum Internet eingesetzt. Im Jahr 2012 hatte ich beim BSI eine Kontrolle hierzu durchgeführt. Dabei musste ich feststellen, dass das BSI unerlaubt Meldungen an den BND, das BfV und den MAD weitergab. Dies führte seinerzeit zu einer Beanstandung des Verfahrens (vgl. 24. TB Nr. 4.7). In 2017 habe ich erneut eine entsprechende Kontrolle beim BSI durchgeführt und mich dabei über das SES, den Malwarescanner MWScan, die Malware Information Sharing Platform MISP, die geplante Protokolldatenauswertung nach § 5 BSI-Gesetz sowie über die Anti-Botnetz-Initiative informiert. Die Kontrolle führte zu dem wesentlichen Ergebnis, dass das Verfahren SES mittlerweile weiterentwickelt wurde. Die entsprechenden Dokumentationen waren jedoch teilweise noch nicht aktualisiert bzw. erstellt. Aufgrund einer gesetzlichen Änderung besitzt das

BSI nunmehr eine Rechtsgrundlage für Meldungen im Verfahren SES an den BND, das BfV und den MAD. Die von mir kontrollierten Verfahren, die wie etwa das SES datenschutzrechtlich sensible Kommunikationsverbindungen auf Angriffsmuster hin untersuchen, sind für die sichere Kommunikation im Regierungsnetz unabdingbar. Insgesamt waren zum Zeitpunkt der Kontrolle keine der kontrollierten Verfahren zu beanstanden.

9.A Zudem von besonderem Interesse

1.1, 1.2 f., 1.4 ff., 1.5, 14.1.1, 17.1, 17.9, Die Arbeit des BfDI in Zahlen

10 Ausschuss für Kultur und Medien

10.1 Einzelthemen

10.1.1 Neue Kontrollzuständigkeit bei der Deutschen Welle

Der Entwurf des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU, vgl. Nr. 1.1) führt hinsichtlich der Verarbeitung reiner Verwaltungsdaten durch die Deutsche Welle zu einer neuen Aufsichtsbefugnis.

Die Rundfunkfreiheit erfordert die staatsferne Ausgestaltung und Organisation des Rundfunks, auch im Hinblick auf dessen datenschutzrechtliche Kontrolle. Das bis zum 24. Mai 2018 geltende BDSG (alt) enthielt deshalb in § 41 Absatz 2 bis 4 und § 42 Sonderregelungen zum Datenschutz bei der Rundfunkanstalt Deutsche Welle. Danach bestand eine „anstaltsautonome Kontrolle“ des Datenschutzes. Ausschließlich der von den Organen des Senders bestellte und nur ihnen gegenüber verantwortliche interne Datenschutzbeauftragte war für die Überwachung der Einhaltung des BDSG und der auf den Rundfunk bezogenen bereichsspezifischen Datenschutzvorschriften zuständig. Diese Zuständigkeit des internen Datenschutzbeauftragten der Deutschen Welle bezog sich sowohl auf den journalistisch-redaktionellen Bereich als auch auf die Verarbeitung personenbezogener Daten zu wirtschaftlich-administrativen Zwecken.

Unter Geltung der europäischen DSGVO musste der Datenschutz bei der Deutschen Welle nunmehr neu geregelt werden. Artikel 85 Absatz 1 DSGVO sieht explizit vor, dass die Mitgliedstaaten, „durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken (…) in Einklang“ bringen. Hierzu enthält Artikel 85 Absatz 2 DSGVO konkrete Mindestvorgaben für die Mitgliedstaaten, Abweichungen oder Ausnahmen von einzelnen Normen oder ganzen Kapiteln der DSGVO vorzusehen. Hinsichtlich der Deutschen Welle soll dieser Regelungsauftrag nunmehr durch das 2. DSAnpUG-EU, das sich zum Zeitpunkt des Redaktionsschlusses noch in der parlamentarischen Beratung befand (vgl. Nr. 1.1), ausgefüllt werden. Der vorliegende Regierungsentwurf (BT-Drs. 19/4674) sieht vor, dass es für die Datenverarbeitung im journalistischen Bereich weiterhin eine „anstaltsautonome Kontrolle“ des Datenschutzes bei der Deutschen Welle gibt und hierzu ein Beauftragter für den Datenschutz der Deutschen Welle als zuständige Aufsichtsbehörde im Sinne des Artikel 51 Absatz 1 DSGVO eingerichtet wird. Der Gesetzesentwurf führt jedoch hinsichtlich der übrigen Verarbeitungen zu wirtschaftlich-administrativen Zwecken eine neue Kontrollzuständigkeit für mich ein. Denn Artikel 85 Absatz 2 DSGVO lässt nur dann bestimmte Ausnahmen von der DSGVO zu, als dies erforderlich ist, um das Recht auf Schutz personenbezogener Daten mit dem Recht auf Meinungs- und Informationsfreiheit in Einklang zu bringen. Für die Datenverarbeitung im wirtschaftlich-administrativen Bereich ist eine solche Ausnahme nicht erforderlich. Schon in der Übergangszeit – bis das 2. DSAnpUG-EU in Kraft tritt – sehe ich mich für die Datenschutzaufsicht über die Deutschen Welle zumindest im wirtschaftlich-administrativen Bereich als zuständig an. Dies ergibt sich mangels abweichender Regelungen schon aus § 9 Absatz 1 Satz 1 BDSG i. V. m. § 1 Absatz 1 des Deutsche-Welle-Gesetzes (DWG) und § 2 Absatz 1 BDSG, da die Deutsche Welle eine öffentliche Stelle des Bundes ist.

10.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

11 Ausschuss für Recht und Verbraucherschutz

11.1 Aus den Gesetzgebungsvorhaben

11.1.1 Gesetz zur Stärkung des fairen Wettbewerbs

Eine abschliessende gerichtliche Klärung des Verhältnisses zwischen Wettbewerbsrecht und DSGVO muss weiterhin bestehende Unsicherheiten beenden. Eine gesetzliche Einschränkung der Möglichkeiten zu einer missbräuchlichen Nutzung von Abmahnungen halte ich parallel für sinnvoll.

Die Anwendbarkeit der DSGVO am 25. Mai 2018 ging insbesondere bei kleinen und mittleren Unternehmen einher mit der Angst vor massenhaften und missbräuchlichen Abmahnungen aufgrund unterstellter Verstöße gegen die DSGVO. Die gefürchtete Abmahnwelle ist zwar ausgeblieben, die Unsicherheit aber noch nicht beseitigt. Die Frage, ob wettbewerbsrechtliche Abmahnungen von Verstößen gegen die DSGVO nach dem Gesetz gegen den Unlauteren Wettbewerb (UWG) zulässig sind, ist in der Literatur umstritten und von der Rechtsprechung noch nicht abschließend geklärt.

Zwischenzeitlich hat das BMJV in seinen Referentenentwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs eine Regelung aufgenommen, die den Anspruch auf Erstattung der Kosten von Abmahnungen für Mitbewerber bei Verstößen gegen sämtliche Informations- und Kennzeichnungspflichten im Internet ausschließt. Hierdurch wird zumindest jeder Anreiz für missbräuchliche Abmahnungen von Verstößen gegen die DSGVO-Vorschriften über Datenschutzerklärungen im Internet verhindert.

Angesichts dieser ungeklärten Rechtslage wird es wohl dem Europäischen Gerichtshof überlassen bleiben, abschließend über das Verhältnis zwischen Wettbewerbsrecht und DSGVO zu entscheiden.

11.1.2 Strafprozessordnung Teil 1 – Verfassungs- und Europarecht verlangen Änderungen

In seinem Urteil über das Bundeskriminalamtgesetz (BKAG) hat das Bundesverfassungsgericht im Jahr 2016 genaue verfassungsrechtliche Vorgaben beschrieben, wie die Ermittlungsbehörden mit Daten aus heimlichen Ermittlungsmaßnahmen umzugehen haben (vgl. dazu 26. TB Nr. 1.3). Darüber hinaus ist die Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) in Kraft getreten (vgl. Nr. 2.1). Beides ist in der Strafprozessordnung (StPO) noch umzusetzen. Dieses Ziel wird mit dem derzeit vorliegenden Gesetzentwurf nicht erreicht.

Strafverfahrensdateien nach § 483 StPO

§ 483 StPO ist eine praktisch sehr bedeutsame und zentrale Vorschrift für die Datenverarbeitung in strafrechtlichen Ermittlungsverfahren. Ihre Zweckbindung wird mit dem neuen Gesetzentwurf (Stand 31.12.2018) wesentlich gelockert und führt zu verfassungsrechtlich bedenklichen Ergebnissen.

§ 483 StPO betrifft bereits in der geltenden Fassung nicht nur Verdächtige und Beschuldigte oder gar nur „Täter“. Nach dieser Vorschrift können die Behörden auch umfangreiche Daten zu Zeugen, Hinweisgebern, Geschädigten und sonstigen Dritten speichern. Die Menge der zulässigen Daten ist unbegrenzt. Damit können bereits jetzt sehr umfangreiche Dateien angelegt werden, die Informationen im Millionenbereich enthalten. Beispiele sind Daten aus Rasterfahndungen, Funkzellenabfragen etc. Ebenso sind umfangreiche Datenbestände zu einzelnen Personen möglich, die auch sensible Informationen enthalten können, zum Beispiel zu Opfern von Sexualstraftaten.

Nach dem derzeitigen § 483 StPO dürfen die Strafverfolgungsbehörden die personenbezogenen Daten allerdings nur in „einer Datei“ und für „ein bestimmtes“ Strafverfahren speichern. Das schließt nach meiner Auffassung verfahrensübergreifende Dateien auf Grundlage des § 483 StPO aus (vgl dazu 26. TB Nr. 10.2.9.3).

Durch die vorgesehene Neufassung können die Daten dagegen auch in den Informationssystemen der Polizeibehörden gespeichert werden. Dies impliziert bei extensiver Auslegung eine übergreifende Speicherung und birgt deshalb die Gefahr deutlich weitergehender und damit verfassungsrechtlich unzulässiger Auswertungen.

Entgegen meinen Stellungnahmen in der Ressortabstimmung wurden die mit der Änderung verbundenen datenschutzrechtlichen Probleme nochmals verschärft. Dort, wo das polizeiliche Datenschutzrecht derzeit noch Grenzen setzt, könnte der geplante § 483 StPO künftig gleichsam wie ein Generalschlüssel wirken. Dies betrifft auch Menschen, die nach den Vorgaben des BKAG nicht im Informationssystem gespeichert werden dürften. Deren Daten können künftig in die Informationssysteme der Polizeibehörden diffundieren, ohne dass Inhalt und Umfang der Datenverarbeitung normenklar und verhältnismäßig festgelegt wären. Das ist verfassungsrechtlich nicht tragfähig.

Zweck einer Datei kann es entweder sein, eine konkrete Aufgabe zu erfüllen oder für künftige Fälle auf Vorrat zur Verfügung zu halten. Der bisherige § 483 StPO dient nur für den erstgenannten Zweck. Er will den Ermittlungsbehörden ein Hilfsmittel für das jeweilige konkrete Strafverfahren zur Verfügung stellen. Dort ist es auch gerechtfertigt, größere Datenmengen zu speichern, weil sie nicht auf Vorrat für die Zukunft vorgehalten werden. Es geht nicht darum, den übergreifenden unbegrenzten Austausch von Informationen zu ermöglichen. Wenn der Gesetzentwurf dies nun ändert, dann schafft er einen völlig neuen Zweck. Dann dienen die Daten auch der Prävention, für die eigentlich speziellere Vorschriften gelten – etwa die zum Informationsverbund nach dem BKAG. Eine derart umfassende Vorratsspeicherung ist nicht zu rechtfertigen.

V-Leute und Datenflüsse an Nachrichtendienste

Das Bundesverfassungsgericht hat den Einsatz von Vertrauenspersonen als schwerwiegenden Grundrechtseingriff eingestuft. Deshalb sei eine hinreichend normenklare und bestimmte Rechtsgrundlage notwendig (BVerfG NJW 2017, 1681, 1790, Rn. 160). Der StPO fehlt seit langem eine entsprechende Vorschrift. Leider wird jetzt die Gelegenheit versäumt, dies nachzuholen. Dies ist nicht nur schlecht für den Datenschutz; es besteht auch das Risiko, dass Beweise in Ermittlungsverfahren wegen schwerwiegender Delikte nicht rechtssicher erhoben werden können und am Ende einer verfassungsrechtlichen Prüfung nicht standhalten.

Zu unbestimmt sind auch die Regeln über den Datenaustausch mit den Nachrichtendiensten. Dies betrifft zum einen die Frage, wie von V-Leuten ermittelte Daten aus polizeilichen oder nachrichtendienstlichen Zusammenhängen in den Strafprozess eingeführt werden sollen, sei es als Beweismittel oder als Anknüpfungstatsache. Dafür fehlt eine klare Erhebungsgrundlage auf Seiten der Strafverfolgungsbehörden. Die Regelung für die umgekehrte Richtung – in der Daten der Strafverfolgungsbehörde an den Nachrichtendienst fließen – ist zu ungenau und enthält keine ausreichenden Schwellen. Sie verweist pauschal auf das Nachrichtendienstrecht. Übermittlungsschwelle sind lediglich „tatsächliche Anhaltspunkte dafür (…), dass die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist." Das Bundesverfassungsgericht hat Übermittlungsvorschriften, die das informationelle Trennungsprinzip berühren, aber lediglich auf die Aufgabenerfüllung abstellen, als nicht ausreichend angesehen (BVerfG NJW 2013, 1499, 1505 und 1518, Rn. 126 und 232). Der Grundsatz der hypothetischen Datenneuerhebung ist ebenfalls nicht berücksichtigt (dazu vgl. 26. Tb, Kasten b zu 1.3.).

Ressortabstimmung

Die Ressortabstimmung zum Gesetzentwurf war von besonderer Hektik geprägt. Für die Stellungnahme wurden überkurze Tagesfristen eingeräumt. Eine Beratung, an der alle beteiligten Ressorts und ich zu einem offenen Gedankenaustausch zusammenkommen konnten, hat nicht stattgefunden. Ich empfehle, in den Gesetzgebungsverfahren zu einem ergebnisoffenen und konstruktiven Dialog zurückzukehren. Meine Beratungsaufgabe kann ich nur wahrnehmen, wenn ich ordnungsgemäß beteiligt werde.

Ich empfehle, die Strafprozessordnung zu überarbeiten. Insbesondere sind die Erhebung und Nutzung von Daten, die von V-Leuten aus polizeilichen oder nachrichtendienstlichen Zusammenhängen ermittelt wurden, im Strafprozess nicht normenklar geregelt. Die Zusammenarbeit mit Verfassungsschutzbehörden bedarf ohnehin einer engeren und präziseren Regelung. Die Rechtsprechung des Bundesverfassungsgerichts ist insoweit umzusetzen.

11.1.3 Strafprozessordnung Teil 2 – Trojaner für Ermittler

Vor der Umsetzung der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) hat der Gesetzgeber die Strafprozessordnung (StPO) erheblich geändert. Zunächst war der entsprechende Entwurf zur Änderung der StPO datenschutzrechtlich eher unscheinbar, aber im parlamentarischen Verfahren wurde auf Grundlage einer sogenannten Formulierungshilfe des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) eine Rechtsgrundlage für Online-Durchsuchung und Quellen-Telekommunikati-

onsüberwachung („Quellen-TKÜ“) eingefügt (umgangssprachlich „Bundestrojaner“). Und die hat es in sich.

Onlinedurchsuchung und Quellen-TKÜ

Die frühere Vorschrift zur Telekommunikationsüberwachung in der StPO war keine ausreichende Grundlage, um die sogenannte Quellen-TKÜ durchzuführen. Viele Ermittlungsrichter und Staatsanwaltschaften waren anderer Auffassung. Für die Online-Durchsuchung war dies aber unstreitig. Beide Maßnahmen hat der Gesetzgeber den Ermittlungsbehörden jetzt mit der Novellierung der StPO erlaubt.

Die Online-Durchsuchung wird landläufig als „Trojaner“ der Ermittlungsbehörden bezeichnet. Technisch gesehen kommt dabei eine Software der Ermittlungsbehörden zum Einsatz, die der weitverbreiteten Schadsoftware ähnelt. Die Behörden können damit Endgeräte der Verdächtigen infiltrieren und dort gespeicherte oder anders verarbeitete Daten auslesen. Das Bundesverfassungsgericht hat für diese stark in Grundrechte eingreifenden Maßnahmen ähnliche Hürden gesetzt, wie für die akustische Wohnraumüberwachung („großer Lauschangriff“). Die Quellen-TKÜ ist technisch ähnlich. Ermittlungsbehörden benötigen diese, wenn die Beschuldigten zum Beispiel verschlüsselt telefonieren. Dann nützt die klassische Überwachung der Übertragungswege nämlich nichts. Sie ist aber anders als die Online-Durchsuchung nicht darauf ausgerichtet, gespeicherte Inhalte auszulesen. Sie darf ausschließlich dazu dienen, die mit einem Gerät durchgeführte „laufende Telekommunikation“ zu überwachen.

Genau an dieser Stelle überschreitet der Gesetzentwurf die verfassungsrechtlichen Grenzen, obwohl davor in einer Anhörung im Bundestag klar gewarnt wurde.

Nach dem neuen § 100a Absatz 1 StPO darf die Behörde auch auf dem System der betroffenen Person gespeicherte Daten auslesen, wenn diese Gegenstand **früherer** Kommunikation waren. Die vorgeschlagene Formulierung lässt den Datenzugriff nämlich bereits für den Fall einer nur hypothetischen Überwachung zu („wenn sie auch während des laufenden Überwachungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.“). An dieser Stelle wird die Quellen-TKÜ zur echten Online-Durchsuchung, ohne aber deren verfassungsrechtliche Grenzen einzuhalten. Die Strafverfolgungsbehörden können deshalb außerhalb der laufenden Kommunikation gespeicherte E-Mail-Postfächer, WhatsApp-Daten, gespeicherte SMS, Anruflisten des Mobiltele-

fons etc. auslesen. Auch der Übertragungsvorgang in die Cloud oder aus der Cloud ist ein Telekommunikationsvorgang. Damit können die Ermittlungsbehörden nach dem Wortlaut auch solche Informationen vom Zielrechner auslesen, die zwischenzeitlich bei einem der Dienste gespeichert bzw. wieder zurückgeholt worden sind (z. B. selbst verfasste Textentwürfe, Tagebücher, Fotos u.v.m.). Man könnte also sagen, dass auf diese Weise ermöglicht wird, auch die Kommunikation der überwachten Person mit sich selbst zu erfassen. Dies gilt auch dann, wenn der Vorgang schon lange abgeschlossen ist. Denn nach dem Wortlaut genügt es ja, wenn die Daten Gegenstand früherer Kommunikation waren.

Rechtssystematisch steht die neue Regelung als Erhebung „alternativer Beweise" für eine grundlegende Zäsur. Sie führt die Figur des „hypothetischen Ersatzeingriffs" ad absurdum. Bislang ging es dabei um die Verwertung bereits vorhandener Erkenntnisse aus einer rechtswidrigen oder eingriffsintensiveren Maßnahme. Damit soll die Verwertung bereits vorhandener Daten verfassungskonform begrenzt werden. Die neue Regelung geht aber den umgekehrten Weg. Nunmehr soll auch die zukünftige – eigentlich nicht zulässige – heimliche Zwangsmaßnahme doch noch möglich gemacht werden. Die Ermittlungsbehörde soll sie darauf stützen dürfen, dass eine Maßnahme in der Vergangenheit mit anderen rechtlich zulässigen Mitteln hypothetisch möglich gewesen wäre. Das gleicht einer Regelung, die in etwa lautet: „Die Behörde darf Daten zur Not mit eigentlich unzulässigen Mitteln erheben, die sie auf andere Weise auch rechtmäßig hätte erheben dürfen".

Aus meiner Sicht wäre es nicht nötig gewesen, für die Quellen-TKÜ den gesamten Straftatenkatalog der „normalen" Telekommunikationsüberwachung zu öffnen. Angesichts der höheren Risiken dieser Maßnahme wäre eine stärkere Eingrenzung zu bevorzugen gewesen. Das Bundesverfassungsgericht hat allerdings dieselben Schranken bestimmt, wie sie allgemein für die Telekommunikationsüberwachung gelten.

Auch zur Regelung der Online-Durchsuchung hatte ich Empfehlungen geäußert. Abzulehnen ist etwa die geplante Reichweite, mit der auch nicht verdächtige Personen davon erfasst werden.

Bewährungshelfer

Angesichts der beschriebenen gravierenden Änderungen sind die weiteren datenschutzrechtlich kritischen Punkte der StPO-Novelle leicht zu übersehen: Dies betrifft etwa Daten, die Bewährungshelfer jetzt leichter an die Polizei übermitteln dürfen.

Schon nach alter Rechtslage durften diese in einer Notsituation die Polizei informieren. Ohne Notsituation mussten sie zuerst die Führungsaufsichtsstelle beim Gericht informieren, die dann den weiteren Informationsfluss steuerte. Der Weg, Daten direkt der Polizei zur Verfügung zu stellen, ist jetzt leichter geworden.

Für die Praxis ist zu befürchten, dass es zur „allgemeinen Gefahrenabwehr" etwa zu Kontrollmitteilungen kommen könnte. Derartige Kontrollmitteilungen o. ä. würden das austarierte System der Führungsaufsicht gefährden. Ebenso kann dies das Vertrauensverhältnis der Bewährungshelfer zu ihren Probanden gefährden – und damit letztlich auch den Erfolg der Resozialisierung.

11.1.4 Der Vorschlag für eine E-Evidence-Verordnung

Mit neuen Anordnungsmöglichkeiten soll die grenzüberschreitende Beweiserhebung grundlegend geändert werden. Dazu hat die Europäische Kommission mit dem Entwurf einer E-Evidence-Verordnung einen Vorschlag gemacht. Diesen lehne ich in seiner gegenwärtigen Fassung ab, weil danach die Justizbehörden am Sitz des Anbieters in der Regel nicht beteiligt werden und damit eine wesentliche Verfahrenssicherung fehlt.

Wenn sich in einem Strafverfahren ein Beweismittel im Ausland befindet, muss die ermittelnde Strafverfolgungsbehörde dort um Rechtshilfe ersuchen. Sollte sich an diesem Grundsatz im digitalen Zeitalter etwas ändern, nur weil „elektronische Beweismittel" ungeachtet des physischen Ortes ihrer Speicherung bzw. territorialer Grenzen nunmehr global verfügbar werden?

Die Europäische Kommission hat einen Vorschlag für eine neue Verordnung vorgelegt, mit der die Strafverfolgungsbehörden in den Mitgliedstaaten der Europäischen Union in strafrechtlichen Verfahren berechtigt wären, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und in Drittstaaten zur Übermittlung von Bestands-, Verkehrs- und Inhaltsdaten zu verpflichten. Die Anordnungen wären für alle Anbieter verbindlich, die ihre Dienste in der EU anbieten. Sollte das Unternehmen keinen Sitz in der EU haben, müsste es einen Repräsentanten bestimmen, dem die Anordnung zugestellt werden würde.

Ich habe Verständnis für das Anliegen der Kommission, mit dem vorgeschlagenen Verfahren strafrechtliche Ermittlungen beschleunigen zu wollen. Den Entwurf in seiner jetzigen Fassung lehne ich jedoch gemeinsam mit meinen Kollegen in den Ländern ab. Diese Position hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in einer Entschließung vom 7. November 2018 verabschiedet (abrufbar unter www.datenschutz.bund.de).

In einer ausführlichen Stellungnahme hat auch der Europäische Datenschutzausschuss unter meiner Mitwir-

kung eine Vielzahl von kritischen Fragen aufgeworfen, von denen ich in diesem Bericht nur einige nennen möchte. Die vollständige Stellungnahme ist abrufbar unter: www.datenschutz.bund.de

Ein wesentlicher Kritikpunkt betrifft die Umgehung der Justizbehörden des Staates, in dem der ersuchte Provider seinen Sitz hat. Von Ersuchen an Anbieter in Deutschland erhält die deutsche Justiz nur Kenntnis, wenn sich das Unternehmen weigert, die Daten zu übermitteln und von der Justizbehörde aus dem ersuchenden Mitgliedstaat zur Vollstreckung der Anordnung ersucht wird. Damit hängt es allein von dem Verhalten des ersuchten Providers ab, ob die Rechtmäßigkeit des Ersuchens außerhalb des ersuchenden Staates überprüft wird. Mir geht es dabei in keiner Weise darum, Providern fehlende Rechtskenntnis oder mangelndes rechtliches Gespür zu unterstellen. Richtig ist aber auch, dass sie eigene wirtschaftliche Interessen verfolgen und anderen Verpflichtungen als Justizbehörden unterliegen.

Problematisch ist auch, dass der Vorschlag die Herausgabe von Daten nicht mehr davon abhängig macht, ob die Tat im ersuchten Staat überhaupt strafbar ist. Es sind somit Fälle denkbar, in denen Unternehmen, die ihren Sitz in Deutschland haben, verpflichtet werden, Daten zur Verfolgung von Straftaten an andere europäische Ermittlungsbehörden zu übermitteln, die in Deutschland keine Straftaten sind, etwa bei politischen Meinungsäußerungen. Die Unternehmen könnten solchen Ersuchen widersprechen, wären ihrerseits allerdings von Sanktionen bedroht, wenn sie der Anordnung nicht nachkommen.

Zu befürchten ist auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Der Entwurf wird gegenwärtig im Rat der Europäischen Union und im Europäischen Parlament beraten.

11.A Zudem von besonderem Interesse

1.1, 1.2 f., 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

12 Ausschuss für Verkehr und digitale Infrastruktur

12.1 Aus Kontrolle und Beratung

12.1.1 Datenschutz bei der Untersuchung von Eisenbahn-, Flug- und Seeunfällen

Ich habe im Berichtszeitraum drei Informations-, Beratungs- und Kontrollbesuche durchgeführt, um verkehrsformübergreifend zu kontrollieren, ob im Zusammenhang mit der Untersuchung von Unfällen die bereichsspezifischen datenschutzrechtlichen Vorschriften eingehalten werden. Diese Kontrollen waren mir deshalb wichtig, weil im Bereich der staatlichen Unfalluntersuchung in erheblichem Umfang personenbezogene Daten verarbeitet werden, die – wie etwa die Gesundheitsdaten von Unfallopfern – besonders sensibel sind.

Bundestelle für Eisenbahnunfalluntersuchung

Die Bundesstelle für Eisenbahnunfalluntersuchung (BEU) hat Daten bei Stellen/Personen erhoben, die für die Erfüllung des Untersuchungsauftrags nach § 5b Absatz 1 AEG nicht erforderlich und damit nicht von der Erhebungsnorm des § 5c AEG gedeckt sind.

Ferner hat die BEU Daten bei Stellen/Personen erhoben, die nicht zu den in § 5c Absatz 1 AEG aufgeführten Stellen/Personen gehören, bei denen sie erheben darf. Damit sind auch diese Erhebungen nicht von § 5c AEG gedeckt.

Nach § 5e AEG sind ausschließlich Übermittlungen an öffentliche Stellen zulässig. Dennoch hat die BEU Daten an Stellen übermittelt, die keine öffentlichen Stellen sind.

Bereits während des Besuchs bestand Einvernehmen, dass die BEU in geeigneter Form (etwa durch eine Hausanordnung) sowie Schulungen,

- die Beachtung des § 5c AEG sicherstellt und Musteranforderungsschreiben entwirft, in denen benannt wird, welche personenbezogenen Daten der BEU übersandt werden dürfen und welche Passagen vor der Übersendung unkenntlich zu machen sind,
- die Beachtung der Übermittlungsvorschrift des § 5e AEG sicherstellt. Die BEU hat mir mitgeteilt, dass sie eine erste Schulung bereits durchgeführt hat und eine hausinterne Arbeitsgruppe eingesetzt hat, die entsprechende Musteranforderungsschreiben entwerfen soll.

Schließlich hat die BEU tagesscharfe Löschfristen nach § 5f AEG nicht eingehalten. Stattdessen löschte sie die Daten jeweils mit Ablauf des Jahres, in dem die Aufbewahrungsfristen nach § 5f Absatz 1 AEG enden. Schon während des Besuchs bestand Einvernehmen, dass die BEU einen tagesscharfen Löschautomatismus implementiert. Die BEU hat dies mittlerweile umgesetzt.

Bundesstelle für Flugunfalluntersuchung

Die Bundesstelle für Flugunfalluntersuchung (BFU) erhebt bei der Aufgabenerfüllung in nicht unerheblichem Maße besondere Arten personenbezogener Daten nach § 3 Absatz 9 BDSG (alt) (z. B. Gesundheitsdaten). Durch klar strukturierte und eingeschränkte Zugriffe, wird den datenschutzrechtlichen Anforderungen grundsätzlich Rechnung getragen. Auf meine Anregung zur weiteren Verbesserung der Datensicherheit hat die BFU intern geeignete Maßnahmen durch personalisierte verschließbare Postfächer sowie durch einen optimierten Zugangsschutz zum Archivbereich der Behörde ergriffen.

Hinsichtlich datenschutzrechtlicher Fragen auf Grundlage internationaler Regelungen, konnte ich mich von einer gesetzeskonformen Umsetzung überzeugen.

Bundesstelle für Seeunfalluntersuchung

Gegenstand des Kontrollbesuchs bei der Bundesstelle für Seeunfalluntersuchung (BSU) war die Verarbeitung personenbezogener Daten nach dem Gesetz zur Verbesserung der Sicherheit der Seefahrt durch die Untersuchung von Seeunfällen und anderen Vorkommnissen (SUG) sowie die organisatorische Einbindung und Aufgabenwahrnehmung der behördlichen Datenschutzbeauftragten nach § 4f Absatz 3 Satz 1 und 2 BDSG (alt).

Es wurde Handlungsbedarf in Bezug auf die Stellung und Einbindung der behördlichen Datenschutzbeauftragten identifiziert. Außerdem fehlten schriftliche Regelungen zum Datenschutzkonzept, zum Verfahrensverzeichnis sowie zur Zutrittskontrolle.

Meinen Empfehlungen folgend hat die BSU inzwischen mitgeteilt, dass die behördliche Datenschutzbeauftragte förmlich bestellt und im erforderlichen Umfang freigestellt wurde. Das Datenschutzkonzept der BSU liegt mir vor. Mit den Vorbereitungen für die Erstellung des Verfahrensverzeichnisses wurde begonnen.

12.A Zudem von besonderem Interesse

1.1, 1.6, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

13 Verteidigungsausschuss

13.1 Aus den Gesetzgebungsvorhaben

13.1.1 Änderung des Soldatengesetzes

§ 58c Soldatengesetz (SG) sieht vor, dass die Meldebehörden dem Bundesamt für das Personalmanagement der Bundeswehr (BAPersBW) den Namen und die gegenwärtige Adresse aller Personen mit deutscher Staatsangehörigkeit, die im darauffolgenden Jahr 18 Jahre alt werden, zum Zweck der Versendung von Informationsmaterial über Tätigkeiten in den Streitkräften übermitteln. Dies sehe ich kritisch.

Im Rahmen der Beratungen zum Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (vgl. hierzu unter Nr. 1.1), in dessen Rahmen auch der § 58c SG an die DSGVO angepasst werden sollte, habe ich diese Bedenken gegenüber dem Gesetzgeber geäußert. Aus meiner Sicht ist der Bedarf an einer bereichsspezifischen Sonderregelung für die Bundeswehr nicht überzeugend dargelegt worden, zumal ich nicht erkennen kann, warum die Datenübermittlung der Meldebehörden an das BAPersBW zur Erfüllung einer rechtlichen Verpflichtung oder aus Gründen des öffentlichen Interesses erforderlich ist.

Unabhängig von der von mir geforderten gesetzlichen Änderung bin ich auch für die datenschutzrechtliche Kontrolle der konkreten Handhabung des § 58c SG zuständig. Ich habe mehrere Beschwerden von Personen erhalten, weil das BAPersBW ihnen Postkarten mit Informationen über eine Tätigkeit in den Streitkräften zugeschickt hat. Den auf den Postkarten angegebenen Datenschutzhinweis hielt ich für missverständlich, da er nicht vollständig gewesen ist. So fehlte der Hinweis auf die Möglichkeit, von dem BAPersBW die Löschung der Daten zu verlangen. Das BAPersBW hat mir mittlerweile mitgeteilt, dass es meinen Hinweis in der Zukunft berücksichtigen möchte, und die Regelung des § 58c Absatz 3 SG zur Klarstellung in das Informationsschreiben aufnehmen wird. Dies begrüße ich ausdrücklich.

Ich rate Jugendlichen, die keine Werbung der Bundeswehr erhalten möchten, der Datenübermittlung bei den Meldebehörden zu widersprechen. Liegt ein solcher Widerspruch vor, ist eine Übermittlung der Kontaktdaten an das BAPerBW unzulässig (§ 36 Abs. 2 Bundesmeldegesetz; § 58c Abs. 1 SG). Hat die Übermittlung von der Meldebehörde an das BAPersBW bereits stattgefunden, rate ich den betroffenen Personen, die Löschung ihrer Daten beim BAPersBW zu beantragen, wenn sie keine Werbung erhalten wollen.

13.2 Aus Kontrolle und Beratung

13.2.1 Beratungs- und Kontrollbesuch im Bundeswehrkrankenhaus Ulm

Institutionelle Stärkung des Datenschutzes im Sanitätsdienst der Bundeswehr

Im Berichtszeitraum habe ich einen Beratungs- und Kontrollbesuch im Bundeswehrkrankenhaus Ulm durchgeführt. Schwerpunkt der Kontrolle war dessen datenschutzrechtliche Organisation. Als Ergebnis des Besuchs hat das Bundeswehrkrankenhaus umfangreiche Maßnahmen zur Verbesserung des Datenschutzes und zur Umsetzung der einschlägigen Regelungen der DSGVO getroffen. So wurde u. a. die für die Verarbeitung von Patientendaten der Zivilpatientinnen und Zivilpatienten maßgebliche Zentrale Dienstvorschrift umfangreich überarbeitet und an die Vorgaben der DSGVO angepasst.

Mit der Erstellung und Anpassung von Informationsblättern kommt das Bundeswehrkrankenhaus auch seinen Informationspflichten nach der DSGVO nach. Von mir sehr begrüßt wurde die in Folge meines Beratungs- und Kontrollbesuchs vom Bundesministerium der Verteidigung begonnene Einrichtung einer Außenstelle der Beauftragten für den Datenschutz im Kommando Sanitätsdienst (vgl. hierzu auch Nr. 9.3.12).

13.A Zudem von besonderem Interesse

1.1, 1.4 ff., 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

14 Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung

14.1 Einzelthemen

14.1.1 Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag

Die Vorschriften der DSGVO gelten entsprechend auch für den Deutschen Bundestag, die Fraktionen und die Abgeordneten. Eine datenschutzrechtliche Aufsicht findet hingegen nicht statt.

Mit Anwendbarkeit der DSGVO zum 25. Mai 2018 stellte sich die Frage, inwieweit die Vorschriften der DSGVO für den Deutschen Bundestag, die Fraktionen und Ausschüsse sowie einzelne Abgeordnete gelten und ob sie meiner datenschutzrechtlichen Aufsicht unterstehen (vgl. auch o. Nr. 1.1). Die vorgenannten Stellen verarbeiten personenbezogene Daten zu vielfältigen Zwecken. So werden beispielsweise Daten von Bürgerinnen und Bürgern im Rahmen von Petitionen oder Anfragen (z. B. aus den Wahlkreisen) verarbeitet. Gleiches gilt bei der Öffentlichkeitsarbeit, etwa über die eigene Homepage oder die vielfältigen Aktivitäten von Abgeordneten in sozialen Netzwerken. Nicht zuletzt sind Abgeordnete auch Arbeitgeberinnen und Arbeitgeber und verarbeiten auch auf diese Weise personenbezogene Daten ihrer Beschäftigten. Diejenigen Verarbeitungen, die im Zusammenhang mit der legislativen Tätigkeit stehen, fallen allerdings nicht in den Anwendungsbereich des Unionsrechts. Die DSGVO gilt insoweit nicht unmittelbar, sondern über § 1 Absatz 8 BDSG entsprechend. Im Ergebnis ist also auch bei diesen Verarbeitungen die DSGVO zu beachten. Da der Deutsche Bundestag, die Fraktionen und Ausschüsse sowie einzelne Abgeordnete öffentliche Stellen des Bundes sind, bin ich für diese sachlich zuständig (§ 9 BDSG). Im Bereich der legislativen Tätigkeit, für den die DSGVO im Range einfachen Bundesrechts gilt, darf ich allerdings keine Aufsichtsbefugnisse ausüben. Verfassungsrechtliche Vorgaben, namentlich der Grundsatz der Gewaltenteilung (Art. 20 Abs. 2 S. 2 GG) und des freien Mandats (Art. 38 Abs. 1 S. 2 GG), stehen dem entgegen. Indes nehme ich auch in diesem Bereich meine Beratungsaufgaben wahr.

Für die Zukunft empfehle ich dem Deutschen Bundestag, sich eine eigene Datenschutzordnung unter Beachtung der Vorgaben der DSGVO zu geben. Die Datenschutzordnung sollte auch ein internes Datenschutzkontrollgremium vorsehen, das Beschwerden von Betroffenen zur Verarbeitung ihrer personenbezogenen Daten entgegennehmen und bearbeiten könnte. Entsprechende Regelungen gibt es beispielsweise in Schleswig-Holstein.

Um den Abgeordneten die drängendsten Fragen zur DSGVO zu beantworten, habe ich eine Handreichung erstellt, die im Dezember 2018 an die Abgeordneten verschickt wurde. Die Handreichung kann auch auf meiner Internetseite unter (https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/BfDIBeraetAbgeordneteBT.html?cms_templateQueryString=Handreichung&cms_sortOrder=score+desc) abgerufen werden.

14.A Zudem von besonderem Interesse

1.1, 17.9, Die Arbeit des BfDI in Zahlen

15 Ausschuss für Wirtschaft und Energie

15.1 Aus den Gesetzgebungsvorhaben

15.1.1 Wirrwarr ob der weiteren Anwendbarkeit des 7. Teils des Telekommunikationsgesetzes

Die Anpassung des Telekommunikationsgesetzes (TKG) an die DSGVO steht in den Sternen, nachdem die Bundesregierung den entsprechenden Gesetzentwurf kurzfristig und ohne Angaben von Gründen zurückgezogen hat.

Seit dem 25. Mai 2018 ist die DSGVO anzuwenden. Als unmittelbar geltende europäische Verordnung geht sie dem nationalen Datenschutzrecht grundsätzlich vor. Etwas anderes gilt nur, wenn nationale Vorschriften aufgrund einer Kollisionsregel, eines Umsetzungsauftrages oder einer Öffnungsklausel der DSGVO vorrangig anwendbar sind. Die nationalen Datenschutzvorschriften des TKG sind nur noch insoweit anzuwenden, als die betreffenden Vorschriften der Umsetzung der E-Privacy Richtlinie (Richtlinie 2002/58/EG) dienen (vgl. Artikel 95 DSGVO). So richtet sich beispielsweise die Verarbeitung von Bestandsdaten, also von Kundendaten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden (§ 3 Nr. 3 TKG), seit dem 25. Mai 2018 überwiegend nach der DSGVO. Einzelheiten, wann die DSGVO und wann das TKG auf einen Sachverhalt anzuwenden ist, sind aber nach wie vor unklar. Dies ist darauf zurückzuführen, dass der 7. Teil des TKG bis heute nicht an die neue Rechtslage angepasst wurde und sich dort irreführenderweise immer noch Vorschriften finden, die wegen des Anwendungsvorrangs der DSGVO seit dem 25. Mai 2018 nicht mehr anzuwenden sind. In der Folge führt dies bei Unternehmen und Kunden zu großer Rechtsunsicherheit. Viele Betroffene haben sich deshalb im Berichtszeitraum an mich gewandt und um Unterstützung bei Rechtsfragen gebeten. Neben der Durchführung von zahlreichen Beratungsgesprächen mit TK-Unternehmen und der Bearbeitung von Bürgeranfragen habe ich deshalb auch mehrfach direkt den Gesetzgeber auf die zwingend erforderliche, zeitnahe Anpassung des TKG hingewiesen. In den ersten Referentenentwürfen für das 2. DSAnpUG-EU war daraufhin zunächst die erforderliche Anpassung des TKG noch vorgesehen. Doch wurde diese dann kurzfristig und ohne Angabe von Gründen nicht weiter verfolgt (vgl. auch unter Nr. 1.1). Hier besteht seitens des Gesetzgebers dringender Handlungsbedarf.

15.1.2 Die langen Geburtswehen der E-Privacy-Verordnung

Über die Reform der E-Privacy-Richtlinie habe ich bereits im 26. TB (Nr. 17.2.4.1) berichtet und mit der Vorstellung des Entwurfes der Europäischen Kommission am 11. Januar 2017 geendet. Die sich seitdem im Gesetzgebungsverfahren befindliche E-Privacy-Verordnung (E-Privacy-VO) soll den Umgang mit Daten und Informationen im Rahmen der elektronischen Kommunikation regulieren und die DSGVO bereichsspezifisch konkretisieren.

Die Entwicklungen in der elektronischen Kommunikation schreiten in hohem Tempo voran – gerade deshalb ist die Verordnung für die Wahrung der Privatsphäre in diesem Bereich von größter Bedeutung. Insofern war der ursprünglich vorgesehene Zeitplan, die E-Privacy-Verordnung zeitgleich mit der DSGVO in Kraft zu setzen, eine durchaus sinnvolle Überlegung, um den schnellen technologischen Innovationen die notwendigen rechtlichen Anpassungen zeitnah folgen zu lassen.

Die Arbeitsgruppe Telekommunikation & Informationsgesellschaft des Europäischen Rates diskutiert seit Februar 2017 den Kommissionsentwurf – bisher ohne abschließendes Ergebnis. Der Rat hat zwischenzeitlich mehrere Entwürfe zur weiteren Diskussion vorgelegt. Insbesondere die letzten Entwürfe lassen eine stufenweise Aufweichung der Vorschriften zu Lasten des Datenschutzes erkennen und eine Ausgewogenheit zwischen den berechtigten Interessen von Nutzern und Wirtschaft vermissen.

- Besonders augenscheinlich wird dies am Beispiel des Artikels 6, dessen Katalog von Erlaubnistatbeständen zur Verarbeitung elektronischer Kommunikationsdaten in vielerlei Hinsicht erweitert werden soll. Kritisch sehe ich z. B. die Vorschläge zur Einführung eines an Artikel 6 Absatz 4 DSGVO angelehnten Erlaubnistatbestandes zur Verarbeitung von Daten zu einem anderen Zweck als dem Erhebungszweck. Eine solche Norm stellt eine nicht hinzunehmende Ausnahme vom datenschutzrechtlichen Zweckbindungsgrundsatz dar und trägt dem sensiblen Charakter elektronischer Kommunikationsdaten, die vom Fernmeldegeheimnis des Artikel 10 GG geschützt sind, nicht angemessen Rechnung.
- Ich habe mich mehrfach dagegen ausgesprochen, den Zugang der Nutzer zu bestimmten Online-Diensten von einer datenschutzrechtlichen Einwilligung des Nutzers abhängig zu machen. Derartige Cookie-Walls erfüllen nicht die Anforderungen an eine freiwillige Einwilligung. Ansonsten müssten finanziell schlechter gestellte Nutzer mit ihren Daten bezahlen oder auf bestimmte Angebote, wie Informationen aus Online-Medien, sogar verzichten. Es ist mir ein wichtiges Anliegen, dass der Zweck von Artikel 8, dem Nutzer die Herrschaft über seine Endeinrichtungen zu geben, nicht unterlaufen wird.

Ich setze mich dafür ein, die Grundsätze von Privacy by Design und Privacy by Default stärker in die Verordnung zu verankern. Deshalb unterstütze ich Artikel 10 des vom Parlament verabschiedeten Entwurfs, wonach Privacy by Design durch datenschutzfreundliche Voreinstellungen bei der Installation von Software umgesetzt werden soll.

Zur Unterstützung und Beschleunigung der Verhandlungen hat die Artikel-29-Gruppe im April 2017 eine erste Bewertung des Entwurfs veröffentlicht (Opinion 01/2017 – WP 247 der Artikel-29-Gruppe). Am 28. Mai 2018 hat der Europäische Datenschutzausschuss (EDSA) eine weitere Stellungnahme zum aktuellen Gesetzgebungsverfahren herausgegeben. Ziel der Veröffentlichung war die Klärung spezifischer Fragen, die durch die vorgeschlagenen Änderungen der gesetzgebenden Organe aufgeworfen worden waren. Der EDSA fordert u. a., dass durch die neue Verordnung das Einwilligungserfordernis für Cookies und ähnliche Technologien durchgesetzt werden muss und dass Diensteanbieter technische Tools für das Einholen der Einwilligung anbieten müssen. Zudem betont er, dass die kommende Verordnung keinesfalls hinter dem aktuell geltenden Schutzniveau zurückbleiben darf.

Auf nationaler Ebene hat es zwischenzeitlich viele Ressortgespräche gegeben, in denen meine Position leider nicht von allen Seiten geteilt wird. So hat der Vertreter Deutschlands in einer öffentlichen Sitzung der EU-Mitgliedstaaten am 8. Juni 2018 in Brüssel gefordert, „dass die Nutzung werbefinanzierter Online-Dienste davon abhängig gemacht werden kann, dass der Nutzer in das Setzen von Cookies für Werbezwecke einwilligt“. Damit wurde meine Forderung und die der Landesdatenschutzbeauftragten ignoriert, die wir bereits am 5. Februar 2015 in der Entschließung unter dem Titel „Keine Cookies ohne Einwilligung“ veröffentlicht hatten. Hintergrund für diese deutsche Position mögen die Stakeholder-Meetings mit Interessensvertretern der Wirtschaft und NGOs gewesen sein. So hat das Bundesministerium für Wirtschaft und Energie beim hauseigenen WIK Institut ein Gutachten zu den Auswirkungen des Kommissionsentwurfs auf die Internet-/Werbewirtschaft erstellen lassen, in welchem ausschließlich Stakeholder aus dem Umfeld der Digitalen Wirtschaft, der Verlage und der Online-Werbewirtschaft befragt wurden. In meiner Pressemitteilung vom 1. Dezember 2017 zu dieser Studie habe ich thematisiert, dass an keiner Stelle auch nur ansatzweise die potenziellen Chancen, die sich für die Branche aufgrund der von mir favorisierten Änderungen ergeben könnten, betrachtet wurden und bereits deutlich kritisiert, dass der Datenschutz nicht von kommerziellen Erwägungen gesteuert sein darf.

Erfreulich ist, dass die Bundesregierung meine Position teilt, dass die E-Privacy-Verordnung auch nach Empfang der Kommunikation und nach Beendigung der Übertragung greifen soll. Dieser Punkt ist ein Manko des Kommissionsentwurfes, der den Daten nur während der Übertragung Schutz zukommen lassen will.

Um im Bereich der elektronischen Kommunikation einen der DSGVO entsprechenden Rechtsrahmen zu schaffen, muss die E-Privacy-Verordnung schnellstens verabschiedet werden. Die aktuelle Anwendung der auf der Grundlage der Richtlinie 2002/58/EG erlassenen nationalen Vorschriften trägt den gegenwärtigen Entwicklungen nicht mehr angemessen Rechnung und stiftet Rechtsunsicherheit – und zwar für alle Beteiligten. Immer wieder ergeben sich Fragen zur Anwendbarkeit des nationalen Rechts neben der DSGVO (vgl. hierzu auch Nr. 15.1.1 und Nr. 15.2.4).

Telemedien: Cookies und mehr

Noch vor dem 25. Mai 2018 erhielt ich sowohl aus dem Bereich der Telekommunikationsdienstleister als auch von öffentlichen Stellen des Bundes diverse Beratungsanfragen mit der Bitte um Klärung, nach welchen Regelungen sich künftig der Einsatz von Cookies richtet. Auch von Bürgern gingen zahlreiche Fragen bei mir ein, inwieweit das Cookie-Setzen unter der DSGVO überhaupt noch zulässig sei. Meine Kollegen in den Ländern haben hier ähnliche Erfahrungen gemacht.

Nachdem den Datenschutzaufsichtsbehörden im März 2018 bekannt wurde, dass das Telemediengesetz (TMG) nicht Teil des Entwurfes eines Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes-EU sein wird, hat sich eine Unterarbeitsgruppe der Datenschutzkonferenz (DSK), an der ich beteiligt bin, unmittelbar damit auseinandergesetzt, wie sich im Bereich der Telemedien die Rechtslage unter Berücksichtigung der DSGVO und dem nicht angepassten TMG gestaltet. Unsere Positionierung zum TMG, das in den §§ 11 bis 15a datenschutzrechtliche Regelungen für das Verhältnis zwischen Anbietern und Nutzern von Telemedien enthält, wurde am 26. April 2018 in der DSK verabschiedet und anschließend veröffentlicht (abrufbar unter www.datenschutz.bund.de).

Demzufolge können die speziellen datenschutzrechtlichen Vorschriften des TMG neben der DSGVO nicht weiter angewendet werden, insbesondere da es sich bei den Vorschriften nicht um eine Umsetzung der E-Privacy-Richtlinie handelt, werden sie nicht über die Regelung von Artikel 95 DSGVO fortgelten. Ob eine Verarbeitung personenbezogener Daten auch im Bereich der Telemedien rechtmäßig ist, beurteilt sich daher nunmehr anhand der DSGVO.

Um mit den betroffenen Unternehmen und Verbänden in einen Meinungsaustausch zu treten, hat die DSK im Sommer 2018 ein Konsultationsverfahren eröffnet. Von dieser Möglichkeit haben 19 Verbände/Unternehmen Gebrauch gemacht. Im Oktober 2018 wurden einzelne Beteiligte zu einem Gespräch mit verschiedenen Datenschutzaufsichtsbehörden eingeladen, um mit ihnen ihre Auffassungen aus dem schriftlichen Konsultationsverfahren zu diskutieren. Nunmehr soll von der Unterarbeitsgruppe eine Kommentierung der Positionsbestimmung finalisiert und von der DSK den betroffenen Kreisen zur Verfügung gestellt werden. Dies ist deshalb wichtig, weil die E-Privacy-Verordnung noch länger auf sich warten lässt und auch mit einer Anpassung des TMG in naher Zukunft nicht zu rechnen ist. Zum Schutz der Daten der Nutzer werde ich auf eine schnelle Veröffentlichung hinarbeiten.

Ich rate dringend, die E-Privacy-Verordnung schnellstmöglich zu verabschieden. Die aktuelle Anwendung der auf der Grundlage der Richtlinie 2002/58/EG erlassenen nationalen Vorschriften trägt den gegenwärtigen Entwicklungen nicht mehr angemessen Rechnung und schafft Rechtsunsicherheit für alle Beteiligten. Dies betrifft insbesondere das Verhältnis zwischen dem deutschen Telekommunikationsgesetz und der DSGVO.

15.1.3 Neue Gesetze und Verordnungen im Bereich der Telekommunikation

Viele der kleineren, aber für die Privatsphäre der Bürger mitnichten unbedeutenden Rechtssetzungsvorhaben im Bereich der Telekommunikation erfolgten auf Wunsch der Sicherheitsbehörden. Dabei wurden meine Bedenken nicht immer aufgegriffen. Dies zeigen die nachfolgenden Beispiele.

Überprüfung der Richtigkeit der für Sicherheitsbehörden gespeicherten Anschlussinhaberdaten

Das von der Bundesnetzagentur (BNetzA) in einer Amtsblattverfügung geregelte Verfahren zur Validierung der Identität der Inhaber von Prepaid-Karten nach § 111 Absatz 4 Telekommunikationsgesetz (TKG) wurde im Berichtszeitraum mehrfach geändert. Dabei wurden u. a. die Regelungen zum Video-Ident-Verfahren ergänzt und die von mir in meinem 26. TB (Nr. 17.2.4.2) kritisierte Verpflichtung gestrichen, 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 muss.

Telekommunikations-Überwachungsverordnung (TKÜV)

Die Änderung der TKÜV, über die ich in meinem 26. TB (Nr. 12.2.2) berichtet habe, ist zum 21. Juni 2017 in Kraft getreten (BGBl. I 2017 S. 1657). Nach dem ursprünglichen Entwurf sollten Telekommunikationsüberwachungsanordnungen nicht mehr per Fax übermittelt werden, was ich in meinem letzten TB als positiven Aspekt hervorgehoben hatte. Diese Form der Übermittlung ist weniger sicher und erfordert eine anschließende Übersendung des Originals. Leider sah der Bundesrat dies anders und hat diese Änderung verhindert.

Neue Befugnisse der Netzbetreiber aus Gründen der Cyber-Sicherheit

Die NIS-Richtlinie (Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen) möchte das Sicherheitsniveau von Netz- und Informationssystemen stärken und nimmt hierzu u. a. die Netzbetreiber in die Pflicht. Das nationale Gesetzgebungsverfahren zur Richtlinienumsetzung wurde zugleich dazu genutzt, die Befugnisse der Netzbetreiber in § 100 Absatz 1 TKG zu erweitern. Mit den neuen Regelungen soll es den Netzbetreibern erleichtert werden, auf Angriffe und Störungen ihrer Netze zu reagieren. Diese im Innenausschuss erstmals eingebrachte Gesetzesänderung dürfte von einem medienwirksamen Angriff auf Router inspiriert worden sein, der zu signifikanten Ausfällen von Telefonanschlüssen bei einem großen

deutschen Telekommunikationsdiensteanbieter geführt hatte. Ein zentraler Teil dieser Änderungen betrifft eine Erlaubnis, die „Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, [zu] erheben und [zu] verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen."

Bereits in meinem 23. TB (Nr. 6.5) hatte ich über den Bedarf der Netzbetreiber für einen solch tiefen Blick in die Kommunikation und im 25. TB (Nr. 8.8.5) über entsprechende Kontrollen berichtet, die ich durchgeführt hatte. Insofern begrüße ich die neuen klaren Regelungen. Jedoch stellt sich nach wie vor die Frage, wo im Einzelfall die Steuerdaten aufhören und die Inhalte der Kommunikation beginnen. Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der Diensteanbieter dem betrieblichen Datenschutzbeauftragten unverzüglich und am Quartalsende auch der BNetzA und mir berichten. Dabei ist keine Einschränkung auf Steuerdaten informationstechnischer Systeme im Gesetzestext zu erkennen, also sind auch nicht automatisierte Verwendungen von Verkehrsdaten zu melden.

In diesem Zusammenhang stellte sich für mich auch die Frage, ob es praktisch keine manuellen Auswertungen gibt oder ob die Meldepflicht einfach weitestgehend ignoriert wird. Obwohl ich die Telekommunikationsdienstleister mehrfach auf diese Berichtspflicht hingewiesen habe, habe ich nur vereinzelte Meldungen erhalten. Eine Einschränkung der Meldepflicht z. B. auf Steuerdaten eines informationstechnischen Protokolls und – nach Vorbild von § 100 Absatz 2 TKG – eine Meldung nur an den betrieblichen Datenschutzbeauftragten, der die Meldungen noch aufbewahrt, würde ich begrüßen.

Des Weiteren wurden in § 109a TKG Möglichkeiten zur Umleitung und Sperrung von Daten eröffnet. Diese Maßnahmen dürften im Allgemeinen sinnvoll sein, können aber auch zu Problemen führen. Wenn ein Netzbetreiber feststellt, dass über den Anschluss des Teilnehmers Viren verbreitet werden und er deshalb den Datenverkehr auf eine Benachrichtigungsseite umleitet, kann dies unter Umständen die Verfügbarkeit anderer Dienste oder Anwendungen, beeinträchtigen. Ebenso darf der Verkehr zu Störquellen, z. B. zum Server oder einer Seite, die Teile eines Schadprogramms nachladen, eingeschränkt werden. Auch hier kann eine zu großzügige Sperrung die Verfügbarkeit anderer Dienste beeinträchtigen. Solche Mittel sollten daher mit Bedacht eingesetzt werden.

15.1.4 Die Datenschutzaufsicht über die Postdienstleister – wer muss hier welches Päckchen tragen?

Die Anpassung des Postgesetzes an die DSGVO hat mehrere Änderungen mit sich gebracht. Diese betreffen nicht nur inhaltliche Fragestellungen, sondern auch die konkrete Durchführung der Datenschutzaufsicht.

Gegenstand des Entwurfes eines Zweiten Datenschutzanpassungs- und Umsetzungsgesetzes-EU (2. DSAnpUG-EU) zur Anpassung datenschutzrechtlicher Vorschriften an die DSGVO, waren auch das Postgesetz (PostG) und die Postdienste-Datenschutzverordnung (PDSV). Ziel war es, auf die Vorgaben der auch im Anwendungsbereich des PostG unmittelbar anwendbaren DSGVO zu verweisen, einzelne fortgeltende postspezifische Regelungen von der PDSV ins PostG zu überführen und die PDSV aufzuheben.

In datenschutzrechtlicher Hinsicht gibt es aber einige kritische Punkte, die ich während des gesamten Gesetzgebungsverfahrens immer wieder zum Ausdruck gebracht habe und die leider bis heute nicht aufgegriffen wurden.

Postgesetz neu: Unterschiedliche Regelungen für natürliche und juristische Personen

Die Anpassung der datenschutzrechtlichen Vorschriften im Postrecht an die DSGVO darf nicht zum Anlass genommen werden, das bisherige, sich aus dem PostG und der PDSV ergebende Datenschutzniveau abzusenken. Deshalb ist m. E. weiterhin am datenschutzrechtlichen Gleichlauf von natürlichen und juristischen Personen festzuhalten. Die in der Vergangenheit angestellten Erwägungen für die Einführung des einfachgesetzlichen, auch für juristische Personen geltenden, Postgeheimnisses durch das PostG i. V. m. der PDSV tragen auch heute noch. Die Vorschriften wurden im Zuge der Privatisierung der Post und der Aufgabe des staatlichen Postmonopols geschaffen. Da es sich bei den Postdienstleistungen um vormals hoheitlich erbrachte Leistungen der Daseinsvorsorge handelt, die ursprünglich dem Fernmeldegeheimnis (Art. 10 GG) unterlagen, hat der Bundesgesetzgeber eine einfachgesetzliche Ausprägung des Postgeheimnisses geschaffen, damit auch bei der Leistungserbringung durch Private weiterhin vergleichbare Datenschutzstandards gelten.

Daher habe ich mich im Berichtszeitraum besonders dafür eingesetzt, dass auch bei der Anpassung der postrechtlichen Vorschriften an die DSGVO die dem Postgeheimnis unterliegenden Einzelangaben über juristische Personen bei der Erbringung geschäftsmäßiger Postdienste den personenbezogenen Daten gleichgestellt bleiben. Die Regelung zur Gleichstellung der Einzelangaben über juristische Personen ist unter Berücksichti-

gung von Erwägungsgrund 14 der DSGVO zulässig, denn dort wird lediglich klargestellt, dass sich die unmittelbare Geltung der DSGVO nicht auf juristische Personen erstreckt. Daraus ergibt sich für den nationalen Gesetzgeber, dass er außerhalb des Anwendungsbereichs der DSGVO Regelungen erlassen kann, die auch darin bestehen können, die DSGVO-Normen für juristische Personen anwendbar zu erklären.

Es sollten daher die Vorgaben der DSGVO, des BDSG und des geänderten PostG auf die dem Postgeheimnis unterliegenden Einzelangaben über juristische Personen entsprechend Anwendung finden.

Befugnisse und Erfüllungsaufwände

Mit der DSGVO und insbesondere der Anpassung des PostG an die DSGVO verschieben sich die datenschutzrechtlichen Zuständigkeiten von der Bundesnetzagentur (BNetzA) zu mir. Künftig bin ich alleinige Aufsichtsbehörde für den Datenschutz im Postbereich. Dies umfasst dann aber nicht mehr (nur) die Kontrolle der ca. 1.100 in Deutschland lizensierten Postdienstleister. Zusätzlich obliegt mir die datenschutzrechtliche Aufsicht und Kontrolle von ca. 60.000 nicht lizenz-, sondern nur anzeigepflichtigen Postdienstleistern, die bislang ausschließlich durch die BNetzA kontrolliert wurden. Und auch die zahlreichen Beschwerden zum Themenkomplex Datenschutz im Postbereich werden künftig alle bei mir zu bearbeiten sein – eine Herausforderung für die Kapazitäten meines Hauses. Nach Artikel 52 Absatz 4 DSGVO hat jeder Mitgliedsstaat der EU sicherzustellen, dass die Datenschutzaufsichtsbehörden mit den personellen Ressourcen ausgestattet werden, die sie für die effektive Wahrnehmung ihrer Aufgaben und Befugnisse benötigt. Im Hinblick auf die Datenschutzaufsicht über die nur anzeigepflichtigen Postdienstleister bin ich mit dem BMWi und der BNetzA im Gespräch, die hierfür bislang bei der BNetzA vorgehaltenen Planstellen zu erhalten. Leider ist die Umsetzung der entsprechenden Stellen noch nicht erfolgt.

15.1.5 Schaffung des rechtlichen Fundaments für ein Bewacherregister

Bei der Errichtung eines Bewacherregisters ist das Gebot der Verhältnismäßigkeit zu beachten. Es galt erneut zu vermeiden, dass der Gesetzgeber hier über das Ziel hinaus schießt.

Schon das (erste) Gesetz zur Änderung bewachungsrechtlicher Vorschriften (BGBl. I 2016, S. 2456), das die Grundentscheidung zur Einführung eines Bewacherregisters traf, ist von mir kritisch gesehen worden (vgl. 26. TB Nr. 17.2.2). Ziel dieses Gesetzes war es, in bestimmten sicherheitsrelevanten Bereichen des Bewachungsgewerbes sämtliche dort eingesetzten Personen einer erweiterten Zuverlässigkeitsprüfung zu unterziehen, indem diese in einem Bewacherregister erfasst und regelmäßig von den Verfassungsschutzbehörden überprüft werden.

Das Zweite Gesetz zur Änderung bewachungsrechtlicher Vorschriften enthält nunmehr einige Regelungen zur Ausgestaltung des Bewacherregisters, insbesondere, wessen Daten dort aus welchen Anlässen, zu welchen Zwecken, wie lange und durch wen verarbeitet werden (BGBl. I 2018 S. 2666). Der von der Bundesregierung vorgelegte Entwurf bedurfte noch der Anpassung, um die Datenverarbeitungen auf das erforderliche Maß zu reduzieren. Meine Stellungnahme an den Ausschuss für Wirtschaft und Energie des Deutschen Bundestages führte hier noch zu einigen entscheidenden datenschutzrechtlichen Verbesserungen. So wurden beispielsweise Löschfristen aufgenommen, nach denen Negativeintragungen im Bewacherregister getilgt werden müssen. Ergänzende Regelungen zur Ausgestaltung des Bewacherregisters sind in Form von zwei Rechtsverordnungen zu treffen.

15.2 Einzelthemen

15.2.1 Videoidentifizierung

Im digitalen Zeitalter steigt der Bedarf nach sicheren Identifizierungsmöglichkeiten, die keine persönliche Anwesenheit erfordern, sondern online abgewickelt werden können. Wirtschaftsunternehmen, wie beispielsweise Online-Banken, aber auch Behörden setzen hier auf Verfahren zur Online-Identifizierung per Video-Chat. Das ist bequem, aber nicht ohne Risiko.

Zuletzt hat die Bundesnetzagentur die Videoidentifizierung als zulässige sonstige Identifizierungsmethode i. S. d. § 11 Absatz 1 Vertrauensdienstegesetz anerkannt. Dieses Gesetz regelt die nationale Durchführung der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung). Die eIDAS-Verordnung gibt einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung von elektronischen Identifizierungsmitteln und Vertrauensdiensten vor. Die elektronische Identifizierung baut auf einer einmaligen sicheren Erstidentifizierung auf, die in Deutschland nun teilweise per Video-Ident möglich ist. Allerdings bleibt das Ausstellen qualifizierter Zertifikate für die Website-Authentifizierung hiervon ausgeschlossen. Das Ausstellen qualifizierter Zertifikate für qualifizierte elektronische Signaturen bzw. qualifizierter elektronischer Siegel ist auf die Ausgabe von nur einmalig nutzbaren Zertifikaten (sog. Ad-Hoc-Zertifikate) beschränkt. Obwohl ich diese Einschränkungen des Nutzungsbereichs begrüße, wird mit

der grundsätzlichen Anerkennung der Videoidentifizierung ein falsches Signal für mögliche weitere Anwendungsfälle der Videoidentifizierung gesetzt.

Bereits in meinem 25. TB hatte ich der Bundesregierung empfohlen, für die Identifizierung von Kunden nach dem Geldwäschegesetz auf die Möglichkeiten einer Videoidentifizierung zu verzichten. Schon damals war nicht sichergestellt, dass die anfallenden personenbezogenen Daten datenschutzkonform verarbeitet werden. Diese Aussage hat weiterhin Bestand.

Die Videoidentifizierung weist nicht das gleiche Sicherheitsniveau auf, wie die Identifizierung unter Anwesenden. Eine Dokumentenprüfung ist nach dem heutigen Stand der Technik in einem Videokanal nicht vollumfänglich möglich. Daher kann bei einer Videoidentifizierung noch schlechter als bei der Identifizierung vor Ort unterschieden werden, ob ein Ausweisdokument echt ist oder eine Fälschung vorliegt (vgl. hierzu auch unter Nr. 6.1.2). Da die Integrität der zur Identifizierung herangezogenen Daten maßgeblich für jedwede sichere Identifizierungsmethode ist, bei der Videoidentifizierung aber nicht erfüllt werden kann, lehne ich diese Identifizierungsmethode ab.

Datenschutzrechtlich problematisch ist zudem, dass durch die Aufnahme und Speicherung von Videosequenzen komplette Kopien der Ausweisdokumente angefertigt werden. Diese sehr umfänglichen Aufzeichnungen von personenbezogenen Daten entsprechen nicht dem für die Verarbeitung personenbezogener Daten geltenden Grundsatz der Erforderlichkeit und der Datensparsamkeit, da mehr Daten gespeichert werden, als für eine Identifikation erforderlich wären. Auch dies spricht gegen die Videoidentifizierung.

Unbestreitbar ist durch die zunehmende Digitalisierung in der Zukunft eine sichere Methode für die Identifizierung unter Abwesenden unverzichtbar. Ein sicheres Verfahren bietet hier die eID-Funktion des Personalausweises bzw. des elektronischen Aufenthaltstitels. Anstelle der Videoidentifizierung sollten diese Funktionen genutzt werden.

15.2.2 Akkreditierung – eine neue Aufgabe

Die DSGVO sieht in Artikel 43 eine Akkreditierung von Zertifizierungsstellen vor. Das Akkreditierungsverfahren bildet eine wesentliche Grundlage für zuverlässige und vertrauenswürdige Datenschutzzertifizierungen und kann somit ganz erheblich zu einem gestärkten und europaweit einheitlichen Datenschutz beitragen. Jetzt kommt es auf die effektive nationale Ausgestaltung der hierfür notwendigen Verfahren an.

Zertifizierungen sind eine Möglichkeit, wie Unternehmen oder Behörden freiwillig nachweisen können, dass sie bei Verarbeitung personenbezogener Daten die datenschutzrechtlichen Vorgaben der DSGVO einhalten. Artikel 42 DSGVO enthält die dafür wesentlichen Regelungen, auf deren Grundlage die Mitgliedstaaten aktuell in enger Zusammenarbeit die geforderten Mechanismen und Kriterien entwickeln. Erste Grundlagenarbeit dazu wurde bereits in der Artikel-29-Gruppe geleistet. Die Finalisierung entsprechender Richtlinien findet aktuell im Europäischen Datenschutzausschuss (EDSA) statt.

Entscheidende Voraussetzung für ein effektives Zertifizierungsverfahren ist, dass nur solche Stellen Zertifizierungen gemäß Artikel 42 DSGVO erteilen dürfen, die im Hinblick auf das hierfür notwendige Fachwissen überprüft und anschließend förmlich akkreditiert worden sind. Artikel 43 DSGVO sieht deshalb eine Akkreditierung von Zertifizierungsstellen als Schnittstelle zwischen staatlichem und privatem Handeln vor, die dem Zweck der Konformitätsprüfung und der Qualitätssicherung dienen soll.

Im Zuge der nationalen Umsetzung des Akkreditierungsprozesses hat sich auch für die deutschen Datenschutzaufsichtsbehörden ein zentraler neuer Aufgabenbereich ergeben. Nach § 39 BDSG soll die Deutsche Akkreditierungsstelle (DAkkS) die Entscheidung über eine Akkreditierung im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde treffen. Die weiteren Regelungen dazu sind im Akkreditierungsstellengesetz (AkkStelleG) festgelegt.

Vor Beginn des eigentlichen Akkreditierungsprozesses sind gemäß Artikel 57 Absatz 1 Buchstabe p) DSGVO entsprechende Kriterien für die Akkreditierung festzulegen und zu veröffentlichen. Auf nationaler Ebene arbeiten die Datenschutzaufsichtsbehörden des Bundes und der Länder seit einiger Zeit intensiv an der Entwicklung der entsprechenden Vorgaben. Diese müssen anschließend zur Genehmigung an den EDSA übermittelt werden und sind eng an die Vorgaben der dort bereits verabschiedeten Leitlinien zu Akkreditierung angelehnt.

Der Ablauf des anschließenden Akkreditierungsprozesses kann grob wie folgt skizziert werden (vgl. hierzu auch Schaubild zu Nr. 15.2.2):

Am Beginn steht die Antragsphase für die Programmprüfung, die zunächst von der DAkkS koordiniert wird, bei der die zuständige Aufsichtsbehörde bereits die Information über den Eingang eines Antrags und alle eingereichten Unterlagen erhält. Das Zertifizierungsprogramm enthält die zentralen Vorgaben für den Zertifizierungsprozess. Qualitativ hochwertige Zertifizierungskriterien sind eine fundamentale Voraussetzung für den

Erfolg und die Reputation eines Zertifikates. Gerade deshalb ist die Prüfung des eingereichten Programms und der darin enthaltenen Kriterien eine wichtige Grundlage für den weiteren Prozessablauf. Die nationale Akkreditierungsstelle prüft zunächst, ob bestimmte Normanforderungen (ISO/IEC 17065 und 17067) eingehalten werden. Danach erfolgt eine Fachprüfung durch die Datenschutzaufsichtsbehörde. Wenn beide Prüfungen erfolgreich verlaufen, kann in diesem Verfahrensschritt die Feststellung der Akkreditierungsfähigkeit des Zertifizierungsprogramms erfolgen.

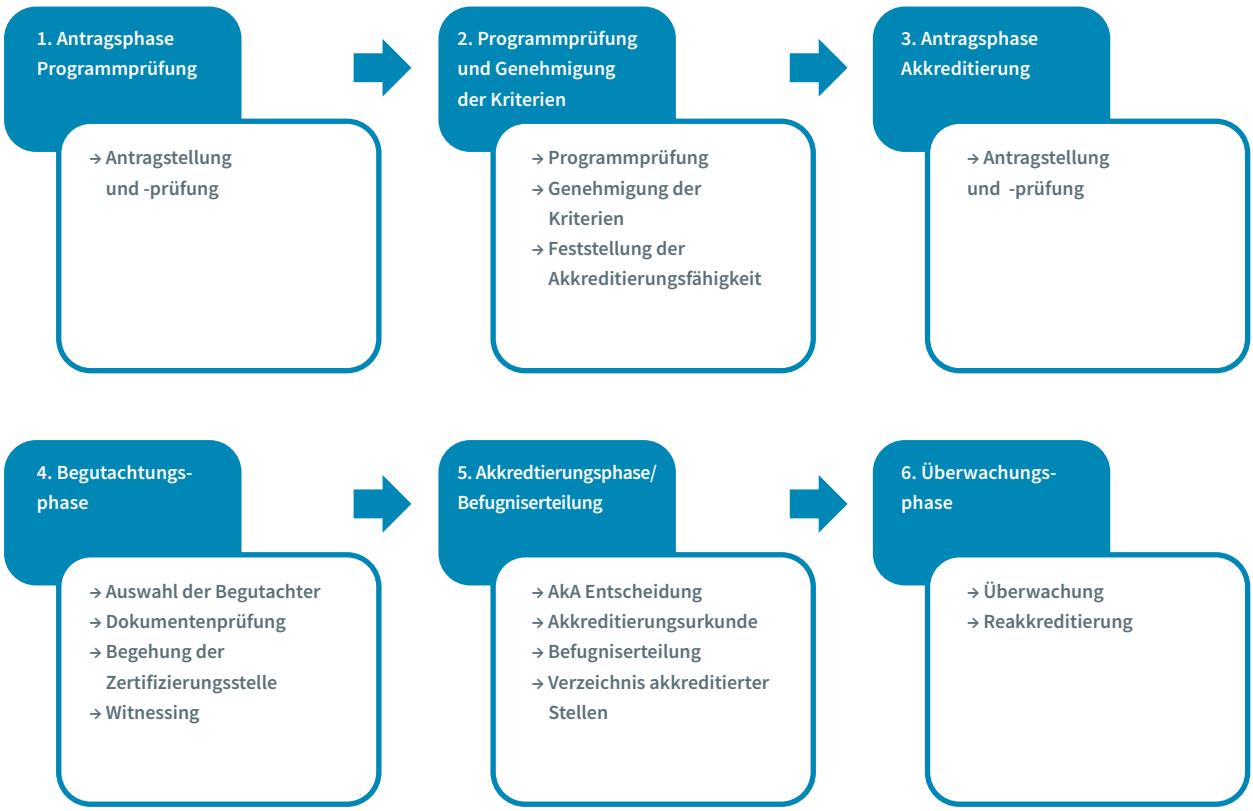
Der nächste Schritt beginnt mit der Einsendung des Akkreditierungsantrags. Wieder werden die Unterlagen geprüft und an die zuständige Aufsichtsbehörde weitergeleitet. Kern dieser Phase ist eine Begutachtung der Zertifizierungsstelle durch ein Gutachterteam. In der Regel prüfen die Gutachter zunächst die eingereichten Dokumente, anschließend findet eine Begehung vor Ort statt. Umfang und Dauer der Begutachtung sind von der Komplexität des jeweiligen Verfahrens abhängig.

Im Anschluss bewertet ein Akkreditierungsausschuss (AkA) die Begutachtungsergebnisse und entscheidet über die Erteilung der Akkreditierung. Der AkA setzt sich aus Mitgliedern der DAkkS sowie aus sach- und fachkundigen Personen zusammen, die Angehörige der die Befugnis erteilenden Behörden sind. Bei positiver Bescheidung wird eine Akkreditierungsurkunde ausgestellt und die Akkreditierung anschließend im Verzeichnis der akkreditierten Stellen bei der DAkkS gelistet. Den tatsächlichen Verwaltungsakt, die Befugnis als Zertifizierungsstelle tätig zu sein, erteilt die zuständige Aufsichtsbehörde der akkreditierten Stelle.

Eine Akkreditierung ist in der Regel fünf Jahre lang gültig. Um den Kompetenznachweis auch innerhalb dieser Zeit sicherzustellen, erfolgen Überprüfungen in festgelegten Intervallen. Informationen zu erteilten oder widerrufenen Zertifikaten leitet die Zertifizierungsstelle an die zuständige Aufsichtsbehörde weiter. Mit dem Auslaufen der Akkreditierung kann eine Zertifizierungsstelle einen Antrag auf Reakkreditierung stellen.

Nur ein belastbares, transparentes und zuverlässiges Akkreditierungsverfahren kann in Verbindung mit eindeutigen und offengelegten Zertifizierungskriterien letztlich glaubwürdige Zertifizierungen gewährleisten und das Vertrauen in den gesamten Zertifizierungsprozess stärken.

Schaubild Akkreditierungsprozess zu Nr. 15.2.2



15.2.3 Neue Listen für kritische IT-Verfahren

Die DSGVO verlangt von den Verantwortlichen, die Risiken abzuschätzen, die sich aus einer geplanten Verarbeitung personenbezogener Daten für die Rechte und Freiheiten der Betroffenen ergeben. Folgt aus dieser Abschätzung, dass die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat, etwa weil besonders sensible Daten davon erfasst werden, so sind die Verantwortlichen verpflichtet, eine ausführliche Abschätzung dieser Folgen durchzuführen und deren Ergebnisse, in einer sogenannten Datenschutz-Folgenabschätzung zu dokumentieren.

Für bestimmte Klassen von Verarbeitungstätigkeiten ist bereits in der DSGVO selbst festgelegt, dass für sie stets eine Datenschutz-Folgenabschätzung durchgeführt werden muss, etwa bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche. Die DSGVO verpflichtet außerdem die Datenschutzaufsichtsbehörden, über die bereits in der DSGVO selbst enthaltene Aufzählung hinaus eine Liste von Verarbeitungsvorgängen zu erstellen, für die in jedem Fall eine solche Datenschutz-Folgenabschätzung durchgeführt werden muss („Muss-Liste"). Sofern die betreffenden Verarbeitungsvorgänge einen „grenzüberschreitenden Charakter" haben, weil sie beispielsweise zu einem Angebot von Waren oder Dienstleistungen gehören, das sich an Personen aus mehreren EU-Mitgliedstaaten richtet, muss die betreffende Liste dem Europäischen Datenschutzausschuss (EDSA) vorgelegt werden, der eine Stellungnahme zu der Liste abgibt und gegebenenfalls Änderungen an der Liste fordern kann. Ziel ist es, im Rahmen des sog. Kohärenzverfahrens eine einheitliche Anwendung der DSGVO in allen EU-Mitgliedsstaaten sicher zu stellen.

Bereits vor Inkrafttreten der DSGVO haben die europäischen Datenschutzaufsichtsbehörden im Rahmen der Artikel-29-Gruppe ein Leitliniendokument erstellt. Diese Leitlinien nennen neun Merkmale, die zu einem hohen Risiko für die davon Betroffenen führen können (vgl. hierzu auch Kriterien zur Datenschutz-Folgeabschätzung). Treffen für eine Verarbeitung zwei dieser Kriterien zu, so muss der Verantwortliche in der Regel davon ausgehen, dass die Verarbeitung ein hohes Risiko für die Betroffenen mit sich bringt, und ist infolge dessen verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen. Für meine eigene „Muss-Liste", die den öffentlichen Bereich der Bundesverwaltung abdeckt, habe ich die Vorgehensweise aus dem WP 248 direkt übernommen.

Die deutschen Datenschutzaufsichtsbehörden hatten im Frühjahr 2018 damit begonnen, eine gemeinsame „Muss-Liste" für Verarbeitungstätigkeiten im nicht-öffentlichen Bereich zu erstellen. Dabei wurden die Kriterien aus dem WP 248 als Ausgangspunkt gewählt, jedoch besteht die gemeinsame „Muss-Liste" der deutschen Datenschutzaufsichtsbehörden aus einer Aufzählung konkret beschriebener Arten von Verarbeitungstätigkeiten. Diese gemeinsame Liste der deutschen Datenschutzaufsichtsbehörden hat inzwischen auch das Kohärenzverfahren im EDSA durchlaufen und wurde aufgrund der Stellungnahme des EDSA geringfügig angepasst.

Nach dem Stichtag 25. Mai 2018 haben außer den deutschen auch der Großteil der anderen europäischen Datenschutzaufsichtsbehörden für ihre jeweiligen „Muss-Listen" das Kohärenzverfahren initiiert. Die Auswertung der Listen und Vorbereitung der Stellungnahmen des EDSA erfolgte durch eine Unterarbeitsgruppe des EDSA. Als wichtigstes Resultat dieses Prozesses wurde vom EDSA bestätigt, dass das vorhandene Leitliniendokument WP 248 auch für die „Muss-Listen" der europäischen Datenschutzaufsichtsbehörden maßgeblich ist und dass jedes Element einer solchen Liste zwei der im WP 248 definierten Merkmale aufweisen muss. Außerdem wurde ein „gemeinsamer Kern" von Risikofaktoren beschlossen, die jede Datenschutzaufsichtsbehörde in ihre „Muss-Liste" aufnehmen muss, um eine möglichst einheitliche Anwendung der DSGVO in Europa zu erreichen. Dies betrifft die Verarbeitung biometrischer oder genetischer Daten, jeweils zusammen mit einem weiteren Kriterium aus dem WP 248.

Die Leitlinien des WP 248 geben zusammen mit den jeweiligen „Muss-Listen" den Verantwortlichen eine relativ verlässliche Anleitung an die Hand, mit der sie ermitteln können, ob eine geplante Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt. Trotzdem sei an dieser Stelle noch einmal darauf hingewiesen, dass für jede geplante Verarbeitungstätigkeit erneut geprüft werden muss, ob ein hohes Risiko vorliegt. Es ist durchaus denkbar, dass auch bei Verarbeitungstätigkeiten, die auf den ersten Blick keines der Kriterien aus dem WP 248 erfüllen und die auch in keiner „Muss-Liste" enthalten sind, ein hohes Risiko vorliegen kann. Die aktuellen Fassungen der Listen habe ich auf meiner Internetseite unter www.datenschutz.bund.de veröffentlicht.

Bisher liegen noch keine großen praktischen Erfahrungen sowohl mit den Kriterien des WP 248 als auch mit den „Muss-Listen" vor. Neue technologische Entwicklungen und Geschäftsmodelle können dazu führen, dass der Begriff eines möglicherweise hohen Risikos, das eine Verarbeitung personenbezogener Daten mit sich bringt, sich verändert. Sowohl das Leitliniendokument WP 248 selbst als auch die auf ihm beruhenden „Muss-Listen" dürften daher in gewissen Abständen eine Überarbeitung erfahren. Ich werde die Entwicklung auf diesem Gebiet aufmerksam verfolgen und mich an entsprechenden Überarbeitungsprozessen aktiv beteiligen.

Kriterien zur Datenschutz-Folgeabschätzung

Das Dokument „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (WP 248) nennt die folgenden neun Kriterien dafür, dass eine Verarbeitung personenbezogener Daten ein hohes Risiko für die Betroffenen mit sich bringt:

- Bewerten oder Einstufen (Scoring)
- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- Systematische Überwachung
- Vertrauliche oder höchst persönliche Daten
- Datenverarbeitung in großem Umfang
- Abgleichen oder Zusammenführen von Datensätzen
- Daten zu schutzbedürftigen Betroffenen
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
- Die Verarbeitung an sich hindert Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags.

Treffen auf eine Verarbeitung zwei dieser Kriterien zu, so muss der Verantwortliche in der Regel davon ausgehen, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringt und sollte daher in diesem Fall eine Datenschutz-Folgenabschätzung durchführen.

Verbindlich sind jedoch die jeweiligen „Muss-Listen“: Ist eine Verarbeitungstätigkeit in der „Muss-Liste“ der für einen Verantwortlichen zuständigen Datenschutzaufsichtsbehörde aufgeführt, so ist dieser in jedem Fall verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen.

15.2.4 Neues Verfahren zur Meldung von Datenschutzverletzungen

Für den Datenschutz im Bereich der Telekommunikation hat sich nicht nur der Rechtsrahmen, sondern auch das Meldeverfahren bei Datenschutzverletzungen geändert.

Die Pflicht, Datenschutzverletzungen der zuständigen Datenschutzbehörde zu melden, gab es bereits vor der DSGVO. Bislang war diese auf EU-Ebene durch zwei Richtlinien vorgegeben. Die Richtlinie 95/46/EG betraf den allgemeinen Datenschutz und die Richtlinie 2002/58/EG den Datenschutz in der elektronischen Kommunikation. Beide Richtlinien bedurften zunächst der Umsetzung in nationales Recht. Der deutsche Gesetzgeber hatte hier mit § 42a und § 1 Absatz 3 BDSG (alt) sowie § 109a Telekommunikationsgesetz (TKG) eine Lösung gefunden, wie sich die auf unterschiedlichen Richtlinien beruhenden Meldepflichten widerspruchsfrei in die deutsche Rechtsordnung einfügen ließen. Die seit dem 25. Mai 2018 anzuwendende DSGVO gilt als EU-Verordnung nunmehr unmittelbar und damit auch die allgemeine Meldepflicht nach Artikel 33 DSGVO. Parallel hierzu gilt im Telekommunikationsbereich weiterhin die Richtlinie 2002/58/EG und die zu ihrer Umsetzung geschaffene Meldepflicht für Telekommunikationsdiensteanbieter nach § 109a TKG.

Die Meldepflichten im Telekommunikationsbereich sind von großer praktischer Bedeutung. So gingen im Jahr 2017 knapp 830 Meldungen über Datenschutzverletzungen nach § 109a TKG bei mir ein, die aufgrund einer Vereinbarung mit der Bundesnetzagentur (BNetzA) je zur Hälfte durch mich und die BNetzA bearbeitet wurden. Nun muss in Abhängigkeit von den vom Datenschutzvorfall betroffenen Daten seit dem 25. Mai 2018 entweder nach Artikel 33 DSGVO ausschließlich an mich oder nach § 109a TKG an mich und an die BNetzA gemeldet werden. Dies führte

immer wieder zu Auslegungs- und Verfahrensfragen. Zur Klärung der offenen Punkte habe ich einen Workshop für die Telekommunikationsdiensteanbieter ausgerichtet, bei dem die Anwendung der beiden Meldepflichten erörtert und anhand praktischer Beispiele vertieft wurde.

Darüber hinaus habe ich in diesem Bereich bei der Wahrnehmung meiner Datenschutzaufsicht unterschiedliche Erfahrungen machen müssen. Nicht nur, dass es zu einer mengenmäßigen Verlagerung bei der Bearbeitung der gemeldeten Datenschutzverletzungen im Telekommunikationsbereich kam, weil sich die Zahl der Meldungen nach § 109a TKG drastisch reduzierte, während sich die Meldungen nach Artikel 33 DSGVO stark erhöhten (vgl. Die Arbeit des BfDI in Zahlen). Damit war zu rechnen. Das teilweise veränderte Meldeverhalten mancher Telekommunikationsdiensteanbieter erstaunte da schon deutlich mehr. So meldet ein großer Telekommunikationsdienstleister, der in Vergangenheit angeblich fast gar keine Datenschutzverletzungen zu melden hatte, seit Mai sehr regelmäßig. Ob dies wohl daran liegt, dass ich nach der DSGVO bei Verstößen gegen die Meldepflicht im Gegensatz zum TKG Bußgelder verhängen kann und hierfür ein gegenüber dem TKG wesentlich höherer Bußgeldrahmen besteht?

15.2.5 Digitale Geschäftsmodelle unter Nutzung von Mobilfunkdaten

Digitale Geschäftsmodelle, die auf der Nutzung von Mobilfunkdaten basieren, müssen unter der DSGVO neu bewertet werden.

Die Analyse digitaler Daten lässt zahlreiche Rückschlüsse auf das Verhalten der betroffenen Personen zu. Besonders aussagekräftig sind Verkehrsdaten – insbesondere Standortdaten – von mobilen Endgeräten. Die daraus gewonnenen Informationen können auf vielfältige Weise wirtschaftlich genutzt und verwertet werden. Denkbar ist z. B. die Nutzung von Standortdaten zur Analyse von Verkehrsströmen oder zu statistischen Zwecken (vgl. 22. TB Nr. 7.8).

Vielen Chancen stehen auch viele Risiken gegenüber

Die Auswertung derart sensibler Daten birgt freilich Risiken. Dies gilt in besonderem Maße im Big Data-Kontext, wenn verschiedene Daten in großer Menge miteinander verknüpft und ausgewertet werden können. Durch den Einsatz valider Anonymisierungstechniken können die damit verbundenen Risiken zwar verringert werden. Anonyme und anonymisierte Daten unterfallen außerdem nicht dem Anwendungsbereich des Europäischen Datenschutzrechts. Wie die Artikel-29-Gruppe in ihrer Stellungnahme vom 10. April 2014 jedoch festgestellt hat, ist es allerdings sehr schwer, aus einem umfassenden Bestand personenbezogener Daten einen tatsächlich anonymen Datenbestand zu generieren (WP 216, S. 3).

Anonym ist nicht gleich anonym!

Dabei kommt es entscheidend darauf an, wie hoch das Risiko der Re-Identifizierung ist (vgl. 25. TB Nr. 8.8.4; 26. TB Nr. 17.2.4.4), wobei gemäß Erwägungsgrund 26 Satz 5 der DSGVO sowohl die zum Zeitpunkt der Verarbeitung verfügbaren Technologien als auch technologische Entwicklungen zu berücksichtigen sind. Angesichts des rasanten technischen Fortschritts muss die Wirksamkeit vorhandener Anonymisierungstechniken dauerhaft überprüft werden. Sowohl für die Verantwortlichen als auch für die Aufsichtsbehörden ist damit die Herausforderung verbunden, den notwendigen Überblick über aktuelle technische Entwicklungen zu behalten.

Digitale Geschäftsmodelle müssen den Anforderungen des geltenden Rechts standhalten

Die rechtlichen Anforderungen an eine hinreichende Anonymisierung müssen unter der DSGVO neu beurteilt werden. Dasselbe gilt für die Frage, ob der Einsatz von Anonymisierungstechniken als solcher eine Verarbeitung personenbezogener Daten darstellt und deshalb einer Rechtsgrundlage bedarf. Den Geltungsbeginn der DSGVO bzw. die damit verbundene Änderung der Rechtslage habe ich zum Anlass genommen, um die digitalen Geschäftsmodelle, die auf der Nutzung von Mobilfunkdaten basieren, auf den Prüfstand zu stellen. Außerdem habe ich eine Diskussion im Kreis der deutschen Aufsichtsbehörden angestoßen, um auch insoweit eine einheitliche Anwendung geltender Rechtsbestimmungen sicherzustellen.

15.2.6 Nutzung von Messenger-Diensten

Die Telekommunikation muss längst nicht mehr nur mobil, sondern auch immer schneller von statten gehen. Hierfür werden dann gerne Messenger-Dienste genutzt. Dabei wird der Datenschutz von Anbietern wie von Nutzern der Apps oftmals vergessen.

Messenger-Dienste erfreuen sich immer größerer Beliebtheit und sind aus unserem Alltag nicht mehr wegzudenken. Insbesondere Unternehmen möchten zur Kommunikation mit ihren Kunden immer häufiger darauf zurückgreifen (vgl. hierzu o. Nr. 7.1.5).

Wie schon im 26. TB (Nr. 17.3.1) angedeutet, handelt es sich bei Messenger-Diensten meiner Rechtsauffassung nach um Telekommunikationsdienste in der Ausprägung sog. OTT (Over-the-top)-Dienste, bei denen die Kommunikation zwischen den Beteiligten über das offene Internet ohne eigene Infrastruktur erfolgt. Solche Dienste unterfallen als Äquivalent zur „klassischen" Telekommunikation im Diensteanbieter-Nutzer-Verhältnis dem Te-

lekommunikationsgesetz (TKG) bzw. der DSGVO. Gemäß § 115 Absatz 4 TKG obliegt die datenschutzrechtliche Aufsicht in Deutschland dabei meiner Behörde (vgl. Nr. 15.1.1), so dass ich mich auch schon in der Vergangenheit immer wieder mit dem Thema Messenger-Dienste auseinandersetzen musste.

Dabei stand in den letzten Jahren besonders der Dienst WhatsApp im Fokus. Wegen der Übermittlung von Nutzerdaten durch die WhatsApp Inc. an Facebook habe ich im Mai 2017 gegenüber der Bundesnetzagentur (BNetzA) eine Beanstandung ausgesprochen. Grund für die Beanstandung war, dass ich keine datenschutzrechtlich wirksame Einwilligung der Nutzer zur Übermittlung der Mobilfunknummer von der WhatsApp Inc. an Facebook erkennen konnte. Dies habe ich als Verstoß gegen §§ 95 Absatz 1 Satz 1 und 3, 94 TKG i. V. m. § 4a BDSG (alt) bewertet. Die Beanstandung und das daraufhin von der BNetzA durchgeführte Verwaltungsverfahren ist von dort nicht abschließend bearbeitet worden. Schließlich hat die BNetzA im August 2018 trotz eines noch nicht vollständig erledigten Verwaltungsverfahrens den Vorgang unter Verweis auf die DSGVO an mich zurückgegeben. Meines Erachtens hätte die BNetzA aber noch zu einer abschließenden Stellungnahme bzgl. des laufenden Beanstandungsverfahrens WhatsApp kommen und mir das Ergebnis mitteilen sollen, denn insoweit ist auf den Rechtszustand vor dem 25. Mai 2018 und den Verstoß gegen §§ 95 Absatz 1 Satz 1 und 3, 94 TKG i. V. m. § 4a BDSG (alt) abzustellen.

Den am stärksten verbreiteten Messenger-Dienst WhatsApp stufe ich derzeit nicht als datenschutzfreundlich ein. Besonders kritisch muss u. a. der potentielle Datenaustausch zwischen WhatsApp und Facebook hinterfragt werden. Dies gilt gleichermaßen im Hinblick auf die Erhebung von Telefonnummern mittels Adressbuchupload durch WhatsApp. Das Unternehmen kann auf diese Art alle Kontaktdaten eines Nutzers verarbeiten, die auf dessen Mobiltelefon hinterlegt sind und zwar unabhängig davon, ob der jeweilige Kontakt selbst WhatsApp nutzt oder nicht.

Zu WhatsApp liegen mir einige Beschwerden und Anfragen vor. Dabei geht es einerseits ganz allgemein um die Datenschutzbestimmungen des Dienstes, andererseits aber auch um nicht bzw. nicht ausreichend beantwortete Auskunftsersuchen und um die Frage, wie Widerspruch gegen eine Datenweitergabe eingelegt werden kann u.a.m.

Messenger-Dienste seit der Anwendbarkeit der DSGVO

Da die populärsten Messenger-Dienste häufig weder ihren Firmensitz noch eine Niederlassung in Deutschland haben, arbeite ich seit dem 25. Mai 2018 immer dann, wenn es um die Verarbeitung von Bestandsdaten geht, die der DSGVO unterliegen, intensiv mit der jeweils federführenden Datenschutzaufsichtsbehörde zusammen. Um dies an einem Beispiel zu verdeutlichen: Meldet sich ein Bürger wegen eines Datenschutzproblems bei mir und der Anbieter sitzt z. B. in den USA, hat aber eine Niederlassung in Irland, wie im Falle der WhatsApp Ireland Ltd., übernehme ich bei den sog. Verfahren der Zusammenarbeit (Artikel 56, 60 DSGVO) die Korrespondenz mit der federführenden Aufsichtsbehörde, und übermittele dieser alle zweckdienlichen Informationen. Sodann analysiert, untersucht und bewertet die federführende Aufsichtsbehörde den Vorgang. Dazu erhält sie nicht nur meine Stellungnahme als betroffene Aufsichtsbehörde, sondern fordert in aller Regel auch das betroffene Unternehmen zur Stellungnahme auf, um auf Basis dieser Erkenntnisse zu entscheiden. Bevor sie eine abschließende Entscheidung trifft, informiert sie mich und legt mir einen Entwurf zur Stellungnahme vor. Soweit die Beschwerde erfolgreich ist, unterrichte ich dann den Beschwerdeführer über den getroffenen Beschluss. Wenn ich mit der beabsichtigten Entscheidung nicht einverstanden bin, kann ich hiergegen Einspruch einlegen. Die federführende Behörde muss sich dann mit meinen Argumenten auseinandersetzen. Bleibt sie bei ihrer Auffassung darf sie den Bescheid dennoch nicht erlassen, sondern muss den Fall dem Europäischen Datenschutzausschuss vorlegen. Dieser trifft dann eine verbindliche Entscheidung.

Auf diese Art und Weise stimmen sich die Aufsichtsbehörden europaweit – in aller Regel über das europäische Binnenmarktinformationssystem (IMI) ab, um so auf ein datenschutzrechtlich einheitliches Niveau hinzuwirken. Natürlich ist das hohe Maß an Abstimmung zunächst einmal sehr aufwändig und auch zeitintensiv. Gerade in den ersten Monaten unter der DSGVO musste ich so manches Mal erfahren, wie sehr in den verwaltungsrechtlichen und verwaltungstechnischen Abläufen der Teufel im Detail steckt. Aber mit der Zeit stellt sich auch hier eine gewisse Verwaltungspraxis ein, so dass die Kooperationsverfahren der Beschwerden nun nach und nach anlaufen. Der weit überwiegende Teil der Verfahren betrifft die Zusammenarbeit mit der irischen Aufsichtsbehörde. Meine irische Kollegin ist aber wahrlich nicht zu beneiden, denn zahlreiche große amerikanische Konzerne haben ihre europäische Niederlassung in Irland und man kann sich leicht vorstellen, in wie vielen Kooperationsanfragen aus ganz Europa die Mitarbeiter dort gefragt sind.

Welchen Messenger-Dienst soll ich denn nun nutzen?

Diese Frage erreichte mich in den letzten Monaten unzählige Male. Unterschiedliche Messenger-Dienste werden von diversen Dienstleistern angeboten. Für welchen Dienst soll man sich nun entscheiden? Welchen Dienst

setzt das eigene soziale Umfeld ein? Welcher Dienst ist sicher und datenschutzgerecht oder welcher nicht? Welcher Dienst läuft auf meinen Endgeräten (Smartphone, Tablet oder Laptop und PC)?

Tatsache ist, dass der bekannteste und am weitest verbreitete Messenger-Dienst sowohl in Deutschland als auch im gesamten europäischen Raum der WhatsApp-Dienst des Unternehmens Facebook ist. Das heißt aber nicht, dass es keine Alternativprodukte im Hinblick auf Funktionalität oder Datenschutz gibt. Zu den gängigsten Messenger-Diensten gehören sicherlich Hoccer, Line, Signal, SIMSme, Skype, Telegram, Threema, Viber und Wire.

Die Entscheidung für oder gegen einen Messenger-Dienst kann aber letzten Endes nur jeder selbst – bzw. im beruflichen Umfeld der Arbeitgeber – treffen. Denn es hängt schließlich immer auch vom individuellen Nutzungszweck und den daraus resultierenden Anforderungen an Vertraulichkeit, Verschlüsselung, Datensicherheit, Löschfristen etc. ab, welcher Messenger-Dienst den Anforderungen am ehesten entspricht. Und leider gilt auch hier: Solange die E-Privacy-Verordnung (vgl. Nr. 15.1.2) nicht verabschiedet ist, sind viele Rechtsfragen der vertraulichen elektronischen Kommunikation noch nicht abschließend geklärt.

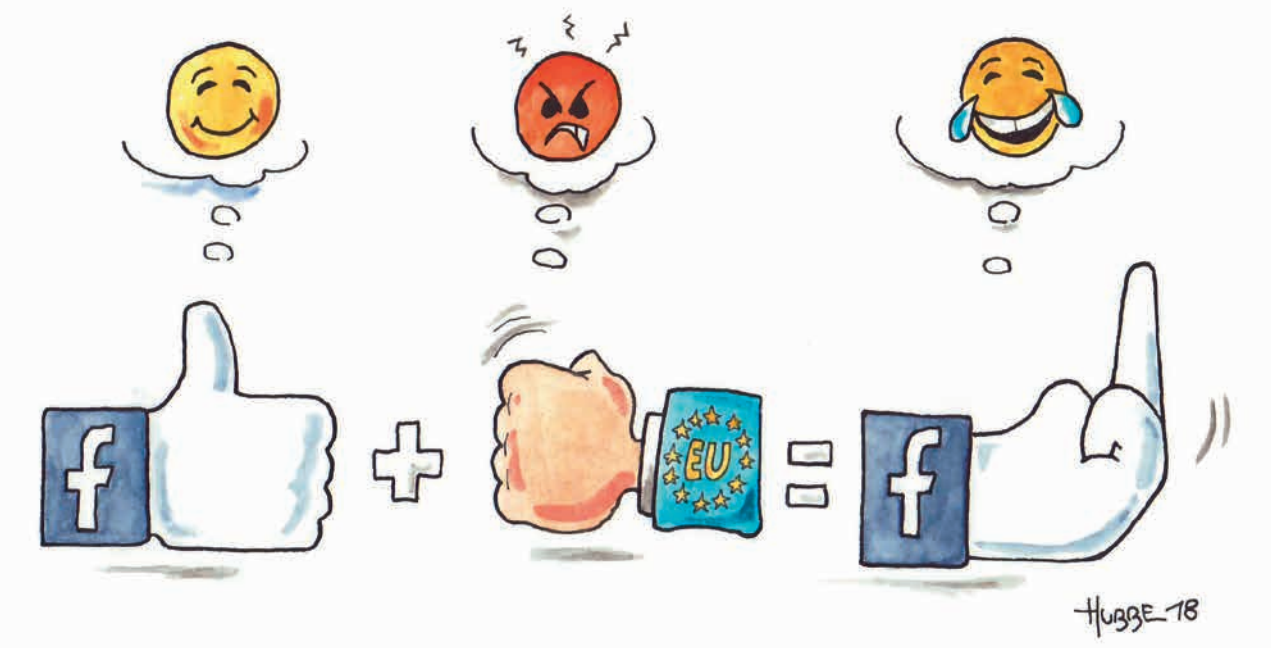
15.2.7 Datenschutz und Soziale Medien

Skandale, Skandale, Skandale, und doch greift der Einsatz Sozialer Medien immer mehr um sich. Als Aufsichtsbehörde bin ich hier in vielerlei Hinsicht gefordert.

Skandal: Was kümmert mich der Datenschutz?

Im Berichtszeitraum ist eine Vielzahl von Datenskandalen bei Sozialen Medien bekannt geworden. Besonders aufsehenerregend war der Fall um Cambridge Analytica, bei dem Daten von Facebook-Nutzern unrechtmäßig abgeflossen sind. In diesem Zeitraum habe ich mehrere Bundestagsausschüsse sowohl im Rahmen von Sitzungen als auch durch schriftliche Informationen über meine datenschutzrechtliche Einschätzung des Vorfalls informiert. Als wäre dieser Skandal noch nicht genug, wurde im September 2018 der sog. Facebook-Hack bekannt, bei dem Hacker Millionen Nutzerdaten erbeuteten. Im Dezember desselben Jahres wurde über eine weitere Sicherheitslücke berichtet, über die App-Entwickler kurzfristig auf Nutzerbilder sowie private Nachrichten zugreifen konnten.

Was den Datenschutz betrifft, sind auch andere Soziale Medien keine Musterknaben. Google hat ein bei Google Plus seit 2015 bestehendes Datenleck nach dessen Entdeckung im März 2018 zunächst sechs Monate lang vor Aufsichtsbehörden und Nutzern geheim gehalten. Im Dezember 2018 wurde eine weitere Lücke entdeckt, die Entwicklern Zugriff auf personenbezogene Daten der Google-Plus-Nutzer ermöglichte. Beim Mikroblogging-Dienst Twitter wurde im Mai 2018 eine schwere Datenpanne bekannt, als sich herausstellte, dass Passwörter der Nutzer im Klartext abgespeichert wurden. Zu einer groben Datenschutzverletzung kam es schließlich auch bei dem zu Facebook gehörenden Online-Dienst Instagram. Das sog. DSGVO-Tool, das den Nutzern die Einsichtnahme ihrer gespeicherten Daten ermöglichen sollte, zeigte das eigene Nutzer-Passwort unverschlüsselt in der Webadresse an, wodurch dieses auch von Dritten ausgelesen werden konnte.



Neue Gremien zum Datenschutz in Sozialen Medien

Den Facebook-Datenskandal um Cambridge Analytica hat die Artikel-29-Gruppe zum Anlass genommen, im April 2018 eine Social Media Working Group ins Leben zu rufen. Diese setzt ihre Arbeit nun als Unterarbeitsgruppe des Europäischen Datenschutzausschusses fort und wird künftig, neben den Betreibern Sozialer Medien, auch andere Akteure – wie App-Entwickler oder Daten-Broker – in den Blick nehmen. In diesem Sinne verfolgt die Social Media Working Group einen auf den Social-Media-Bereich bezogenen ganzheitlichen Ansatz.

Soziale Medien bei den Bundesbehörden

Im Berichtszeitraum habe ich mich auch mit der Nutzung von Sozialen Medien bei den meiner Zuständigkeit unterliegenden öffentlichen Stellen des Bundes beschäftigt, denn auch dort erfreut sich der Einsatz solcher Kommunikationskanäle wachsender Beliebtheit. Dabei ist unbestritten, dass Behörden auch medial nach außen vertreten sein müssen. Bürgerinnen und Bürger fragen diese Dienste nach und erwarten, aktuelle Informationen über die unterschiedlichsten Kanäle abrufen zu können. Gleichwohl darf dies nicht auf Kosten der Privatheit der Nutzer gehen.

Angesichts der vielen gravierenden Datenschutzvorfälle bei Sozialen Medien, sowie dem Risiko, für Datenschutzverstöße rechtlich gegebenenfalls mit verantwortlich zu sein (vgl. u. Nr. 15.2.8), rate ich den öffentlichen Stellen des Bundes dazu, die Erforderlichkeit des Einsatzes Sozialer Medien kritisch zu hinterfragen. Wichtige Informationen dürfen nicht exklusiv über Soziale Medien bereitgestellt werden. Sensible personenbezogene Daten haben in Sozialen Medien nichts zu suchen; weder sollten öffentlichen Stellen selbst solche Daten einstellen, noch sollten sie Bürger dazu ermuntern, diese dort preiszugeben. Ein Negativbeispiel bietet sich etwa, wenn Geflüchtete mit Behörden über deren Facebook-Fanpages kommunizieren und hierbei ihre Verfolgungsgeschichte für jedermann einsehbar schildern. Für die vertrauliche Kommunikation gibt es geeignete sicherere Kommunikationskanäle, auf die verwiesen werden sollte, etwa SSL-verschlüsselte Formulare, verschlüsselte E-Mails oder De-Mail.

Ergänzende Informationen zum Datenschutz bei Sozialen Medien sind auf meiner Internetseite unter www.datenschutz.bund.de zu finden.

Ich rate den öffentlichen Stellen des Bundes dazu, die Erforderlichkeit des Einsatzes Sozialer Medien kritisch zu hinterfragen. Wichtige Informationen sollten nicht ausschließlich über Soziale Medien bereitgestellt werden. Sensible personenbezogene Daten haben in Sozialen Medien nichts zu suchen; weder sollten öffentlichen Stellen selbst solche Daten einstellen, noch sollten sie Bürger dazu ermuntern, diese dort preiszugeben. Für die vertrauliche Kommunikation gibt es geeignete sicherere Kommunikationskanäle, auf die verwiesen werden sollte, etwa SSL-verschlüsselte Formulare, verschlüsselte E-Mails oder De-Mail.

15.2.8 EuGH nimmt Fanpage-Betreiber in die Pflicht

Anfang Juni 2018 hat der EuGH ein wegweisendes Urteil zur datenschutzrechtlichen Verantwortlichkeit beim Betrieb von Facebook-Fanpages getroffen (EuGH, Urteil vom 05.06.2018, Az. C-210/16).

Bei einer Facebook-Fanpage handelt es sich um eine Art Homepage, die von den Fanpage-Betreibern, z. B. Bundesbehörden, eingerichtet und durch Facebook publiziert (gehostet) wird. Fanpage-Betreiber können die Fanpages dazu nutzen, sich den Facebook-Nutzern sowie Personen, die die Fanpage besuchen, zu präsentieren und Äußerungen aller Art in den Medien- und Meinungsmarkt einzubringen. Beim Aufruf der Facebook-Fanpages werden personenbezogene Daten der Besucher verarbeitet, u. a. durch den Einsatz von Cookies. Facebook nutzt diese Daten zum Teil für eigene Zwecke, stellt das Ergebnis der Verarbeitung aber auch den Fanpage-Betreibern in Form einer konfigurierbaren Statistikfunktion („Seiten-Insights“) zur Verfügung. Der EuGH hat entschieden, dass für diese im Zusammenhang mit den Fanpages stattfindenden Verarbeitungen die Fanpage-Betreiber gemeinsam mit Facebook verantwortlich sind. Dem vorausgegangen war eine Vorlage des Bundesverwaltungsgerichts an den EuGH in einem Verfahren zwischen der Wirtschaftsakademie Schleswig-Holstein GmbH und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Soweit die gemeinsame Verantwortlichkeit reicht, müssen sich Fanpage-Betreiber etwaige Datenschutzverletzungen Facebooks als eigene zurechnen lassen. Darüber hinaus sind Fanpage-Betreiber verpflichtet, mit Facebook eine Vereinbarung zur gemeinsamen Verantwortlichkeit zu schließen, in der geregelt ist, wer von beiden welche Pflichten nach der DSGVO erfüllt (Artikel 26 DSGVO). Die Datenschutzbehörden aus Bund und Ländern befassen sich in einer extra dafür gegründeten Taskforce Fanpages intensiv mit dieser Thematik, den Folgen des EuGH-Urteils sowie den zwischenzeitlich von Face-

book ergriffenen Umsetzungsmaßnahmen. Ich bin der Auffassung, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Artikel 5 Absatz 1 DSGVO) nachweisen müssen. Um bewerten zu können, ob die der eigenen Verantwortung unterliegenden Verarbeitungen rechtskonform durchgeführt werden, benötigen Fanpage-Betreiber – zusätzlich zu den von Facebook bereitgestellten Informationen – noch weitere Informationen. Hier sehe ich nicht nur Facebook in der Pflicht, weitere Informationen bereitzustellen, sondern auch die Fanpage-Betreiber, die benötigten Informationen aktiv einzufordern. Selbiges gilt auch für den Abschluss einer Vereinbarung zur gemeinsamen Verantwortlichkeit, die den Anforderungen des Artikel 26 DSGVO entspricht. Als Orientierungshilfe für die mit Facebook zu klärenden Punkte kann der Fragenkatalog aus dem Beschluss der Datenschutzkonferenz vom 5. September 2018 dienen (vgl. Kasten zu Nr. 15.2.8).

Solange diese Punkte nicht mit Facebook geklärt sind, empfehle ich den Fanpage-Betreibern, zu prüfen, ob der Betrieb einer Facebook-Fanpage zur Erfüllung ihrer Aufgaben unbedingt erforderlich ist oder sie sich nicht – zumindest bis zur Klärung der Situation – auf datenschutzfreundlichere Kommunikationskanäle konzentrieren können. Bundesbehörden sollten dabei besonders sensibel sein.

Ich empfehle den Bundesbehörden, die eine Fanpage betreiben, zu prüfen, ob der Betrieb einer Facebook-Fanpage zur Erfüllung ihrer Aufgaben unbedingt erforderlich ist oder sie sich nicht – zumindest bis zur rechtlichen Klärung der Situation – datenschutzfreundlichere Kommunikationskanäle nutzen können.

Fragenkatalog

- In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Art. 26 Abs. 1 DSGVO)
- Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DSGVO nachkommt?
- Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?
- Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DSGVO, auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, auf Widerspruch nach Art. 21 DSGVO und auf Auskunft nach Art. 15 DSGVO?
- Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?
- Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?
- Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?
- Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

15.2.9 Werbung im Fokus der Deutschen Post AG

Die Deutsche Post AG hat Ende 2016 mit einer Pilotierungsphase zum Einsatz von sog. Kamera-Analyse-Werbe-Systemen in ca. 100 ihrer Partnerfilialen begonnen. Datenschutzrechtlich problematisch ist der damit verbundene Einsatz von Gesichtserkennungssoftware.

Im Fall der Deutschen Post AG handelt es sich um das System „adpack" der IDA Indoor Advertising GmbH (IDA). Durch einen Beratungs- und Kontrollbesuch im Februar 2018 konnte ich mir vor Ort in einer Partnerfiliale in Köln ein Bild über den konkreten Einsatz machen.

Kamera-Analyse-Werbe-Systeme arbeiten grundsätzlich nach ähnlichen Prinzipien, können sich aber in den Einzelheiten der technischen Realisierung erheblich unterscheiden. Eine Kamera erfasst einen bestimmten Bereich und nimmt ein Video auf. Diese Videodateien werden dann auf Einzelbilder reduziert und normalerweise im Übrigen wieder verworfen, ohne dass es zu einer dauerhaften Speicherung kommt. Die ebenfalls nur flüchtig gespeicherten (RAM) Einzelbilder werden dann von einer Gesichtserkennungssoftware ausgewertet und ebenfalls in der Regel wieder verworfen. Das aus der Erkennungssoftware erzeugte Template wird nach bestimmten Merkmalen untersucht, die über eine Programmierschnittstelle zur weiteren Nutzung ausgegeben werden. Anschließend wird auch das Template wieder gelöscht. Unterschiedliche Varianten der Realisierung sind hier insbesondere im Hinblick darauf möglich, zu welchem Teil die Verarbeitung „lokal" auf dem Endgerät erfolgt, auf dem letztlich auch die Werbemedien angezeigt werden und welche Daten auf einen zentralen Server übertragen werden. Die Zeitdauer, nach der die jeweiligen Zwischenprodukte der Verarbeitung wieder verworfen werden, hat ebenfalls einen erheblichen Einfluss darauf, wie ein Gesamtsystem aus Sicht des Datenschutzes zu bewerten ist. Auch die ausgegebenen Daten hängen vom konkreten System ab. Bei dem von der Deutschen Post AG eingesetzten System sind dies lediglich Geschlecht und Alterskohorte. Es ist aber davon auszugehen, dass andere Systeme bei entsprechender Konfiguration wesentlich detailliertere Informationen liefern können.

Bei meiner datenschutzrechtlichen Bewertung des Systems konnte ich feststellen, dass es sich um ein sehr komplexes Verfahren zur personalisierten Werbung handelt. Derartige Kamera-Analyse-Werbe-Systeme finden bislang im Markt noch keine flächendeckende Verwendung, so dass ich nicht auf bereits vorhandene datenschutzrechtliche Beurteilungsmaßstäbe zurückgreifen konnte. Dies führt letztendlich auch zu der zeitlich aufwändigen Sachverhaltsermittlung, die derzeit noch mit einem sowohl in technischer als auch in rechtlicher Hinsicht umfangreichen Abstimmungsprozess verbunden ist.

Die bisherigen Erläuterungen durch die Deutsche Post AG lassen erkennen, dass von dort im Vorfeld der Pilotierungsphase Maßnahmen ergriffen wurden, um einen rechtmäßigen Einsatz des komplexen Systems sicherzustellen.

Von grundlegender Bedeutung für die datenschutzrechtliche Beurteilung ist aber, ab wann seriell hintereinander geschaltete Datenverarbeitungsvorgänge derartig miteinander verschränkt sind, dass sie als einheitlicher Vorgang zu bewerten sind. Soweit serielle Datenverarbeitungen nicht als ausreichend verschränkt zu betrachten sind, sondern als klar voneinander trennbare Vorgänge, sind sie dementsprechend einzeln zu bewerten und jeder Datenverarbeitungsprozess muss durch eine entsprechende Rechtsgrundlage legitimiert sein.

Die Komplexität der Verfahren und die Befassung vieler deutscher Datenschutzaufsichtsbehörden mit solchen Systemen haben dazu geführt, dass sich auch eine Unterarbeitsgruppe der Datenschutzkonferenz, an der ich beteiligt bin, mit diesem Themenkomplex beschäftigt. Ich werde mich dafür einsetzen, dass die deutschen Datenschutzaufsichtsbehörden zu einer einvernehmlichen Bewertung derartiger Systeme gelangen, damit das Datenschutzrecht in Deutschland einheitlich und konsistent angewandt wird.

15.3 Aus Kontrolle und Beratung

15.3.1 In Stein gemeißelt?

Auch wenn die Daten eines ehemaligen Kunden nicht mehr für die Vertragserfüllung erforderlich sind, müssen sie noch aus steuer- und handelsrechtlichen Gründen für Jahre aufbewahrt werden. Die Umsetzung dieser gesetzlichen Vorgaben ist nicht immer unproblematisch.

Bereits häufiger musste ich feststellen, dass eine Löschung von Bestandsdaten ehemaliger Kunden, die aus steuer- und handelsrechtlichen Gründen erst nach zehn Jahren zu erfolgen hat, in den IT-Systemen von Telekommunikationsunternehmen nicht vorgesehen war (vgl. 25. TB Nr. 8.8.3 und 23. TB Nr. 6.3). Dabei konnte ich den Eindruck gewinnen, dass gerade bei SAP-Systemen ein Löschen von Bestandsdaten eher unüblich ist. Die nachträgliche Planung und Umsetzung eines Löschkonzepts erfordern regelmäßig einen hohen Aufwand an Zeit und Ressourcen. Insofern sollte die Löschung von personenbezogenen Daten bereits bei der Planung von Datenverarbeitungssystemen berücksichtigt werden.

Bei einer Kontrolle zur Verarbeitung von Bestandsdaten bei einem Telekommunikationsunternehmen wurden mir diverse Systeme ausführlich vorgestellt. Dies betraf jedoch nicht die SAP-Systeme, die Teil des Bestandsdatensystems waren. Auf Rückfrage konnte das Unternehmen keine Angaben zur Löschung von den in diesen Systemen gespeicherten personenbezogenen Daten machen. Im Rahmen eines weiteren Termins erklärte der Telekommunikationsdiensteanbieter, dass eine Löschung von Daten nicht erfolge. In einem System waren sogar noch Daten aus den 1990er Jahren gespeichert.

Bereits die fehlende Löschung der Daten entspricht nicht den gesetzlichen Vorgaben. Hinzu kam in dem von mir kontrollierten Fall, dass die Problematik der konzerninternen Datenschutzabteilung zwar bereits seit 2012 bekannt war, bis zu meinem Kontrollbesuch aber nur eine unzureichende Löschung vorgesehen worden war. Dies hat mich dazu veranlasst, eine Beanstandung gegenüber dem Telekommunikationsunternehmen auszusprechen. Die Beanstandung hat zu einem deutlich erhöhten Engagement bei den Projekten zur Datenlöschung geführt. Im Dezember 2018 wurde mir mitgeteilt, dass die Datenlöschung planmäßig abgeschlossen worden sei.

15.3.2 Kein Handy für Daniel Düsentrieb

Eine Neuregelung von § 111 Absatz 1 Telekommunikationsgesetz (TKG) soll sicherstellen, dass auch bei im Voraus bezahlten Mobilfunkdiensten (Prepaid-Karten) nur korrekte Namen in den Kundendateien eingetragen werden. Bisher konnten zum Leidwesen der Sicherheitsbehörden bei Vertragsschluss oft auch Phantasienamen angegeben werden. Die neuen Verfahren habe ich mir bei einem Netzbetreiber angesehen.

Eine Mobilfunk-Prepaid-Karte gibt es seit Anfang Juli 2017 nur noch nach Vorlage des Personalausweises (oder bestimmter vergleichbarer Dokumente), wobei die Ausweisnummer vom Anbieter gespeichert werden muss. Zur Prüfung sind nur bestimmte, von der Bundesnetzagentur (BNetzA) vorgegebene Verfahren zulässig. Über die Einführung dieses problematischen Verfahrens hatte ich bereits in meinem 26. TB (Nr. 17.2.4.2) berichtet.

Ich habe bei einem Anbieter von Prepaid-Mobilfunkleistungen zwei Kontrollen durchgeführt, um die praktische Umsetzung der verschiedenen Verfahren zu überprüfen. Sofern die Validierung nicht vor Ort im Elektronikhandel oder einem Mobilfunkshop erfolgt, kann der Kunde zwischen einer Identifikation per Video-Ident-Verfahren und einer Kontrolle des Ausweises in einer Filiale eines beauftragten Dienstleisters wählen. Diese Verfahren werden schon länger für andere Zwecke, insbesondere bei der Eröffnung von Bankkonten nach den Vorschriften des Geldwäschegesetzes (GWG) durchgeführt (vgl. hierzu auch unter Nr. 6.1.2). Wegen der speziellen Vorgaben des § 111 Absatz 1 TKG erfolgte eine Anpassung der Verfahren. Danach muss eine Kopie des Ausweises an den Anbieter zur Prüfung übermittelt werden.

Im Rahmen der Prüfung des Verfahrens in einer Filiale des Dienstleisters zeigten sich verschiedene Mängel. So wurden beim Einscannen auch der Geburtsort und der Geburtsname erfasst und an den Anbieter weitergegeben. Dies ist für das Verfahren nach § 111 Absatz 1 TKG nicht erforderlich und somit aufgrund der Pflicht zur Datenminimierung auch nicht zulässig. Weiterhin musste ich feststellen, dass der Dienstleister die Daten einschließlich der Ausweiskopie im Rahmen der Auftragsverarbeitung für fünf Monate speichert. Begründet hat der Mobilfunkanbieter dies mit befürchteten IT-Problemen und einem möglichen Datenverlust. Hier hat der Anbieter im Rahmen meiner Kontrolle einer Reduzierung der Speicherdauer auf sieben Tage zugestimmt. Allerdings wird von der Datenbank ein Backup für vier Wochen gespeichert, so dass die Daten faktisch erst nach fünf Wochen irreversibel gelöscht werden – dies halte ich für zu lange.

Bei dem Verfahren in der Filiale sind mir noch zwei weitere Probleme aufgefallen. § 20 Absatz 2 Personalausweisgesetz und die Amtsblattverfügung der BNetzA fordern eine Kenntlichmachung des Scans als Kopie. Diese erfolgte jedoch nicht. Weiterhin gab es keine Möglichkeit, irrelevante Daten auf dem Ausweis zu schwärzen. Der Mitarbeiter in der besuchten Filiale erklärte hierzu, dass die Identifikation in diesem Fall sogar abgebrochen werde und der Kunde damit seine erworbene Prepaid-Karte vorerst nicht nutzen könne.

Im Video-Ident-Verfahren, bei dem der Kunde seinen Ausweis vor eine Webcam hält, werden zwar auch die nicht erforderlichen Daten zunächst erfasst, allerdings werden diese vor einer Versendung an den späteren Anbieter geschwärzt. Die Sicherheit des Video-Ident-Verfahrens gegen aufwändigere Angriffe wurde hier nicht betrachtet. Ich möchte dazu auf Nr. 15.2.1 in diesem Bericht verweisen. Bei der genannten Kontrolle fiel außerdem noch auf, dass der eingesetzte Dienstleister recht unauffällig die Identifikation des Prepaid-Kunden nutzt, um die Kunden auch noch für ein eigenes Validierungsverfahren zu gewinnen, mit dem man sich für weitere Angebote authentifizieren kann. Da die Information darüber leicht zu übersehen ist und der Kunde deshalb keine wirkliche Wahl hat, ob seine Daten für die Kundengewinnung des Dienstleisters verwendet werden, was formal als zweckändernde Verarbeitung in eigener Verantwortlichkeit zu werten ist, dürfte es sich nicht um eine wirksame Einwilligung handeln. Ich habe den Anbieter aufgefordert, das Verfahren zu ändern, so

dass die Teilnehme an dem Validierungsverfahren optional ist und die Informationen transparent sind.

Das Vor-Ort-Verfahren im Mobilfunkshop hätte darüber hinaus einen sehr guten Eindruck hinterlassen, wäre das erforderliche Foto vom Ausweis nicht mit dem privaten Handy des Kundenberaters aufgenommen worden. Die hier verwendete spezielle App des Anbieters speichert die Ausweiskopie allerdings nicht lokal auf dem Handy.

15.3.3 Sanftes Drängen

Im Rahmen der Störungserkennung findet seit Jahren eine unzulässige Speicherung von SMS-Inhalten statt. Trotz meiner Beanstandung gegenüber der BNetzA hat nur ein Netzbetreiber erklärt, dass er diese rechtswidrige Praxis beendet hat.

Bereits in meinem 24. TB (Nr. 6.8.2) hatte ich darüber berichtet, dass Signalisierungsdaten, die als Verkehrsdaten zu werten sind, für wenige Tage zur Eingrenzung, Erkennung und Beseitigung von Störungen aufgezeichnet werden. Dies ist zulässig – allerdings nur dann, wenn keine Inhalte mitgespeichert werden. Zum Problem werden hier Kurzmitteilungen (SMS), weil bei denen auch die Inhalte mit im Signalisierungskanal übertragen werden. Bei zwei Mobilfunkanbietern hatte ich diese Speicherung im Nachgang von Kontrollen gegenüber der BNetzA beanstandet (vgl. 25. TB Nr. 8.8.3). Bei einem weiteren habe ich im Rahmen einer späteren Kontrolle festgestellt, dass auch dieser betroffen ist. Einer der Anbieter hat inzwischen die Speicherung eingestellt, was ich im 26. TB (Nr. 17.3.1) bereits angekündigt hatte.

Die BNetzA hat sich aufgrund der Beanstandungen mit der Thematik beschäftigt. Zunächst wurde meine Forderung, die Speicherung der SMS-Inhalte zu unterlassen, als technisch unmöglich bezeichnet. Nachdem ein Netzbetreiber das „Unmögliche“ möglich gemacht hat, hatte ich die BNetzA darauf aufmerksam gemacht, die anderen Netzbetreiber aufzufordern, ebenfalls auf diese unzulässige Speicherung zu verzichten. Die BNetzA hatte mir daraufhin zugesagt, mich über den Fortgang des Verfahrens zu informieren. Erst auf Rückfrage wurde ich später darüber informiert, dass die übrigen Netzbetreiber Stellung genommen hätten und kein weiterer Handlungsbedarf bestünde. Ich habe der BNetzA gegenüber erläutert, dass ich den mir vorliegenden Schreiben der Netzbetreiber nicht entnehmen könnte, dass die unzulässige Speicherung von Kommunikationsinhalten beendet worden sei und um Information zu den weiteren Schritten gebeten. In der Antwort der Bundesregierung auf eine kleine Anfrage (BT-Drs. 18/13394) wird zwar ausgeführt, dass die BNetzA bei den Diensteanbietern nach wie vor auf die Implementierung einer Lösungsmöglichkeit drängt; dieses Drängen erscheint mir jedoch recht sanft zu sein. Ich werde über den Fortgang berichten.

15.3.4 Und es gibt sie doch! Eine Kontrolle zur Vorratsdatenspeicherung

Nachdem die Bundesnetzagentur (BNetzA) mitgeteilt hat, dass sie die Vorratsdatenspeicherung nicht durchsetzt, haben alle Telekommunikationsdiensteanbieter auf die Aktivierung ihrer bereits weitgehend fertiggestellten Systeme verzichtet… Alle Anbieter? Nein! Zwei Anbieter sind diesem Trend nicht gefolgt und haben einen Dienstleister mit der Vorratsdatenspeicherung beauftragt.

Nachdem die BNetzA die Vorratsdatenspeicherung praktisch ausgesetzt hat (vgl. Nr. 9.2.7), habe ich eine Umfrage bei Telekommunikationsdiensteanbietern durchgeführt. Ein Anbieter teilte mir mit, dass er seinen Auftrag bei einem Dienstleister aufrechterhalten hat. Anschließend habe ich erfahren, dass bei diesem Dienstleister noch ein weiterer Anbieter dort Verkehrsdaten auf Vorrat speichern lässt. Dort habe ich einen Beratungs- und Kontrollbesuch zur Vorratsdatenspeicherung durchgeführt.

Während viele große Telekommunikationsanbieter die Vorratsdatenspeicherung in Eigenregie durchführen wollten, haben andere, insbesondere kleinere Anbieter einen Dienstleister mit der Vorratsdatenspeicherung beauftragt. Der von mir kontrollierte Dienstleister bietet auch die Schaltung von Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) an.

Bei dem Besuch musste ich feststellen, dass zwar umfangreiche Sicherheitsmaßnahmen implementiert waren, so dass bis auf kleinere Ausnahmen ein Niveau erreicht war, das für die Schaltung von TKÜ-Maßnahmen angemessen war. Jedoch gelten für die Vorratsdatenspeicherung höhere und z. T. spezifische Anforderungen aus dem Anforderungskatalog nach § 113f Absatz 1 und 3 TKG. Die Serverschränke etwa verfügten nicht über spezielle Schlösser, so dass auch Personal, das „nur“ Server zur Schaltung von TKÜ-Maßnahmen betreut, direkten Zugang zu den Servern hatte, auf denen die Vorratsdatenspeicherung erfolgte. Auch eine regelmäßige Überwachung der Log-Files fand nicht statt. Auf diese Weise wurde etwa ein Problem bei der Löschung der verwendeten Schlüssel übersehen. Auch bei formalen Punkten gab es Defizite, insbesondere fehlte die in § 113d TKG geforderte Ermächtigung der Mitarbeiter. Problematisch war auch die Nutzung von Hash-Werten, um in den verschlüsselten Daten effektiv suchen zu können. Hier hängt es von der Länge der Hash-Werte und der Art der Daten ab, inwieweit anhand dieser Informationen noch – wenn auch vage – Rückschlüsse aus den Indizes gezogen werden können. Hier mussten Anpassungen vorgenom-

men werden. Generell dürfte es eine Herausforderung sein, eine valide Verschlüsselung bei gleichzeitig effektiver Suchmöglichkeit umzusetzen.

Im Ergebnis konnte ich feststellen, dass die Umsetzung der besonders hohen Anforderungen für die Vorratsdatenspeicherung in der Praxis hochkomplex ist.

15.3.5 Nichts kann so einfach ins Ausland transportiert werden wie Daten. Da werden wir aber sehr genau hinsehen …

Im Berichtszeitraum habe ich spezifische Beratungs- und Kontrollbesuche bei drei großen Telekommunikationsdiensteanbietern durchgeführt, deren Gegenstand die Übermittlung personenbezogener Daten an Stellen außerhalb der EU und des EWR war. Dabei habe ich festgestellt, dass bei der Erbringung von Telekommunikationsdienstleistungen personenbezogene Daten unter anderem nach Indien, Kanada, in die Schweiz, die Türkei und die USA übermittelt werden.

Die Beratungs- und Kontrollbesuche erfolgten noch vor dem 25. Mai 2018, so dass die DSGVO nicht Prüfmaßstab war. Mit Blick auf die neue Rechtslage kann festgehalten werden, dass die Übermittlung personenbezogener Daten in Drittstaaten vor allem auf der Grundlage von Standarddatenschutzklauseln (vgl. Artikel 46 Absatz 2 Buchstabe c) DSGVO) sowie auf der Grundlage von Angemessenheitsbeschlüssen der Europäischen Kommission (vgl. Artikel 45 Absatz 1 DSGVO) erfolgt. Vereinzelt wird die Datenübermittlung auch auf die ausdrückliche Einwilligung der betroffenen Personen (Artikel 49 Absatz 1 Satz 1 Buchstabe a) DSGVO) und auf verbindliche interne Datenschutzvorschriften (Artikel 46 Absatz 2 Buchstabe b) DSGVO) gestützt.

Mit der DSGVO wurde die europäische Rechtslage zur Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen reformiert. Die Thematik befindet sich derzeit in vielerlei Hinsicht noch im Fluss. Ihr kommt zunehmende Bedeutung zu. Ich werde dies weiter eng verfolgen und darüber berichten.

15.3.6 Ein WLAN ist ein WLAN ist ein WLAN – oder?

Die Geschäftsmodelle und auch die daraus resultierenden datenschutzrechtlichen Herausforderungen an Diensteanbieter in der gleichen Branche sind meist recht ähnlich. Bei drei Kontrollen von WLAN-Anbietern konnte ich jedoch erhebliche Unterschiede feststellen.

In einem Fall wollte eine Stadt die Fußgängerzone mit WLAN-Hotspots attraktiver gestalten. Bei der Kontrolle des WLAN-Anbieters waren hier nur einige wenige Punkte kritisch anzumerken. Dies betraf etwa die Datenschutzerklärung und die Forderung nach Angabe einer E-Mail-Adresse, um ein größeres Datenvolumen zu erhalten, ohne dass dies notwendig gewesen wäre. Insgesamt war der Umfang der Datenverarbeitung recht überschaubar.

Deutlich komplexer war da schon die Datenverarbeitung für die WLAN-Dienste eines großen Netzbetreibers. Hier bestand eine Vielzahl an zum Teil kostenpflichtigen Abrechnungsmodellen. Signifikante Probleme waren nicht festzustellen. Lediglich in Bezug auf die unübersichtliche Darstellung der Datenschutzhinweise bzw. im Hinblick auf die Komplexität des Diensteangebots gab es Gründe für kritische Anmerkungen.

Wirklich herausfordernd war dagegen ein dritter Anbieter, der gesponserte WLAN-Hotspots für Geschäfte, Cafés etc. anbietet. Hier werden recht umfangreich pseudonyme Daten erhoben, um dem Auftraggeber möglichst aussagekräftige Statistiken als Mehrwert bieten zu können. Dabei ist einerseits eine Anonymisierung das Ziel, durch die eine Person nicht direkt identifizierbar sein soll. Andererseits sollen Endgeräte für eine bestimmte Zeit wiedererkannt werden, z. B. um mehrfache Besuche eines Ladengeschäfts zu erkennen. Diese Nutzung halte ich für problematisch. Hier sind die Probleme ähnlich gelagert wie bei den unter Nr. 15.2.5 beschriebenen Anwendungen. Ich erwarte diesbezüglich Regelungen in der kommenden E-Privacy-Verordnung, die leider länger auf sich warten lässt, als ursprünglich erwartet.

15.3.7 Aus der Beratungs- und Kontrolltätigkeit im Postbereich

Die DSGVO strahlt auch auf die datenschutzrechtlichen Regelungen im Postbereich aus.

Mit dem Anwendungsbeginn der DSGVO bekamen das Postgesetz (PostG) und die Postdienste-Datenschutzverordnung (PDSV) ein neues, umfangreiches Regelwerk an die Seite gestellt. Mit dieser veränderten Rechtslage gingen viele allgemeine Beratungsanfragen von Postdienstleistern aber auch von Unternehmen bei mir ein, die regelmäßig auf Versanddienstleistungen angewiesen sind.

Zudem erreichten mich viele Anfragen von Postdienstunternehmen zu datenschutzrechtlichen Aspekten bei konkreten Projekten bzw. Geschäftsmodellen. Neben Fragen technischer Natur wurden vor dem Hintergrund der Geltung der DSGVO insbesondere rechtliche Problemstellungen an mich herangetragen. Ich begrüße es, dass die Postunternehmen mich frühzeitig in die Entwicklungsprozesse von neuartigen Verfahren einbeziehen, um bereits in der Konzeptionsphase datenschutzrechtliche Aspekte berücksichtigen zu können. Dies zeigt, dass der Datenschutz immer mehr an Bedeutung

gewinnt und bei den Planungen der Unternehmen rechtzeitig mitgedacht wird.

Bei den im Berichtszeitraum durchgeführten Kontrollen bei großen wie kleinen Unternehmen, die geschäftsmäßig Postdienste erbringen, konnte ich einen durchweg positiven Eindruck der Verarbeitungsprozesse gewinnen. Sofern es im Rahmen von Kontrollbesuchen zu unterschiedlichen (Rechts-)Auffassungen kam, so konnten diese nach eingehender Erörterung zu einer zufriedenstellenden Lösung für beide Seiten gebracht werden – auf formale Beanstandungen konnte ich daher verzichten.

Aber auch durch eine stark steigende Anzahl der Anfragen und Beschwerden von Bürgerinnen und Bürgern wurde das ein oder andere datenschutzrechtliche Thema aus dem Postbereich an mich herangetragen. Diese zunehmende Aufmerksamkeit der betroffenen Bürgerinnen und Bürger für den Datenschutz und das kritische Hinterfragen von Verarbeitungsprozessen (Darf der das? Ist das denn überhaupt erforderlich?) begrüße ich ausdrücklich.

15.3.8 Vertrauen ist gut – Kontrolle ist besser

Einige Monate nach Anwendbarkeit der DSGVO habe ich ein öffentliches Wirtschaftsunternehmen des Bundes kontrolliert.

Die Kontrolle wurde mir nur widerwillig ermöglicht, nachdem zunächst meine Zuständigkeit angezweifelt worden war. Bei der Kontrolle hatte ich den Eindruck, als seien einige datenschutzrechtliche Vorgaben, die bereits nach dem BDSG (alt) gegolten haben – etwa die Bestellung eines/r Datenschutzbeauftragten – erst kurzfristig umgesetzt worden. Auch wenn ich zum Zeitpunkt der Kontrolle von einem grundsätzlichen Bewusstsein für den Datenschutz ausgehen konnte, habe ich dennoch eine größere Unregelmäßigkeit gefunden: Bei der Datensicherung wurden undifferenziert sämtliche Datenbestände, d. h. auch solche mit personenbezogenen Daten, auf Bandlaufwerke überspielt und unbegrenzt lange aufbewahrt. Die ältesten Datenbestände datierten mehr als zehn Jahre zurück. Dies verstößt gegen den Erforderlichkeitsgrundsatz, wonach personenbezogene Daten nur solange gespeichert werden dürfen, wie dies notwendig ist. Je nach Speicherzweck sind entsprechende Fristen festzulegen, nach denen nicht mehr benötigte personenbezogene Daten gelöscht werden. Zur Umsetzung dessen stehe ich noch im Austausch mit der kontrollierten Stelle.

15.A Zudem von besonderem Interesse

1.1, 14.1.1, 17.9, Die Arbeit des BfDI in Zahlen

16 Weitere Ausschüsse

Nachfolgend habe ich dargestellt, welche Beiträge meines Berichtes für weitere Ausschüsse des Deutschen Bundestages von besonderem Interesse sein können:

Auswärtiger Ausschuss

1.1. Umsetzung der Datenschutz-Grundverordnung;

2.1. Der Europäische Datenschutzausschuss;

2.3. Abschluss der Revision der Datenschutz-Konvention 108;

2.4. Europäische Datenschutzkonferenz;

2.5. Internationale Datenschutzkonferenz;

17.8.1 Veranstaltung zu Binding Corporate Rules;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

17.10. Besuche ausländischer Delegationen;

Die Arbeit der BfDI in Zahlen

Ausschuss für Bau, Wohnen, Stadtentwicklung und Kommunen

1.1. Umsetzung der Datenschutz-Grundverordnung;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss Digitale Agenda

1.1. Umsetzung der Datenschutz-Grundverordnung;

9.2.7 Aktuelles zur Vorratsdatenspeicherung;

14.1.1 Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

15.1.2. Die langen Geburtswehen der E-Privacy-Verordnung;

15.2.5. Digitale Geschäftsmodelle unter Nutzung von Mobilfunkdaten;

15.2.6. Nutzung von Messenger-Diensten;

15.2.7. Datenschutz und Soziale Medien;

15.2.8. EuGH nimmt Fanpage-Betreiber in die Pflicht;

15.2.9. Werbung im Fokus der Deutschen Post AG;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss für Ernährung und Landwirtschaft

1.1. Umsetzung der Datenschutz-Grundverordnung

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss für die Angelegenheiten der Europäischen Union

1.1. Umsetzung der Datenschutz-Grundverordnung

2.1. Der Europäische Datenschutzausschuss;

2.2. Europäisches Visa-Informationssystem;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss für Menschenrechte und humanitäre Hilfe

1.1. Umsetzung der Datenschutz-Grundverordnung;

2 ff. Schwerpunktthemen – europäisch und international;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Petitionsausschuss

1.1. Umsetzung der Datenschutz-Grundverordnung;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Sportausschuss

1.1. Umsetzung der Datenschutz-Grundverordnung;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss für Tourismus

1.1. Umsetzung der Datenschutz-Grundverordnung;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss für Umwelt, Naturschutz und nukleare Sicherheit

1.1. Umsetzung der Datenschutz-Grundverordnung;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

Ausschuss für wirtschaftliche Zusammenarbeit und Entwicklung

1.1. Umsetzung der Datenschutz-Grundverordnung;

2.1. Der Europäische Datenschutzausschuss;

14.1.1. Zwischen Datenschutz und freiem Mandat – Zur Geltung der DSGVO im Deutschen Bundestag;

17.9. Öffentlichkeitsarbeit;

Die Arbeit der BfDI in Zahlen

17 Aus meiner Dienststelle

17.1 Umsetzung der DSGVO im eigenen Haus

Die DSGVO hat auch Neuerungen mit sich gebracht, die für mich als Datenschutzaufsichtsbehörde umzusetzen waren. Zur Implementierung der notwendigen organisatorischen Veränderungen und zur Anpassung der behördeninternen Prozesse habe ich eine Projektgruppe aus Beschäftigten unterschiedlicher Referate eingerichtet. Auf diese Weise ist es gelungen, dass mein Haus weitgehend reibungslos zum 25. Mai 2018 die neuen Verfahren und Strukturen anwenden konnte.

Paradigmenwechsel – Vom Petitionsverfahren zum Beschwerdeverfahren

Unter Geltung des BDSG (alt) waren Eingaben von Bürgerinnen und Bürgern ausschließlich nach den Grundsätzen des Petitionsrechts zu bearbeiten: Ein Anspruch bestand lediglich dahingehend, dass sich die Aufsichtsbehörde überhaupt in irgendeiner Form mit der Eingabe befasst. Weitergehender ist das neu geschaffene Recht auf Beschwerde bei der Aufsichtsbehörde (Artikel 77 DSGVO): Von einem Datenschutzverstoß betroffene Personen (Beschwerdeführer) können nunmehr beanspruchen, dass sich die Aufsichtsbehörde mit ihrer Beschwerde befasst, den Gegenstand in angemessenem Umfang untersucht und sie über den Fortgang unterrichtet. Die Bearbeitung von Beschwerden läuft nunmehr in einem formellen Verwaltungsverfahren ab. Nach spätestens drei Monaten ist dem Beschwerdeführer eine Zwischennachricht zu erteilen. Nach Artikel 78 DSGVO hat jede betroffene Person, die ihre Rechte verletzt sieht oder deren Beschwerde unbearbeitet bleibt, das Recht auf einen gerichtlichen Rechtsbehelf. Die hohe Anzahl von Beschwerden bei mir (und allen anderen Aufsichtsbehörden) zeigt, dass das neue Beschwerderecht bei den Bürgerinnen und Bürgern auf große Resonanz stößt. (vgl. o. Die Arbeit des BfDI in Zahlen). Die stark gestiegenen Fallzahlen bringen es in Verbindung mit dem etwas aufwändigeren Verfahren allerdings mit sich, dass die Bearbeitung vielfach länger dauert, als ich mir dies wünsche.

Durchsetzung von Abhilfebefugnissen und Bußgeldern

Bei festgestellten Datenschutzverstößen konnte ich bislang nicht unmittelbar gegen die Verantwortlichen vorgehen. Stattdessen hatte ich meine Beanstandungen an die allgemeinen Aufsichtsbehörden (Rechts-, Fachaufsichts- oder Regulierungsbehörden) zu richten, mit dem Ziel, dass diese ein eigenes Vorgehen gegen die Verantwortlichen prüfen. Mit Anwendbarkeit der DSGVO kann ich nunmehr eigene verbindliche Abhilfemaßnahmen (z. B. Verwarnungen oder Anordnungen) gegenüber den Verantwortlichen ergreifen. Außerhalb des Anwendungsbereichs der DSGVO bin ich allerdings weiterhin auf das Mittel der bloßen Beanstandung beschränkt (vgl. auch unter Nr. 1.2). Um eine einheitliche Anwendung der neuen Abhilfebefugnisse zu gewährleisten, wurden neue Prozesse etabliert und die Beschäftigten im Umgang mit den neuen Befugnissen geschult. Zudem wurde zum 1. März 2018 ein Justitiariat mit einer hieran angegliederten Zentralen Bußgeldstelle (ZBS) eingerichtet.

Bußgeldverfahren, die lediglich bei nicht-öffentlichen Stellen sowie am Wettbewerb teilnehmenden öffentlichen Stellen möglich sind, werden zentral durch die ZBS eingeleitet und durchgeführt. Dieser obliegt auch die Durchführung etwaiger Settlement-Gespräche. Im Falle der Bußgeldvollstreckung kann meine Behörde erforderlichenfalls auf die Unterstützung durch die Hauptzollämter zurückgreifen.

Neue Online-Formulare zur vereinfachten Kommunikation von Bürgerinnen und Bürgern sowie Verantwortlichen mit meinem Haus

Mit Anwendbarkeit der DSGVO zum 25. Mai 2018 nehme ich im Rahmen meiner Zuständigkeit Meldungen von Datenschutzverstößen (Artikel 33 DSGVO), Daten von behördlichen bzw. betrieblichen Datenschutzbeauftragten (Artikel 37 Absatz 7 DSGVO) sowie Beschwerden betroffener Personen (Artikel 77 DSGVO) auch über einen hierfür auf meiner Internetseite www.datenschutz.bund.de zur

Verfügung gestellten Online-Service entgegen. Hiervon erhoffe ich mir eine Vereinfachung der Kommunikation. Besonders hervorzuheben ist die Schaffung einer Funktionalität, mit der Verantwortliche die Angaben zu ihren Datenschutzbeauftragten in einem selbst verwalteten Benutzerkonto pflegen und aktuell halten können.

Mit dem Online-Beschwerdeformular komme ich zugleich den Anforderungen gemäß Artikel 57 Absatz 2 DSGVO nach, die Einreichung von Beschwerden zu erleichtern.

17.2 Aufgaben und Errichtung der Zentralen Anlaufstelle

Nach Artikel 51 Absatz 3 i. V. m. dem Erwägungsgrund 119 der DSGVO muss Deutschland als Mitgliedstaat mit mehreren Datenschutzbehörden eine zentrale Anlaufstelle (ZASt) einrichten, die eine wirksame Beteiligung aller deutschen Aufsichtsbehörden sowie eine reibungslose Zusammenarbeit mit den europäischen Stellen in den Verfahren der DSGVO gewährleistet. Nachdem der deutsche Gesetzgeber die Funktion der ZASt meiner Behörde zugewiesen hat, waren im Berichtszeitraum die notwendigen organisatorischen Voraussetzungen zu schaffen.

Aufgaben und Errichtung im Einzelnen:

Die bei mir eingerichtete, aber organisatorisch getrennte ZASt (§ 17 Absatz 1 BDSG) wird im gemeinsamen Interesse der 18 Aufsichtsbehörden des Bundes und der Länder tätig. Sie fungiert als Bindeglied zwischen diesen auf der einen Seite sowie den Aufsichtsbehörden der anderen Mitgliedstaaten, dem Europäischen Datenschutzausschuss (EDSA) und der Europäischen Kommission auf der anderen Seite. Zu diesem Zweck leitet die ZASt alle ihr zugeleiteten Informationen sowie den bei ihr eingehenden Geschäftsverkehr an die hiervon betroffenen deutschen Aufsichtsbehörden weiter. Umgekehrt können sich die deutschen Aufsichtsbehörden bei grenzüberschreitender Kommunikation mit den vorgenannten Stellen der ZASt bedienen. Ferner soll die ZASt insbesondere den Organen der EU und den Aufsichtsbehörden anderer Mitgliedstaaten ermöglichen, ohne Kenntnis der innerstaatlichen Zuständigkeitsverteilung effektiv mit den deutschen Aufsichtsbehörden zu kommunizieren. Eine der wichtigsten Aufgaben der ZASt ist die Koordinierung bei der Festlegung gemeinsamer Standpunkte der deutschen Datenschutzbehörden in europäischen Angelegenheiten (vgl. Nr. 17.3). Die ZASt nimmt darüber hinaus weitere unterstützende Aufgaben wahr, beispielsweise die Fristenkontrolle für Verfahren der Zusammenarbeit und Kohärenz nach der DSGVO, die Vermittlung von Kontaktpersonen, die Begleitung zu Terminen in Brüssel oder auch die organisatorische Unterstützung bei der Anmeldung der deutschen Vertreter für Sitzungen des EDSA und seiner Arbeitsgruppen. Hingegen übt die ZASt keine hoheitliche Verwaltungsaufgaben aus und wird Bürgerinnen und Bürgern, Behörden und Unternehmen gegenüber nicht tätig.

Das Binnenmarktinformationssystem als Werkzeug der Zusammenarbeit der deutschen und europäischen Aufsichtsbehörden

Zur Koordinierung der grenzüberschreitenden Kooperations- und Kohärenzverfahren nach der DSGVO verwenden die beteiligten Datenschutzaufsichtsbehörden das Binnenmarkinformationssystem (Internal Market Information System – IMI). IMI ist eine über das Internet zugängliche Anwendung, die grenzüberschreitend alle europäischen und deutschen Datenschutzaufsichtsbehörden miteinander verbindet. Dadurch ist eine schnelle und einfache Kommunikation der angeschlossenen Behörden möglich und eine europäische Verwaltungszusammenarbeit gewährleistet. Betreut wird das System auf europäischer Ebene durch das Sekretariat des EDSA, das einen eigenen IMI-Helpdesk eingerichtet hat. Rechtsgrundlage für die Anwendung des Programms ist die europäische Verordnung Nr. 1024/2012 vom 25. Oktober 2012 sowie ein Durchführungsrechtsakt. Dabei regelt die vorgenannte Verordnung auch die Rechte der Betroffenen. Dadurch gibt es beispielsweise besondere Auskunfts- und Löschrechte. Datenschutzrechtlich hatte ich das System, wenngleich auch in Bezug auf eine andere Fachanwendung, bereits im Dezember 2012 geprüft und nicht beanstandet (vgl. 24. TB Nr. 2.3.1). Für die neuen grenzüberschreitenden Verfahren nach der DSGVO wurden in Zusammenarbeit mit der Europäischen Kommission und in Rücksprache mit Vertretern der Mitgliedsstaaten eigene Eingabeformulare geschaffen, die gewährleisten, dass nur die jeweils erforderlichen Daten erfasst werden.

17.3 Koordination und Abstimmung zwischen den Aufsichtsbehörden des Bundes und der Länder

Gemäß § 17 Absatz 1 BDSG nehme ich die Funktion des Gemeinsamen Vertreters der deutschen Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA) wahr. Als Stellvertreter des Gemeinsamen Vertreters wählt der Bundesrat eine Leiterin oder einen Leiter einer Aufsichtsbehörde der Länder.

Die Kernaufgabe des EDSA besteht darin, die einheitliche Anwendung der DSGVO in der Europäischen Union sicherzustellen (vgl. hierzu unter Nr. 2.1). Im Rahmen

dieses Harmonisierungsauftrags kommen ihm weitreichende Kompetenzen zu. EU-Mitgliedstaaten wie Deutschland, die über mehrere nationale Aufsichtsbehörden verfügen, müssen einen „Gemeinsamen Vertreter“ im Sinne des Artikel 51 Absatz 3 DSGVO für den EDSA benennen. Dem Gemeinsamen Vertreter kommen in der Regel die Verhandlungsführung und das Stimmrecht im EDSA zu. In Angelegenheiten, in denen die Länder das alleinige Recht zur Gesetzgebung haben oder die die Einrichtung oder das Verfahren von Landesbehörden betreffen, überträgt der Gemeinsame Vertreter dem Stellvertreter gemäß § 17 Absatz 2 BDSG auf Verlangen das Stimmrecht im EDSA.

Bestimmung der deutschen Verhandlungsposition für den EDSA

Im EDSA verfügt jeder Mitgliedstaat über eine Stimme, unabhängig von der Zahl seiner Datenschutzbehörden. Das BDSG enthält entsprechende Verfahrensvorgaben, wie die deutsche Position für die Sitzungen des EDSA herzustellen ist. Als Grundsatz sieht § 18 Absatz 1 BDSG vor, dass die Aufsichtsbehörden des Bundes und der Länder in EU-Angelegenheiten miteinander kooperieren und gemeinsame Standpunkte im Einvernehmen erarbeiten. Können sich die deutschen Aufsichtsbehörden im Vorfeld der Sitzungen des EDSA nicht im Wege des auch formlos möglichen Einvernehmens auf einen gemeinsamen Standpunkt einigen, sieht § 18 Absatz 2 BDSG ein abgestuftes Verfahren zur Entscheidungsfindung vor, an dessen Ende die deutsche Position auf der Grundlage von Mehrheitsentscheidungen aller Aufsichtsbehörden des Bundes und der Länder bestimmt werden kann. Hierbei wird die gemeinsame Willensbildung regelmäßig von der Zentralen Anlaufstelle (ZASt) koordiniert (vgl. hierzu o. Nr. 17.2). Der Gemeinsame Vertreter und sein Stellvertreter sind bei der Ausübung des Stimmrechts im EDSA an die gemeinsamen Standpunkte der Aufsichtsbehörden des Bundes und der Länder gebunden. Unter Beachtung dieser Standpunkte legen sie einvernehmlich die jeweilige Verhandlungsführung fest.

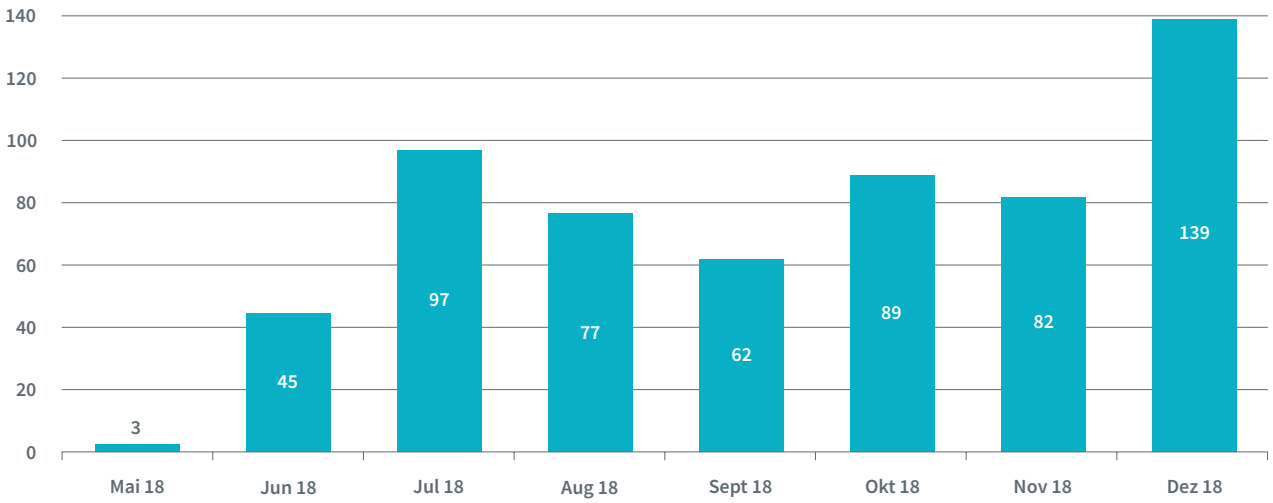
17.4 Statistischer Überblick über die Verfahren der Zusammenarbeit und Kohärenz auf europäischer Ebene aus Sicht der Zentralen Anlaufstelle

Mit Anwendungsbeginn der DSGVO am 25. Mai 2018 wurde ein neues Kapitel der Zusammenarbeit der europäischen Datenschutzbehörden aufgeschlagen. Erste Statistiken geben Aufschluss zu Art und Umfang der Zusammenarbeit.

Die Zusammenarbeit der europäischen Datenschutzbehörden erfolgt mit dem Ziel einer europaweit einheitlichen Anwendung der DSGVO. Technisch erfolgt die Zusammenarbeit über einen eigens geschaffenen Arbeitsablauf im Binnenmarktinformationsystem (IMI) (vgl. hierzu unter Nr. 17.2). Dort werden die verschiedenen Verfahrensarten statistisch erfasst.

Bei der Bearbeitung grenzüberschreitender Fälle muss zunächst die innerhalb Europas federführend zuständige Datenschutzbehörde identifiziert werden (Verfahren nach Artikel 56 DSGVO). Die diesbezüglichen Verfahrenszahlen aus dem IMI-System belegen, dass die europäischen Datenschutzbehörden sehr zügig damit begonnen haben, die nach Anwendungsbeginn der DSGVO eingegangenen grenzüberschreitenden Fälle einer Bearbeitung zuzuführen.

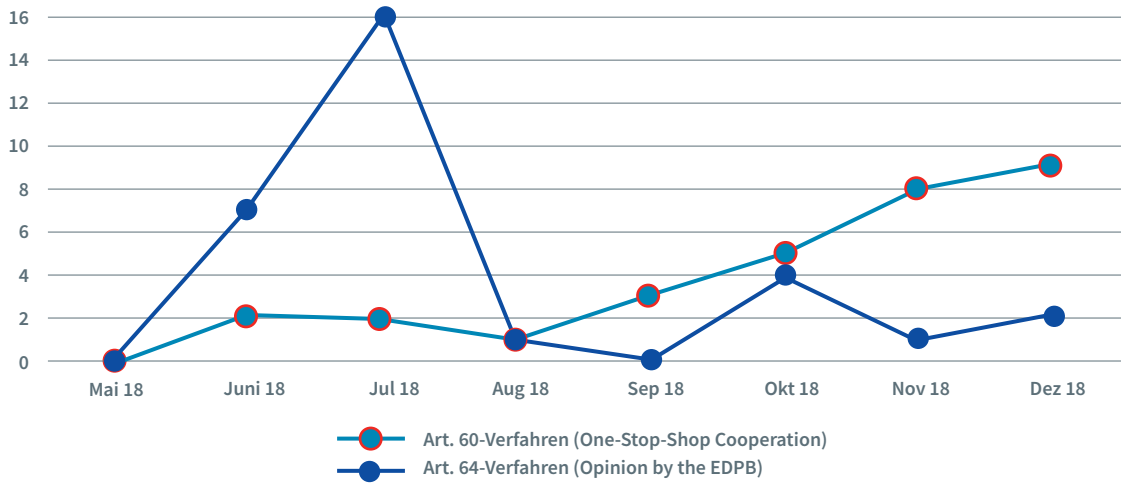
Eingeleitete Verfahren nach Artikel 56 DSGVO



Die deutschen Aufsichtsbehörden zählen insgesamt zu den Aktivsten. So wurden von den **insgesamt 594** im Zeitraum vom 25. Mai bis 31. Dezember 2018 eingeleiteten Artikel-56-Verfahren allein **236 von deutschen Aufsichtsbehörden** initiiert.

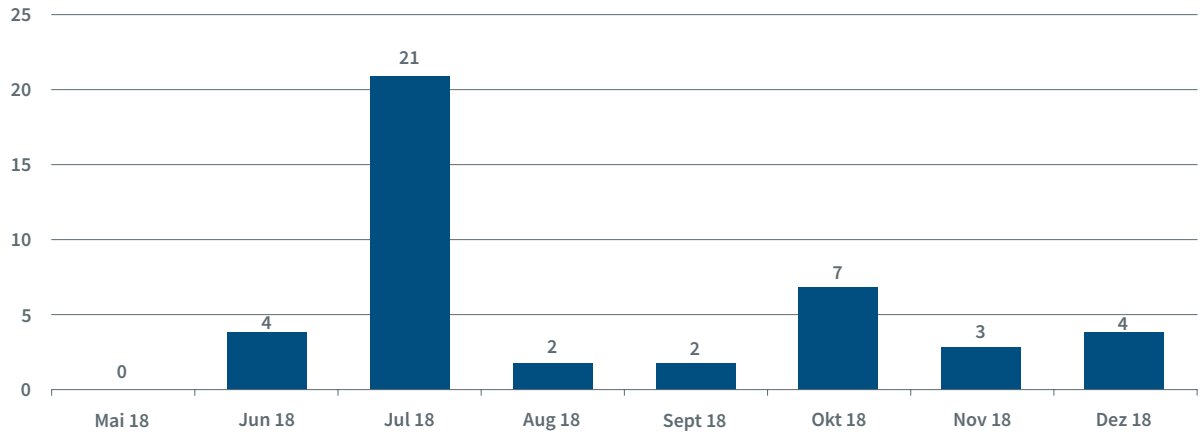
Auch die inhaltliche Abstimmung zwischen den europäischen Aufsichtsbehörden im Rahmen des sogenannten One-Stop-Shop-Verfahrens nach Artikel 60 DSGVO zeigt einen stetigen Zuwachs. Auffallend ist zudem die Spitze an Artikel-64-Verfahren im Juli 2018. Zu diesem Zeitpunkt haben zahlreiche Aufsichtsbehörden der EU-Mitgliedstaaten, auch die deutschen, ihre nationalen Datenschutzfolgeabschätzungslisten (DSFA) nach Artikel 35 Absatz 4 DSGVO dem EDSA zur Stellungnahme vorgelegt.

Eingeleitete Verfahren nach Artikel 60 und 64 DSGVO



Eine wesentliche Aufgabe der ZASt ist es, die Herstellung gemeinsamer Standpunkte der deutschen Aufsichtsbehörden nach § 18 BDSG zu koordinieren. Hierfür wird im IMI-System eine „Interne Konsultation“ unter Einbindung der Aufsichtsbehörden des Bundes und der Länder von der ZASt initiiert und der so ermittelte gemeinsame Standpunkt an den EDSA wiederum über das IMI-System übermittelt. Dies betraf im Berichtszeitraum auch die vorgenannten DSFA-Listen im Juli. Wenn Aufsichtsbehörden anderer EU-Mitgliedstaaten im Wege des Amtshilfeverfahrens nach Art. 61 DSGVO Antworten der deutschen Datenschutzbehörden begehrten, wurde die Abstimmung der deutschen Rückmeldungen ebenfalls auf diesem Wege koordiniert.

Eingeleitete interne Konsultationen der ZASt



17.5 Personelle und organisatorische Entwicklung

Seit der Unabhängigkeit des BfDI wächst meine Dienststelle kontinuierlich. Dies ist zur Erfüllung der stetig zunehmenden Aufgaben auch dringend notwendig. Aufgrund der nach wie vor erheblichen Personal- und Raumbedarfe ist dieser Prozess jedoch noch keineswegs abgeschlossen.

Seit dem 1. Januar 2016 ist der BfDI eine eigenständige oberste Bundesbehörde. Die Zahl der Planstellen bzw. Stellen hat sich von 90 im Jahr 2015 auf etwas mehr als 250 im Haushalt 2019 erhöht. Der Haushalt stieg von 9,3 Millionen € im Jahr 2015 auf 25,2 Millionen € für das Jahr 2019. Dieses erhebliche Wachstum ist kein Selbstzweck, sondern zwingende Folge der stetig zunehmenden Aufgaben, insbesondere aufgrund der DSGVO (vgl. o. Nr. 1.1) sowie der Rechtsprechung des Bundesverfassungsgerichts zur Kontrollfunktion des BfDI gegenüber den Sicherheitsbehörden (vgl. 26. TB Nr. 10.2.10.1). Durch die dynamisch voranschreitende Digitalisierung aller Lebensbereiche und die zunehmende Überwachungstätigkeit der Sicherheitsbehörden setzt sich dieser Aufgabenzuwachs weiter fort.

Entsprechend ist die personelle, organisatorische und infrastrukturelle Weiterentwicklung der Dienststelle noch längst nicht abgeschlossen.

17.6 BfDI als Ausbildungsbehörde

Referendare, Praktikanten und Anwärter zeigen weiterhin Interesse am Datenschutz.

Das Interesse an Praktikumsaufenthalten in meiner Dienststelle ist unverändert groß. Nachdem im vorherigen Berichtszeitraum aufgrund eingeschränkter Kapazitäten lediglich zwei Referendare Teile ihrer Ausbildung in meinem Hause absolvieren konnten, bietet meine Dienststelle seit dem Jahr 2017 wieder in deutlich mehr Fällen die Möglichkeit, hier Teile der Ausbildung bzw. Pflichtpraktika zu absolvieren. Dies betraf zehn Praktika sowie sechs Referendariate. Ferner leisteten fünf Anwärter des gehobenen Verwaltungsdienstes das Pflichtpraktikum in meiner Dienststelle ab. Erstmals nimmt ein Anwärter meiner Dienststelle am Studiengang Verwaltungsinformatik der Hochschule des Bundes für öffentliche Verwaltung teil. Diese Studienmöglichkeit möchte ich auch zukünftig eröffnen, um den Personalbedarf an der Schnittstelle zwischen den klassischen Verwaltungstätigkeiten und dem Bereich der Informationstechnik zu decken.

17.7 Weiterer Dienstsitz in Bonn/ Verbindungsbüro in Berlin

Das Verbindungsbüro in Berlin stellt eine wirkungsvolle und direkte Teilnahme am politischen Geschehen in Berlin sicher.

Ende 2018 umfasste das Verbindungsbüro in Berlin-Mitte zwölf Beschäftigte. 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, deren erster Dienstsitz in Berlin angesiedelt ist. Damit wird eine wirkungsvolle und direkte Teilnahme am politischen Geschehen in der Bundeshauptstadt sichergestellt. Zugleich wird der Dienstreiseaufwand meiner Bonner Dienststelle deutlich reduziert. Schließlich werden auch Besuchergruppen im Verbindungsbüro in Berlin empfangen.

Bezüglich der Unterbringung des zusätzlichen Personals aus dem Haushalt 2017 am Standort Bonn wurden entsprechende Büroräume in der Godesberger Allee 136 angemietet. Untergebracht wurden in der Godesberger Allee die Zentrale Anlaufstelle (ZASt), das Referat 14 und die Arbeitsgruppe 12 (insgesamt 40 Büros).

17.8 Veranstaltungen

Als Veranstalter von Fachsymposien wird im Rahmen der Öffentlichkeitsarbeit jedes Jahr ein neuer fachlicher Schwerpunkt gesetzt. Auf weitere Veranstaltungen werden Bürgerinnen und Bürger zu diversen Themen rund um den Datenschutz informiert.

Im Berichtszeitraum habe ich zwei Fachveranstaltungen organisiert. Beim 2017 ausgerichteten „Symposium zum Datenschutz im automatisierten und vernetzten Auto“ konnte ein wichtiges Zukunftsthema mit Experten aus Politik, Wirtschaft und Zivilgesellschaft beleuchtet und diskutiert werden (vgl. hierzu unter Nr. 1.6). Nicht minder wichtig war die Dialogkonferenz zur Wahrnehmung von Datenschutzrechten durch Kinder, die ich 2018 zusammen mit „Deutschland sicher im Netz“ (DsiN) und dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) veranstaltet habe (vgl. hierzu unter Nr. 1.7).

Neben diesen Symposien beteiligte sich meine Dienststelle in den Jahren 2017 und 2018 erfolgreich am Tag der offenen Tür der Bundesregierung in Berlin. Dabei informierten meine Mitarbeiterinnen und Mitarbeiter und ich über verschiedene Aspekte von Datenschutz und Informationsfreiheit und führten viele interessante Gespräche mit Bürgerinnen und Bürgern.

17.8.1 Veranstaltung zu Binding Corporate Rules

Im Juni 2017 war die BfDI Gastgeberin eines internationalen Workshops für die europäischen Datenschutzaufsichtsbehörden zum Thema „Binding Corporate Rules“.

Innerhalb global agierender Konzerne werden personenbezogene Daten auch an Konzernunternehmen übermittelt, die in Ländern ihren Sitz haben, in denen die datenschutzrechtlichen Vorgaben der EU nicht gelten (sog. Drittstaaten). Um personenbezogene Daten auch in diesen Fällen angemessen zu schützen, sind entsprechende Schutzmaßnahmen, insbesondere geeignete Garantien, vorzusehen. Solche Garantien bestehen üblicherweise darin, dass sich die Unternehmen verbindliche unternehmensinterne Datenschutzvorschriften (Binding Corporate Rules, kurz BCR) geben. In dem internationalen Workshop haben Fachleute aus verschiedenen Aufsichtsbehörden die inhaltlichen Anforderungen an BCR, die von den Unternehmen erfüllt werden müssen, sowie die Prozesse für ihre europaweite Anerkennung abgestimmt und fortentwickelt.

17.9 Öffentlichkeitsarbeit

Auf vielfältige Art und Weise habe ich in den beiden vorangegangenen Jahren die Öffentlichkeit über datenschutzrechtliche Themen informiert und aufgeklärt. Wie so oft stand auch hier die DSGVO im Zentrum.

Besuchergruppen

Meine Mitarbeiterinnen und Mitarbeiter des Berliner Verbindungsbüros betreuten wieder Besuchergruppen von Mitgliedern des Deutschen Bundestages. Insgesamt 15 Gruppen mit jeweils 50 Teilnehmerinnen und Teilnehmern wurden empfangen. Darüber hinaus waren fünf weitere Besuchergruppen von Universitäten und Bildungsträgern in meiner Dienststelle zu Gast.

Informationsmaterial

Ein zentraler Bestandteil der Öffentlichkeitsarbeit ist die Herausgabe zahlreicher Broschüren und Flyer. Dabei wenden sich die Informationsbroschüren an Leserinnen und Leser, die sich vertieft in ein Themengebiet einarbeiten möchten. Diese „Info“-Broschüren enthalten neben Beiträgen zur Rechtsmaterie auch die einschlägigen gesetzlichen Vorschriften. Demgegenüber sollen die knapperen und handlicheren Flyer vor allem Bürgerinnen und Bürger ansprechen, die kurze Informationen und klare Handreichungen zum Datenschutz suchen. Anlässlich des Wirksamwerdens der DSGVO am 25. Mai 2018 wurde das Informationsmaterial umfassend überarbeitet. Die DSGVO führte zu einer stark gestiegenen Nachfrage bei den Publikationen. Allein die Broschüre zum neuen Datenschutzrecht (bis Mitte 2018 „Info 6“, seitdem „Info 1“) wurde im Berichtszeitraum über 100.000-mal aufgelegt. Die auch sonst gestiegenen Bestellzahlen zeigen noch einmal deutlich das verstärkte Interesse am Thema Datenschutz (vgl. Kasten a und Kasten b zu Nr. 17.9). Sämtliches Informationsmaterial kann auf meiner Internetseite unter www.datenschutz.bund.de heruntergeladen oder bestellt werden.

Informationen für Abgeordnete

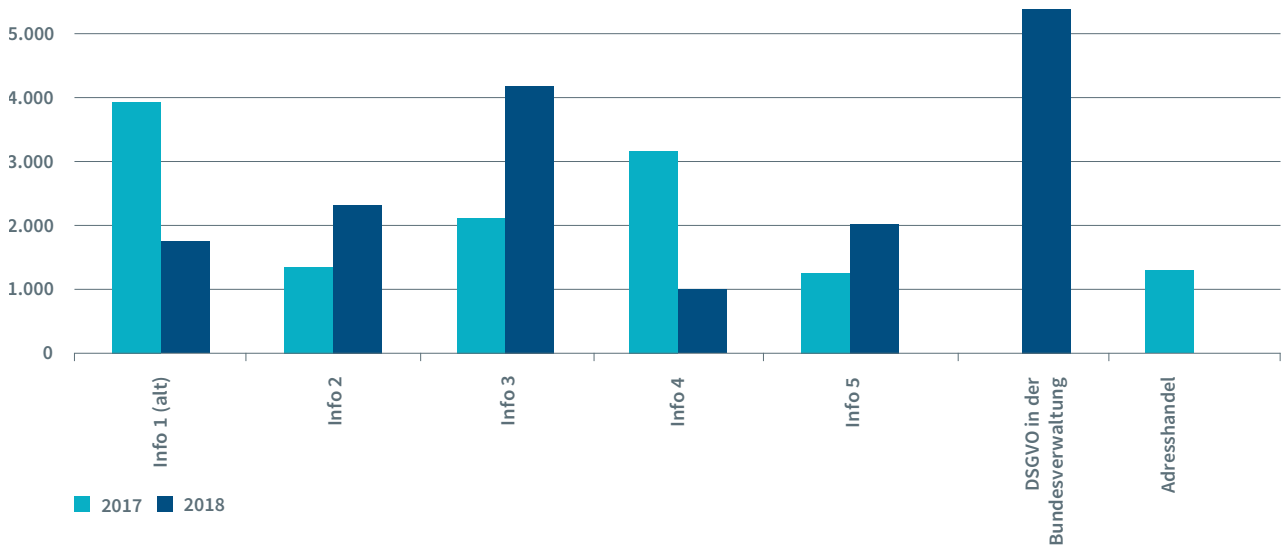
Auch meine Publikationsreihe „Datenschutz kompakt“ konnte ich erweitern. Diese befasst sich im übersichtlichen Format mit aktuellen Themen zum Datenschutz. Dabei geht es weniger darum, datenschutzpolitische Positionen zu vermitteln, als neutral über relevante datenschutzrechtliche Zusammenhänge zu informieren. Im Berichtszeitraum waren dies beispielsweise Informationen zu Themen wie dem neu geschaffenen Europäischen Datenschutzausschuss (vgl. o. Nr. 2.1), dem digitalen Sprachassistenten oder dem europäischen

Gesetzgebungsverfahren für eine neue E-Privacy-Verordnung (vgl. o. Nr. 15.1.2). Auch wenn sich die Reihe insbesondere an Abgeordnete des Deutschen Bundestages richtet, werden sämtliche Ausgaben von „Datenschutz kompakt“ auch auf meiner Website bereitgestellt und können somit von allen Interessierten gelesen und heruntergeladen werden. Daneben erhielten die Abgeordneten des 19. Deutschen Bundestages zu Beginn der Legislaturperiode eine Informationsmappe, mit der sie sich einen Überblick über meine Aufgaben sowie Zusammenarbeit mit dem Bundestag verschaffen konnten. Da die DSGVO für viele Mitglieder des Bundestages im letzten Jahr nicht nur ein politisches Thema darstellte, sondern sie auch ganz unmittelbar bei ihrer täglichen Arbeit mit personenbezogenen Daten betraf, erreichten mich viele Unterstützungsersuchen von Abgeordneten, wie am besten mit dem neuen Recht umzugehen sei. Die Fragen reichten dabei vom Umgang mit Daten von Bürgern, die sich im Rahmen von Anfragen oder Petitionen an die Abgeordneten wenden, über die Nutzung von Sozialen Medien bis hin zur Verarbeitung von Daten der in den Büros beschäftigten Mitarbeiterinnen und Mitarbeiter. Eine Antwort auf diese und weitere Fragen im Zusammenhang mit dem neuen Datenschutzrecht habe ich in meiner Handreichung für die Mitglieder des Deutschen Bundestages unter dem Titel „Datenschutz-Grundverordnung für Abgeordnete“ veröffentlicht (vgl. hierzu auch unter Nr. 14.1.1).

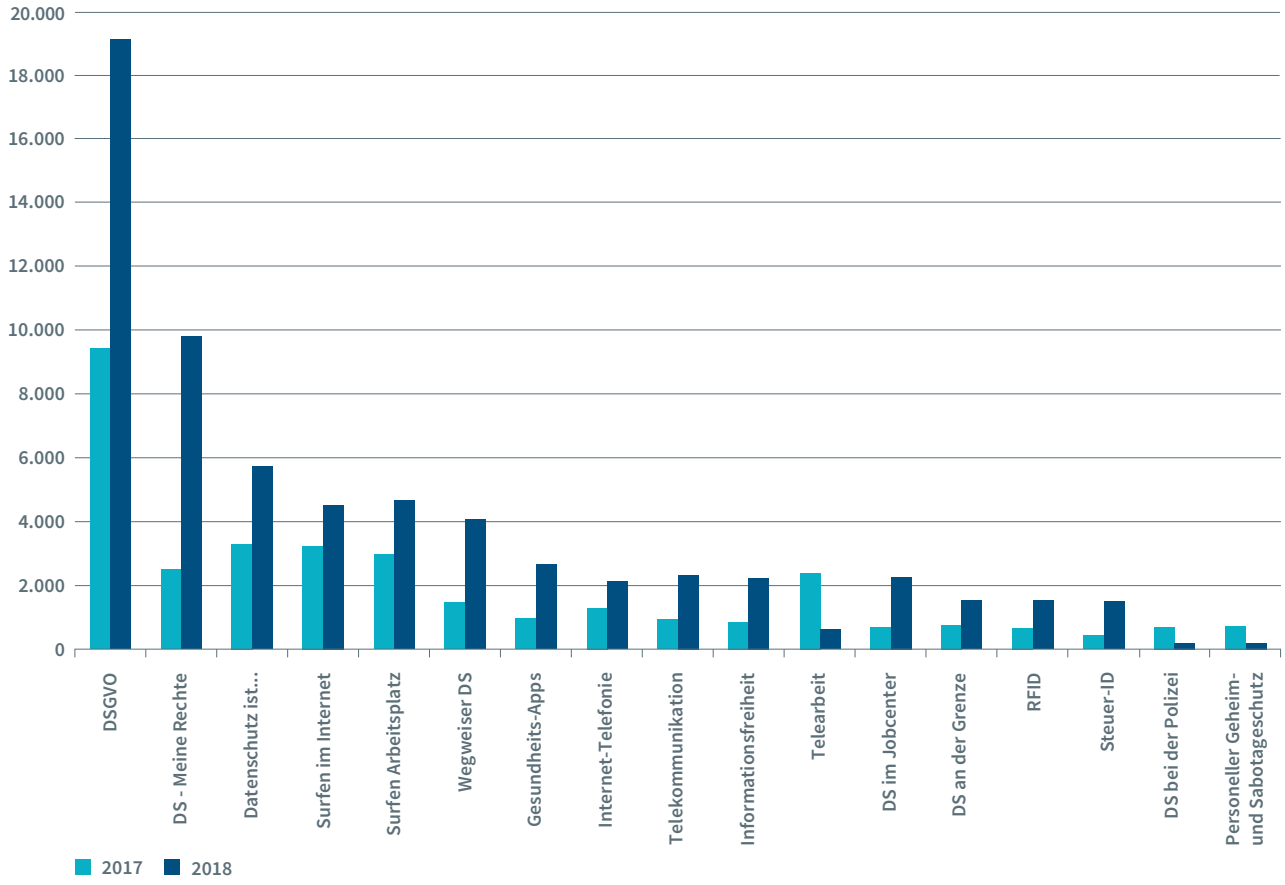
Kurzpapiere der Datenschutzkonferenz

Neben vielen eigenen Veröffentlichungen habe ich auch an der Erstellung der Kurzpapiere der Datenschutzkonferenz (DSK) zum neuen Datenschutzrecht mitgewirkt. Diese dienen der ersten Orientierung, wie bestimmte Fragestellungen von den Datenschutzaufsichtsbehörden des Bundes und der Länder bewertet werden. Im Berichtszeitraum wurden von der DSK insgesamt 19 Kurzpapiere beschlossen (vgl. Kasten zu Nr. 17.9).

Abgegebene Broschüren



Abgegebene Flyer



Liste der Kurzpapiere der Datenschutzkonferenz

- → 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DSGVO
- → 2 Aufsichtsbefugnisse/Sanktionen
- → 3 Verarbeitung personenbezogener Daten für Werbung
- → 4 Datenübermittlung in Drittländer
- → 5 Datenschutz-Folgenabschätzung nach Art. 35 DSGVO
- → 6 Auskunftsrecht der betroffenen Person, Art. 15 DSGVO
- → 7 Marktortprinzip: Regelungen für außereuropäische Unternehmen
- → 8 Recht auf Löschung / „Recht auf Vergessenwerden“
- → 9 Maßnahmenplan „DSGVO“ für Unternehmen
- → 10 Zertifizierung nach Art. 42 DSGVO
- → 11 Informationspflichten bei Dritt- und Direkterhebung
- → 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
- → 13 Beschäftigtendatenschutz
- → 14 Videoüberwachung nach der Datenschutz-Grundverordnung
- → 15 Auftragsverarbeitung, Art. 28 DSGVO
- → 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO
- → 17 Besondere Kategorien personenbezogener Daten
- → 18 Risiko für die Rechte und Freiheiten natürlicher Personen
- → 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO

17.10 Besuche ausländischer Delegationen

Verschiedene Gruppen von Datenschutzexperten aus Asien und Afrika besuchten meine Dienststelle, um aktuelle Fragen des Datenschutzes zu diskutieren und Erfahrungen auszutauschen. Auch führte ich ein bilaterales Gespräch mit der britischen Datenschutzbeauftragten zu den Folgen des „Brexit“.

Entsprechend der Praxis in den Vorjahren habe ich auch im Berichtszeitraum ausländische Delegationen in meiner Dienststelle gerne empfangen. Eine Delegation der japanischen „Personal Information Protection Commission (PIPC) und eine Gruppe der „Personal Data Protection Commission“ der Republik Singapur informierten sich über das Konzept des Datenschutzes in Deutschland und die nationalen Erfahrungen mit dem europäischen Recht.

Aus gegebenem Anlass empfing ich die britische Datenschutzbeauftragte, Elizabeth Denham, zu einem bilateralen Besuch in Bonn. Dabei standen die Folgen des „Brexit“ im Mittelpunkt der Erörterungen.

Besonderes Augenmerk legte ich zudem auf Gespräche mit den Leitern neu gegründeter Datenschutzaufsichtsbehörden. Für alle Beteiligten bereichernd erwiesen sich in diesem Zusammenhang der Meinungsaustausch mit der Vorsitzenden der südafrikanischen Behörde „Information Regulator (South Africa)“ sowie das Gespräch mit dem Präsidenten der türkischen Datenschutzbehörde.

Gerne bin ich bereit, den Aufbau und die Tätigkeit ausländischer Datenschutzbehörden zu unterstützen und zu diesem Zweck den Erfahrungsaustausch fortzusetzen.

Anlagen

Anlage 1
Übersicht über die durchgeführten Kontrollen, Beratungs- und Informationsbesuche

Bundesministerium des Innern, für Bau und Heimat

- Bundesverwaltungsamt (AZR)
- Bundesamt für Migration und Flüchtlinge (2, Zentrale und Außenstelle)
- Bundesanstalt Technisches Hilfswerk (2)
- Statistisches Bundesamt
- Bundesinstitut für Bevölkerungsforschung
- Bundeskriminalamt (6)
- Bundespolizei (6)
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesamt für Verfassungsschutz (3)

Bundeskanzleramt

- Bundesnachrichtendienst (3)

Bundesministerium für Arbeit und Soziales

- Bundesagentur für Arbeit (Zentrale)
- Bundesagentur für Arbeit (Agentur für Arbeit Köln)
- Bundesagentur für Arbeit (Agentur für Arbeit Mainz)
- 6 Jobcenter (Kreis Wesel, Prignitz, Ludwigslust-Parchim, Duisburg, Mittelsachsen, Cochem-Zell)

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

- Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
- Gesellschaft für internationale Zusammenarbeit

Beauftragte der Bundesregierung für Kultur und Medien

- Behörde des Bundesbeauftragten für die Stasi-Unterlagen (2)

Bundesministerium der Justiz und für Verbraucherschutz

- Bundesamt für Justiz

Bundesministerium der Verteidigung

- Bundeswehrkrankenhaus Ulm (2)
- Bundesamt für Personalmanagement der Bundeswehr
- Bundesamt für den Militärischen Abschirmdienst (2)

Bundesministerium der Finanzen

- Bundesministerium der Finanzen (2)
- Senatsverwaltung für Finanzen Berlin (Steuerabteilung)
- Finanzämter (Friedrichshain-Kreuzberg, Lichtenberg)
- Zollkriminalamt (2)

Bundespräsidialamt

- Bundespräsidialamt

Auswärtiges Amt

- Auswärtiges Amt (2, Zentrale, Auslandsvertretung Bangkok)

Bundesministerium für Bildung und Forschung

- Bundesministerium für Bildung und Forschung

Bundesministerium für Verkehr und digitale Infrastruktur

- Bundesministerium für Verkehr und digitale Infrastruktur (Bonn)
- Bundesstelle für Flugunfalluntersuchung
- Generaldirektion Wasserstraßen und Schifffahrt
- Bundesstelle für Seeunfalluntersuchung
- Kraftfahrt-Bundesamt
- Gemeinsames Lagezentrum See im Maritimen Sicherheitszentrum
- Bundesaufsichtsamt für Flugsicherung
- Deutscher Wetterdienst
- Bundesstelle für Eisenbahnunfalluntersuchung
- Bundesanstalt für Wasserbau

Bundesministerium für Ernährung und Landwirtschaft

- Bundesanstalt für Landwirtschaft und Ernährung
- Bundessortenamt
- Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
- Max-Rubner-Institut

Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit

- Bundesamt für Naturschutz (Bonn)

Bundesministerium für Gesundheit

- Bundesministerium für Gesundheit (13)
- GKV Spitzenverband
- Bundesversicherungsamt (4)
- Gemeinsamer Bundesausschuss (2)
- Robert-Koch-Institut
- Deutsches Institut für Medizinische Dokumentation und Information

Telekommunikationsunternehmen

- Tele Columbus Betriebs GmbH
- Vodafone GmbH (4)
- Lebara Germany Ltd.
- 1 & 1 Internet SE
- Deutsche Telekom AG (3)
- Deutsche Telekom Service GmbH
- BITel Gesellschaft für Telekommunikation mbH
- EWE TEL GmbH
- QSC AG
- valantic GmbH
- abl social federation GmbH
- Telefónica Germany GmbH & Co. OHG (2)
- GELSEN-NET Kommunikationsgesellschaft mbH

Postdienstunternehmen

- Goldmann Consulting e.K.
- MEDIA Logistik GmbH
- Postcon Deutschland B.V. & Co. KG
- Hermes Germany GmbH
- Euregio MH Boten GmbH
- Deutsche Post AG

Sonstige

- Bundesdruckerei
- Leibnitz-Institut für Bildungsverläufe e. V.
- WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH
- DRV Bund (Zentrale - 2)
- DRV Bund, Versicherungs- und Rentenabteilung in Gera
- DRV Bund, Prüfdienst (Hamburg und Schleswig-Holstein)

DRV Bund, Reha-Zentrum Stieben

DRV Bund, Reha-Zentrum Römerberg

DRV Knappschaft Bahn See (Zentrale)

DRV Knappschaft Bahn See, Knappschaftsklinikum Saar, Püttlingen

Deutsche Angestellten Krankenkasse (DAK)

BARMER

Techniker Krankenkasse

atlas bkk ahlmann

Bertelsmann BKK

BIG direkt

BKK B. Braun Melsungen

BKK Diakonie

BKK ZF & Partner

Pronova BKK

Salus BKK

Berufsgenossenschaft Handel und Warendistribution

Berufsgenossenschaft Rohstoffe und chemische Industrie

Verwaltungsberufsgenossenschaft

Unfallkasse des Bundes

Sozialversicherung für Landwirtschaft, Forsten und Gartenbau

Künstlersozialkasse

Treuhandstelle der Nationalen Kohorte

Unternehmen aus der Geheimschutzbetreuung des BMWi (4)

Anlage 2
Übersicht über Beanstandungen

Bundesministerium des Innern, für Bau und Heimat

Bundeskriminalamt

Die Speicherung der personenbezogenen Daten in der »Zentraldatei ST 15 Funkzellendatenabgleich Brandanschläge/Sprengstoffanschläge (BA/SP)« und den auf Grundlage dieser Daten durchgeführten Datenabgleich habe ich gemäß § 25 Absatz 1 BDSG (alt) beanstandet.

Es fehlt an einer Rechtsgrundlage. § 7 Absatz 1 BKAG trägt die Maßnahme nicht, weil diese inhaltlich eine Rasterfahndung darstellt oder einer solchen zumindest gleichkommt. Auch § 98a StPO kommt als Rechtsgrundlage schon deshalb nicht in Betracht, weil die Maßnahme nicht als Rasterfahndung in einem konkreten Strafverfahren angeordnet wurde.

Bundespolizei

Die Bundespolizei führt die Datei »Geschützter Grenzfahndungsbestand«, ohne dass eine Rechtsverordnung das Nähere über die Art der Daten bestimmt, die nach §§ 30 Absatz 1 Satz 2, 31 Absatz 1 Satz 2 BPolG bei der Ausschreibung zur grenzpolizeilichen Beobachtung gespeichert werden dürfen. Dies habe ich gemäß § 25 Absatz 1 BDSG (alt) als Verstoß gegen §§ 30 Abs. 1 Satz 2 und 31 Absatz 1 Satz 2 BPolG beanstandet.

Bundesministerium für Arbeit und Soziales

Bundesagentur für Arbeit, Jobcenter

Der Datenmüll eines Jobcenters, einer Agentur für Arbeit und eines Ärztlichen Dienstes wurde in einem großen abschließbaren Container entsorgt. Dieser Container war jedoch defekt, sodass ein Zugriff auf die darin enthaltenen sensiblen Daten für Dritte möglich war. Aufgrund des großen Umfangs und der hohen Sensibilität der vorgefundenen Daten habe ich Beanstandungen gegenüber dem Jobcenter und der Bundesagentur für Arbeit ausgesprochen. Diese haben den defekten Container umgehend ersetzt. Das Jobcenter hat seine Papierentsorgung vollständig auf das bewährte System mit Datenschutzmülltonnen umgestellt.

Telekommunikationsunternehmen

M-Net Telekommunikations GmbH

Verstoß gegen §§ 3a, 4 und 5 BDSG i. V. m. § 25 Absatz 1 BDSG (alt) wegen eines rechtswidrig durchgeführten Rufnummernportierungsverfahrens

Deutsche Telekom AG

Verstoß gegen § 95 Absatz 3 TKG gemäß § 115 Absatz 4 TKG i. V. m. § 25 Absatz 1 BDSG (alt) wegen unbefristeter Speicherung von Bestandsdaten

WhatsApp Inc.

Verstoß gegen § 95 Absatz 1 Satz 1 und 3 TKG, § 94 TKG i. V. m. § 4a BDSG (alt). wegen keiner datenschutzrechtlich wirksamen Einwilligung zur Übermittlung der Mobilfunknummer von der WhatsApp Inc. an Facebook

Rapidata GmbH

Beanstandung gemäß § 115 Absatz 4 TKG i. V. m. § 25 Absatz. 1 BDSG (alt). der Rapidata GmbH wegen mangelnder Zusammenarbeit

Gesetzliche Krankenkassen und Gesetzliche Unfallversicherungsträger

Unfallkasse des Bundes

Vier Beanstandungen

zwei Verstöße gegen die Regelungen der §§ 106 ff. BBG

Verstoß gegen das in § 24 Absatz 4 BDSG (alt) normierte Unterstützungsgebot

Verstoß gegen § 35 Absatz 1 SGB I (Sozialgeheimnis)

Gesetzliche Krankenkassen

Zwei Beanstandungen

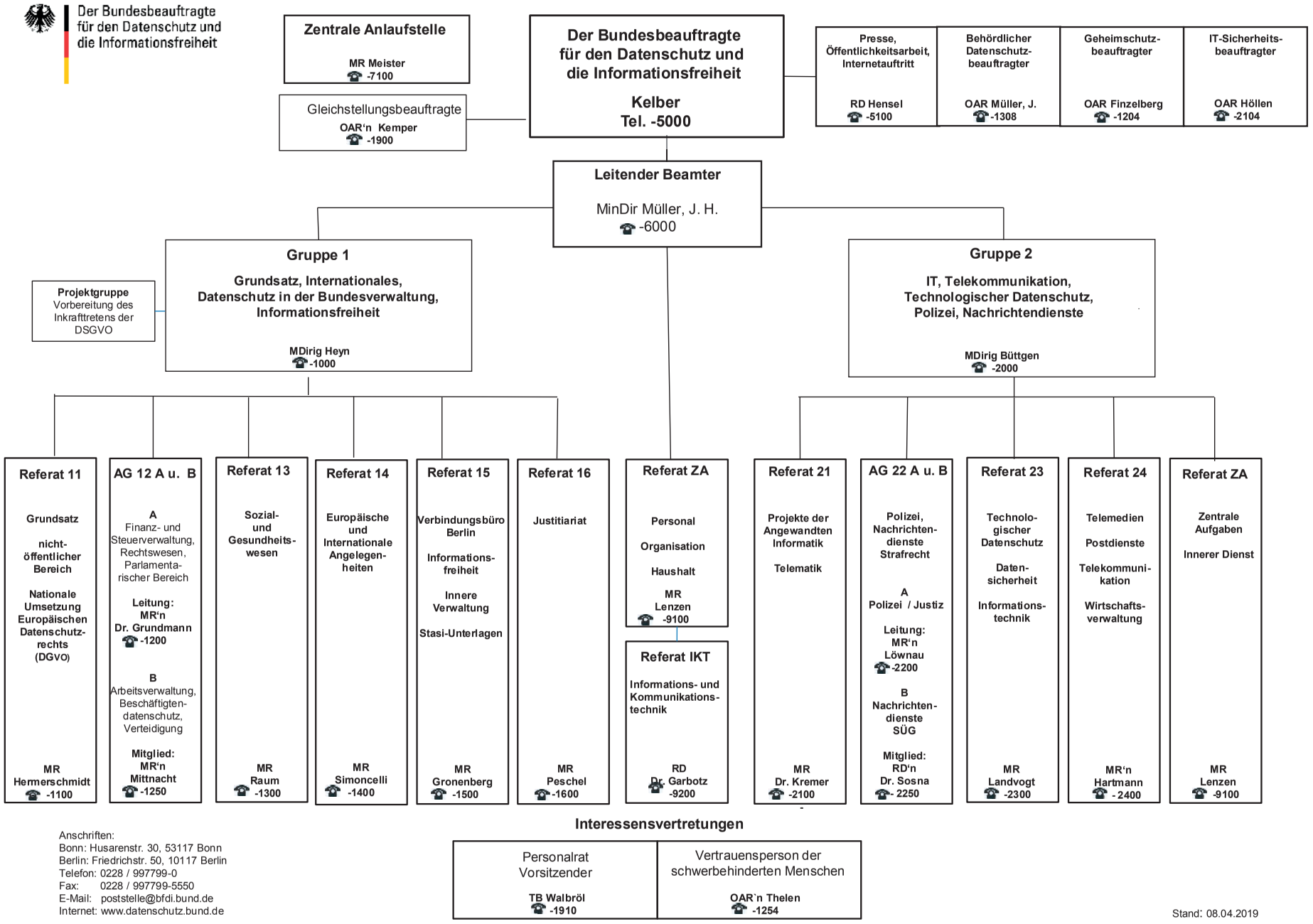
Verstoß gegen § 81 Abs. 4 SGB X i. V. m. § 25 Absatz 1 BDSG (alt). und § 83a SGB X (alt) wegen Nichtmitteilung eines Datenschutzverstoßes

Verstoß gegen § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG (alt). und Verstoßes gegen § 276 Absatz 2 SGB V wegen rechtswidriger Erhebung von Gesundheitsdaten

Gesetzliche Unfallversicherung

Eine Beanstandung

Verstoß gegen § 81 Absatz 4 SGB X i. V. m. § 25 Absatz 1 BDSG (alt) und § 200 Absatz 2 SGB VII sowie § 35 Absatz 1 Satz 1 SGB I (alt) wegen rechtswidriger Beauftragung eines Gutachters sowie Übermittlung von Sozialdaten an diesen



Anschriften:
Bonn: Husarenstr. 30, 53117 Bonn
Berlin: Friedrichstr. 50, 10117 Berlin
Telefon: 0228 / 997799-0
Fax: 0228 / 997799-5550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de

Stand: 08.04.2019

Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis/Begriffe

a.a.O	am angegebenen Orte
AA	Agenturen für Arbeit
AA	Auswärtiges Amt
ABG	Automatisierte und biometriegestützte Grenzkontrolle
ABl.	Amtsblatt der Europäischen Union
ABMG	Autobahnmautgesetz
Abs.	Absatz
ACTA	Anti Counterfeiting Trade Agreement
AEO	Authorized Economic Operator
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft, aber auch: Arbeitsgruppe
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
AnaCredit	Analytical Credit Datasets
AND	Ausländische Nachrichtendienste
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
APAK	Abschlussprüferaufsichtskommission
APEC	Asia Pacific Economic Cooperation
APOK	Anwenderportal Onlinekanal
ARGE	Arbeitsgemeinschaften nach dem Sozialgesetzbuch II
Art.	Artikel
AS	Autorisierte Stelle
ATD	Anti-Terror-Datei
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
BfD/BA	Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BfDBW	Beauftragte(r) für den Datenschutz der Bundeswehr
BFDG	Bundesfreiwilligendienstgesetz
BfDI	Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit
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 Übermittlung 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
BMUB	Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
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
d.h.	das heißt
DA KG	Dienstanweisung zum Kindergeld nach dem Einkommensteuergesetz
DA PVD	Dienstanweisung für den Polizeivollzugsdienst beim Deutschen Bundestag
DB	Deutsche Bahn
DDR	Deutsche Demokratische Republik
DECT	Digital Enhanced Cordless Telecommunications
DEK	Datenethikkommission
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 Umsetzungsgesetz EU
DSGVO	Datenschutz Grundverordnung
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSL	Digital Subscriber Line
DSRV	Datenstelle der Träger der Rentenversicherung
DTAG	Deutsche Telekom AG
DV/dv	Datenverarbeitung
DVB C	Digital Video Broadcasting Cable
DWH	Data Warehouse
e. V.	eingetragener Verein
E-Akte	elektronische Akte
eAT	elektronischer Aufenthaltstitel
E Commerce	Elektronic Commerce/Elektronischer Handel
ED	Erkennungsdienst
EDPS	Europäischer Datenschutzbeauftragter
EDSA	Europäischer Datenschutzausschuss
EDV	Elektronische Datenverarbeitung
EES	Ein- und Ausreiseregister
EETS / EEMD	Europäischer Elektronischer Mautdienst
eFBS	Einheitliches Fallbearbeitungssystem
EG	Europäische Gemeinschaft(en)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
eGK	elektronische Gesundheitskarte
EGovG	Gesetz zur Förderung der elektronischen Verwaltung
EG ZIS	Europäisches Zollinformationssystem
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
EKD	Evangelische Kirche in Deutschland
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
FAQ	Frequently Asked Questions (häufig gestellte Fragen)
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
FBI	Federal Bureau of Investigation, USA
FDZ	Forschungsdatenzentrum
ff.	folgende
FFI	Foreign Financial Institution (ausländische Finanzinstitute)
FG	Finanzgericht
FGO	Finanzgerichtsordnung
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
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
gem.	gemäß
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	Handlungsempfehlung/Geschäftsanweisung der BA
HIS	Hinweis- und Informationssystem
HKP	häusliche Krankenpflege
HPC	Health Professional Card
HS Bund	Hochschule des Bundes für öffentliche Verwaltung
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
HZA	Hauptzollamt
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
IAB	Institut für Arbeitsmarkt- und Berufsforschung
IATA	International Air Transport Association
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
KDAV	Kundendatenauskunftsverordnung
KdU	Kosten der Unterkunft und Heizung
KEV	Kontrolleinheit Verkehrswege
KFU	Krebsfrüherkennungsrichtlinien
Kfz	Kraftfahrzeug
KGSG	Gesetz zur Neuregelung des Kulturgutschutzrechts
KI	Künstliche Intelligenz
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
m.w.N.	mit weiteren Nachweisen
MAD	Militärischer Abschirmdienst
MAK	Mindestanforderungen an das Kreditgeschäft der Kreditinstitute
MBR	Mitarbeiter- und Beschwerderegister
MDK	Medizinischer Dienst der Krankenversicherung
MfS	Ministerium für Staatssicherheit
Mi1Nw	Militärisches Nachrichtenwesen
MI6	Military Intelligence, Section 6
ML	Maschinelles Lernen
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
MZG	Mikrozensusgesetz
NADIS	Nachrichtendienstliches Informationssystem
NADIS-WN	Nachrichtendienstliches 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
o.g.	oben genannt
OCR	Optical Character Recognition (Optische Zeichenerkennung)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OK	Organisierte Kriminalität
OLAF	Europäisches Amt für Betrugsbekämpfung
OMS	Optimierte Meldeverfahren in der sozialen Sicherung
OpoI	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.	Ratsdokument (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	Schuldnerverzeichnisführungs-verordnung
SchwarzArbG	Schwarzarbeitsbekämpfungsgesetz
SDDSG	Suchdienstedatenschutzgesetz
SDM	Standard-Datenschutzmodell
SDÜ	Schengener Durchführungsüberein-kommen
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 IX	Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinder-ter Menschen)
SGB IV	Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozi-alversicherung)
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 X	Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozial-datenschutz)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SGB XII	Sozialgesetzbuch Zwölftes Buch (Sozialhilfe)
SiBe	Sicherheitsbevollmächtigter
SigG	Signaturgesetz
SIM	Subscriber Identity Module
SiMKo2	Sichere Mobile Kommunikation
SMS	Short Message Service
SNS	Sichere Netzübergreifende Sprachkom-munikation
SOG	Gesetz über öffentliche Sicherheit und Ordnung
sog.	so genannt
SPD	Sozialdemokratische Partei Deutsch-lands
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 Staats-sicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi Unterlagen Gesetz)
StVBG	Steuerverkürzungsbekämpfungsgesetz
StVergAbG	Steuervergünstigungsabbaugesetz
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
SÜFV	Sicherheitsüberprüfungsfeststellungs-verordnung
SUG	Seesicherheits-Untersuchungs-Gesetz
SÜG	Sicherheitsüberprüfungsgesetz
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 Maß-nahmen zur Überwachung der Tele-kommunikation
TMG	Telemediengesetz
TNB	Teilnehmernetzbetreiber
TOP	Tagesordnungspunkt
TPG	Transplantationsgesetz
TR	Technische Richtlinie
TR TKÜV	Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwa-chung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten

TrEinV	Transparenzregistereinsichtnahmeverordnung
TS	Technology Subgroup
TTIP	Transatlantic Trade and Investment Partnership
u.a.	unter anderem
u.ä.	und ähnliches
u.U.	unter Umständen
UAS	Unmanned Aerial Systems
UBSKM	Unabhängiger Beauftragter für Fragen des sexuellen Kindesmissbrauchs
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
usw.	und so weiter
UWG	Gesetz gegen den Unlauteren Wettbewerb
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
WehrMed StatInstBw	Institut für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr
WehrRÄndG	Wehrrechtsänderungsgesetz 2011
WiMax	Wordwide Interoperability for Microwave Access Standard gemäß IEEE 802.16a für lokale Funknetze
WLAN	Wireless Local Area Network
WoGG	Wohngeldgesetz
WP	Working Paper
WPersAV	Personalaktenverordnung Wehrpflichtige
WpHGMaAnzV	WpHG Mitarbeiteranzeigeverordnung
WPK	Wirtschaftsprüferkammer
WPO	Wirtschaftsprüferordnung
WPPJ	Working Party Police and Justice (Arbeitsgruppe Polizei und Justiz)
WSA	Wasser- und Schifffahrtsamt
www	World wide web
XML	Extensible Markup Language
z.B.	zum Beispiel
z.T.	zum Teil
ZAG	Zentren für Arbeit und Grundsicherung
ZAUBER	Abrufverfahren
ZAV	Zentrale Auslands- und Fachvermittlung der Bundesagentur für Arbeit
ZDG	Zivildienstgesetz
ZensG 2011	Zensusgesetz 2011
ZensVorbG2021	Zensusvorbereitungsgesetz 2021
ZentrLuR MedLw	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
26.	2015–2016	18/12500

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn

Tel. +49 (0) 228 997799-0
Fax +49 (0) 228 997799-5550
E-Mail: poststelle@bfdi.bund.de
Internet: www.datenschutz.bund.de

Bonn 2019

Dieser Bericht ist als Bundestagsdrucksache 19/9800 erschienen.

Druck:
Silber Druck oHG
Am Waldstrauch 1
34266 Niestetal