Tätigkeitsbericht 2019

28. Tätigkeitsbericht zum Datenschutz

BfDI

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

28

Dieser Bericht wurde dem Präsidenten des Deutschen Bundestages, Herrn Dr. Wolfgang Schäuble, überreicht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Prof. Ulrich Kelber

Vorwort

Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass die unabhängigen Datenschutzaufsichtsbehörden nun jährlich über ihre Tätigkeiten berichten. Der 28. Tätigkeitsbericht zum Datenschutz umfasst daher das Jahr 2019.

Der Bericht beleuchtet die wichtigsten (datenschutz)-politischen Themen, mit denen sich der BfDI 2019 befasst hat, berichtet über die Beratungen und Kontrollen in Deutschland sowie die zunehmend engere Zusammenarbeit der europäischen Aufsichtsbehörden zur Umsetzung der DSGVO in der Europäischen Union und enthält eine Reihe von Statistiken zur Arbeit des BfDI.

Darüber hinaus gibt der Bericht eine Übersicht, wie es um die Umsetzung der Empfehlungen des BfDI aus den Vorjahren steht.

Dieser Tätigkeitsbericht ist im Vergleich zu früheren Tätigkeitsberichten neu gegliedert. An die Stelle der Aufteilung nach Bundestagsausschüssen ist eine thematische Darstellung getreten. Für die Mitglieder des Deutschen Bundestages wurden jeweils am Ende eines jeden Beitrags die Ausschüsse aufgelistet, für die das Thema relevant ist. Zudem findet sich am Ende des Tätigkeitsberichts eine Tabelle, in der die einzelnen Beiträge noch einmal unter den jeweiligen Ausschüssen aufgelistet werden.

Der 28. Tätigkeitsbericht wird zudem der letzte reine Datenschutzbericht des BfDI sein. Ab dem Berichtszeitraum 2020 wird der Tätigkeitsbericht die Themen Datenschutz und Informationsfreiheit gemeinsam umfassen.

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht für das Jahr 2019 zum Datenschutz
– 28. Tätigkeitsbericht –

Inhaltsverzeichnis

1 Einleitung

Das Thema „Künstliche Intelligenz“ (KI) und dessen Bedeutung für den Datenschutz war im Jahr 2019 ein Schwerpunkt meiner Arbeit. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) legte mit der „Hambacher Erklärung zur Künstlichen Intelligenz“ ein Grundsatzpapier mit den wichtigsten datenschutzrechtlichen Anforderungen vor. In bewusster Anlehnung an die auf dem Hambacher Fest 1832 erhobenen Forderungen nach Freiheit und Demokratie betont die DSK, dass der Einsatz Künstlicher Intelligenz dem Menschen und seinen Grundrechten und Grundfreiheiten verantwortlich sein muss. (s. 3.1)

Diese Grundsätze wurden auch im Gutachten der von der Bundesregierung eingesetzten Datenethikkommission (DEK), deren Mitglied ich war, festgeschrieben. Darüber hinaus hat die DEK in 75 Handlungsempfehlungen für die Bundesregierung u. a. mehr Transparenz für Verbraucherinnen und Verbraucher und eine wirksame Algorithmenkontrolle gefordert. (s. 4.6)

Auch die 41. Internationale Datenschutzkonferenz, die im Oktober 2019 in Tirana/Albanien stattfand, machte das Thema KI zu einem der Arbeitsschwerpunkte für die nächsten Jahre. Darüber hinaus beschlossen die rund 120 unabhängigen Datenschutzbehörden aus mehr als 80 Ländern eine „Resolution zur Bedeutung des Datenschutzes als Grundrecht und als Voraussetzung für die Wahrnehmung weiterer Grundrechte“. Darin wird an die Regierungen weltweit appelliert, Datenschutz als Grundrecht anzuerkennen und in ihren nationalen Gesetzgebungen zu verankern. (s. 3.4)

Doch auch jenseits der KI zeigte sich in 2019 erneut, dass der Datenschutz ein Querschnittsthema ist, das Auswirkungen auf sämtliche Lebensbereiche hat. Dementsprechend gab es erneut viel zu tun. In Deutschland war es vor allem die Beratung und Begleitung in der Gesetzgebung, die mein Haus und mich intensiv beschäftigte. Abgesehen von dem sogenannten Omnibusgesetz zur Datenschutz-Grundverordnung (DSGVO) war in diesem Jahr – neben der erneut ausufernden Gesetzgebung im Sicherheitsbereich – besonders der Gesundheitsbereich arbeitsreich. Allein aus dem Bundesgesundheitsministerium (BMG) kamen 23 Gesetzentwürfe mit zum Teil gravierenden datenschutzrechtlichen Herausforderungen.

Beispielhaft können hier die nach wie vor ungelösten Probleme bei der Telematikinfrastruktur und dem Rechtemanagement der elektronischen Patientenakte angeführt werden, die für meine Kolleginnen und Kollegen sehr beratungsintensiv waren. Der Druck aus dem BMG, die ePatientenakte möglichst schnell flächendeckend einzuführen, führt von dort aus zum Verzicht auf lange bekannte und grundlegende Datenschutzregelungen. Das hat in diesem besonders sensiblen Datenbereich fatale Folgen für die Patientinnen und Patienten.

Auch der aus meiner Sicht oft zu laxe Umgang mit Patientendaten in den geplanten neuen Gesundheitsregistern (Implantateregister und Datentransparenzregister) hat zu einer Vielzahl von Beratungsgesprächen mit den Beteiligten geführt. (s. 4.2 und 5.6)

Neben der Beratung von Bundesregierung und Bundestag in der Gesetzgebung ist ein wichtiger Teil meiner Arbeit die Beratung und Kontrolle der von mir beaufsichtigten Behörden und Unternehmen. Dabei steht für mich die Beratung und Information immer an erster Stelle. Dies ist sicher einer der Gründe dafür, warum die Verhängung von Geldbußen eine Ausnahme, nicht die Regel bei Ver-

stößen gegen die DSGVO ist. Gleichwohl musste ich im Jahr 2019 die ersten größeren Geldbußen verhängen.

Immer wiederkehrende Themen gerade bei den Beschwerden von Bürgerinnen und Bürgern sind die Fragen zur Einwilligung in die Datenweitergabe und zur Datenminimierung.

Die Frage der Einwilligung zur Datenweitergabe ist insbesondere im Bereich der Forschung ein weites und schwieriges Feld, begegnet uns aber auch tagtäglich bei den lästigen Cookiebannern auf Webseiten. (s. 4.5)

Die Frage, welche Daten überhaupt gesammelt werden dürfen und wie lange sie gespeichert werden, ist ein Dauerthema bei allen Datenschutzaufsichtsbehörden. Das Ziel der Datenminimierung wird in Behörden und Unternehmen nicht immer zufriedenstellend umgesetzt. (s. 4.3)

In der DSK und im Europäischen Datenschutzausschuss (EDSA) haben wir Vorschläge für die Weiterentwicklung der DSGVO gemacht, als Teil des Evaluierungsprozesses durch die EU-Kommission. Wir wollen Vereine und kleinere Unternehmen bei den Informations- und Dokumentationspflichten entlasten, bessere Regelungen beim Profiling und Scoring etablieren und sehen Weiterentwicklungsbedarf bei der Behandlung großer grenzüberschreitender Fälle. (s. 4.1.)

Die Zusammenarbeit der europäischen Aufsichtsbehörden wird immer wichtiger. Im EDSA haben wir viele wichtige Entscheidungen zur Auslegung der DSGVO getroffen und z. B. die Grundlagen für Zertifizierungen gelegt. Leider warten die Bürgerinnen und Bürger, aber auch ich, noch immer auf erste Entscheidungen zu Datenschutzbeschwerden gegen die großen US-Internetkonzerne. Diese haben fast ausnahmslos ihre europäischen Zentralen in Irland oder Luxemburg, wo in den letzten 20 Monaten von den dortigen Datenschutzaufsichtsbehörden noch keine grenzüberschreitende Beschwerde in den zentralen Punkten abschließend bearbeitet wurde. Das ist für mich nur schwer verständlich und mehr als ärgerlich. Ich hoffe sehr, dass wir gemeinsam diesen Missstand, den ich bei den monatlichen Treffen des EDSA immer wieder anspreche, im Jahr 2020 beseitigen können.

Meinen Mitarbeiterinnen und Mitarbeitern möchte ich für den erneut hohen Einsatz danken. Der Tätigkeitsbericht zeigt, in wie vielen Aufgabengebieten und Einzelthemen mein Haus aktiv ist, um die Grundrechte der Bürgerinnen und Bürger zu schützen. Unser Ziel, Beratungshaus für die beaufsichtigten Behörden und Unternehmen, sowie die Politik und Öffentlichkeit zu sein, haben meine Mitarbeiterinnen und Mitarbeiter genauso mit Leben erfüllt, wie sie bei Kontrollen und der Zusammenarbeit in einer hohen Zahl von Arbeitsgruppen, Kommissionen, Ausschüssen und Organisationen auf nationaler, europäischer und internationaler Ebene aktiv waren.

Zuletzt und besonders herzlich bedanke ich mich bei allen Bürgerinnen und Bürgern, die durch Eingaben und Anfragen mein Haus in die Pflicht genommen haben. Sie sind unsere Partnerinnen und Partner bei der Durchsetzung des Datenschutzes.

Prof. Ulrich Kelber

2 Empfehlungen

2.1 Zusammenfassung der Empfehlungen dieses Tätigkeitsberichts

Ich empfehle, das sog. „Prinzip der Erklärbarkeit“ gesetzlich zu verankern und bei der vielfältigen Umsetzung der Künstlichen Intelligenz (KI) die sieben datenschutzrechtlichen Anforderungen der „Hambacher Erklärung zur Künstlichen Intelligenz“ zu beachten. (Nr. 3.1 und 4.4)

Ich empfehle im Rahmen der ersten Evaluation der DSGVO die Position der nationalen Datenschutzaufsichtsbehörden sowie des Europäischen Datenschutzausschusses (EDSA) zu unterstützen. Das gilt insbesondere für sinnvolle Entlastungen kleiner und mittelständischer Unternehmen beim zu leistenden bürokratischen Verfahrensaufwand und für die Forderung nach einer Verschärfung des geltenden Rechtsrahmens für das Profiling. (Nr. 4.1)

Ich empfehle die Implementierung eines differenzierten Rollen- und Rechtemanagements bei der elektronischen Patientenakte. (Nr. 4.2.1)

Ich empfehle ein Sicherheitsgesetzmoratorium auszusprechen und einen Evaluationsprozess der sicherheitsbehördlichen Eingriffskompetenzen einzuleiten. (Nr. 5.3)

Ich empfehle bei der Registermodernisierung, statt auf eine einheitliche Personenkennziffer auf mehrere bereichsspezifische Identifikatoren zurückzugreifen. (Nr. 5.5)

Ich empfehle, aufgrund der Fehlerquote und fehlenden Rechtsgrundlage auf eine Videoüberwachung mit biometrischer Gesichtserkennung im öffentlichen Raum zu verzichten. (Nr. 6.2)

Ich empfehle, den Bürgerinnen und Bürgern im Zusammenhang mit Diensten nach dem Onlinezugangsgesetz eine nutzerfreundliche Möglichkeit einzuräumen, um die stattfindenden Datenverarbeitungsprozesse nachvollziehen und kontrollieren zu können. (Nr. 8.2)

Ich rate den öffentlichen Stellen des Bundes, personenbezogene Daten per E-Mail grundsätzlich nur verschlüsselt zu versenden. Ein unverschlüsselter Datenversand per E-Mail ist bei sensiblen Daten auch dann nicht rechtmäßig, wenn vorher eine entsprechende Einwilligungen des Empfängers eingeholt wurde, da diese in der Regel nicht datenschutzkonform erteilt werden kann. Nationale Vorschriften, die einen unverschlüsselten E-Mailversand legitimieren, sind darüber hinaus nicht DSGVO-konform. (Nr. 8.3)

Ich empfehle einen diskriminierungsfreien Zugriff auf Fahrzeugdaten und im Fahrzeug generierter Daten über eine sichere Telematikplattform im Fahrzeug, etwa nach dem Vorbild von Smart-Meter-Gateways. (Nr. 8.7)

2.2 Empfehlungen aus dem 27. Tätigkeitsbericht – Stand der Umsetzung

	Empfehlung	Stand der Umsetzung
🟡	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 im 27. TB).	In dem dem BfDI zugesandten Entwurf eines neuen BPolG sind zwar Abhilfebefugnisse des BfDI vorgesehen. Vorbild ist hier auch das BKAG. Allerdings werden höhere Anforderungen aufgestellt, als es die Richtlinie vorgibt. So soll etwa eine Anordnung nur nach einer Beanstandung möglich sein. Es fehlt zudem an der ausdrücklichen Möglichkeit zur Löschanordnung. Eine wirksame Abhilfe ist so gefährdet.
🔴	Ich empfehle dem Gesetzgeber, Sanktionsbefugnisse für den BfDI auch im Bereich der Nachrichtendienste einzuführen (Nr. 1.2.1 im 27. TB).	Ein Aufgreifen dieser Empfehlung durch den Gesetzgeber erfolgte bislang nicht.
🔴	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 im 27. TB).	Bislang ist der Gesetzgeber hier nicht weiter tätig geworden, so dass bei den gesetzlichen Krankenkassen Unsicherheit besteht. Einerseits regelt § 85a SGB X, dass gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden dürfen. Andererseits agieren die gesetzlichen Krankenkassen als öffentlich-rechtliche Wettbewerbsunternehmen, was auch durch das am 13. Februar 2020 vom Deutschen Bundestag verabschiedete Fairer-Kassenwettbewerb-Gesetz noch gefördert wird. § 2 Absatz 5 Bundesdatenschutzgesetz bestimmt insoweit, dass öffentliche Stellen als nicht öffentliche Stellen gelten, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Gesetzliche Krankenkassen werben wie private Krankenversicherungen etwa bei Sportveranstaltungen um ihre Kunden (Versicherte). Für öffentliche Wettbewerbsunternehmen gilt Artikel 83 Datenschutz-Grundverordnung.
🟡	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 im 27. TB).	Wenngleich einige Jobcenter dieser Empfehlung gefolgt sind, besteht nach unserer Kenntnis weiterhin erheblicher Handlungsbedarf in Bezug auf den Umfang der Freistellung von Datenschutzbeauftragten. Die Empfehlung ist daher aufrecht zu erhalten.
🔴	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 im 27. TB).	Mehrere Grundsatzfragen betreffend die Vereinbarkeit der PNR-RL und nationaler PNR-Gesetze sind Gegenstand laufender Vorabentscheidungsersuchen vor dem EuGH (u. a. Vorlage des belgischen Verfassungsgerichts C 817/19). Nach Auffassung der Bundesregierung sind die vorhandenen Regelungen, teils aufgrund anderer Ausgestaltung als bei PNR Kanada, teils wegen anderer Zweckbestimmung und Verhältnismäßigkeitsbewertung mit der Europäischen Grundrechtecharta vereinbar. Vor Abschluss des Verfahrens und insbesondere Klärung der Zulässigkeit der Langzeitspeicherung ist nicht mit Anpassungen zu rechnen.

	Empfehlung	Stand der Umsetzung
	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 im 27. TB).	Eine Umsetzung ist bis zum Redaktionsschluss nicht erfolgt. Inwieweit derzeit laufende Gesetzgebungsverfahren die Empfehlung umsetzen werden, kann noch nicht abgeschätzt werden.
	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 im 27. TB).	Das Vertragsmuster wird in der Bundesverwaltung noch nicht flächendeckend eingesetzt oder zumindest als Grundlage verwendet.
	Ich empfehle, bei Zugriffen auf Eurodac und auf das VIS-Informationssystem durch Polizeibehörden auf eine aussagekräftige Dokumentation zu achten (Nr. 9.3.5 im 27. TB).	Maßnahmen zur Optimierung der Dokumentation wurden von den verantwortlichen Stellen zugesagt und erscheinen geeignet, Verbesserungen herbeizuführen. Nachkontrollen müssen dies noch bestätigen.
	Ich empfehle dem Gesetzgeber angesichts des festgestellten geringen Nutzwerts von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen (Nr. 9.3.5 im 27. TB).	Ein Aufgreifen dieser Empfehlung durch den Gesetzgeber erfolgte bislang nicht.
	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 im 27. TB).	Trotz mehrerer Änderungen der StPO wurde diese Empfehlung in keinem Gesetzgebungsverfahren umgesetzt.

	Empfehlung	Stand der Umsetzung
	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 im 27. TB).	Der Vorschlag einer E-Privacy-Verordnung wird seit 2017 diskutiert. Im Rat der EU konnte bislang keine allgemeine Ausrichtung herbeigeführt werden. Die kroatische Ratspräsidentschaft, die seit Januar 2020 den Vorsitz hat, hat am 21.02.2020 einen Vorschlag vorgelegt
	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 (Nr. 15.2.7 im 27. TB).	Informationen werden zumindest nicht exklusiv in sozialen Medien verbreitet. Einzelne Behörden zeigen ein Problembewusstsein und prüfen den Einsatz alternativer Dienste.
	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 nicht – zumindest bis zur rechtlichen Klärung der Situation – datenschutzfreundlichere Kommunikationskanäle nutzen können (Nr. 15.2.8 im 27. TB).	Fanpages werden weiterhin genutzt. Die Transparenz der Datenverarbeitung bei Facebook ist – trotz einzelner Verbesserungen – weiter unzureichend. Die Datenschutzbehörden setzen sich verstärkt auf europäischer Ebene für eine Klärung der offenen Rechtsfragen ein.

2.3 Empfehlungen aus früheren Tätigkeitsberichten – Stand der Umsetzung

	Empfehlung	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 zu 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 der 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 dabei jedoch 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). Diesem Nachbesserungsbedarf ist im weiteren Gesetzgebungsverfahren überwiegend nicht entsprochen worden. So wurden u. a. entgegen ursprünglicher Absicht keine Geldbußen für Datenschutzverstöße der gesetzlichen Krankenkassen verankert und die zwingend notwendigen Änderungen des TKG nicht vorgenommen.
🔴	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 auch weiterhin empfehle, spezifische nationale Regelungen zum Beschäftigtendatenschutz zu erlassen (vgl. Nr. 3.1.3); mit der Erarbeitung eines entsprechenden Gesetzesentwurfs wurde bislang nicht begonnen; auch die zu diesem Zweck beabsichtigte Gründung eines Beirats erfolgte bislang nicht.
🟡	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 (s. Nr. 7.1.1). Mit dem 2. DSAnpUG-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.

	Empfehlung	Stand der Umsetzung
	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 des 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).	Erfreulicherweise ist der Haushaltsgesetzgeber meiner Empfehlung gefolgt. Dem BfDI wurden in den Haushalten 2019 und 2020 44 zusätzliche Stellen für den Sicherheitsbereich zugebilligt. Es bleibt zu wünschen, dass die Notwendigkeit, einen Stellen- und Kompetenzzuwachs im Bereich der Sicherheitsbehörden auch zwingend mit einer Personalverstärkung bei der Datenschutzaufsicht einhergehen zu lassen, auch in den künftigen Haushalten berücksichtigt wird.
	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).	In weiten Teilen ist eine Umsetzung noch immer nicht erfolgt. Inwieweit derzeit laufende Gesetzgebungsverfahren die Empfehlung weitergehend umsetzen werden, kann noch nicht abgeschätzt werden.
	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 im Frühling 2019 öffentlich gewordene Entwurf eines IT-Sicherheitsgesetzes 2.0 wurde im weiteren Jahresverlauf nicht weiter verfolgt. Ich erhoffe mir, dass meine Bedenken gegen die erheblichen Verschärfungen des Straf- und Strafprozessrechts bei weiteren Gesetzesinitiativen berücksichtigt werden. Gleichzeitig ist es wichtig, den Schutz von Gesellschaft und Wirtschaft in der digitalen Welt weiter voranzutreiben – dies muss aber datenschutzkonform geschehen.

3 Gremienarbeit

3.1 Konferenz der der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Die DSK, die dieses Jahr unter dem Vorsitz des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz tagte, hat in zwei ordentlichen Datenschutzkonferenzen und drei Zwischenkonferenzen ein neues Kurzpapier erstellt und neun Entschließungen sowie elf Beschlüsse gefasst.

Ein arbeitsintensives Jahr liegt hinter den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Auch nach dem Geltungsbeginn der DSGVO am 25. Mai 2018 besteht weiterhin viel Abstimmungsbedarf zwischen den Aufsichtsbehörden. Um eine möglichst einheitliche datenschutzrechtliche Auffassung zu bilden, werden auf der DSK Themen diskutiert und grundsätzliche Positionen beschlossen. Im Fokus stehen dabei solche Themen, die die Zusammenarbeit der Aufsichtsbehörden im nationalen und internationalen Kontext betreffen. Ebenso werden anlassbezogen aktuelle datenschutzrechtliche Fragestellungen erörtert, die von grundsätzlicher Bedeutung sind und zu denen Informationsbedarf besteht. Hierbei wird die DSK auch von Arbeitskreisen unterstützt.

Hambacher Erklärung

Kernthemen der 97. DSK auf dem Hambacher Schloss in Neustadt an der Weinstraße waren die datenschutzrechtlichen Anforderungen an die Entwicklung und Anwendung von Künstlicher Intelligenz sowie die Haftung von Unternehmen im Rahmen von Art. 83 DSGVO für schuldhafte Datenschutzverstöße ihrer Mitarbeiter.

Die Hambacher Erklärung fordert dazu auf, den sieben datenschutzrechtlichen Anforderungen bei der technischen Entwicklung und der Anwendung von Künstlicher Intelligenz in den verschiedensten Lebensbereichen Rechnung zu tragen.

Betriebliche Datenschutzbeauftragte und Austausch mit spezifischen Aufsichtsbehörden

Zudem positionierte sich die DSK mit einer Entschließung zur Rechtsstellung der betrieblichen Datenschutzbeauftragten, denn es war vielfach die Kritik geäußert worden, dass nach der DSGVO in zu vielen Fällen ein Erfordernis der Benennung von Datenschutzbeauftragten bestehe. Diese Kritik teilt die DSK nicht. Die Regelungen zur Benennungspflicht der DSGVO haben zu keiner inhaltlichen Änderung gegenüber dem bis dahin geltenden Datenschutzrecht geführt. Vielmehr hätte ein Verzicht auf diese Benennungspflicht den Aufwand für den Verantwortlichen erhöht, denn Beratung und Kontrolle durch den Datenschutzbeauftragten sind eine wertvolle Unterstützung des Verantwortlichen, seine datenschutzrechtlichen Pflichten zu erfüllen.

Die DSK erweiterte den Informationsaustausch mit den spezifischen Aufsichtsbehörden aus den Bereichen der Medien und der Kirchen im Hinblick auf die Datenschutzgremien der EU.

Kennzeichenerfassung und Digitalisierung im Gesundheitswesen

Die 98. DSK in Trier befasste sich unter anderem mit der massenhaften automatisierten Erfassung von Kfz-Kennzeichen und der Verarbeitung von personenbezogenen Daten im Gesundheitswesen.

Nach Auffassung der DSK stellte die massenhafte und anlasslose automatisierte Erfassung von Kfz-Kennzeichen für die Zwecke der Strafverfolgung einen Verstoß gegen das Grundgesetz und eine Verletzung der Bürgerinnen und Bürger in ihrem Recht auf informationelle Selbstbestimmung dar. Die von den Polizeibehörden und den Staatsanwaltschaften praktizierte umfassende und unterschiedslose Erfassung, Speicherung und Auswertung von Kraftfahrzeugen durch Kennzeichenerfassungssysteme seien zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder
Hambacher Schloss, 3. April 2019

Hambacher Erklärung zur Künstlichen Intelligenz

Sieben datenschutzrechtliche Anforderungen

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I. Künstliche Intelligenz und Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ […].“[1]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

---

1 BT-Drs. 19/1982 zu 1., Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor (Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 9.10.2018;).

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DSGVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO). Diese Grundsätze müssen gemäß Art. 25 DSGVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. **KI darf Menschen nicht zum Objekt machen**
   Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DSGVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DSGVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DSGVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. **KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben**
   Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO). Zweckänderungen sind mit Art. 6 Abs. 4 DSGVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. **KI muss transparent, nachvollziehbar und erklärbar sein**
   Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DSGVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und ggf. auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DSGVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DSGVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DSGVO).

4. **KI muss Diskriminierungen vermeiden**
   Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen

auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u. a. gegen bestimmte Anforderungen der DSGVO, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. **Für KI gilt der Grundsatz der Datenminimierung**
   Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. **KI braucht Verantwortlichkeit**
   Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DSGVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DSGVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO erforderlich sein.

7. **KI benötigt technische und organisatorische Standards**
   Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gem. Art. 24 und 25 DSGVO zu treffen, wie z. B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutzaufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

Ein weiterer Schwerpunkt der Arbeit der DSK bestand im Bereich der Digitalisierung des Gesundheitswesens. Die Verarbeitung von Gesundheitsdaten ist mit besonderen Risiken verbunden. Die DSK fordert demnach sicherzustellen, dass unabhängig von der Größe medizinischer Einrichtungen Patientendaten nach dem Stand der Technik geschützt würden. Insbesondere Gesundheitswebseiten und -Apps müssten die Erwartungen an die Vertraulichkeit gewährleisten und bei der Weitergabe von personenbezogenen Daten bestimmte Anforderungen einhalten.

Akkreditierung von Überwachungsstellen für Codes of Conduct

Nach Art. 57 Abs. 1 lit. p DSGVO muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet die Anforderungen an die Akkreditierung einer Stelle für die Überwachung der Einhaltung der Verhaltensregeln gemäß Art. 41 DSGVO, sogenannte Codes of Conduct, abfassen und veröffentlichen. Codes of Conduct „präzisieren" die Anwendung der Datenschutz-Grundverordnung. Das Bedürfnis für eine solche Präzisierung ergibt sich daraus, dass die Verordnung an vielen Stellen unbestimmt ist und Generalklauseln enthält. Codes of Conduct können als Auslegungshilfen herangezogen werden und dienen daher der Rechtssicherheit. Sie sind zwar keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, aber ein wichtiges Instrument, um – beispielsweise für bestimmte Branchen – die praktische Umsetzung der zum Teil sehr abstrakten Regelungen der DSGVO zu erleichtern.

Ich hatte bereits an der Erstellung der europäischen „Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679" mitgewirkt (s. 3.2). Diese Leitlinien sollen praktische Hinweise und Auslegungshilfen zur Anwendung der Artikel 40 und 41 der DSGVO geben. Sie sollen die Vorschriften und das Verfahren zur Einreichung, Genehmigung und Veröffentlichung von Codes of Conduct auf nationaler und europäischer Ebene erläutern.

Die Leitlinien sehen unter anderem vor, dass ein Code of Conduct (für den nicht-öffentlichen Bereich) eine akkreditierte Überwachungsstelle festlegt. Diese kontrolliert (neben der zuständigen Datenschutzaufsichtsbehörde), ob die Mitglieder, die sich dem Code of Conduct unterworfen haben, dessen Vorgaben einhalten.

Die deutschen Akkreditierungskriterien für Überwachungsstellen eines Codes of Conduct wurden dem Europäischen Datenschutzausschuss zur Billigung im Kohärenzverfahren gemäß Art. 64 Absatz 1 Satz 2 lit. c DSGVO übermittelt.

Weitere Themen

Zudem hat sich die DSK unter anderem mit einer datenschutzgerechten Nutzung von Windows 10 (s. 8.12) beschäftigt und einen Erfahrungsbericht über die Anwendung der DSGVO beschlossen. Mit Letzterem möchte die DSK die Erfahrungen der deutschen Aufsichtsbehörden aus der praktischen Anwendung seit Geltungsbeginn der DSGVO in den Evaluierungsprozess nach Art. 97 DSGVO einbringen. In diesem Prozess sollen auch Vorschläge für Verbesserungen unterbreitet werden, um die Umsetzung der DSGVO praxistauglicher zu gestalten.

Die von der der DSK veröffentlichten Papiere sind abrufbar unter:

https://www.bfdi.bund.de/entschließungen
https://www.bfdi.bund.de/beschlüsse-positionspapiere
https://www.bfdi.bund.de/kurzpapiere

Arbeitskreise (AK) der DSK

AK Steuerverwaltung

Seit dem 25. Mai 2018 bin ich nicht nur für die Bundesfinanzbehörden zuständig, sondern auch für die Finanzbehörden der Länder im Anwendungsbereich der Abgabenordnung (AO). Deshalb bin ich nunmehr gemäß § 32h AO anstelle der Datenschutzaufsichtsbehörden der Länder für alle Finanzämter Deutschlands zuständig, soweit diese Aufgaben nach der AO wahrnehmen. Darüber hinaus bin ich für die kommunalen Steuerämter zuständig, soweit diesen die Verwaltung der Grund- und Gewerbesteuer übertragen worden ist.

Diesem Zuständigkeitswechsel folgt nun folgerichtig der Wechsel im Vorsitz des AK Steuerverwaltung. Dieser ist nach wie vor ein wichtiges Gremium, um Abstimmungsbedarfe zwischen mir und den Datenschutzaufsichtsbehörden der Länder zu klären.

AK Grundsatz

Der AK Grundsatz besteht unter meinem Vorsitz aus Vertretern aller Landesdatenschutzbeauftragten und tagt zweimal jährlich. Inhaltlich werden grundsätzliche Fragen des Datenschutzes aufbereitet sowie entsprechende Positionen zur Vorlage bei der DSK ausgearbeitet.

In diesem Jahr hat sich der AK Grundsatz eingehend mit den Erfahrungen bei der Anwendung der DSGVO auseinandergesetzt. Der Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO wurde in einem eigens dafür eingerichteten Unterarbeitskreis erstellt und durch den AK Grundsatz finalisiert (vgl. 4.1). Daneben wurde die Kooperation und Zusammenarbeit mit den nach Art. 85 und 91 DSGVO eingerichte-

ten spezifischen Aufsichtsbehörden vertieft, um eine entsprechende Anwendung des § 18 Abs. 1 S. 4 BDSG zu gewährleisten. Weiterhin hat sich der AK Grundsatz mit verschiedenen Einzelfragen grundsätzlicher Art bezüglich der Umsetzung der Informationspflichten nach Art. 13 DSGVO, den Auskunftspflichten nach Art. 15 DSGVO sowie mit unterschiedlichen Fragestellungen betreffend der Gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO und der Auftragsverarbeitung gemäß Art. 28 DSGVO auseinandergesetzt.

Ich empfehle, bei der vielfältigen Umsetzung der KI die sieben datenschutzrechtlichen Anforderungen der „Hambacher Erklärung zur Künstlichen Intelligenz" zu beachten.

Querverweise:

3.2 Europäischer Datenschutzausschuss, 4.1 Evaluierung der Datenschutz-Grundverordnung, 4.2 Digitalisierung im Gesundheitswesen, 4.4 Künstliche Intelligenz, 4.5.1 Einwilligung in der Forschung

3.2 Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) hat im Berichtszeitraum weitere Leitlinien zur einheitlichen Anwendung der Datenschutz-Grundverordnung angenommen und die grenzüberschreitende Zusammenarbeit der europäischen Datenschutzbehörden intensiviert.

Mit der DSGVO wurde der EDSA geschaffen. Seine Aufgabe besteht vor allem darin, die europaweit einheitliche Anwendung der DSGVO sicherzustellen. Hierzu nimmt der Ausschuss Leitlinien, Empfehlungen und bewährte Verfahren an und kann in grenzüberschreitenden Verfahren der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten verbindliche Entscheidungen treffen.

Mitglieder des Gremiums sind die Leiterinnen und Leiter der Datenschutzaufsichtsbehörden der Mitgliedstaaten und der Europäische Datenschutzbeauftragte. Mitglied für Deutschland ist der BfDI als gemeinsamer Vertreter aller deutschen Aufsichtsbehörden.

Der Schwerpunkt der Arbeiten lag auf der Erarbeitung von Leitlinien im Sinne des Art. 70 DSGVO zur einheitlichen Umsetzung. Daneben hat der Ausschuss Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO angenommen und sich mit aktuellen datenschutzpolitischen Fragen auf internationaler und EU-Ebene befasst.

Leitlinien

Der EDSA hat im Berichtszeitraum zahlreiche Leitlinien verabschiedet, an deren Erarbeitung ich regelmäßig als Mitberichterstatter mitgewirkt habe, und anschließend der öffentlichen Konsultation unterzogen. Es handelt sich um:

- Leitlinien 1/2019 zu Verhaltensregeln und Überwachungsstellen

  Die Leitlinien geben praktische Hinweise und Auslegungshilfen zur Anwendung der Art. 40 und 41 DSGVO. Sie erläutern die Vorschriften und das Verfahren zur Einreichung, Genehmigung und Veröffentlichung von Verhaltensregeln, sogenannter „Codes of Conduct", auf nationaler und europäischer Ebene. Die Leitlinien sehen u. a. vor, in Verhaltensregeln für den nicht-öffentlichen Bereich eine akkreditierte Überwachungsstelle festzulegen, die neben der zuständigen Datenschutzaufsichtsbehörde kontrolliert, ob die Mitglieder, die sich den Regeln des Codes unterworfen haben, diese Regeln auch einhalten.

- Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 lit. b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten

  Die Leitlinien enthalten Ausführungen dazu, unter welchen Voraussetzungen und Bedingungen Unternehmen, die Dienste im Internet anbieten, die Verarbeitung von Daten der Nutzerinnen und Nutzer auf die Rechtsgrundlage „Vertrag" stützen können. Nach Art. 6 Abs. 1 lit. b DSGVO ist die Verarbeitung personenbezogener Daten zulässig, soweit sie zur Vertragserfüllung erforderlich ist. In den Leitlinien wird klargestellt, dass die Beurteilung, ob eine Datenverarbeitung zur Vertragserfüllung erforderlich ist, nicht allein davon abhängt, was im Vertrag vereinbart wurde. Vielmehr ist eine wertende Entscheidung unter Berücksichtigung der in Art. 5 DSGVO niedergelegten Datenschutzgrundsätze (Sparsamkeit, Fairness, Transparenz) notwendig. Beispielsweise kann eine Datenverarbeitung zu Zwecken der nutzerbedingten Onlinewerbung danach grundsätzlich nicht auf die Rechtsgrundlage „Vertrag" gestützt werden.

- Leitlinien 3/2019 zu Datenverarbeitungen durch Videoanlagen

  Die Leitlinien enthalten Vorgaben zur Standortwahl von Videoanlagen, zur Speicherdauer von Überwachungsaufnahmen und sie befassen sich mit aktuellen Technologien wie der biometrischen Videoüberwachung. Sie stellen klar, dass biometri-

sche Daten, die eine dauerhafte Identifizierung von Personen ermöglichen, zu den besonders schützenswerten Daten zählen und daher nur unter strengen Voraussetzungen verarbeitet werden dürfen. Das Tracking von Personen mittels dauerhafter biometrischer Identifizierung, beispielsweise um das Bewegungs- und Kaufverhalten einer Person in einem Kaufhaus nachzuverfolgen, ist nach den Leitlinien grundsätzlich nur mit ausdrücklicher Einwilligung der Betroffenen zulässig.

- Leitlinien 4/2019 zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen („Data Protection by Design and by Default“)

  Die Leitlinien enthalten Hinweise dazu, wie Verantwortliche die Vorgaben des Art. 25 DSGVO durch geeignete technische und organisatorische Maßnahmen und notwendige Sicherheitsvorkehrungen umsetzen können, um die Rechte und Freiheiten betroffener Personen wirksam zu schützen.

- Schließlich hat der EDSA die bereits im Jahre 2018 angenommenen Leitlinien 1/2018 zu Zertifizierungen, 3/2018 zum räumlichen Anwendungsbereich der DSGVO und 4/2018 zur Akkreditierung von Zertifizierungsstellen nach öffentlicher Konsultation überarbeitet und final verabschiedet (vgl. 8.10).

Stellungnahmen im Kohärenzverfahren

Die vom EDSA im Berichtszeitraum angenommenen Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO betrafen Listen von Datenverarbeitungen, für die gemäß Art. 35 Abs. 4 DSGVO Datenschutzfolgenabschätzungen erforderlich beziehungsweise gemäß Art. 35 Abs. 5 DSGVO nicht erforderlich sind. Solche Listen werden durch die nationalen Aufsichtsbehörden vorgelegt und von der Technology-Expertenuntergruppe analysiert, um unterschiedliche Anforderungen für Datenschutzfolgeabschätzungen in den Mitgliedstaaten zu vermeiden. Durch die Stellungnahmen des EDSA zu einzelnen Listen wurden den betreffenden Aufsichtsbehörden Vorschläge für Änderungen empfohlen. Auf diese Weise trägt der Kohärenzmechanismus zur einheitlichen Anwendung der DSGVO bei.

Ebenfalls im Verfahren nach Art. 64 DSGVO hat der EDSA Stellungnahmen abgegeben zur Genehmigung der verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules – BCR) des britischen Unternehmens Equinix Inc. und zur Genehmigung von Standardvertragsklauseln für Auftragsdatenverarbeitungen gemäß Art. 28 Abs. 8 DSGVO, die von der dänischen Aufsichtsbehörde vorgelegt wurden.

Weitere Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO betrafen das Verhältnis der DSGVO zur E-Privacy-Richtlinie und eine Verwaltungsvereinbarung zur Ermöglichung von Datenübermittlungen zwischen den Finanzbehörden des Europäischen Wirtschaftsraums (EWR) und Finanzbehörden aus Drittstaaten.

Sonstige Arbeiten des EDSA

Neben den allgemeinen Leitlinien und Stellungnahmen im Kohärenzverfahren hat sich der EDSA mit unterschiedlichen datenschutzpolitischen Themen befasst und hierzu Stellungnahmen und Berichte angenommen. Unter anderem betrifft dies das Gesetzgebungsverfahren zur E-Privacy-Verordnung und die Folgen des Brexit für Datentransfers von der EU in das Vereinigte Königreich im Falle des „No-Deal-Brexit“; hierzu wurden Informationen für Unternehmen veröffentlicht (vgl. 8.1.1).

Ein weiterer Schwerpunkt der Arbeiten des EDSA betrifft den Datenschutz im Sicherheitsbereich. Hier hat der Ausschuss zusammen mit dem Europäischen Datenschutzbeauftragten (EDPS) eine Stellungnahme zum U.S. Cloud Act erarbeitet (vgl. 6.1.1) und sich mit der Überprüfung des sogenannten Privacy Shields befasst (vgl. 8.1.3).

Der Ausschuss hat sich auch zum Thema „Future of Supervision“ beraten. Hierbei geht es um die koordinierte Datenschutzaufsicht über europäische IT-Großsysteme und Agenturen wie Eurojust, das Schengener Informationssystem (SIS), das Visa-Informationssystem (VIS) und das Einreise-Ausreise-Register („EES“) durch den EDPS und die nationalen Aufsichtsbehörden. Zu diesem Zweck wurde im Rahmen des EDSA das „Coordinated Supervision Committee“ (CSC) eingerichtet.

Darüber hinaus wurde das Thema Interoperabilität erörtert und in einem Schreiben an den LIBE-Ausschuss des Europäischen Parlaments Kritik an der Schaffung des sogenannten Interoperabilitäts-Rechtsrahmens für die technische Verknüpfung einer Vielzahl von EU-Datenbanken im Bereich Justiz und Inneres geäußert. Die Arbeiten des EDSA im Sicherheitsbereich werden auf Fachebene von der Expertenuntergruppe „Borders, Travel, Law Enforcement – BTLE“ geleistet, in der ich als Koordinator, Mitberichterstatter und Mitglied des Privacy Shield-Überwachungsteams fungiere.

Ein weiterer wichtiger Aspekt der Arbeit des EDSA besteht in der Zusammenarbeit der Aufsichtsbehörden in grenzüberschreitenden Datenschutzfällen. Hierzu tauschen die Behörden im Rahmen des sog. Kooperationsverfahrens nach Artikel 60 DSGVO sachdienliche Informationen aus und führen gemeinsame Bewertungen durch. Aus meiner Sicht ist eine gemeinsame

Vorgehensweise der Aufsichtsbehörden, insbesondere bei Datenschutzverstößen durch die weltweit führenden Tech-Unternehmen, die enorme Datenmengen verarbeiten und auswerten, von besonderer Bedeutung. Hier hat der Ausschuss sein volles **Handlungspotenzial** noch nicht erschöpft. Ende 2019 war noch in keinem einzigen großen grenzüberschreitenden Fall, der diese Unternehmen betrifft, ein Entwurf für eine Entscheidung der federführenden nationalen Aufsichtsbehörde ergangen.

Querverweise:

6.1.1 CLOUD Act, 8.1.1 Drittstaatentransfers und 8.1.3 Entwicklungen beim EU-US Privacy Shield

3.3 Datenschutz-Ausschuss des Europarats

Der beratende Ausschuss, der gemäß Art. 18 des Übereinkommens des Europarates zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten (Konvention 108) eingerichtet worden ist, übernimmt zentrale Aufgaben bei der Bearbeitung datenschutzrelevanter Themen im Bereich des Europarates. Wegen der Vielzahl seiner Mitglieder und der Vertragsparteien der Konvention 108 hat dies hohe Bedeutung für die Menschen in Europa und darüber hinaus.

Nach dem erfolgreichen Abschluss der Verhandlungen für ein Änderungsprotokoll zur Modernisierung der Konvention 108 des Europarates, die ursprünglich aus dem Jahr 1981 stammt und das erste rechtsverbindliche zwischenstaatliche Übereinkommen zum Datenschutz war, begann im Oktober 2018 der Prozess der Unterzeichnung und Ratifizierung des Änderungsprotokolls durch die bisherigen Vertragsparteien der Konvention 108. Ich freue mich, dass Deutschland zu den ersten Unterzeichnern des Änderungsprotokolls gehört und hoffe, dass der aktuell noch laufende innerstaatliche Ratifikationsprozess für Deutschland zeitnah abgeschlossen werden wird. Eine rasche Ratifizierung durch eine Vielzahl der bisherigen Vertragsparteien ist wichtig, weil für das Inkrafttreten des Änderungsprotokolls ein Mindest-Quorum an Signatarstaaten erreicht werden muss. Erst dann können die neuen und vertieften Datenschutz-Grundsätze der modernisierten Konvention 108 – bzw. der häufig so bezeichneten „Konvention 108 +“ – Wirkung entfalten.

Bereits die Konvention 108 in ihrer Ursprungsfassung sieht in ihrem Art. 18 die Einrichtung eines „Beratenden Ausschuss“ vor, der gemäß Art. 19 folgende Aufgaben hat:

- Erarbeitung von Vorschlägen zur Erleichterung oder Verbesserung der Anwendung der Konvention 108;
- Vorlage von Vorschlägen zur Änderung der Konvention 108;
- Beschluss von Stellungnahmen zu jeder (seitens der Vertragsparteien) vorgeschlagenen Änderung der Konvention 108;
- Entwurf von Stellungnahmen zu allen Fragen im Zusammenhang mit der Anwendung der Konvention 108 auf Ersuchen einer Vertragspartei.

Jede Vertragspartei ist im Beratenden Ausschuss vertreten. Infolge der Einrichtung meiner Dienststelle als eigenständige oberste Bundesbehörde nehme ich, neben den Vertretern des Bundesinnenministeriums, als Beobachter an den Sitzungen des Beratenden Ausschusses teil und wirke an der Tätigkeit des Ausschusses mit. Insbesondere im Hinblick auf die erste der oben genannten Aufgaben hat der Beratende Ausschuss im Laufe der Jahre viele wichtige Empfehlungen und Leitlinien beschlossen. Im Berichtszeitraum 2019 befasste sich der Ausschuss u. a. mit den Themen Profilbildung, Gesichtserkennung und Datenschutz im Erziehungswesen. Im Vorgriff auf die Konvention 108+ begann er zudem mit der Ausgestaltung einer neuen Aufgabe, die darin bestehen wird, neue Vertragsparteien erstmals und bestehende Signatarstaaten in regelmäßigen Abständen einer Evaluierung ihrer jeweiligen datenschutzrechtlichen innerstaatlichen Situation zu unterziehen.

Auch die globale Bedeutung der Konvention 108 des Europarats verdient Beachtung: 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 immer mehr außereuropäische Staaten die Konvention 108 – und teilweise auch das Änderungsprotokoll zur Modernisierung der Konvention – ratifiziert; aktuell sind dies die Länder Kapverdische Inseln, Mauritius, Mexiko, Senegal, Tunesien, Uruguay sowie, im Berichtszeitraum 2019 der Konvention 108 beigetreten, Argentinien und Marokko. Beitrittsgesuche von Burkina Faso und von anderen Ländern liegen dem Europarat vor.

3.4 Internationale Datenschutzkonferenz

Die Internationale Datenschutzkonferenz (International Conference of Data Protection and Privacy Commissioners bzw. ICDPPC) befasste sich 2019 mit dem Zusammenwirken der Datenschutzaufsicht mit anderen Regulierungsbehörden, z. B. für Verbraucherschutz oder für Wettbewerb, und wählte für sich einen neuen Namen; sie heißt nun „Global Privacy Assembly“.

Die 41. ICDPPC in Tirana, Albanien, stand unter dem Motto “Convergence and Connectivity: Raising Global Data Protection Standards in the Digital Age” und befasste sich mit der Frage, ob die Rechtsgebiete des Datenschutzes, des Verbraucherschutzes und der Sicherung des Wettbewerbs sich annähern oder sogar überschneiden. Außerdem wurde diskutiert, inwieweit die Datenschutzaufsichtsbehörden mit den Regulierungsbehörden zum gegenseitigen Nutzen zusammen wirken können. Als Beispiel für ein derartiges Zusammenwirken habe ich im Rahmen einer Podiumsdiskussion die Facebook-Entscheidung des Bundeskartellamts vom Februar 2019 dargestellt und dabei auch erläutert, warum ich sie – trotz der vorläufigen Aussetzung der Entscheidung durch das Oberlandesgericht Düsseldorf – nach wie vor für richtig halte.

In eigener Sache hat sich die ICDPPC mit dem Weg in die weitere Zukunft befasst und sich für die Jahre 2019 bis 2021 einen Arbeitsplan (Entschließung zur „Strategic Direction“) mit bestimmten Themen-Schwerpunkten gegeben. Als Steuerungsgruppe für diesen Arbeitsplan wurde eine neue „Policy Strategy Working Group“ (PSWG) eingerichtet. Ferner strebt die Internationale Konferenz an, aktuelle und global relevante Fragen nicht mehr nur im Rahmen des jährlichen Treffens zu diskutieren, sondern in einem kontinuierlichen Prozess über das gesamte Jahr hinweg zu beraten. Zu diesem Zweck wurde eine neue ständige Arbeitsgruppe zur generellen oder auch Einzelfall-bezogenen Zusammenarbeit der ICDPPC -Mitglieder eingesetzt. In den beiden neuen Arbeitsgruppen wirke ich mit, um die wichtige Arbeit der Internationalen Konferenz zu diesen Zwecken zu unterstützen. Die Arbeit in den Gruppen zur Zukunft der Konferenz und zum Umgang mit künstlicher Intelligenz bleibt bestehen.

Außerdem hat die ICDPPC eine für ihre Außenwirkung bedeutende Neuerung beschlossen: Um eine kürzeren, prägnanteren Namen zu erhalten, aber auch um ihren Charakter als feststehenden Zusammenschluss von Datenschutzaufsichtsbehörden aus aller Welt besser zum Ausdruck zu bringen, wurde die neue Bezeichnung “Global Privacy Assembly” (GPA) angenommen. Mit Wirkung vom 15.11.2019 trat die Änderung in Kraft. Dokumente sowohl der Internationalen Konferenz wie auch der GPA finden sich nun auf der Internet-Seite https://globalprivacyassembly.org.

Inhaltlich hat die 41. ICDPPC eine Reihe von Entschließungen gefasst, z. B. zum raschen Löschen bestimmter Inhalte, die von Akteuren extremistischer oder terroristischer Gewalt, wie z. B. durch den Täter in Christchurch, Neuseeland, in sozialen Netzwerken verbreitet werden. Hervorzuheben ist auch eine grundlegende Entschließung, die das Verhältnis und die mögliche Interaktion des Datenschutzes zu und mit anderen Grundrechten sowie zum Funktionieren demokratischer Prozesse zum Gegenstand hat. Diese Entschließung soll als Basis dienen für künftige, weitere Resolutionen der GPA in Bezug auf bestimmte, einzelne Grundrechte oder Prozesse, z. B. die Freiheit bzw. Nicht-Beeinflussung der Wahlentscheidung des Bürgers.

Die Entschließungen der ICDPPC bzw. der GPA stehen in englischer Sprache auf meiner Internetseite (www.bfdi.bund.de/gpa) zum Abruf bereit; dort finden sich auch Arbeitsübersetzungen der Entschließungen in deutscher Sprache.

4 Schwerpunktthemen

4.1 Evaluierung der Datenschutz-Grundverordnung

Zum Ende des Berichtszeitraums dieses Tätigkeitsberichts ist die DSGVO gut anderthalb Jahre wirksam und in der Praxis von den Verantwortlichen und Auftragsverarbeitenden, den Betroffenen im Hinblick auf ihre Rechte und nicht zuletzt den Datenschutzaufsichtsbehörden anzuwenden. Bereits im Mai 2019 fanden zahlreiche öffentliche und nicht-öffentliche Veranstaltungen (Tagungen, Diskussionsrunden und Vorträge) statt, auf denen eine erste Bilanz gezogen wurde. Im Hinblick auf die von der Europäischen Kommission gem. Art. 97 DSGVO durchzuführende Evaluierung der DSGVO zum Stichtag 25. Mai 2020 haben die unabhängigen Aufsichtsbehörden des Bundes und der Länder einen Erfahrungsbericht zur Anwendung der DSGVO erstellt, an dem ich maßgeblich mitgewirkt habe.

Ungeachtet einiger Anlaufschwierigkeiten, die die Umsetzung einer solchen umfangreichen neuen gesetzlichen Regelung mit sich bringt (s. 27. TB Nr. 1.1) und einer teils absurden Panikmache, lässt sich festhalten, dass wesentliche mit der europäischen Datenschutzreform verfolgten Zielsetzungen erreicht wurden. Die weitgehende Harmonisierung des Datenschutzrechts in der EU zum Abbau von Hindernissen für den digitalen Binnenmarkt und ein gesteigertes Bewusstsein für den Datenschutz bei Unternehmen, Behörden sowie Bürgerinnen und Bürgern führen zu einem verbesserten Schutz des Grundrechts auf informationelle Selbstbestimmung. Dazu tragen auch die wirksameren Sanktionsmöglichkeiten der Aufsichtsbehörden bei, von denen diese, in Form von Geldbußen, mehr und mehr Gebrauch machen. In Ländern wie den USA, Japan, Südkorea, Mexiko, Brasilien und Indien wird die DSGVO als Vorbild oder Anstoß für eine nationale Datenschutzgesetzgebung gesehen. Die DSGVO hat somit den Datenschutz nicht nur in Deutschland und Europa, sondern weltweit erheblich gestärkt.

Trotz dieser insgesamt positiven Bilanz sehe ich weiterhin Verbesserungspotenzial. Knackpunkt bleibt die Durchsetzung des Datenschutzes insbesondere gegenüber den großen, internationalen IT-Unternehmen. Hier sind alle europäischen Aufsichtsbehörden gefordert, das Verfahren der Zusammenarbeit im Europäischen Datenschutzausschuss so mit Leben zu füllen, dass hinreichender Vollzugsdruck auf die Konzerne ausgeübt wird. An anderer Stelle gilt es Bedenken und Kritik an der DSGVO aufzugreifen und im Rahmen des anstehenden Evaluierungsprozesses auf europäischer Ebene zu diskutieren. Hierbei sollte sowohl versucht werden, unnötige bürokratische Hürden, z. B. bei den Informations- und Dokumentationspflichten abzubauen, als auch bestehende Datenschutzlücken im Recht, etwa im Bereich Profiling, bestmöglich zu schließen.

Erfahrungsbericht der DSK zur Anwendung der DSGVO

Gem. Art. 97 Abs. 1 DSGVO legt die Europäische Kommission zum 25. Mai 2020 dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der DSGVO vor. Dazu kann die Kommission nach Art. 97 Abs. 3 DSGVO Informationen, u. a. bei den Aufsichtsbehörden, anfordern. Die DSK hat dies zum Anlass genommen, einen Bericht über die Erfahrungen bei der Anwendung der DSGVO zu verfassen und an den EDSA zu senden, der von der Kommission nach Art. 97 Abs. 3 DSGVO konsultiert wurde. Der Bericht wurde auch auf den Internetseiten der DSK veröffentlicht. Inhaltlich werden die folgenden neun Schwerpunktthemen behandelt:

- Alltagserleichterung und Praxistauglichkeit,
- Datenpannenmeldungen,
- Zweckbindung,
- Data Protection by Design,
- Befugnisse der Aufsichtsbehörden und Sanktionspraxis,

- Zuständigkeitsbestimmung, Zusammenarbeit und Kohärenz,
- Direktwerbung,
- Profiling,
- Akkreditierung.

Unabhängig von einem insgesamt positiven Fazit zur DSGVO sieht die DSK in diesen Bereichen Verbesserungsbedarf und unterbreitet teils auch konkrete Vorschläge für Gesetzesänderungen. So wird u. a. eine Ausweitung des Grundsatzes „data protection by design“ auf die Hersteller von Produkten gefordert und eine Verschärfung des geltenden Rechtsrahmens zum Profiling, um der Nutzung personenbezogener Daten zu Zwecken der Profilbildung effektive und faktisch durchsetzbare Grenzen zu setzen. Im Hinblick auf die Alltagserleichterung und Praxistauglichkeit der DSGVO schlägt die DSK vor, dass die Informationspflichten nach Art. 13 DSGVO in bestimmten Konstellationen nur auf Verlangen der Betroffenen zu erfüllen sein sollen. Dies gilt, soweit Datenverarbeitungen vorgenommen werden, die nach den konkreten Umständen zu erwarten sind.

Ich empfehle, im Rahmen der Evaluation der DSGVO die Position der nationalen Datenschutzaufsichtsbehörden sowie des Europäischen Datenschutzausschusses (EDSA) zu unterstützen. Das gilt insbesondere für sinnvolle Entlastungen kleiner und mittelständischer Unternehmen beim zu leistenden bürokratischen Verfahrensaufwand und für die Forderung nach einer Verschärfung des geltenden Rechtsrahmens für das Profiling.

4.2 Digitalisierung im Gesundheitswesen

Die Digitalisierung des deutschen Gesundheitswesens kann viele Vorteile bringen – für Patientinnen und Patienten, Medizin, Pflege, Kostenträger und Gesellschaft. Sie kann allerdings ohne ein hohes Datenschutz- und Datensicherheitsniveau nicht gelingen, da sie auf die Verarbeitung zahlreicher sensibler Gesundheitsdaten ausgerichtet ist. Die Kontrolle über die Daten der Patientinnen und Patienten muss bei diesen selbst liegen. Außerdem muss stets sichergestellt sein, dass die digitalisierten Gesundheitsdaten nicht zu Missbrauch durch private oder staatliche Stellen, zu Stigmatisierungen oder Gesundheitsprofilbildung führen.

Die Digitalisierung im Gesundheitswesen umfasst zahlreiche Aspekte, wie beispielsweise den Aufbau einer sicheren Telematikinfrastruktur (s. 4.2.1), die Verbesserung der Kommunikation zwischen den Akteuren des Gesundheitswesens, wachsende Möglichkeiten zu Datenerfassung und -auswertung, Telemedizin und Unterstützung ärztlicher Behandlung durch digitale Produkte.

Nach jahrelangen Verzögerungen wird die Digitalisierung des deutschen Gesundheitswesens derzeit stark gefördert und forciert. Ein Beispiel bildet das Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgungs-Gesetz – DVG, s. 5.6), durch das u. a. digitale Gesundheitsanwendungen („DiGA“), sogenannte Gesundheits-Apps, von Ärztinnen und Ärzten verschrieben und von den Krankenkassen erstattet werden können.

Themen wie der Einsatz von Künstlicher Intelligenz und Big Data, die Nutzung von Cloud-Diensten für sensible Gesundheitsdaten, die Anwendung von Messenger-Diensten im Krankenhausbereich oder die unberechtigte Weitergabe von Gesundheitsdaten an Dritte, wie beispielsweise Tracking-Dienste, stellen den Gesundheitsbereich vor große datenschutzrechtliche Herausforderungen. Die jüngsten Gesundheitsdatenschutzskandale verdeutlichen, wie hoch der Schaden für den identifizierbaren, betroffenen Menschen und die Gesellschaft sein kann, wenn sensible, personenbezogene Gesundheitsdaten oder genetische Daten unbeabsichtigt an die Öffentlichkeit gelangen. Natürlich müssen im Rahmen der Digitalisierung des Gesundheitswesens mitunter gewachsene Strukturen verändert und Prozesse angepasst werden. Dabei sollte stets das Recht auf informationelle Selbstbestimmung Priorität haben und Risiken minimiert werden. Die datenschutzrechtlichen Grundsätze der Erforderlichkeit der Datenerhebung, der Zweckbestimmung der gespeicherten Daten und der Datenminimierung dürfen nicht weiter von interessierter Seite in Frage gestellt, sondern müssen stets eingehalten werden.

Querverweise:

5.6 Gesetzgebung im Gesundheits- und Sozialwesen

4.2.1 Die Telematikinfrastruktur mit ihren Anwendungen

Für eine sichere Kommunikation im Gesundheitswesen schafft die Bundesregierung gemeinsam mit den Verbänden des Gesundheitswesens die dazu erforderliche Telematikinfrastruktur (TI). Im Berichtszeitraum wurden erste Anwendungen eingeführt und für weitere Anwendungen, wie etwa die elektronische Patientenakte, wurden die Planungen abgeschlossen. Der Anschluss der Arztpraxen an die TI ist dabei nicht ganz reibungslos verlaufen.

Verantwortlich für die Sicherheit, die Interoperabilität, den Aufbau und die Weiterentwicklung der TI ist die gematik GmbH. Die Leistungserbringer des Gesundheitswesens sind seit dem 1. Januar 2019 gesetzlich

verpflichtet, das Versichertenstammdatenmanagement (VSDM) als erste Anwendung der TI durchzuführen (vgl. § 291 Abs. 2b SGB V). Hierfür müssen sie einen für die TI zertifizierten Konnektor erwerben und ihr Praxisverwaltungssystem mit diesem Gerät an die TI anschließen. Seit dem 1. Juli 2019 drohen Leistungserbringern Honorarabzüge, sofern sie sich nicht an die TI anschließen. Daher wurde die Klärung der Frage dringend notwendig, wer für die TI im Sinne der DSGVO datenschutzrechtlich verantwortlich ist. Diese Frage habe ich intensiv mit meinen Kolleginnen und Kollegen in den Ländern erörtert. Die DSK hat daraufhin am 12. September 2019 befunden, dass die gematik GmbH eine datenschutzrechtliche Mitverantwortung für die TI trägt, weil sie mit ihren Vorgaben und Festlegungen Mittel und Zweck für die Datenverarbeitung in der TI bestimmt. Insbesondere für den Betrieb der Konnektoren sind aber auch die Leistungserbringer mitverantwortlich, insofern sie gewisse Sorgfaltspflichten zu erfüllen haben und auf Dauer diese Konnektoren auch für die sichere Übermittlung von Patientendaten nutzen werden. Den konkreten Beschluss können Sie im unten stehenden Kasten nachlesen.

Mich haben eine Reihe von Leistungserbringern angeschrieben, die eine standardisierte „Datenschutz-Folgenabschätzung“ hinsichtlich der Aufstellung des erforderlichen Konnektors vorgenommen haben. Im Rahmen dieser „Datenschutz-Folgenabschätzungen“ kommen sie zu dem Ergebnis, dass der Anschluss ihrer Praxen an die TI nicht zu verantworten sei. Aus der Verantwortlichkeit der gematik GmbH für einen sehr wesentlichen Teil der TI ergibt sich allerdings die Unzuständigkeit der Leistungserbringer für diesen Teil der TI und damit auch die Unzulässigkeit der Durchführung einer „Datenschutz-Folgenabschätzung“ in dem Bereich, in dem die gematik GmbH die Verantwortung trägt.

Eine der wichtigsten Anwendungen wird nach den jetzigen Planungen des BMG die geplante Einführung der elektronischen Patientenakte zum 1. Januar 2021 werden. Hier ist aus meiner Sicht unter der Prämisse, dass die Versicherten freiwillig diese Akte nutzen und souverän über die Nutzung ihrer dort gespeicherten Daten bestimmen können, darauf zu achten, dass ein differenziertes Rollen- und Rechtemanagement implementiert wird. Dies bedeutet, dass die Versicherten in die Lage versetzt werden, dokumentengenau die Zugriffe an einzelne Leistungserbringer erteilen zu können. Im Berichtszeitraum habe ich mich verstärkt gegenüber dem BMG für die Implementierung dieses differenzierten Rollen- und Rechtemanagements eingesetzt und werde dies auch weiterhin tun.

Außerdem muss der Zugang zur elektronischen Patientenakte nach dem Stand der Technik auf höchstem Niveau gesichert sein. Mit der elektronischen Gesundheitskarte ist dies möglich, weil nur jemand im Besitz dieser Karte plus der zugehörigen PIN Zugang erlangen kann.

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12.09.2019

Die Datenschutzkonferenz vertritt zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur nach § 291a Abs. 7 SGB V folgende Auffassung:

Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) ist

a) datenschutzrechtlich alleinverantwortlich für die zentrale Zone der TI („TI-Plattform Zone zentral“) sowie

„b) im Sinne des Artikel 26 DSGVO datenschutzrechtlich mitverantwortlich für die dezentrale Zone der TI („TI-Plattform Zone dezentral“). Der Umfang der Verantwortung der gematik für die dezentrale Zone der Telematik-Infrastruktur bedarf einer gesetzlichen Regelung. Die gematik ist verantwortlich für die Verarbeitung, insbesondere soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist.“

Mit einem gesetzlich zulässigen, alternativen Verfahren der Zugangsgewährung könnte man das erforderliche Sicherheitsniveau derzeit nicht erreichen, weil das für den Zugang erforderliche Schlüsselmaterial an einem Ort außerhalb der eigenen Kontrolle gespeichert wäre. Vor dem Hintergrund, dass eine ungewollte Offenlegung von Gesundheitsdaten schwerwiegende Konsequenzen haben kann, rate ich von der Nutzung eines alternativen Zugangsverfahrens ab, solange mit diesem nicht das gleiche Sicherheitsniveau erreicht werden kann, wie mit der Nutzung der elektronischen Gesundheitskarte. Hier habe ich mich dafür eingesetzt, dass spätestens 2022 zu überprüfen ist, ob eine zum kartenbasierten Zugangsverfahren gleichwertige Alternative geschaffen werden kann, z. B. mittels sogenannter secure elements im Smartphone oder Tablet.

Ich empfehle, bei der elektronischen Patientenakte von Beginn an ein differenziertes Rollen- und Rechtemanagement zu implementieren.

4.2.2 Das Implantateregister

Die Einrichtung von zentralen Registern und deren Nutzung zu Forschungszwecken ist im Gesundheitsbereich von zunehmender Bedeutung. Ziele sind die Fortentwicklung der Medizin und die Verbesserung der Versorgung. Diese Entwicklung bedarf aber besonderer datenschutzrechtlicher Aufmerksamkeit.

Das BMG hat im Berichtsjahr 23 Gesetze in den Bundestag eingebracht. Hierzu zählt auch das Gesetz zur Errichtung des Implantateregisters Deutschland und zu weiteren Änderungen des Fünften Buches Sozialgesetzbuch (EIRD – Implantateregister-Errichtungsgesetz).

Im Implantateregister werden in einem ersten Schritt die bisher bei medizinischen Fachgesellschaften geführten Spezialimplantateregister zusammengeführt. Die Fachgesellschaften hatten bislang die Daten auf freiwilliger Basis bei den Implantateempfängern erhoben. Nunmehr wird das Implantateregister das erste Gesundheitsregister sein, das auf einer bundesweit geltenden Meldepflicht beruht. Es ist in mehrfacher Hinsicht von datenschutzrechtlicher Bedeutung: Die Erhebung der Daten beruht auf einer gesetzlichen Verpflichtung, nicht auf einer freiwillig erteilten Einwilligung. Zudem werden die Betroffenenrechte der Einschränkung der Verarbeitung nach Art. 18 DSGVO und des Widerspruchs nach Art. 21 DSGVO ausgeschlossen. Dies ist besonders brisant, da das Register – anders als der Name vermuten lässt – eben kein Produktregister ist, sondern eine Vielzahl von besonders geschützten Gesundheitsdaten erfasst. Hierzu gehören beispielsweise klinische und zeitliche Daten zum Versorgungsprozess, wie insbeson-

dere Daten zur Anamnese, Implantat relevante Befunde, Indikationen, Voroperationen und Gewicht. Diese Daten werden unter einem Pseudonym im Register gespeichert, das zuvor durch eine Vertrauensstelle gebildet wurde. Als Zweck des Gesetzes nennt das BMG die Gewährleistung der Sicherheit der Medizinprodukte und der Versorgungsqualität mit Implantaten sowie die Marktüberwachung (Vigilanz). So ermöglicht die pseudonymisierte Speicherung bei Produktmängeln die Warnung von betroffenen Patienten. Außerdem haben verschiedene Stellen die Möglichkeit, mit diesen Daten wissenschaftlich zu forschen.

In den Beratungen konnte ich bereits auf eine ordnungsgemäße Zuweisung der Vertrauensstelle an eine von der Register- bzw. Geschäftsstelle unabhängige Institution hinwirken. Bei den Ressortberatungen zum Gesetzentwurf monierte ich den geplanten Ausschluss aller datenschutzrechtlichen Betroffenenrechte, konnte aber lediglich erreichen, dass auch auf den zunächst vorgesehenen Ausschluss der Betroffenenrechte der Auskunft nach Art. 15 DSGVO und der Berichtigung nach Art. 16 DSGVO verzichtet wurde.

Für die Forschung werden nach Möglichkeit anonymisierte Daten zur Verfügung gestellt, also meist zusammengefasste (aggregierte) Daten mehrerer Personen. Hinsichtlich der Bereitstellung pseudonymisierter Daten waren besondere Anforderungen vorgesehen. Wie das Verfahren zur Prüfung dieser Anforderungen durchgeführt wird und wie die zuständige Geschäftsstelle insbesondere die nötige Erforderlichkeit des Zugangs zu den Daten für ein bestimmtes Forschungsvorhaben bewertet, werde ich nach Aufnahme des Wirkbetriebes des Registers beobachten. Die zunächst vorgesehene Ansiedlung des Registers beim Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) hielt ich für sachgerecht. Durch die vom BMG geplante Eingliederung des DIMDI in das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) ergab sich aber eine neue Problematik, nämlich wie ein neutrales Verfahren für die Entscheidung über einen Antrag auf Zugang zu den Registerdaten gewährleistet werden könnte, wenn das BfArM selbst als Nutzungsberechtigter im Gesetz genannt ist und daher über die eigenen Anträge zu entscheiden hätte. Hier habe ich wegen der hohen Sensibilität nachdrücklich eingefordert, eine unabhängige Stelle mit den Registeraufgaben zu betrauen, um einen datenschutzkonformen Registerbetrieb zu ermöglichen.

Diese Notwendigkeit besteht auch für andere Register im Gesundheitsbereich. Das BMG hat zur Klärung dieser Frage die Fusion des DIMDI auf das BfArM zunächst ausgesetzt.

Ich empfehle, statt einer Verlagerung von Registern ins Bundesinstitut für Arzneimittel und Medizinprodukte eine eigenständige unabhängige Registerbehörde im Gesundheitsbereich zu schaffen.

Querverweis:

5.6 Gesetzgebung im Bereich Gesundheits- und Sozialwesen

4.3 Datenminimierung

Der Grundsatz der Datenminimierung ist ein datenschutzrechtlicher Dauerbrenner. Auch im vergangenen Jahr erreichten mich zu dieser Thematik wieder zahlreiche Beschwerden.

Datenminimierung gehört zu den in Art. 5 DSGVO festgeschriebenen Grundprinzipien des europäischen Datenschutzrechts. Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen sein und sich auf das notwendige Maß beschränken. Es ist daher immer Aufgabe der Verantwortlichen, sich genau zu überlegen, welche Daten für die Erfüllung einer Aufgabe tatsächlich benötigt werden und wie lange sie verarbeitet werden müssen.

Welche Auswirkung dieser Grundsatz auf die praktische Arbeit der Behörden hat, veranschaulichen die folgenden Fälle:

Einkommensteuerbescheide für Beitragsberechnung der gesetzlichen Krankenkassen

Zu Zwecken der Beitragsermittlung oder der Überprüfung der Zuzahlungsbefreiung sind die Krankenkassen auf die Erhebung bestimmter Daten angewiesen. Die Aufforderung zur Vorlage des Einkommensteuerbescheids betrifft zum einen die Selbstzahlenden in der gesetzlichen Krankenversicherung, zum anderen Versicherte mit familienversicherten Partnern.

Da bei den Selbstzahlenden die Meldung der Daten zur Berechnung der Beitragshöhe vom Arbeitgeber entfällt, sind die Krankenkassen gehalten, diese Daten auf andere Weise zu erheben. Im Sozialverwaltungsverfahren darf die Behörde die Beweismittel heranziehen, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält (§ 21 SGB X).

Um eine einheitliche Beitragsermittlung zu garantieren, hat der Gesetzgeber den Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) mit der Regelung der Beitragsbemessung beauftragt. So ist in den „Einheitlichen Grundsätze[n] zur Beitragsbemessung freiwilliger Mitglieder der gesetzlichen Krankenversicherung […] (Beitragsverfahrensgrundsätze Selbstzahler)“ des GKV-Spitzenverbandes, ergänzt um den Katalog von Ein-

nahmen und deren beitragsrechtlicher Bewertung nach § 240 SGB V festgelegt, welche Einnahmen dem Einkommensbegriff zugrunde gelegt werden.

Ebenso ist dort bestimmt, dass die Krankenkassen die entsprechenden Nachweise jährlich erheben müssen. Dabei ist das Einkommen des Ehe- oder Lebenspartners nur dann relevant, wenn dieser nicht gesetzlich krankenversichert ist. Jedoch kann dieses Datum zur Feststellung der Familienversicherung herangezogen werden.

Beim Einkommensteuerbescheid handelt es sich um ein amtliches Dokument, das seiner Nachweisfunktion rechtlich nur dann genügt, wenn es vollständig vorgelegt wird. Die zwingend notwendigen Bestandteile eines Steuerbescheides sind nach § 157 Abgabenordnung (AO) die Bezeichnung der festgesetzten Steuer nach Art und Betrag, eine Rechtsbehelfsbelehrung und die Benennung der ausstellenden Behörde. Unter Beachtung dieser Anforderungen dürfen auch die Angaben im Einkommensteuerbescheid geschwärzt werden, die für die Ermittlung des beitragsrelevanten Einkommens nicht erforderlich sind.

Aus meiner Sicht sollte über weitere datenschutzfreundlichere Lösungen nachgedacht werden. Z. B. eine vom Finanzamt bestätigte, persönliche Erklärung der Versicherten über das beitragsrelevante Einkommen, die auf Wunsch auch unmittelbar elektronisch an die zuständige Krankenkasse weitergeleitet wird.

Datenerhebung durch Jobcenter bei selbständigen Leistungsbeziehenden

Zu den Beziehenden von Leistungen zur Grundsicherung nach dem Sozialgesetzbuch (SGB) II zählen auch viele selbständig Tätige, deren Einkommen zur Bestreitung des Lebensunterhaltes nicht ausreicht. Die Prüfung des Leistungsanspruches ist für diesen Personenkreis besonders anspruchsvoll, da hierfür alle Einnahmen aus der selbständigen Tätigkeit berücksichtigt werden müssen. Zudem müssen die mit der Tätigkeit zusammenhängenden zwingend notwendigen Ausgaben auf die Einnahmen angerechnet werden. Hierbei kommt es immer wieder zu einer zu umfassenden Forderung von Angaben und Nachweisen durch die Jobcenter. Insbesondere die personenbezogenen Daten der Kundinnen und Kunden sind für die Aufgabenerfüllung der Jobcenter regelmäßig nicht erforderlich, wenn die einzelnen Einnahmen und Ausgaben durch Rechnungsnummern oder auf andere geeignete Weise zugeordnet werden können. Die Jobcenter haben die Leistungsbeziehenden daher auf entsprechende Schwärzungsrechte hinzuweisen, damit sie keine Daten von Personen erhalten, die sie für die Erfüllung ihrer gesetzlichen Aufgabe nicht benötigen.

Vorlage der Rentenauskunft beim Jobcenter

Leistungen zur Grundsicherung nach dem SGB II werden nur erbracht, wenn die betroffenen Personen keinen Anspruch auf vorrangige Sozialleistungen haben. Daher müssen die betroffenen Personen einen Rentenantrag stellen, wenn sie einen ausreichend hohen Anspruch auf eine Altersrente haben und das Eintrittsalter naht.

Die Jobcenter dürfen die betroffenen Personen jedoch nur zur Stellung eines Rentenantrages auffordern, wenn durch den Bezug der Altersrente die Hilfebedürftigkeit vollständig wegfällt, sie also nicht mehr auf Leistungen zur Grundsicherung angewiesen sind. Um dies zu prüfen, fordern die Jobcenter regelmäßig die vollständige Rentenauskunft an.

Soweit ein nur sehr geringer Anspruch auf eine Altersrente besteht, kann jedoch auch die Vorlage einer Renteninformation genügen. Weist diese aus, dass der voraussichtliche Rentenanspruch bei Weitem nicht zur Beendigung der Hilfebedürftigkeit führen wird, liegen die Voraussetzungen für die verpflichtende Stellung eines Rentenantrages nicht vor. Weitere Nachweise sind dann nicht erforderlich.

Besteht ein Anspruch, der die Beendigung der Hilfebedürftigkeit durch den Rentenbezug möglich erscheinen lässt, muss die aktuelle Rentenauskunft vorgelegt werden, da aus dieser der genaue Zeitpunkt und die voraussichtliche Höhe der vorzeitigen Inanspruchnahme der Altersrente hervorgeht. Es ist jedoch nicht erforderlich, die vollständige Rentenauskunft zu fordern. Die Auflistung rentenrechtlicher Zeiten und die Aufschlüsselung der Entgeltpunkte sind für die Aufgabenerfüllung der Jobcenter nicht relevant.

Anforderung der Mietbescheinigung durch Jobcenter

Bereits im 24. und 26. Tätigkeitsbericht wurde festgestellt, dass Empfangende von Leistungen nach dem SGB II unter Hinweis auf die Mitwirkungspflichten zur Vorlage einer von Vermietern ausgefüllten Mietbescheinigung aufgefordert wurden. Leider ist dieses Vorgehen noch immer nicht in allen Jobcentern abgestellt.

Die Mietbescheinigung kann nur auf freiwilliger Basis verwendet werden. Mit ihr können die erforderlichen Daten für die Prüfung des Anspruchs auf Übernahme der Kosten für Unterkunft und Heizung auf einfachem Weg umfassend nachgewiesen werden. Diese Form des Nachweises kommt jedoch nur für Personen in Betracht, deren Vermieter bereits Kenntnis vom Leistungsbezug hat oder die die Kenntnisnahme des Leistungsbezuges durch die Vermieter als unproblematisch ansehen.

Viele betroffene Personen möchten jedoch nicht, dass ihre Vermieter Kenntnis vom Leistungsbezug erhalten. Dies ist im Regelfall auch nicht erforderlich, da die benötigten Angaben für die Berechnung des Anspruchs auf Übernahme der Kosten für Unterkunft und Heizung auf andere Weise, beispielsweise durch Vorlage des Mietvertrages, der Nebenkostenabrechnung und Kontoauszüge, erfolgen kann. Die Jobcenter müssen bei ihrer Arbeit darauf achten, dass sie keine unnötige Datenverarbeitung, wie die Bekanntgabe des Leistungsbezuges, gegenüber den Vermietern verursachen.

Veröffentlichung personenbezogener Daten von Markenanmeldern

Das Deutsche Patent- und Markenamt (DPMA) veröffentlicht nach den Vorschriften des MarkenG und der MarkenV personenbezogene Daten von Anmeldern einer Marke im von ihm betriebenen Onlineregister. Hierfür bestehen zunächst gute Gründe. Beispielsweise müssen sich die Inhabenden von Rechten an bereits bestehenden Marken mit den Anmeldenden einer neuen Marke auseinandersetzen können, wenn die neue Anmeldung zu einer Verwechselungsgefahr führen würde.

Das DPMA veröffentlicht die Daten des Anmeldenden allerdings auch dann weiterhin, wenn die Anmeldung einer Marke aus verschiedenen Gründen gescheitert ist. Sobald die Anmeldung einer Marke gescheitert ist, besteht für Dritte keine Notwendigkeit mehr, sich mit diesem Anmeldenden auseinander zu setzen. Soweit das DPMA vorträgt, die Veröffentlichung diene dem Zweck, der Allgemeinheit eine gewisse Einsicht in die Entscheidungspraxis der Behörde zu gewähren, kann dies dadurch erfüllt werden, dass die gescheiterte Markenanmeldung ohne personenbezogene Daten des Anmeldenden veröffentlicht wird.

Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) hat sich, als ich ihm angekündigt hatte, gegenüber dem DPMA von meinen Befugnissen aus Art. 58 Absatz 2 DSGVO Gebrauch machen zu wollen, meiner Rechtsauffassung angeschlossen. Das DPMA wurde aufgefordert, die von mir gerügte Praxis zu ändern und die Veröffentlichung personenbezogener Daten von Anmeldenden bei gescheiterten Markenanmeldungen einzustellen. Außerdem soll das DPMA ein Verfahren festlegen, nach dem die Anmeldedaten gelöscht werden, wenn ihre weitere Speicherung nicht mehr erforderlich ist. Die notwendigen technischen Anpassungsarbeiten befinden sich derzeit in der Umsetzung und werden voraussichtlich im Jahr 2020 abgeschlossen sein.

4.4 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist aktuell zu Recht eines der dominierenden Technologiethemen. Denn KI ist eine Schlüsseltechnologie, die bereits seit einiger Zeit unsere Wirtschaft und Gesellschaft auf verschiedenen Ebenen grundlegend verändert.

KI kann uns in vielen Lebenslagen helfen: Mit ihr werden beispielsweise Ärztinnen und Ärzte in die Lage versetzt, bessere Diagnosen zu stellen und neue Therapiewege zu beschreiten. Wir können mit ihr den Einsatz unserer Ressourcen optimieren und so etwa den ÖPNV besser steuern. Mit KI können wir Energie effizienter nutzen und den Energieverbrauch senken. Diese wenigen Beispiele zeigen, welche großen Chancen mit ihr verbunden sind.

Bei der KI geht es insbesondere darum, „technische Systeme“ so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ und mit Unsicherheiten umzugehen, statt klassisch programmiert zu werden.[1]

Unsere Aufgabe: Chancen und Risiken ausbalancieren

Auch alle Datenschützerinnen und -schützer sind sich dieser vielfältigen Chancen bewusst. Wir überlegen selbst, wie KI uns bei der Kontrolle von Datenverarbeitungen unterstützen kann. In aller Regel führen Chancen aber auch zu (neuen) Risiken. KI benötigt eine Vielzahl an Daten, häufig auch solche mit Personenbezug. So kann die Versicherungswirtschaft etwa mit KI neue anreizorientierte – und damit z. B. gesundheitsfördernde – Beitragsmodelle anbieten. Wer hier zunächst von günstigen Versicherungsbeiträgen profitiert, spürt aber möglicherweise schnell die Ambivalenz moderner KI-Datenanalysen, wenn eine Veränderung von Lebensgewohnheiten oder eine bekannt werdende gesundheitliche Disposition sich vollautomatisch im nächsten Beitragsbescheid manifestiert oder gar zu einem Versicherungsausschluss führt.

Ziel: Proaktive Technikgestaltung

Ich möchte die Gestaltung von KI im Sinne einer positiven Technikgestaltung aktiv begleiten. Es ist wichtig, dass die Menschenwürde und das in ihr verankerte Grundrecht auf informationelle Selbstbestimmung bei der Nutzung

1 Verständnis der Bundesregierung, BT-Drs. 19/1982.

von KI-Systemen Maßstab unseres Handelns bilden. Der Mensch darf nicht zum bloßen Objekt degradiert werden. Datenschutz hilft bei dieser „menschzentrierten" Gestaltung von KI-Systemen. Denn zahlreiche ethische Grundsatzfragen haben bereits eine normative Ausprägung im Datenschutzrecht erhalten. Die Stimme des Datenschutzes ist daher für die ethische und grundrechtsverträgliche Gestaltung von KI-Systemen essenziell.

Datenschutz ist Erfolgsfaktor

In diesem Sinne ist Datenschutz ein wichtiger Erfolgsfaktor. Auch aus industriepolitischer Sicht sind wir gut beraten, den Weg einer datenschutzkonformen Gestaltung von KI-Lösungen in Europa weiter auszubauen. Die Rolle des Datenschutzes wird dabei oft verkannt: Er zielt nicht darauf ab, Innovationen einzuschränken oder zu erschweren. Datenschutz sucht vielmehr den Ausgleich zwischen den Interessen einer Datennutzung durch Dritte und der Souveränität des Individuums. Ziel muss es sein, Privatheit selbstbestimmt zu ermöglichen und gleichzeitig die Chancen der Digitalisierung zu nutzen. Wir müssen die Privatsphäre schützen, auch und gerade um einen Freiraum zur unbeobachteten persönlichen Entfaltung zu schaffen. Datenschutzfreundliche KI kann in einem weltweiten Markt zu einem positiven Differenzierungsmerkmal ausgebaut werden. In den nächsten Jahren werden hier entscheidende Weichenstellungen getroffen.

Hambacher Erklärung – unser initiales Thesenpapier

„KI und Datenschutz" war im Jahr 2019 auch das Leitthema der DSK. Bereits Anfang April 2019 wurde von der DSK ein erstes Thesenpapier für eine datenschutzfreundliche Technikgestaltung von KI vorgelegt, die sog. Hambacher Erklärung (s. Kasten in Beitrag 3.1). In bewusster Anlehnung an die auf dem Hambacher Fest 1832 erhobenen Forderungen nach Freiheit und Demokratie hat die DSK betont, dass der Einsatz von KI mit dem Menschen und seinen Grundrechten und Grundfreiheiten in Einklang stehen muss.

Aus dem geltenden Datenschutzrecht werden sieben Anforderungen abgeleitet:

- KI darf den Menschen nicht zum bloßen Objekt machen.
- KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben.
- KI muss transparent, nachvollziehbar und erklärbar sein.
- KI muss Diskriminierungen vermeiden.
- Für KI gilt der Grundsatz der Datenminimierung.
- KI braucht Verantwortlichkeit.
- KI benötigt technische und organisatorische Standards.

Konkrete Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Die DSK hat die Anforderungen der Hambacher Erklärung zu konkreten Empfehlungen für KI-spezifische, technische und organisatorische Maßnahmen fortentwickelt. Dieses Positionspapier „Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen" wurde am 6. November 2019 auf der 98. DSK beschlossen.[2] Das Papier gibt den Verantwortlichen Hilfestellung für eine datenschutzrechtliche Orientierung bei der Planung und dem Betrieb von KI-Systemen. Das Positionspapier soll auch dazu dienen, den Dialog mit den relevanten Akteuren, wie den Verbrauchervereinigungen, auf dieser Grundlage weiter zu intensivieren.

Nur ein übergreifender Dialog sichert interessengerechte Lösungen für alle

Diesen Dialog habe ich im vergangenen Jahr intensiv geführt. So richtete ich am 24. September 2019 in Berlin

2 Die Empfehlungen sind abrufbar unter https://www.bfdi.bund.de/beschlüsse-positionspapiere

ein Symposium unter dem Titel „Chancen und Risiken für den datenschutzgerechten Einsatz von Künstlicher Intelligenz“ aus. Die Veranstaltung bot eine Diskussionsplattform für mehr als 150 Teilnehmerinnen und Teilnehmer aus ganz unterschiedlichen Disziplinen und ermöglichte einen Austausch über die vielfältigen, komplexen und teilweise gegenläufigen Interessen der KI. Als Mitglied der Datenethikkommission (DEK) konnte ich die enorme Bedeutung datenschutzrechtlicher Grundprinzipien betonen. Ganz zentral ist die Forderung nach Transparenz, aber auch nach einer wirksamen Algorithmenkontrolle. Hier verfolgt die DEK einen risikobasierten Regulierungsansatz. Je größer das Schädigungspotenzial ist, umso mehr Anforderungen sind an den Einsatz des Algorithmus zu stellen und umso mehr Kontrollmöglichkeiten sind vorzusehen. Ausführlichere Informationen zur DEK finden sich in einem eigenen Beitrag unter Punkt 4.6 Datenethikkommission.

Auch die „Strategie Künstliche Intelligenz“ der Bundesregierung begleite ich intensiv, u. a. durch meine Teilnahme an einem Datenschutz-Roundtable. KI endet natürlich nicht an unseren Landesgrenzen. Deshalb setze ich mich auch auf europäischer und internationaler Ebene dafür ein, die Belange des Datenschutzes bei KI stärker in den Fokus zu nehmen. Hier engagiere ich mich insbesondere bei der Ende 2018 eingerichteten Arbeitsgruppe zu „Datenschutz und Ethik in der KI“ der Internationalen Datenschutzkonferenz.

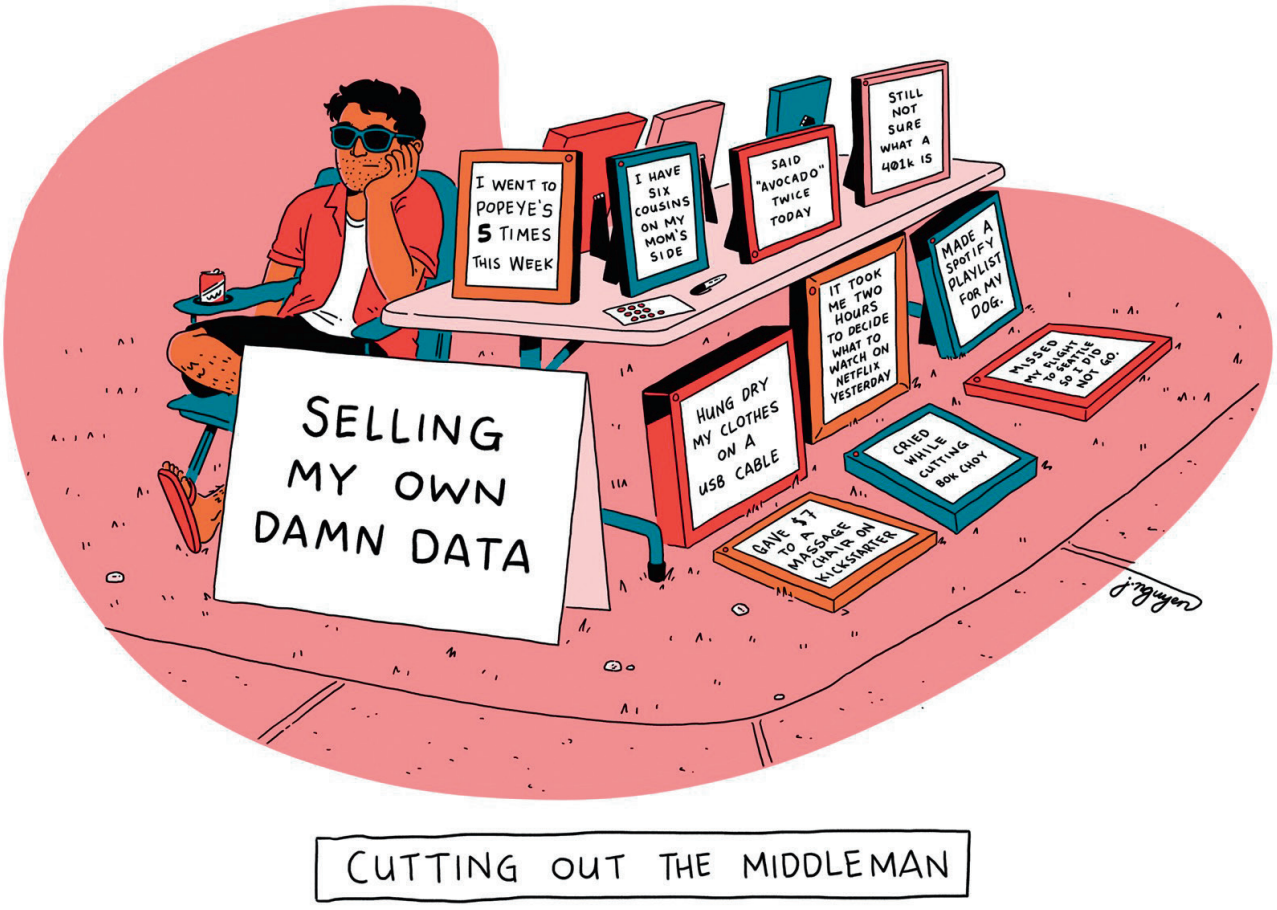
Querverweis:

4.6 Das Gutachten der Datenethikkommission

4.5 Datenschutzrechtliche Einwilligung

Die Einwilligung ist eine der zentralen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Sie sollte den Willen der Betroffenen direkt reflektieren und stellt damit die unmittelbarste Grundlage für eine Datenverarbeitung dar. Gerade deshalb ist es wichtig, dass ihre gesetzlichen Voraussetzungen konsequent und strikt eingehalten werden.

Art. 6 Abs. 1 S. 1 lit. a DSGVO lässt die Verarbeitung personenbezogener Daten u. a. dann zu, wenn die betroffene Person dazu ihre Einwilligung gegeben hat. Die gesetzlichen Anforderungen an die Einwilligung sind über die genannte Vorschrift hinaus in Art. 4 Nr. 11 und



Art. 7 Abs. 2 und 3 DSGVO geregelt. Danach muss die Einwilligung in die konkrete Datenverarbeitung grundsätzlich freiwillig, informiert und unmissverständlich abgegeben werden sowie auf einen bestimmten Zweck bezogen sein.

Im Zusammenhang mit der Einwilligung werden aktuell die beiden folgenden Themenschwerpunkte diskutiert.

4.5.1 Einwilligung in der Forschung

Die DSGVO ist wissenschaftsfreundlich ausgerichtet. Allerdings bedeutet das keine völlige Freiheit der Forschung bei der Verarbeitung personenbezogener Daten. Zwischen dem Grundrecht auf Wissenschaftsfreiheit und dem Grundrecht auf Datenschutz ist im Wege der „praktischen Konkordanz" ein angemessener Ausgleich zu schaffen.

Art. 89 DSGVO gibt für die wissenschaftliche Forschung vor, dass für diese die Datenschutz-Grundverordnung gilt. Soweit nicht gesetzlich geregelt, kann die Verarbeitung personenbezogener Daten zu wissenschaftlichen Studien auf Basis einer Einwilligung der betroffenen Person zulässig sein. Die Einwilligung muss dabei den Anforderungen an eine informierte Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO („informed consent") genügen, d. h., die betroffene Person muss „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich" erklärt haben, dass die Daten für eine bestimmte wissenschaftliche Studie zur Verfügung stehen.

Von diesem Grundsatz macht die DSGVO im Erwägungsgrund 33 eine Ausnahme. Vor dem Hintergrund, dass „oftmals […] der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden" kann, soll es der betroffenen Person erlaubt sein, unter engen Voraussetzungen

1. für bestimmte Forschungsbereiche oder
2. für Teile von Forschungsprojekten, wenn
3. anerkannte ethische Standards der wissenschaftlichen Forschung eingehalten werden,

die Einwilligung zu erteilen (sog. breite Einwilligung – „broad consent"). Diese Ausnahmeregelung wurde in der wissenschaftlichen Praxis begrüßt, allerdings zu weit ausgelegt:

Die DSK hat in einem Beschluss vom 3. April 2019 darauf hingewiesen, dass nur dann bei einer der Datenerhebung zeitlich vorgelagerten Einwilligung unter engen Voraussetzungen Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden können, wenn das konkrete Design des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung nicht zulasse. Die DSK unterstreicht in diesem Beschluss, dass es mit der DSGVO nicht mehr vereinbar ist, wenn die Verwendung der erhobenen Daten pauschal auf bestimmte Forschungsbereiche ausgeweitet wird. Zudem weist sie darauf hin, dass „in den Einzelfällen, in denen das Arbeiten mit breiten Einwilligungen […] für zwingend erforderlich gehalten wird", mit notwendigen Korrektiven zu arbeiten ist, um die abstraktere Fassung des Forschungszweckes zu kompensieren. Diese sind zusätzliche Sicherungsmaßnahmen zur Gewährleistung der Transparenz und zur Vertrauensbildung sowie zusätzliche Garantiemaßnahmen zur Datensicherheit.

Für die „breite Einwilligung" verweist Erwägungsgrund 33 der DSGVO auf die Einhaltung der „anerkannten ethischen Standards der wissenschaftlichen Forschung". Zu denen gehört seit dem Nürnberger Kodex von 1949 die informierte Einwilligung, nicht zuletzt aufgrund der Erfahrungen in der medizinischen Forschung im Dritten Reich, aber auch anderen ethisch bedenklichen Studien weltweit. Der Deutsche Ethikrat brachte in seiner Stellungnahme „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung" aus dem Jahr 2017 das Modell einer „Datenspende" ins Spiel. Dieses Modell soll im Sinne einer umfassenden Zustimmung der Betroffenen eine Datennutzung ohne enge Zweckbindung zugunsten der klinischen und medizinbezogenen Grundlagenforschung erlauben. Es handelt sich dabei nicht mehr um eine informierte Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO oder eine „breite Einwilligung" im Sinne des Erwägungsgrundes 33, sondern um eine offene Einwilligung („blanket consent"), die mit den Vorgaben der DSGVO nicht zu vereinbaren ist.

Im Berichtszeitraum lagen den Datenschutzaufsichtsbehörden des Bundes und der Länder gleichwohl Einwilligungsformulare vor, die eine solche „Datenspende" vorsahen. Durch eine entsprechende Intervention unsererseits konnte erreicht werden, dass ein Einwilligungsformular datenschutzkonform ausgestaltet wurde.

Im Rahmen der DEK habe ich mich an der Erarbeitung von Vorschlägen beteiligt, wie die Datennutzung für die medizinische Forschung datenschutzfreundlich durch Instrumente wie die dynamische Einwilligung oder Datentreuhänder weiter erleichtert werden kann.

4.5.2 Tracking und Cookies

Viele Internetseiten setzen Tracking-Dienste ein. Cookiebanner, die beim Weitersurfen eine Zustimmung unterstellen, sind rechtlich unwirksam. Zahlreiche, auch bekannte Internetseiten haben diese Anforderung noch nicht rechtskonform umgesetzt.

Wer eine Internetseite betreibt, möchte z. B. wissen, wie viele Besucher es gab und welche Seiten angeklickt wurden. Dies ist in vielen Fällen legitim und nachvollziehbar. Problematisch ist allerdings, wenn Drittanbieter eingebunden werden und diese ebenfalls Daten über die Nutzer erhalten. Verarbeitet der Drittanbieter diese Daten zu eigenen Zwecken weiter (wie z. B. Google Analytics in der Standardkonfiguration), benötigt er dafür die Einwilligung des Nutzers.

Auf vielen Internetseiten finden sich hierzu sogenannte Cookiebanner. Diese suggerieren fälschlich, dass das Weitersurfen eine Einwilligung bedeutet. Eine Einwilligung muss jedoch ausdrücklich und informiert erfolgen. Das heißt: Die Anbieterinnen und Anbieter müssen zunächst genau informieren, welche Daten zu welchem Zweck erhoben werden. Erst wenn die Nutzerinnen und Nutzer daraufhin zustimmen, dürfen die Daten erhoben und verarbeitet werden. Vorangekreuzte Kästchen oder versteckte Widerspruchsmöglichkeiten sind unzulässig.

Das bedeutet jedoch nicht, dass hier jedes Mal eine Einwilligung abgefragt werden muss. Erstaunlich ist, dass viele Seitenbetreiber großflächige Cookiebanner einsetzen und bei Beschwerden von Nutzerinnen und Nutzern angeben, die DSGVO bzw. die Aufsichtsbehörden würden dies verlangen. Dies ist nicht der Fall. Reine Besuchsstatistiken können ohne Einwilligung und völlig „bannerfrei“ datenschutzkonform umgesetzt werden. Wie das geht, hat die Datenschutzkonferenz in einer ausführlichen „Orientierungshilfe“ beschrieben (zu finden unter: www.bfdi.bund.de/orientierungshilfen).

4.6 Das Gutachten der Datenethikkommission

Die Datenethikkommission (DEK) betont in ihrem Abschlussgutachten die herausragende Rolle des Datenschutzes und gibt konkrete Handlungsempfehlungen zur Gestaltung unserer digitalen Zukunft. Es liegt nun an der Bundesregierung und dem Deutschen Bundestag, die Empfehlungen aufzugreifen und entsprechende Maßnahmen umzusetzen.

Die DEK wurde am 18. Juli 2018 von der Bundesregierung eingesetzt, um sich mit den Leitfragen zu den Themenkomplexen Algorithmische Prognose- und Entscheidungsprozesse, Künstliche Intelligenz (KI) und Daten auseinanderzusetzen. Sie bestand aus 16 Persönlichkeiten aus den Bereichen Wissenschaft, Wirtschaft, Verbraucher- und Datenschutz. Der Datenschutz wurde durch die Landesbeauftragte für Datenschutz Schleswig-Holstein und Leiterin des Unabhängigen Landeszentrums für Datenschutz, Frau Marit Hansen, und mich vertreten.

Den inhaltlichen Rahmen für die DEK hatte die Bundesregierung mit einem initialen Fragenkatalog vorgegeben. Die DEK sollte danach „Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstandes im Informationszeitalter entwickeln.“ Zudem sollten Handlungsempfehlungen ausgesprochen werden, wie diese „ethischen Leitlinien entwickelt, beachtet, implementiert und beaufsichtigt werden können“.

Mit den vorgegebenen Fragen hätte sich die DEK mehrere Jahre beschäftigen können. Doch von der Bundesregierung war nur ein Jahr Zeit zur Verfügung gestellt worden. Die Mitglieder der DEK übergaben nach intensiver Arbeit im Oktober 2019 ihr Abschlussgutachten an die Bundesregierung. Das Gutachten wurde einstimmig und ohne Sondervoten beschlossen. Die DEK hebt in ihrem Gutachten nicht nur die abstrakte Wichtigkeit des informationellen Selbstbestimmungsrechts des Einzelnen hervor, sondern gibt konkrete Handlungsempfehlungen, wie diese Selbstbestimmung besser in die digitale Entwicklung integriert werden kann.

Daten und Grundrechtsschutz im digitalen Zeitalter

Für mich stand von Beginn an fest, dass eine ethische und gerechte Datenpolitik nur mit einem starken Datenschutz möglich ist. Dies entspricht auch der Überzeugung der DEK, die sich deutlich für eine Nachschärfung des Datenschutzes ausspricht. Die DEK wendet sich damit gegen den Irrglauben, es helfe der Digitalisierung, möglichst wenig zu regulieren und bestehende gesetzliche Vorgaben weitestgehend abzuschaffen. Regulierung ist jedoch keineswegs Selbstzweck. Sie dient dazu, die Werte unserer Rechtsordnung zu gewährleisten und Grundrechte zu schützen. Sie muss insbesondere dort ansetzen, wo die Gefahren für die Rechtsgüter besonders hoch sind. Spätestens seit dem 19. Jahrhundert wurde technologische Entwicklung immer auch durch einen Rechtsrahmen flankiert, um etwa die Allgemeinheit vor bestimmten Risiken zu schützen. Beispiele dafür sind der Arbeitsschutz oder Vorschriften für die Konstruktion von Kraftfahrzeugen.

Die Regulierung der Digitalisierung betrifft aber nicht nur das informationelle Selbstbestimmungsrecht und den Datenschutz. Da die Digitalisierung nach und nach alle Lebensbereiche durchdringt, bestehen auch Auswirkungen auf weitere Rechtsgüter, wie die Gesundheit, die Berufsfreiheit oder das Recht auf Gleichbehandlung. Zu denken ist hier beispielsweise an KI in der Gesundheitsforschung, Pflegeroboter, automatisierte Bewerbungsverfahren oder die Risiken der Diskriminierung durch schlechte bzw. fehlerhafte Datensätze.

Die DEK spricht sich daher an den Stellen für Regulierung aus, wo Gefahren für die Rechtsgüter einzelner Personen oder der Allgemeinheit drohen. Dies betrifft beispielsweise klarere Vorgaben und mehr Transparenz bei Profilbildungen, das Verbot von Algorithmen mit unvertretbarem Schädigungspotenzial oder spezifische Regelungen zum Datenhandel.

Transparenz

Das Thema Transparenz zieht sich wie ein roter Faden durch das Abschlussgutachten. Aus Datenschutzsicht spielt Transparenz im Rahmen der zunehmenden Digitalisierung eine entscheidende Rolle. Nur wenn ausreichend informiert wird, können das informationelle Selbstbestimmungsrecht und die daraus abgeleiteten Datenschutzrechte wahrgenommen werden. Nur wer weiß, welche Daten über die eigene Person gesammelt, wozu diese genutzt und an wen sie weitergegeben werden, ist in der Lage, eine informierte Einwilligung abzugeben. Nur wer weiß, welche Verantwortlichen die persönlichen Daten nutzen, kann die Rechte auf Auskunft, Berichtigung oder Löschung geltend machen.

Die Datennutzungen sind heute so komplex und umfassend geworden, dass die Einzelnen häufig nicht mehr in der Lage sind, einen Überblick über die Nutzung ihrer Daten zu gewinnen. Datenschutzhinweise werden oft gar nicht mehr gelesen, es wird zu allem ein Einverständnis erteilt. Andere – gerade die ältere Generation – verzichten aus Angst vor Datenmissbrauch auf digitale Teilhabe. Dies kann nicht die Lösung sein. Vielmehr sollte durch gezielte Transparenzpflichten den Bürgerinnen und Bürgern ihre digitale Selbstbestimmung über ihre Daten zurückgegeben werden.

Die DEK formulierte daher den ethischen Grundsatz der interessenadäquaten Transparenz: „Derjenige, der Daten als Verantwortlicher verarbeitet, muss bereit und in der Lage sein, dafür Rechenschaft abzulegen. Dies erfordert ein angemessenes Maß an Transparenz und Dokumentation des Handelns und gegebenenfalls auch entsprechende Haftungsregelungen." Die Anwendung dieses Grundsatzes führt zu verschiedenen Handlungsempfehlungen zur Stärkung der Transparenz. Diese betreffen u. a. die Themen Profilbildung, Scoring, Piktogramme für Produkte und Dienstleistungen sowie die Kennzeichnung von Bots.

Profilbildung und Scoring

Im Bereich von Profilbildung und insbesondere Scoring fordere ich seit Jahren eine wirksamere Regulierung und mehr Transparenz (vgl. 25. TB Nr. 5.3). Dieser Forderung hat sich auch die DEK angeschlossen. Die DEK spricht von „spezifischen Kennzeichnungs-, Informations- und Auskunftspflichten bezüglich der Profilbildung als solcher". Die Informationspflichten sollen nicht nur bei automatisierten Entscheidungen greifen, sondern allgemein beim Einsatz von Algorithmen zur Profilbildung. Hiermit verbunden fordert die DEK auch ein Recht auf einen „digitalen Neuanfang" durch Löschung der gebildeten Profile, z. B. beim Erreichen der Volljährigkeit.

Piktogramme für Produkte und Dienstleistungen

Die DEK setzt sich für verbindliche Vorgaben zum datenschutzfreundlichen Design von Produkten und Dienstleistungen ein; insbesondere wenn sich die Produkte/Dienstleistungen an Verbraucher richten. In diesem Zusammenhang fordert die DEK einheitliche Bildsymbole (Piktogramme) einzuführen, die den Verbrauchern eine informierte Kaufentscheidung ermöglichen sollen. Verbraucherinnen und Verbraucher könnten beispielsweise auf einen Blick erkennen, ob ein Gerät personenbezogene Daten durch Sensoren, wie Kamera oder Mikrofone, erfasst und ob diese via Internet an den Hersteller oder sogar Dritte übermittelt werden.

Kennzeichnung von Bots

Die DEK fordert eine Kennzeichnungspflicht für Social Bots. Die Authentizität zwischenmenschlicher Kommunikation ist nach Ansicht der DEK Grundbedingung für einen vertrauensvollen Umgang miteinander. Daher sollten Social Bots, sobald eine Verwechselungsgefahr zwischen Mensch und Maschine besteht, gekennzeichnet werden. Besonders akut ist die Kennzeichnungspflicht im Bereich sozialer Netzwerke und anderer intermediärer Medien. Hier besteht eine Gefahr für den demokratischen Diskurs, indem durch Social Bots versucht wird, Einfluss auf die öffentliche Meinungsbildung zu nehmen. Dabei wird nicht verkannt, dass auch durch Menschen (Stichwort: Online-Trolle) manipulativ in die öffentliche Meinungsbildung eingegriffen werden kann und der Umfang der Einflussnahme durch Bots umstritten ist.

Kontrolle Algorithmischer Systeme

Ein weiteres wichtiges Anliegen der DEK ist eine risikobasierte Kontrolle algorithmischer Systeme. Der Fokus bezüglich der ethischen Implikationen von Algorithmen liegt in der öffentlichen Debatte stark auf dem Einsatz von KI und dem maschinellen Lernen. Doch die ethischen Fragestellungen für den Einsatz von Algorithmen stellen sich ebenso bei normalen „klassischen" Algorithmen wie beim Einsatz von KI (weitere Informationen zu KI unter Nr. 4.4). Daher macht die DEK in ihren Handlungsempfehlungen generell keine Unterscheidungen zwischen der Art des Algorithmus, sondern spricht von algorithmischen Systemen.

Die DEK hat – wie in anderen Bereichen auch – für den Einsatz algorithmischer Systeme einen risikoadaptierten Regulierungsansatz gewählt. Künftige Regulierung soll sich am Schädigungspotenzial des algorithmischen Systems ausrichten.

Die DEK empfiehlt ein übergreifendes Modell zu entwickeln, nach dem algorithmische Systeme Kritikalitätsstufen zugeordnet werden (siehe Abbildung). Je größer das Schädigungspotenzial ist, umso mehr Anforderungen sind an den Einsatz des Algorithmus zu stellen und umso mehr Kontrollmöglichkeiten müssen vorgesehen werden. Dies reicht von Anwendungen ohne oder mit geringem Schädigungspotential (Stufe 1), bei denen es weder spezieller Qualitätsanforderungen noch besonderer Kontrollmechanismen bedürfte, bis hin zu Anwendungen mit unvertretbarem Schädigungspotential (Stufe 5), die komplett oder zumindest teilweise verboten werden müssten.

Um das Regulierungsmodell umzusetzen, empfiehlt die DEK der Bundesregierung eine horizontale Algorithmen-Verordnung auf EU-Ebene hinzuwirken. Diese sollte die zentralen Grundprinzipien für algorithmische Systeme enthalten. Wichtig sind dabei u. a. Regelungen zur Zulässigkeit und Gestaltung algorithmischer Systeme, zu Transparenz und zu Betroffenenrechten.

Innovative Datenmanagementsysteme

Die DEK möchte mit ihren Empfehlungen nicht nur Schranken für neue digitale Produkte aufzeigen, sondern es sollen auch Entwicklungen gefördert werden, die einen besonderen Nutzen für die einzelnen Bürger oder die Allgemeinheit versprechen. Die DEK spricht sich daher für die Förderung innovativer Datenmanagement- und Datentreuhandsysteme aus.

Digitalisierung und Datenschutz stellen keine unvereinbaren Gegensätze dar. Dass digitale Innovationen vielmehr auch einen wichtigen Beitrag zur Stärkung des Datenschutzes leisten können, zeigen beispielsweise neue Entwicklungen im Bereich von Datenmanagement- und Datentreuhandsystemen.

Unter Datenmanagement- und Datentreuhandsystemen werden verschiedenste Modelle verstanden. Zu den Privacy Management Tools (PMT) werden Anwendungen zur vereinfachten Einwilligungsverwaltung gezählt, wie beispielsweise Dashboards, aber auch KI-Tools, die individuelle Nutzerpräferenzen automatisch umsetzen (sog. „Datenagenten“). Daneben gibt es Personal Information Management Systems (PIMS). Bei diesen Systemen stehen nicht die Herstellung und der Support technischer Anwendungen im Vordergrund, sondern Dienstleistungen bis hin zu mehr oder weniger umfassender Fremdverwaltung der Nutzerdaten (sog. Datentreuhand-Modelle). Gemeinsames Ziel ist die Befähigung der Einzelnen zur Kontrolle über ihre personenbezogenen Daten. Die DEK empfiehlt, Forschung und Entwicklung im Bereich von Datenmanagement- und Datentreuhandsystemen intensiv zu fördern.

Bei fehlerhafter Ausgestaltung von PMT/PIMS besteht allerdings die Gefahr, dass sich ihr Einsatz ins Gegenteil verkehrt. Statt echte Selbstbestimmung zu ermöglichen, könnten PMT/PIMS auch zur unbewussten oder sorglosen Fremdbestimmung eingesetzt werden. Die DEK empfiehlt daher eine begleitende Regulierung von Datenmanagement- und Datentreuhandsystemen. Es bedarf der Erarbeitung von Qualitätsstandards für PMT/PIMS sowie ein Zertifizierungs- und Überwachungssystem.

Damit PMT/PIMS eine hinreichende Breitenwirkung erzielen können, sind sie auf die Kooperation aller betroffenen Verantwortlichen angewiesen. Die datenschutzrechtlichen Verantwortlichen sollten daher – unter sachgerechten Bedingungen – verpflichtet werden, die Kontrolle des Zugangs zu personenbezogenen Daten durch PMT/PIMS zu ermöglichen.

Werden diese Vorgaben eingehalten, können PMT/PIMS die Funktion einer wichtigen Schnittstelle zwischen Belangen des Datenschutzes und der Datenwirtschaft einnehmen. Insbesondere können sie die Nutzung von personenbezogenen Daten für die medizinische Forschung erleichtern.

Anonymisierung von Daten

Auch die Thematik der Anonymisierung von Daten wird im Abschlussgutachten angesprochen. In der Praxis besteht häufig das Problem, dass unklar ist, ob es sich bei einem Datensatz um eindeutig personenbezogene, pseudonymisierte oder anonyme Daten handelt. Je nachdem greifen aber unterschiedliche Rechtsvorschriften, so dass es für die datenverarbeitenden Stellen von enormer Bedeutung ist, Klarheit darüber zu haben, wann sie mit personenbezogenen Daten arbeiten und wann nicht.

Die DEK fordert, die Entwicklung von Verfahren und Standards zur Anonymisierung von Daten zu intensivieren. Um mehr Rechtssicherheit zu erreichen, sollten auf EU-Ebene handhabbare Standards zur Anonymisierung festgelegt werden. Damit verbunden können Vermutungsregelungen sein, die bei Einhaltung der Standards eingreifen. Dabei muss es den Datenschutzbehörden aber möglich bleiben, die Vermutung notfalls auch zu widerlegen, wenn die Standards von der technischen Realität überholt werden und eine Personenbeziehbarkeit wieder möglich wird.

Weitere wichtige Themen aus dem Gutachten will ich hier nur stichpunktartig aufführen:

- den Vorschlag, in bestimmen Sektoren (beispielsweise Messenger) Anbieter zur Interoperabilität bzw. Interkonnektivität ihrer Anwendungen zu verpflichten,
- den Vorschlag, das Haftungsrecht bezogen auf den Einsatz von Algorithmen anzupassen,
- die Forderung nach einer Ausweitung des Konzepts von Open Government Data,
- die Handlungsempfehlungen zum Zugang der Forschung zu Datensätzen
- sowie die Forderung, den Schutz der Daten von Unternehmen zu verbessern.

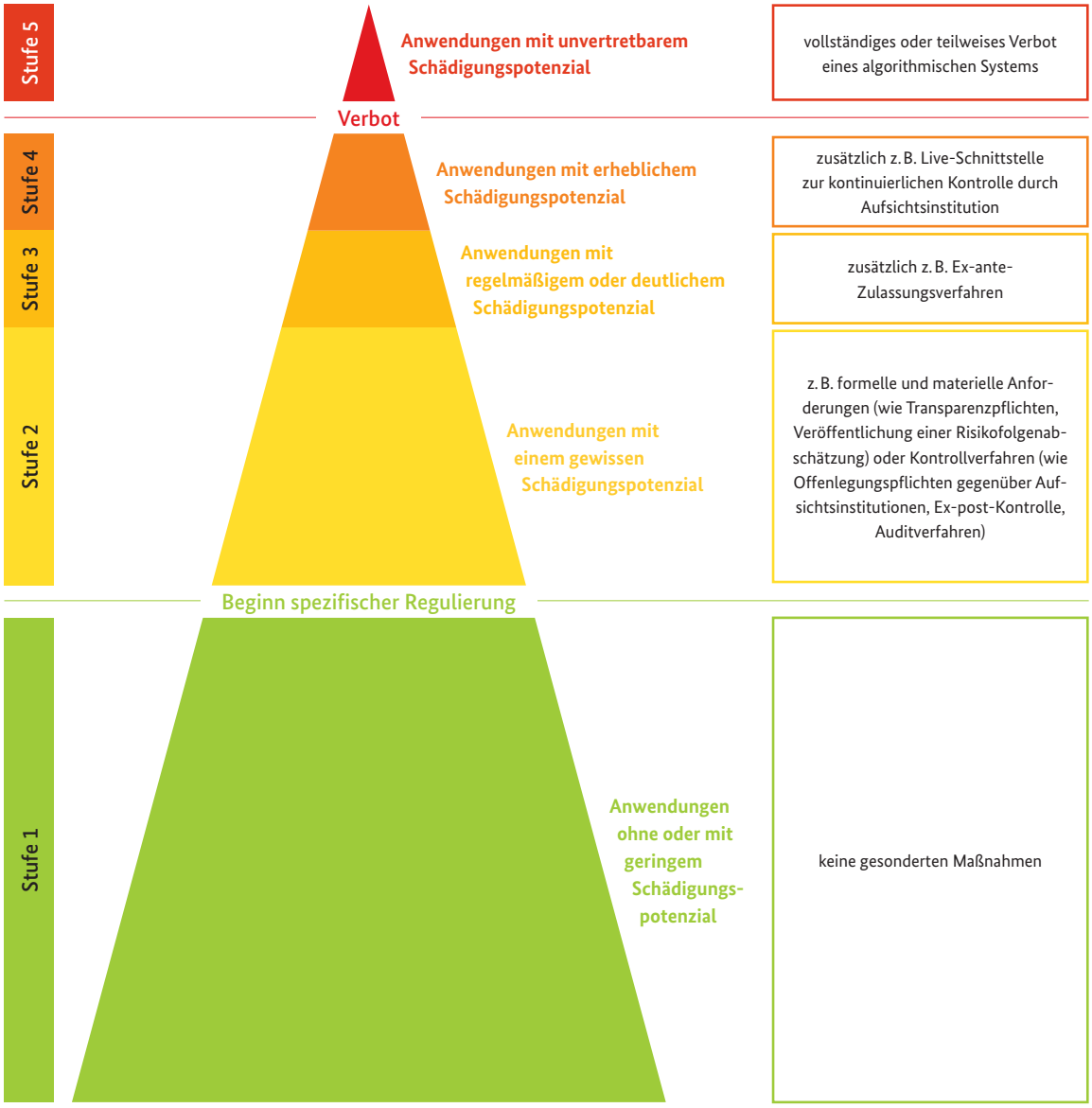
Sie können jedoch auf meiner Internetseite nachgelesen werden. Das Gutachten findet sich unter: www.bfdi.bund.de/dek

Ich empfehle, die Vorschläge der Datenethikkommision gesetzlich zu verankern.

Querverweis:

4.4 Künstliche Intelligenz

Abbildung 2:
Kritikalitätspyramide und risikoadaptiertes Regulierungssystem für den Einsatz algorithmischer Systeme



5 Gesetzgebung

5.1 Das Omnibusgesetz zur Datenschutz-Grundverordnung

Durch Änderungen von über 150 Gesetzen mittels des sogenannten Omnibusgesetzes sind nunmehr auch bereichsspezifische Datenschutzregelungen des Bundes an die unionsrechtlichen Vorgaben angepasst worden.

Seit dem 25. Mai 2018 ist die DSGVO unmittelbar geltendes Recht in allen Mitgliedstaaten der EU. Neben einer Reihe von Regelungsspielräumen für den nationalen Gesetzgeber, enthält sie zugleich konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Danach ist es erforderlich, auch das bereichsspezifische Datenschutzrecht auf die Vereinbarkeit mit der DSGVO zu überprüfen und, soweit nötig, anzupassen. Diese Anpassungen sind Gegenstand des 2. DSAnpUG-EU, dem sogenannten Omnibusgesetz.

Um ein reibungsloses Zusammenspiel der DSGVO und der JI-RL mit dem stark ausdifferenzierten deutschen Datenschutzrecht sicherzustellen, wurden in einem ersten Schritt bereits das bisherige Bundesdatenschutzgesetz (BDSG a. F.) durch ein neues Bundesdatenschutzgesetz (BDSG) abgelöst und mit Änderungen der Abgabenordnung sowie des Ersten und des Zehnten Buches des Sozialgesetzbuchs bereits wesentliche Normen des Steuerrechts und des Sozialdatenschutzrechts an die DSGVO angepasst (vgl. 27. TB, Nr. 1.2, 3.1.1 und 6.1.1).

Durch das Omnibusgesetz wurden weitere große Teile der bestehenden bereichsspezifischen Datenschutzregelungen des Bundes an die unionsrechtlichen Vorgaben angepasst. Dabei wurden über 150 Gesetze geändert, von denen nachfolgend einige erwähnt werden.

Meldegesetz

Im Bundesmeldegesetz wurden neben den erforderlichen terminologischen Anpassungen auch inhaltliche Veränderungen vorgenommen. Hierzu habe ich im Rahmen der Ressortbeteiligung zahlreiche Vorschläge gemacht. So wurde etwa die bislang in § 10 Bundesmeldegesetz vorgesehene Beschränkung des Auskunftsrechts der betroffenen Person auf Fälle einer Datenübermittlung durch ein automatisiertes Abrufverfahren oder eine automatisierte Melderegisterauskunft aufgehoben. Die Meldebehörden haben somit künftig auf Antrag Auskunft über alle Fälle von Datenübermittlungen aus den Melderegistern zu geben. Bürgerinnen und Bürger können sich somit neben den zu ihrer Person im Melderegister gespeicherten Daten jetzt auch grundsätzlich umfassend über etwaige Empfänger dieser Daten informieren. Grundsätzlich abgeschafft wurde zudem die Möglichkeit der Erteilung einer Melderegisterauskunft für Zwecke der Werbung oder des Adresshandels. Eine weitere wesentliche inhaltliche Änderung hat sich bei der erweiterten Melderegisterauskunft ergeben: War bislang die Meldebehörde nach § 45 Abs. 2 Bundesmeldegesetz dazu verpflichtet, Betroffene über die Erteilung von erweiterten Melderegisterauskünften zu informieren, liegt diese Pflicht nunmehr wegen Art. 14 DSGVO beim Empfänger der Auskunft.

Aufweichung der Pflicht zur Benennung von Datenschutzbeauftragten

Ich bedauere die Aufweichung der Pflicht zur Benennung von Datenschutzbeauftragten. Nunmehr benennen die Verantwortlichen und die Auftragsverarbeiter einen Datenschutzbeauftragten nicht mehr ab zehn, sondern erst, wenn sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Meine Position und die Position der DSK diesbezüglich waren im Gesetzgebungsverfahren eindeutig. Die Datenschutzbeauftragten sorgen – bei überschaubaren Aufwand für das Unternehmen – für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Diese in Deutschland seit den 1970er Jahren bestehende Regelung hat sich ganz besonders bei der Umstellung auf die DSGVO bewährt.

Fehlende Anpassung des Telekommunikationsgesetzes

Das Omnibusgesetz enthält keine Anpassung der datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG) an die DSGVO. Deutschland ist dieser europarechtlichen Verpflichtung bislang nicht nachgekommen. Dadurch, dass die telekommunikationsgesetzlichen Datenschutzvorschriften im bisherigen Umfang formal weiterbestehen, ist vielmehr nicht immer klar ersichtlich, welche datenschutzrechtlichen Bestimmungen – diejenigen der DSGVO oder diejenigen des TKG – auf einen bestimmten telekommunikationsrechtlichen Sachverhalt anzuwenden sind und inwieweit das TKG vom grundsätzlichen Anwendungsvorrang der DSGVO erfasst wird. Dies führt bei den Betroffenen zu erheblicher Rechtsunsicherheit (vgl. 5.2.).

Fehlende Regelungen hinsichtlich der gesetzlichen Krankenkassen

Im Bereich der gesetzlichen Krankenkassen fehlt es an einer klarstellenden Regelung zur Wirkung der Einwilligung im Verhältnis der Versicherten zur gesetzlichen Krankenkasse. Wie ich den zahlreichen Beschwerden von Versicherten entnehme, besteht hier eine große Unsicherheit, wie damit umzugehen ist, wenn Versicherte von Krankenkassen dazu veranlasst werden, eine Einwilligung zum Erhalt medizinischer Daten ihrer Versicherten zu erteilen, die den Krankenkassen gesetzlich nicht zustehen.

Es herrscht Uneinigkeit darüber, ob Geldbußen bei Datenschutzverstößen durch gesetzliche Krankenversicherungen verhängt werden dürfen. Ein nachvollziehbarer Grund, die sich verstärkt als Wirtschaftsunternehmen verstehenden gesetzlichen Krankenkassen hier zu privilegieren, ist nicht ersichtlich. Dies gilt besonders, da der Gesetzgeber durch das Fairer-Kassenwettbewerb-Gesetz (GKV-FKG) den Wettbewerb unter den Krankenkassen noch verstärkt. Ohne die Möglichkeit, Geldbußen bei Datenschutzverstößen zu verhängen, wird Datenschutz nicht zum gleichrangigen Faktor in der wirtschaftlichen Betrachtung von Prozessen der gesetzlichen Krankenkassen.

Querverweis:

5.2. Anpassung des Telekommunikationsgesetzes steht aus

5.2 Anpassung des Telekommunikationsgesetzes steht aus

Aufgrund des Anwendungsvorrangs der DSGVO sind Teile der telekommunikationsgesetzlichen Datenschutzvorschriften unanwendbar, obwohl sie immer noch im Telekommunikationsgesetz (TKG) stehen. Die fehlende Gesetzesanpassung führt zu Rechtsunsicherheit aller Beteiligten. Bereits in meinem letzten Tätigkeitsbericht habe ich dazu Stellung genommen (27. TB Nr. 15.1.1.) und mehrfach bei den politisch Verantwortlichen den Handlungsbedarf aufgezeigt.

Reformbedürftig ist auch die aktuelle Zuständigkeitsverteilung zwischen der Bundesnetzagentur (BNetzA) und mir. Nach aktueller Rechtslage verfüge ich über keine Befugnisse zur Durchsetzung der Datenschutzvorschriften des TKG. Vielmehr bin ich gehalten, meine Beanstandungen an die BNetzA zu übermitteln. Diese Regelung steht aus meiner Sicht nicht im Einklang mit dem Europäischen Primärrecht. Die Einhaltung der Vorschriften über den Datenschutz muss von unabhängigen Behörden überwacht werden (Art. 8 Abs. 3 GRCh und Art. 16 Abs. 2 Satz 2 AEUV). Die BNetzA, die zum Geschäftsbereich des Bundesministeriums für Wirtschaft und Energie gehört und damit weisungsgebunden ist, erfüllt diese Anforderungen nicht. Diese Rechtslage führt dazu, dass die Durchsetzung des Datenschutzrechts im Bereich des TKG weitgehend losgelöst von der Tätigkeit von Datenschutzaufsichtsbehörden z. B. im Rahmen des EDSA stattfindet.

Die mehrfach geforderten und notwendigen Reformen sind bis jetzt ausgeblieben.

Bedauerlicherweise sind auch keine nennenswerten Fortschritte bei der Überarbeitung des Europäischen Rechtsrahmens für die elektronische Kommunikation zu verzeichnen. Über den Prozess der Überarbeitung der E-Privacy-Richtlinie, die durch eine – in den Mitgliedstaaten unmittelbar anwendbare – E-Privacy-Verordnung ersetzt werden soll, habe ich bereits ausführlich berichtet (vgl. 26. TB Nr. 17.2.4.1; 27. TB Nr. 15.1.2). Die Europäische Kommission hat am 10. Januar 2017 den Entwurf einer E-Privacy-Verordnung beschlossen. Der Berichtsentwurf des federführenden LIBE-Ausschusses des Europäischen Parlaments wurde am 26. Oktober 2017 vom Plenum angenommen. Für die notwendigen Trilogverhandlungen bedarf es noch einer allgemeinen Ausrichtung des Ministerrates. Im Rat wird seit Mitte Januar 2017 über das Dossier beraten, bislang ohne Erfolg.

Die in meinem letzten Tätigkeitsbericht kritisierte stufenweise Aufweichung der Vorschriften der E-Privacy-Verordnung zu Lasten des Datenschutzes (27. TB Nr. 15.1.2) setzt sich in der aktuellen Diskussion fort. Aus Sicht des Datenschutzes ist bei der Festlegung der Befugnisse der Kommunikationsdiensteanbieter zur Verarbeitung elektronischer Kommunikationsdaten Zurückhaltung geboten. Die Zwecke der Verarbeitung müssen klar und abschließend geregelt werden.

Bis zum 21. Dezember 2020 ist die Richtlinie (EU) 2018/1972 („Kodex“) in nationales Recht umzusetzen. Vor dem Hintergrund des Urteils des EuGH vom 13.06.19

(C-193/18) kommt dieser Richtlinie für das TKG große Bedeutung zu. Denn der EuGH hat entschieden, dass ein internetbasierter E-Mail-Dienst wie Gmail kein Telekommunikationsdienst i. S. d. TKG ist. Zumindest vorübergehend fallen diese Dienste damit aus dem Anwendungsbereich des TKG heraus. Der „Kodex" wird hier zu einer Klarstellung führen und den neuen Begriff der „interpersonellen Kommunikationsdienste" einführen. Ich empfehle nachdrücklich, dass der Gesetzgeber diese Anpassung fristgerecht vornimmt.

Im Rahmen der Diskussion zur Sicherheit von 5G-Mobilfunknetzen wurde eine Überarbeitung des Katalogs von Sicherheitsanforderungen nach § 109 TKG beschlossen, der von der BNetzA im Einvernehmen mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) und dem BfDI erstellt wird. Dabei geht es nicht nur um die Wahrung des Fernmeldegeheimnisses, sondern auch um eine sichere Verfügbarkeit der Netze. In dem aktuellen Entwurf werden z. B. eine Zertifizierung von kritischen Komponenten und Verpflichtungen der Bezugsquelle, also dem Lieferanten, gefordert. Dies ist zwar zu begrüßen, jedoch muss sich die Praktikabilität noch erweisen. Eine Zertifizierung von hochkomplexen Komponenten, die häufig aktualisiert werden müssen, ist natürlich alles andere als trivial. Eine weitere Anforderung ist ein Monitoring im Netz. Dies halte ich für ein zweischneidiges Schwert. Einerseits erfordert dies eine Monitoring-Infrastruktur, die – allerdings nur zur Erkennung von Störungen – den Verkehr teilweise überwachbar macht, andererseits würde ein Verzicht auf ein Monitoring den Anbieter blind für Angriffe in seinem Netz machen. Hier sind die rechtlichen Anforderungen aus § 100 Abs. 1 und 2 TKG zu berücksichtigen. In weiteren Bereichen sehe ich deutliche Verbesserungen, wie beispielsweise die Vorgabe, dass die Daten bei Voice over IP verschlüsselt übertragen werden. Diese Regelung war m. E. längst überfällig. Eine vergleichbare Forderung für E-Mail-Dienste ist jedoch nicht vorgesehen, da es sich nach aktueller Rechtslage nicht um Telekommunikation handelt.

Ich empfehle, das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) an die DSGVO anzupassen.

5.3 Sicherheitsgesetzgebung

Gerade im Sicherheitsbereich gehen gesetzgeberische Vorhaben in der Regel mit Eingriffen in die Rechte von Bürgerinnen und Bürgern einher. Hier sollte allgemein evaluiert werden, welche Kompetenzen tatsächlich noch benötigt werden.

Wie schon in den letzten Jahren wurden auch in diesem Berichtszeitraum erneut viele Gesetze auf den Weg gebracht, die den Sicherheitsbehörden weitergehende Eingriffsbefugnisse einräumen. Dieser Trend wird allerdings nicht von einer parallelen Evaluierung der bereits bestehenden Kompetenzen der Behörden begleitet.

Gerade vor dem Hintergrund der bereits 2010 vom Bundesverfassungsgericht thematisierten sogenannten Überwachungsgesamtrechnung, sehe ich diese konstante Akkumulation sicherheitsbehördlicher Eingriffsmöglichkeiten äußerst kritisch. Deshalb appelliere ich auch an die am Gesetzgebungsprozess Beteiligten, ein Sicherheitsgesetzmoratorium auszusprechen.

Hiernach sollten vor der Einführung weiterer sicherheitsbehördlicher Kompetenzen zunächst in einer Bestandsaufnahme überprüft werden, welche bereits bestehenden Befugnisse überhaupt noch benötigt werden. Meine Erfahrungen aus Kontroll- und Informationsbesuchen legen nahe, dass bei weitem nicht sämtliche Möglichkeiten zur Verarbeitung personenbezogener Daten auch so genutzt werden, dass ihr Wegfall ein erhebliches Defizit bei der Arbeit der Sicherheitsbehörden darstellen würde (vgl. 6.7.1). Losgelöst von der datenschutzrechtlichen Betrachtung würde ein entsprechender Evaluierungsprozess auch das Vertrauen der Bevölkerung dahingehend stärken, dass der Gesetzgeber tatsächlich bestmöglich sicherstellt, die Eingriffsmöglichkeiten in ihre Grundrechte so weit wie nötig aber gleichzeitig auch so restriktiv wie möglich auszugestalten.

Ich empfehle, ein Sicherheitsgesetzmoratorium auszusprechen und einen Evaluationsprozess der sicherheitsbehördlichen Eingriffskompetenzen einzuleiten, um mögliche Vollzugsdefizite zu identifizieren.

5.3.1 Zollfahndungsdienstgesetz

Bereits in meinem 27. TB (Nr. 9.1.4) habe ich über die Novellierung des Zollfahndungsdienstgesetzes (ZFdG) und über meine im Rahmen des Abstimmungsprozesses aufgeworfenen datenschutzrechtlichen Bedenken im Einzelnen berichtet. Das vom Deutschen Bundestag mittlerweile beschlossene Gesetz soll die Vorgaben der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) und die Grundsatzentscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz umsetzen.

Das Gesetz sieht neue Eingriffsbefugnisse für die Behörden der Zollfahndung, insbesondere im Bereich der Gefahrenabwehr vor, und entspricht damit der aktuellen politischen Tendenz, den Sicherheitsbehörden immer weitere Befugnisse einzuräumen. Konnte sich die Zollfahndung bisher lediglich im Bereich der Strafverfolgung eines verdeckten Ermittlers bedienen, so ist dies künftig auch im Gefahrenabwehrbereich möglich.

Gleichzeitig wird der Zollfahndung die Befugnis zur Identifizierung und Lokalisierung von Mobilfunkkarten und Telekommunikationsendgeräten, bspw. durch IMSI-Catcher oder WLAN-Catcher, im Rahmen der Gefahrenabwehr eingeräumt. Neu ist auch eine spezielle Rechtsgrundlage für die sogenannte Quellen-Telekommunikationsüberwachung. Diese ermöglicht es dem Zollkriminalamt künftig auch Kommunikation zu erfassen, bevor diese verschlüsselt wird oder nachdem diese entschlüsselt wurde.

Durch das neue ZFdG werden mir umfangreiche neue Pflichtkontrollen auferlegt, die mindestens alle zwei Jahre durchgeführt werden müssen. Dies gilt sowohl für die besonders eingriffsintensiven heimlichen Ermittlungsmaßnahmen als auch für Datenübermittlungen und allgemein für Zugriffe auf personenbezogene Daten im Zollfahndungsinformationssystem. Gerade bei den Eingriffsmaßnahmen, die ohne Wissen der betroffenen Person erfolgen, haben entsprechende Kontrollen eine wichtige Kompensationsfunktion. Für die Wahrnehmung dieser neuen Aufgaben entsteht für mich ein erheblicher personeller Mehraufwand. Der Gesetzgeber ist meiner Forderung nach einer personellen Stärkung meiner Behörde mit dem Bundeshaushalt 2020 nachgekommen.

5.3.2 Strafprozessordnung

In der jüngeren Vergangenheit hat die Bundesregierung in kurzen Abständen immer wieder Gesetzentwürfe vorgelegt, die auch die Strafprozessordnung (StPO) betrafen. Dabei tangierten die Entwürfe immer auch datenschutzrechtliche Fragestellungen. Es stellt sich daher die Frage, welchem durchgängigen Konzept diese Gesetzgebungstätigkeit folgt. Teilweise werden sogar Vorschriften geändert, die erst vor kurzem überarbeitet worden waren.

Beispielhaft möchte ich den Entwurf für ein „Gesetz zur Modernisierung des Strafverfahrens“ nennen. Was nach einem großen Wurf klingt, ist in Wirklichkeit nur eine Sammlung von Einzeländerungen, die die Strafverfolgung beschleunigen sollen, aber unter anderem den Datenschutz schwächen. Abzulehnen sind insbesondere die Vorschläge, mit denen der Gesetzgeber die DNA-Analyse erweitern will. Danach soll den Ermittlungsbehörden erlaubt werden, aus den DNA-Proben zusätzlich Feststellungen über Augen-, Haar- und Hautfarbe sowie das biologische Alter der Person zu analysieren. Damit sind erstmals Analysen im sogenannten codierenden Bereich der DNA zulässig. Den codierenden Teil auszuwerten, stellt aber einen Eingriff in den Kernbereich der Persönlichkeit dar. Da dieser durch die Menschenwürdegarantie geschützt und damit unantastbar ist, hat das Bundesverfassungsgericht nur Zugriffe auf den nicht-codierenden Teil erlaubt. Zudem ist zweifelhaft, ob die neuen Analysemöglichkeiten den Ermittlern wirklich helfen, Straftaten aufzuklären. Der Wert des Ermittlungsinstruments darf nämlich nicht überbewertet werden. Nach dem derzeitigen Stand der Technik kann die Analyse die im Entwurf angegebenen Eigenschaften niemals sicher individualspezifisch bestimmen. Vielmehr sind nur Wahrscheinlichkeitsaussagen möglich. Und die sind bei weitem nicht so hoch, wie der Gesetzesentwurf suggeriert. So besteht Einigkeit, dass zum Beispiel Mischfarben unzuverlässig vorausgesagt werden (z. B. mittelbraune Haare, leicht dunklerer Teint, grüne Augen). Solche Vorhersagen bieten im Ermittlungsverfahren daher nicht den versprochenen Nutzen. Sie bergen vielmehr das Risiko, sich zu früh auf eine möglicherweise falsche Ermittlungsrichtung festzulegen. Welche Auswirkungen die Analyse des codierenden Bereiches haben wird, ist nicht absehbar. Mit dem Zugriff darauf wird ggf. die „Büchse der Pandora“ geöffnet. Zu befürchten ist, dass die Erwartungen wachsen werden, mit Fortentwicklung des wissenschaftlichen Standards in Zukunft auf weitere Erkenntnisse, wie z. B. Erbkrankheiten, Charaktereigenschaften oder – vermeintlich – genetisch veranlagte kriminelle Neigungen zugreifen zu können.

5.3.3 Darknet

Der Bundesrat hat einen Entwurf zur Verfolgung von Straftaten im „Darknet“ vorgelegt, der offenbar rechtspolitisches Gehör gefunden hat, aber noch nicht verabschiedet worden ist. Er richtet sich nicht nur gegen illegale Handelsplätze, sondern erfasst mit seinem unklaren Wortlaut auch legales Verhalten.

Anonymisierung und Verschlüsselung gehören zum Kern datenschutzfreundlicher Technikgestaltung. Schon deshalb sind an dieser Stelle zu weit formulierte Straftatbestände abzulehnen, die diese Datenschutzgrundsätze konterkarieren.

Die von dem Gesetzentwurf als strafrechtlich relevant beschriebenen Internetangebote müssen nicht nur darauf gerichtet sein, Straftaten „zu begehen“, sondern lediglich darauf, „die Begehung zu fördern oder zu ermöglichen“. Es genügt, wenn der Anbieter ein Umfeld schafft, in dem solche Straftaten naheliegen, der Zweck des Angebots selbst muss nicht die Begehung einer Straftat sein. Diese Unterscheidung könnte sich als entscheidende Weichenstellung erweisen. Damit könnten bei extensiver Auslegung alle Angebote erfasst werden, die Internetverkehre anonymisieren oder die einen passwortgeschützten und verschlüsselten Austausch ermöglichen (z. B. soziale Netzwerke). Denn niemals ist es ausgeschlossen, dass solche Angebote für kriminelle Aktivitäten genutzt werden.

Mit dem Strafrecht sollte nur tatsächlich strafwürdiges Handeln sanktioniert werden. Daher muss der Gesetzgeber präzise umschreiben, welches Verhalten er mit einer Strafrechtsnorm konkret erfassen möchte. Der vorliegende Vorschlag tut dies in meinen Augen nicht in hinreichendem Maße. Die Gesetzesbegründung sagt dazu, man wolle so Beweisprobleme lösen. Es ist fraglich, ob dies ein geeigneter Ansatz ist. An den unpräzisen und weit formulierten Tatbestand knüpfen Ermittlungsbefugnisse an, für die ein Anfangsverdacht genügen wird. Damit wird die Zahl derjenigen zunehmen, die unschuldig in das Visier von Ermittlungen geraten.

Schon in seiner Einleitung setzt der Gesetzentwurf das „Tor"-Netzwerk pauschal mit dem „Darkweb" gleich. Dies ist eine unzutreffende Annahme, weil der Tor-Browser auch genutzt wird, um datenschutzfreundlich im „normalen" Web zu surfen. Darüber hinaus ist dieses Netzwerk unentbehrlich für politisch Verfolgte, Journalisten oder Whistleblower in vielen Ländern. Dafür, den Tor-Browser für das „normale Surfen" zu benutzen, gibt es gute und legitime Gründe. So ist es praktisch nur damit möglich, das Internet ohne Nutzertracking zu nutzen.

5.4 Der Zensus 2021

Am 3. Dezember 2019 ist das Gesetz zur Durchführung des Zensus im Jahr 2021 (ZensG 2021) in Kraft getreten. Zukünftig soll der Zensus ohne Bürgerbefragungen und ausschließlich auf Basis bereichsübergreifenden Auswertungen einer Vielzahl von Registern durchgeführt werden. Im Detail sind die Regelungen weiterhin datenschutzrechtlich problematisch.

Seit dem Jahr 2011 ist aufgrund von EU-Vorgaben alle zehn Jahre ein Zensus durchzuführen. Der Zensus 2021 ist erneut als registergestützte Bevölkerungsbefragung angelegt. Die Ergebnisse der Zählung resultieren aus vorhandenen Informationen in Registern (z. B. der Meldebehörden), Bürgerbefragungen (z. B. im Rahmen der Gebäude- und Wohnungszählung oder der Haushaltebefragung auf Basis einer Stichprobe) sowie aus Erhebungen an Anschriften mit Sonderbereichen (Gemeinschaftsunterkünften und Wohngemeinschaften). Das Bundesverfassungsgericht hat diese Vorgehensweise in seiner Entscheidung zum ZensG 2011 am 19. September 2018 für verfassungsgemäß erachtet.

Wie bereits beim Zensus 2011, wird erneut nicht überzeugend dargelegt, warum Befragungen zu Bewohnern in Gemeinschaftsunterkünften nicht generell anonymisiert durchgeführt werden können. Den legitimen Interessen Betroffener, für die schon die Tatsache ihres Aufenthalts in einer solchen Einrichtung eine sehr sensible Information darstellt, würde auf diese Weise Rechnung getragen. Ein entsprechender Erforderlichkeitsnachweis fehlt auch für die erneut bestehende Verpflichtung, die rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft zu erheben – zumal der Gesetzgeber hiermit die EU-Vorgaben zum Zensus überschreitet.

Neu ist beim Zensus 2021 die erstmals zentral dem Statistischen Bundesamt obliegende Verwaltung des Gesamtdatenbestands. Die Zusammenarbeit des Bundesamtes mit den Landesämtern für Statistik in Bezug auf die Vorbereitung, Durchführung und Auswertung des Zensus und die Vorgaben der DSGVO bedingen insbesondere die Notwendigkeit, die datenschutzrechtlichen Verantwortlichkeiten der statistischen Ämter gesetzlich eindeutig und hinreichend trennscharf zu regeln. Dies ist u. a. für die Wahrung der Betroffenenrechte von zentraler Bedeutung. Leider ist der Gesetzgeber meinem diesbezüglichen Petitum nicht gefolgt. Auch im Lichte dessen werde ich die weiteren Vorbereitungen und die Durchführung des Zensus eng begleiten und vor allem auch die Einhaltung der Vorgaben zur Löschung nicht mehr benötigter Informationen in den Blick nehmen.

Zudem richtet sich meine Aufmerksamkeit auf die jetzt schon eingeleiteten ersten Schritte hin zu einem künftig registerbasierten Zensus, der gänzlich ohne Befragungen der Bevölkerung auskommen soll. Insbesondere die hierfür erforderlichen Verknüpfungen von Informationen aus – bestehenden und noch neu zu errichtenden – Registern unterschiedlicher Bereiche stellen den Datenschutz vor neue Herausforderungen.

5.5 Registermodernisierung in Deutschland

Die Registermodernisierung in Deutschland ist eines der wichtigsten Projekte innerhalb der Digitalisierungsstrategie der Bundesregierung. Ein zentraler Baustein ist die Einführung eines eindeutigen Kennzeichens für jede Person. Ein solches Kennzeichen birgt aber auch erhebliche Gefahren. Deshalb stellt eine datenschutzgerechte und damit verfassungskonforme Lösung eine enorme Herausforderung dar.

Ich habe mich bereits in meinem letzten Tätigkeitsbericht zur Registermodernisierung geäußert (s. 27. TB Nr. 9.2.2). Im Jahr 2017 veröffentlichte der Nationale Normenkontrollrat ein Gutachten, das die Vorteile und die Machbarkeit einer Modernisierung untersuchen ließ. Der aktuelle Koalitionsvertrag griff das Projekt erneut auf. Die Parteien kamen überein, dass eine Umstrukturierung und Vernetzung der Registerlandschaft in Deutschland mithilfe eindeutiger, registerübergreifender Identifikatoren ermöglicht werden soll. Aus Sicht der Bundesregierung sei ein Personenkennzeichen die

nächstliegende Form eines solchen Identifikators. Derartige Kennzeichen sind in der Regel als Nummer oder als Kombination aus Ziffern und Buchstaben ausgestaltet.

Die Idee eines Personenkennzeichens ist nicht neu. Viele Staaten wie Schweden, Dänemark oder Estland nutzen einen eineindeutigen Identifikator. Auch die Bundesregierung plante bereits in den 1970er Jahren die Einführung eines solchen Systems. Im wegweisenden Volkszählungsurteil von 1983 (Az. 1 BvR 209/83) machte das Bundesverfassungsgericht allerdings deutlich, dass die Einführung eines Personenkennzeichens ein unüberschaubares Risiko darstellt, den Bürger in seiner ganzen Persönlichkeit erfassen und katalogisieren zu können. Das Verfassungsgericht nannte das Kennzeichen ausdrücklich als Negativbeispiel.

Schon die Einführung eines Personenkennzeichens stellt ein erhöhtes Risiko der Zusammenführung aller Informationen zu einer Person auf staatlicher Seite dar. Der Eingriff in das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger ist schon zum Zeitpunkt der Bereitstellung erfolgt. Eine tatsächliche Nutzung des Personenkennzeichens verschärft den Eingriff nur noch. Es muss daher geprüft werden, ob ein eindeutiger Identifikator überhaupt verfassungsgemäß umgesetzt werden kann.

Obwohl die Umsetzung politisch und datenschutzrechtlich eine enorme Herausforderung darstellt, haben sich mehrere Regierungsebenen des Projektes angenommen. Nach verschiedenen Beschlüssen der Innenministerkonferenz und des IT-Planungsrates bis Mitte 2019, wurde dem Bundesministerium des Innern, für Bau und Heimat (BMI) die Aufgabe übertragen, mehrere Gesetzesentwürfe auszuarbeiten. Dabei geht es sowohl um die Einführung eines eineindeutigen Identifikators, als auch um die Nutzung eines solchen für digitalisierte Verwaltungsleistungen. Ein Anwendungsfall könnte beispielsweise das bereits im Aufbau befindliche Projekt „Erleichterte Leistungen für Eltern“ (ELFE) sein. Die Bürgerinnen und Bürger sollen Identität oder Einkommen nicht mehr einzeln nachweisen müssen. Stattdessen soll es einen Abruf in den entsprechenden Datenregistern der Verwaltung geben. Die richtige Person soll dabei über ebenjenen eineindeutigen Identifikator gefunden werden.

Das BMI suchte für die verschiedenen Workshops, Arbeits- und Expertengruppen früh die Beratung durch die Datenschutzaufsichtsbehörden des Bundes und der Länder. Diesen Schritt begrüße ich ausdrücklich, gerade aufgrund der Bedeutung und der datenschutzrechtlichen Komplexität des Themas. In diesen Gremien zeigte sich allerdings zu meinem Bedauern früh eine Präferenz der Regierung für den Einsatz der Steueridentifikationsnummer (Steuer-ID) und des damit verknüpften Stammdatensatzes.

Diesen Plan halte ich für problematisch und bedenklich. Die Nutzung der Steuer-ID wäre genau die Lösung, die das Verfassungsgericht 1983 ausdrücklich kritisiert hatte. Aus diesem Grund hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im September 2019 eine Entschließung veröffentlicht, in der ein derart einheitliches Kennzeichen abgelehnt wird.

Deswegen bleibt die Frage offen, ob überhaupt eine Form des Personenkennzeichens verfassungsrechtlich zulässig sein kann. Dies kann nur in einem System möglich sein, das das Risiko einer Katalogisierung vermindert oder unterbindet. Ein derartiges System muss die Beteiligung des Bürgers gewährleisten, umfassende Transparenz über alle staatlichen Datenübermittlungen schaffen und strukturelle Hemmnisse beinhalten, die das Risiko einer übermäßigen Zusammenführung von vornherein mindern. Derartige Hemmnisse müssen sich dabei sowohl auf die bereichsübergreifende Identifikation als auch für den darauf basierenden Datenaustausch beziehen. Natürlich ohne den ursprünglichen Zweck eines verbesserten, digitalen Datenaustauschs zwischen den Behörden zu gefährden.

Eine mögliche Lösung wäre die Verwendung von bereichsspezifischen oder auf andere Weise beschränkten Kennzeichen. Dies ist der Weg, für den sich auch die DSK ausspricht. Ein sektorspezifischer Identifikator hätte aus datenschutzrechtlicher Sicht weitere Vorteile. Wenn ein eineindeutiger Identifikator in die falschen Hände gelangt, hätten Unbefugte einen wesentlich leichteren Zugriff auf sämtliche Bereiche der betroffenen Person. Mit einem sektorspezifischen Identifikator wäre dagegen nur ein einzelner Bereich betroffen. Die Folgen eines Datenverlustes hätten zumindest Grenzen.

Dies alleine reicht allerdings nicht aus. Die angeführte umfassende Transparenz des Systems dient dazu, die ungleichen Machtverhältnissen zwischen Bürger und Staat auszugleichen. Die Betroffenen, welche die im Hintergrund laufenden Verarbeitungen der Daten nicht durchdringen können, wären gegenüber einem undurchsichtig handelnden Staat im Nachteil. Es wäre unklar, welche Daten der Staat bereits erhoben hätte und wann welche Stelle darauf zugegriffen hat. Eine Realität, die im normalen Verwaltungsalltag sicherlich zutrifft. Dies gilt heute noch genauso wie 1983. Insofern hat das Urteil nicht an Aktualität verloren.

Um eine verfassungsgemäße Form eines eineindeutigen Identifikators zu finden, muss dieses Machtgefälle durchbrochen werden. Aus Sicht der Datenschutzaufsichtsbehörden sind dabei einige Mittel von besonderer Bedeutung. Für alle Betroffenen bedarf es der Herstellung einer größtmöglichen Transparenz hinsichtlich der über sie existierenden Datenflüsse. Nur dieses Wissen

versetzt sie in die Lage, ihre Rechte effektiv nutzen zu können. Auch die Daten, die bei den Behörden gespeichert sind, sollten leicht und unkompliziert abrufbar sein. Die einzelnen Personen müssten zudem vor Beginn des Datenaustauschs beteiligt werden.

Ich empfehle, bei der Registermodernisierung, statt auf eine einheitliche Personenkennziffer auf mehrere bereichsspezifische Identifikatoren zurückzugreifen.

5.6 Gesetzgebung im Gesundheits- und Sozialwesen

Im Berichtszeitraum war das Bundesministerium für Gesundheit (BMG) bei der Erarbeitung von Gesetzentwürfen besonders aktiv. Die vorgelegten 23 Gesetzentwürfe waren zum Teil sehr umfangreich und damit beratungsintensiv.

Eine Vorbemerkung: Wie auch andere Ressorts missachtet das BMG zunehmend die Vorgaben der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO), in der die Zusammenarbeit unter anderem mit mir bei der Erstellung von Gesetzentwürfen geregelt ist. Dies ist angesichts der Vielzahl von Gesetzentwürfen und der besonderen datenschutzrechtlichen Fragestellungen besonders misslich.

Von besonderer Bedeutung waren im Berichtszeitraum die Gesetzgebung zum Digitale-Versorgung-Gesetz, zum Implantateregistergesetz und zum Masernschutzgesetz.

Gesundheits-Apps auf Rezept und Novellierung von Forschungsregelungen durch das Digitale-Versorgung-Gesetz (DVG)

Öffentliche Aufmerksamkeit erregte insbesondere die mit dem DVG vorgenommene Novellierung der Regelung über das sogenannte Datentransparenzregister, dessen ursprüngliche Regelungen bereits durch das GKV-Modernisierungsgesetz vom 30.11.2003 (BGBl. I S. 2190) geschaffen und durch das GKV-Versorgungsstrukturgesetz vom 22.12.2011 (BGBl. I S. 2983) erstmals grundlegend überarbeitet worden waren. Nach Erlass der Datentransparenzverordnung vom 10.9.2012 (BGBl. I S. 1895) war beim Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) in der Folgezeit bereits die entsprechende Datenbank unter der Bezeichnung Informationssystem Versorgungsdaten aufgebaut worden (vgl. meinen 24. TB, Tz. 11.1.3 S. 141 f.). Mit dem DVG wurde der Meldeweg geändert und die Anzahl der Daten, die für Forschungszwecke in der Datenbank gespeichert werden, erhöht. Erfreulich ist, dass die Daten nunmehr nicht, wie ursprünglich geplant, mit dem unveränderbaren Teil der Krankenkassennummer übermittelt werden sollen. Vielmehr werden die Datensätze nunmehr vor der Absendung bei der gesetzlichen Krankenkasse mit einem sog. Lieferpseudonym versehen, das in der Vertrauensstelle dann noch einmal in ein endgültiges Pseudonym umgewandelt wird. Hierdurch soll die Re-Identifizierung der sensiblen Daten erschwert werden. Aufgrund der neuen Regelungen werden die Daten nunmehr parallel sowohl an das Bundesversicherungsamt (seit dem 1. Januar 2020: Bundesamt für soziale Sicherung) für Zwecke des Risikostrukturausgleiches als auch an das Forschungsdatenzentrum übermittelt. Dies wird dazu führen, dass die Daten deutlich aktueller sein werden. Bisher waren die Daten, die einem unveränderten Kreis an Zugangsberechtigten zur Verfügung gestellt werden können, in der Regel vier Jahre alt. Auch wenn sich die gesetzliche Regelung insoweit nicht geändert hat, gehe ich davon aus, dass aufgrund des gesetzlich vorgesehenen Ausbaus zu einem Forschungsdatenzentrum das BMG nunmehr eine gesonderte Vertrauensstelle bestimmt. Die bisherige Sonderregelung, wonach die Vertrauensstelle sowie die datenhaltende Stelle das DIMDI waren, war aufgrund der besonderen Umstände als absolute Ausnahmeregelung mit meinem Haus abgestimmt. Durch das DVG wurden zwar die Möglichkeiten zur Datennutzung durch die Forschung erweitert. Zusätzliche datenschutzrechtliche Sicherheiten wurden im Gegenzug durch weitere Zugangsvoraussetzungen und eine ausdrückliche Strafbewehrung in § 307b SGB V sowie die Möglichkeit des Ausschlusses vom Datenzugang in § 303e Absatz 6 SGB V geschaffen.

Geschäftsgrundlage während der Gesetzgebung zum DVG war die bisherige Datenhaltung durch das DIMDI, das künftig als Forschungsdatenzentrum die Daten auch über Gastwissenschaftsarbeitsplätze für die Forschung bereitstellen sollte. Derartige Forschungsdatenzentren sind im Wissenschaftsbereich durchaus üblich und in aller Regel datenschutzgerecht ausgerichtet. Umso überraschender war, dass das BMG nur zwei Wochen nach dem Gesetzesbeschluss zum DVG mit Wirkung zum 2. Januar 2020 durch Erlass verfügte, dass das DIMDI aufzulösen und dessen Aufgaben, und damit auch die Datenbank, an das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zu übertragen. Nicht nur dieses Vorgehen begegnet erheblichen verfahrensrechtlichen Bedenken. Aus datenschutzrechtlicher Sicht ist besonders kritisch, dass die Datenbank mit hochsensiblen Daten auf das BfArM übertragen werden soll, das nach § 303e Absatz 1 Nr. 16 SGB V selbst Nutzungsberechtigter der Datenbank ist und nach § 303e Absatz 3 SGB V nur über einen Antrag Zugang zu den sensiblen Gesundheitsdaten erhält, den es nun selbst zu prüfen hätte.

Im Rahmen der Ausübung meiner Aufsichtsbefugnisse habe ich daraufhin gegenüber dem DIMDI und dem BfArM angekündigt, nach § 16 Absatz 1 BDSG i. V. m. Art. 58 Absatz 2 lit. d) DSGVO die Nutzung der

Forschungsdatenbank zu untersagen, soweit mir nicht eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vorgelegt wird, aus der hervorgeht, wie man die Rechte und Freiheiten der Versicherten schützen möchte. Hierauf hat das BMG insoweit kurzfristig reagiert und per Erlass relevante Teile des Auflösungserlasses einstweilen ausgesetzt sowie die Bereitstellung von Daten an Nutzungsberechtigte untersagt.

Erfolgreich konnte ich mich gegen ein trägerübergreifendes Versichertenverzeichnis wenden. Eine dadurch mögliche direkte Weiterleitung oder Verlinkung auf das Verwaltungsportal der tatsächlich zuständigen Kranken- oder Pflegekasse ist zwar ein bequemer Service für den versicherten Nutzer, die datenschutzrechtliche Bewertung einer solchen umfassenden Datensammlung ergibt jedoch sowohl einen Widerspruch zu dem Grundsatz der Datenminimierung im Sinne des Art. 5 Absatz 1 lit. c) DSGVO als auch zum Grundsatz der Erforderlichkeit im Sinne des Art. 6 Absatz 1 DSGVO.

Das DVG sieht zudem vor, dass Gesundheits-Apps nun durch Ärzte verschrieben oder durch Krankenkassen genehmigt werden können, was zu einer Kostenerstattung durch die gesetzlichen Krankenkassen führt. Leider wurden viele meiner Anregungen für eine datenschutzgerechte Ausgestaltung dieses gänzlich neuartigen Konstrukts nicht aufgenommen. Ich hatte darauf gedrungen, sicherzustellen, dass die Gesundheits-Apps den Nutzern ausschließlich in der Telematikinfrastruktur und ohne Beteiligung von „App-Stores“ zur Verfügung gestellt werden und dass die Hersteller oder andere Dritte außerhalb des Gesundheitswesens keine sensiblen Gesundheitsdaten über die App-Nutzer erhalten sowie kein Tracking stattfindet. Zudem hätten die an digitale Gesundheitsanwendungen zu stellenden Datenschutz- und Datensicherheitsanforderungen im Gesetz konkret festgelegt werden sollen. Wenigstens konnte ich erreichen, dass bei der Zulassung auch geprüft wird, ob die Anwendung den Anforderungen an den Datenschutz entspricht und die Datensicherheit nach dem Stand der Technik gewährleistet ist. Unbeschadet dessen sollten zumindest im Wege der nach dem DVG vorgesehenen Verordnung, die erforderlichen Konkretisierungen hinsichtlich des Genehmigungsverfahrens durch die Krankenkassen und hinsichtlich der datenschutzrechtlichen Verantwortlichkeit i. S. d. DSGVO vorgenommen werden. Insbesondere die Festlegung der datenschutzrechtlichen Verantwortung bei von Ärzten verschriebenen bzw. von Krankenkassen genehmigten digitalen Anwendungen ist wichtig. Hieran knüpft die Klarstellung an, gegenüber wem die datenschutzrechtlichen Betroffenenrechte geltend zu machen sind und wer im Einzelfall die erforderliche Datenschutz-Folgenabschätzung (Art. 35 DSGVO) durchzuführen hat.

Erfassung bestimmter Implantate durch das Implantateregistergesetz

Durch das Implantateregister-Errichtungsgesetz werden die bisher bei medizinischen Fachgesellschaften geführten Spezialimplantateregister zusammengeführt. Es ist das erste Gesundheitsregister, das auf einer bundesweit geltenden Meldepflicht beruht (s. 4.2.2).

Masernschutzgesetz

Durch das „Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention“ (Masernschutzgesetz) wurden die in Einrichtungen wie z. B. Kindergärten oder Schulen Beschäftigten (Erzieher, Lehrer, Tagespflegepersonen und medizinisches Personal [soweit diese Personen nach 1970 geboren sind]) verpflichtet, vor der Aufnahme oder vor Beginn einer Tätigkeit einen „Nachweis […] darüber zu erbringen, dass bei ihnen ein Impfschutz gegen Masern besteht, […] oder eine ärztliche Bescheinigung“ vorzulegen, „die bestätigt, dass eine Immunität gegen Masern oder dass eine gesundheitliche Kontraindikation gegen eine Schutzimpfung gegen Masern vorliegt“. Gleiches gilt für Kinder ab dem vollendeten ersten Lebensjahr beim Eintritt in die Schule oder den Kindergarten. Hier konnte ich immerhin erreichen, dass neben dem Impfpass zum Nachweis der Impfung gegen Masern auch eine einfache Bescheinigung eines Arztes über die Immunität gegen Masern ausreicht. Es ist nicht nachvollziehbar, in jedem Fall gegenüber den Leitungen von Kindergärten und Schulen alle Impfungen zu offenbaren, wenn sie für den Kindergarten- oder Schulbesuch völlig irrelevant sind.

MDK-Reformgesetz

Mit dem „Gesetz für bessere und unabhängigere Prüfungen (MDK-Reformgesetz)“ wird die Organisation der Medizinischen Dienste der Krankenkassen einheitlich und eigenständig strukturiert. Die Medizinischen Dienste unterstützen die gesetzlichen Krankenversicherungen u. a. bei der Entscheidung über die Gewährung von Leistungen, wenn dabei medizinische Sachverhalte bewertet werden müssen. Die Stärkung der Unabhängigkeit der Medizinischen Dienste begrüße ich. Zahlreichen Eingaben lagen eine unklare Aufgabenabgrenzung von Krankenkasse und Medizinischem Dienst der Krankenkassen und daraus folgend unzulässige Datenverarbeitungsvorgänge zugrunde. Hier dürfte die neue Struktur für mehr Sicherheit in der konkreten Fallbearbeitung auch bezüglich der Datenschutzbelange sorgen.

Ebenso begrüße ich meine vorgesehene Beteiligung beim Erlass von Richtlinien durch den neu einzurichtenden Medizinischen Dienst Bund, zumal dies dem Verfahren beim Fassen von Beschlüssen des Gemeinsamen Bundesausschusses entspricht.

Querverweis:

4.2.2 Das Implantateregister

6 Sicherheitsbereich

6.1 Grenzüberschreitender sicherheitsbehördlicher Datenzugriff

Mit dem CLOUD Act, der e-Evidence Verordnung und der Cyber-Crime Convention gibt es aktuell drei Verfahren, mit denen ein direkter grenzüberschreitender sicherheitsbehördlicher Datenzugriff ermöglicht werden soll. Diese Abkehr vom bisher vorherrschenden Grundsatz der internationalen Rechtshilfe wirft an mehreren Stellen datenschutzrechtliche Probleme auf.

6.1.1 CLOUD Act

Der CLOUD Act stellt sicher, dass U.S.-amerikanische Strafverfolgungsbehörden weitreichend auf Daten von Internet-Unternehmen zugreifen können, unabhängig davon, wo diese gespeichert sind. Das kann Rechtskonflikte schaffen. Denn nach der ersten Einschätzung des EDSA sind direkte Übermittlungen an U.S.-Strafverfolgungsbehörden außerhalb des Rechtshilfeweges nur sehr begrenzt mit der DSGVO vereinbar. Neue Abkommen können die Lösung sein, aber die Hürden sind hoch.

Der CLOUD Act ist im März 2018 in den USA in Kraft gesetzt worden. Mit ihm werden zwei Ziele verfolgt: Zum einen macht er Vorgaben für den Abschluss von Verwaltungsabkommen, mit denen sich die USA mit anderen Staaten bzw. der EU grundsätzlich gegenseitigen Zugriff auf personenbezogene Daten zusichern, die bei Internetprovidern im jeweils anderen Staat gespeichert sind. Die U.S.-Regierung sieht hierin vor allem ein Angebot an andere Staaten. Denn wegen der dominanten U.S.- Internetindustrie benötigen viele ausländische Strafverfolgungsbehörden gerade die dort gespeicherten Daten für ihre Ermittlungen. Zum anderen stellt der CLOUD Act aber auch klar, dass U.S.-amerikanische Strafverfolgungsbehörden weitreichend auf Daten von Internet-Unternehmen zugreifen können, die der U.S.-amerikanischen Jurisdiktion unterliegen, und zwar unabhängig davon, wo diese Daten gespeichert sind.

Besondere Brisanz liegt in diesem zweiten Aspekt. Denn eine derartige Regelung kann leicht Rechtskonflikte schaffen, wenn die ersuchten Daten zugleich dem Schutz einer anderen Rechtsordnung unterliegen, wie etwa der DSGVO. Der Europäische Datenschutzausschuss (EDSA) hat in einer ersten Einschätzung die Position vertreten, dass eine Übermittlung an die U.S.-Strafverfolgungsbehörde ausschließlich auf Grundlage des CLOUD Acts nach der DSGVO regelmäßig nicht zulässig sein dürfte. Solange keine lebenswichtigen Interessen des Betroffenen berührt werden, setze eine rechtskonforme Übermittlung bei strafrechtlichen Ermittlungen vielmehr die Einhaltung des bestehenden Rechtshilfeweges voraus.

Zugleich präsentiert der EDSA Lösungswege, wie mit entsprechenden Auskunftsersuchen künftig rechtskonfliktfrei umgegangen werden könnte. Hierfür sei insbesondere eine neue Generation von Rechtshilfeabkommen erforderlich, die eine schnellere Bearbeitung der Ersuchen und ein höheres Niveau an Datenschutz sicherstellen sollen. Ein anderer Weg könne in einem die Materie regelnden Abkommen zwischen der EU und den USA liegen, wie es gegenwärtig schon verhandelt wird. In diesem müssten allerdings hinreichende Verfahrenssicherungen und ein hohes Datenschutzniveau vereinbart werden, um einerseits die gewünschte Rechtssicherheit zu schaffen und andererseits für alle Beteiligten einen Vorteil zum Status Quo zu schaffen.

6.1.2 Die e-Evidence-Verordnung

Hinter dem Stichwort „e-Evidence“ verbirgt sich ein Verordnungsvorschlag der Europäischen Kommission, wonach europäische Strafverfolgungsbehörden Bestands, Verkehrs- und Inhaltsdaten unmittelbar bei Providern von Telekommunikations- und Internetdienstleistungen in anderen EU-Mitgliedstaaten erheben können sollen. Die Anordnungen wären auch für Provider aus Drittstaaten verbindlich, sofern sie ihre Dienste in der EU anbieten.

Bereits in meinem letzten Tätigkeitsbericht habe ich die fehlende Einbeziehung von Justizbehörden zumindest des Staates, in dem der angefragte Provider seinen Sitz hat, als Hauptkritikpunkt bezeichnet (vgl. 27. TB Nr. 11.1.4). Es sollte nicht allein den Providern überlassen bleiben, die Rechtmäßigkeit einer Anordnung zu überprüfen, denn Unternehmen haben grundsätzlich andere Interessen und unterliegen anderen Verpflichtungen als Justizbehörden. Die Verantwortung der rechtlichen Prüfung und damit auch der Schutz der Betroffenen sollte – mit anderen Worten – nicht (gänzlich) von staatlichen auf private Akteure verlagert werden. Deshalb begrüße ich den Vorschlag der Berichterstatterin im Europäischen Parlament, eine zwingende parallele Unterrichtung der Justizbehörden der beteiligten Mitgliedsstaaten einzuführen.

Die e-Evidence-Verordnung sollte weiterhin das Ziel haben, auch drittstaatliche Vorschriften zu achten, wenn diese die Grundrechte in dem Drittstaat schützen und der Herausgabe der ersuchten Daten durch den Provider entgegenstehen könnten. Diese Forderung erheben die europäischen Datenschutzbehörden auch gegenüber drittstaatlichen Zugriffsregelungen auf Daten, die dem Anwendungsbereich der DSGVO unterliegen. Insofern sehe ich es kritisch, dass sich die Mitgliedstaaten dafür ausgesprochen haben, eine notwendige Vorschrift über die zwingende Konsultation einer zuständigen Stelle im betroffenen Drittstaat zu streichen.

Ein weiterer problematischer Aspekt betrifft die nur schwer mögliche Authentifizierung der ersuchenden Behörde und Personen. Denn an die Provider könnte sich eine Vielzahl von Behörden anderer Mitgliedstaaten wenden, die nach dem nationalen Recht eines Mitgliedstaates als Ermittlungsbehörde in einem Strafverfahren dazu berechtigt sind.

Die e-Evidence-Verordnung befand sich bei Redaktionsschluss noch nicht im sog. Trilogverfahren zwischen Europäischem Parlament, Europäischer Kommission und Rat. Die aufgeworfenen Fragen dürften in den nächsten Monaten allerdings in den hierfür anstehenden Verhandlungen entschieden werden.

6.1.3 Cybercrime-Konvention

Die datenschutzrechtlichen Fragen, die sich im Zusammenhang mit der sog. e-Evidence-Verordnung (vgl. oben 6.1.2) stellen, stehen auch im Zentrum der Verhandlungen eines zweiten Zusatzprotokolls zur sog. Cybercrime-Konvention.

Die Cybercrime-Konvention ist ein Vertragswerk zur Bekämpfung von Straftaten, die über das Internet und andere Computernetzwerke begangen werden, das im Rahmen des Europarates verhandelt wird. Zugleich ist es aber auch offen für Staaten, die nicht Teil des Europarates sind. Gegenwärtig haben 64 Staaten die Konvention unterzeichnet, unter ihnen beispielsweise Australien, Israel, Japan, Kanada, Senegal, Tonga, Türkei und die USA.

Die beiden aus datenschutzrechtlicher Sicht wesentlichen Vorschriften, die bei dem gegenwärtig verhandelten Zusatzprotokoll diskutiert werden, befassen sich mit dem grenzüberschreitenden Zugriff von Sicherheitsbehörden sowohl auf Nutzer- als auch auf Verkehrsdaten. Es handelt sich dabei zum einen um eine Vorschrift, die die Voraussetzungen für eine direkte grenzüberschreitende Erhebung durch Strafverfolgungsbehörden eines Signatarstaates bei Providern in einem anderen Signatarstaat regelt. Das ist datenschutzrechtlich problematisch, weil in den 64 Unterzeichnerstaaten eine Vielfalt von teilweise sehr unterschiedlichen Rechtssystemen und Datenschutzstandards existieren.

Eine weitere Vorschrift des Zusatzprotokolls soll zu einem beschleunigten Verfahren im Rahmen der klassischen Rechtshilfe zwischen Strafverfolgungsbehörden führen. Hier könnten Lösungen für ein schnelleres Rechtshilfeverfahren und ein verbessertes Datenschutzniveau entwickelt werden. Aus meiner Sicht kommt es dabei u. a. darauf an, die Datenkategorien, auf die zugriffen werden darf, eng zu begrenzen. Die Ersuchen müssten zudem von unabhängigen Behörden gestellt bzw. genehmigt werden. Schließlich sollten die Justizbehörden in den Staaten beteiligt werden, in denen die Provider sitzen, deren Daten abgefragt werden.

Eine abschließende Bewertung des Zusatzprotokolls ist mir allerdings erst dann möglich, wenn die im Rahmen der Cybercrime-Konvention verhandelten Datenschutzvorschriften veröffentlicht werden. Die Annahme der Entwürfe für das Zusatzabkommen ist gegenwärtig für Ende 2020 geplant.

Querverweis:

6.1.2 Die e-Evidence Verordnung

6.2 Pilotprojekt zur „intelligenten“ Videoüberwachung am Bahnhof Berlin-Südkreuz

Nachdem das erste Teilprojekt zur Erprobung von Gesichtserkennungssoftware abgeschlossen werden konnte, befindet sich das zweite Teilprojekt gegenwärtig in der Auswertungsphase. Sollte eine Rechtsgrundlage für die biometrische Gesichtserkennung im Polizeibereich geschaffen werden, führt dies nicht nur zu tiefgreifenden Grundrechtseingriffen, sondern bedeutet auch eine gesellschaftspolitische Richtungsentscheidung.

Im 27. TB hatte ich unter Punkt 9.3.3 bereits zum Pilotprojekt der Deutschen Bahn AG, des BMI und der Bundespolizei (BPol) berichtet. Hier ging es um das erste von zwei Teilprojekten. Die BPol hatte biometrische Gesichtserkennungssoftware von mehreren Unternehmen getestet. Daraufhin wurde ein Abschlussbericht veröffentlicht. Das Ergebnis ist nach meiner Rechtsauffassung aus mehreren Gründen äußerst bedenklich. Grundlegenden Vorbehalten begegnet bereits die Methodik des Testaufbaus und damit die Aussagekraft der Ergebnisse. Die Rate der falsch erkannten Personen ist für einen flächendeckenden Einsatz im Wirkbetrieb nach meiner Überzeugung viel zu hoch (s. https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile).

Die Analyse biometrischer Daten eines Menschen und der anschließende Abgleich mit Datenbanken greift tief in die Grundrechte der betroffenen Person ein. Eine Rechtsgrundlage für den Einsatz biometrischer Videoanalyse existiert bisher nicht. Die verfassungsrechtlichen Anforderungen an entsprechende Vorschriften sind aus guten Gründen sehr hoch.

Die Einführung der biometrischen Gesichtserkennung in den Polizeialltag ist datenschutzrechtlich und gesellschaftspolitisch eine überaus kritisch zu beurteilende Überwachungstechnologie. Digitale Überwachungskameras sind bereits allgegenwärtig. Die erforderlichen Daten sind also bereits vorhanden. Erfahrungen haben darüber hinaus gezeigt, dass vielfach zunächst vorgesehene gesetzliche Beschränkungen des Datenzugriffs im Laufe der Zeit sukzessive wegfallen. Wird die biometrische Gesichtserkennung der Polizei per Gesetz erlaubt, besteht durchaus eine reelle Gefahr, dass die Möglichkeiten zur Überwachung der Bevölkerung anhand biometrischer Merkmale nach und nach ausgeweitet werden. Diese Entwicklung berührt den Kern unseres gesellschaftlichen Zusammenlebens. Die Frage der Schaffung einer solchen Möglichkeit braucht eine breite gesellschaftliche Debatte. Biometrische Videoanalyse ist nicht bloß ein weiteres Einsatzmittel der Polizei.

Nachdem 2018 das erste Teilprojekt zur Gesichtserkennung abgeschlossen wurde, startete am 18. Juni 2019 der zweite Testteil, der inzwischen ebenfalls beendet ist. Auch hierbei wurde der Einsatz von Software zur „intelligenten“ Videoanalyse getestet. Es wurden dabei einzelne Situationen – unter anderem von Darstellern – simuliert, wie z. B. liegende Person, herrenlose Gepäckstücke, Menschenansammlungen oder das Betreten bestimmter gesperrter Bereiche. Die Software sollte die einzelnen Gefahrensituationen erkennen und diese in der Leitstelle der Deutsche Bahn AG und der BPol anzeigen. Biometrische Komponenten der Software wie Gesichtserkennung waren nach Aussage der Hersteller dabei ausgeschaltet. Die BPol und die Deutsche Bahn AG werten derzeit die angefallenen Daten und Erkenntnisse

Corona – Alarm in China

aus. Nach Mitteilung der Testergebnisse werde ich auch diese wieder eingehend bewerten.

Bei diesem Testteil konnte ich im Vorfeld beratend tätig werden und hatte dabei die Gelegenheit, im Bereich der Testaufstellung und der Information der Öffentlichkeit meine Vorstellungen einzubringen. So konnte ich erreichen, dass von der ursprünglichen Idee, an den Testtagen das ganze Bahnhofsgelände in den Test einzubeziehen, abgesehen wurde und nur in bestimmten, abgegrenzten Bereichen getestet wurde. Auch auf eine bessere Information der Öffentlichkeit durch mehr und besser platzierte Hinweisschilder konnte ich hinwirken.

Ich empfehle, auf eine Videoüberwachung mit biometrischer Gesichtserkennung im öffentlichen Raum zu verzichten.

Querverweise:

27. TB, 9.3.3

6.3 Polizei 2020

Nachdem der Gesetzgeber das neue Bundeskriminalamtgesetz (BKAG) verkündet hatte, kündigte die Bundesregierung 2018 das IT-Großprojekt „Polizei 2020“ an. Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat mir den Projektfahrplan vorgestellt und zugesagt, mich in die Diskussion zu den einzelnen Planungsabschnitten einzubeziehen.

Bereits in meinem letzten Tätigkeitsbericht habe ich über das Programm „Polizei 2020“ berichtet (vgl. 27. TB, Nr. 9.3.4). Mit diesem Projekt soll die Dateienlandschaft der Polizei grundlegend verändert werden. Ziel ist es, ein gemeinsames „Datenhaus“ der Polizeien des Bundes und der Länder zu schaffen. Mittels einer zentralen Speicherung sollen auf diese Weise Mehrfachspeicherungen in unterschiedlichen polizeilichen Systemen vermieden werden.

Das BMI und das Bundeskriminalamt (BKA) versprechen sich dadurch eine erhöhte Datenqualität, bessere Verfügbarkeit der polizeilich relevanten Informationen sowie eine Bündelung der Ressourcen mit dem BKA als dienstleistungsorientierte Zentralstelle. Letztlich stünden mit dem geplanten Datenhaus einheitliche Protokollierungs- und Analysemöglichkeiten zur Verfügung.

Aus meiner Sicht kann dies aber dazu führen, dass Informationen im Polizeienverbund umfassender und breiter gestreut zur Verfügung stehen. Problematisch kann dies beispielsweise sein, wenn eine gespeicherte Person keinen Anlass hierzu gegeben hat. Dies gilt für Geschädigte, Zeugen oder für Personen, bei denen ein bestehender Anfangsverdacht im Laufe des Verfahrens nicht verdichtet oder bestätigt werden kann.

Anfang des Jahres wurde ich zu einer Veranstaltung des BKA eingeladen, um an der Erprobung des Datenhauses (sog. Proof of Concept/PoC Datenkonsolidierung) teilzunehmen. Konkret wurde mir eine Datenverarbeitung unterhalb der Schwelle der nach dem BKAG geforderten Verbundrelevanz dargestellt. Diese frühzeitige Initiative des BKA begrüße ich außerordentlich. Nachdem ich jedoch erhebliche Einwände gegen das der Erprobung zu Grunde liegende System geäußert hatte, wurde ich für künftige Termine vom BMI zu meinem Bedauern nicht mehr eingeladen.

Zum Jahresende – kurz vor Redaktionsschluss – hat das BMI mich jedoch über den aktuellen Stand des Projektes „Polizei 2020“ informiert. Dabei ist aufgefallen, dass der ambitionierte Name „Polizei 2020“ wohl eher den Beginn der Veränderung der IT-Landschaft und nicht das Ende des Projektes bezeichnet. Tatsächlich stehen das BMI und das BKA weiterhin am Anfang der Veränderung und entwickeln den „Bebauungsplan“ der neuen IT-Architektur. In einer ersten Phase wurde eine Interimslösung angestoßen. Hierbei sollen die Vorgangsbearbeitungssysteme **(VBS)** der Länderpolizeien weitestgehend zentralisiert werden. Gleiches gilt für das Fallbearbeitungssystem **eFBS** und das Asservatensystem **AMS**. Die Datei **INPOL-Z** sowie der polizeiliche Informations- und Analyseverbund (**PIAV**) sollen zu einem Verbund verschmelzen.

Jeder Teilnehmer soll hierbei – wie auch in der bisherigen Datenlandschaft – für seine Daten verantwortlich sein (Besitzerprinzip). Zur Einhaltung der polizei- und datenschutzrechtlichen Regelungen arbeitet das BMI an einem attributbezogenen und dynamischen Zugriffs- und Rollenberechtigungskonzept, das nicht nur jeden Datensatz, sondern jedes einzelne Datum berücksichtigt. Perspektivisch gedacht – das BMI sieht hier einen Zeitrahmen von mehr als 10 Jahren – sollen in einer zweiten Phase alle Systeme in ein einziges System übergehen. Unabhängig vom Anwendungsgebiet soll dann nur noch ein Gesamtsystem mit individualisierter Oberfläche genutzt werden. Vorgangs-, fallrelevante und landesspezifische Informationen stünden dann ausschließlich im gemeinsamen Datenhaus zur Verfügung.

Dieses Projekt stellt das BMI und das BKA sowohl in technischer als auch in datenschutzrechtlicher Sicht vor große Herausforderungen. Ein detailliertes schriftliches Konzept zur datenschutzrechtlichen Prüfung liegt mir nicht vor. Das BMI hat mir jedoch nach einem konstruktiven Austausch zugesagt, mich zukünftig regelmäßig zu beteiligen.

6.4 Speicherung von Fluggastdaten

Seit dem 29. August 2018 speichert die beim Bundeskriminalamt (BKA) eingerichtete Fluggastdatenzentrale (Passenger Information Unit, PIU) die von Luftfahrtunternehmen übermittelten Passagierdaten von Flugreisenden. Das betrifft potentiell alle in Deutschland ankommenden und von Deutschland abgehenden Flüge über die Schengen-Grenzen sowie über innereuropäische Staatsgrenzen. Inzwischen ist eine sechsstellige Anzahl von Fluggastdatensätzen (PNR-Daten) zusammengekommen. Rechtsgrundlage für die Sammlung und Auswertung dieser Daten ist das Fluggastdatengesetz, mit dem die europäische PNR-Richtlinie umgesetzt wurde.

Die Verarbeitung von Fluggastdaten habe ich schon in mehreren Tätigkeitsberichten kritisch beleuchtet (vgl. 22. TB Nr. 13.5.4; 26. TB Nr. 2.3.2; 27. TB Nr. 1.3). Spätestens seit dem Gutachten des Europäischen Gerichtshofes (EuGH) vom 26. Juli 2017 zum geplanten Fluggastdaten-Abkommen zwischen Kanada und der Europäischen Union (EU) bestehen erhebliche Zweifel, ob die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PNR-RL) mit der Grundrechtecharta der EU vereinbar ist. Das gilt auch für das hiesige nationale Fluggastdatengesetz (FlugDaG).

In seinem Gutachten hat der EuGH der anlasslosen langfristigen Speicherung der Daten sämtlicher Flugpassagiere eine klare Absage erteilt. Mit Blick auf die Übermittlung von PNR-Daten an Kanada stellte der EuGH bei der zulässigen Speicherdauer maßgeblich auf den Ausreisezeitpunkt ab. Wenn bei der Einreise oder während des Aufenthaltes einer Person keine objektiven Anhaltspunkte für Gefahren aus dem Bereich des internationalen Terrorismus oder der schweren grenzübergreifenden Kriminalität durch diese Person ermittelt werden können, ist nach Auffassung des Gerichts der ursprüngliche Übermittlungszweck erfüllt und die weitere Speicherung der Fluggastdaten unzulässig. Eine weitere Speicherung hält das Gericht nur dann für zulässig, wenn in konkreten Einzelfällen objektive Anhaltspunkte dafür vorliegen, dass bestimmte Fluggäste auch nach ihrer Ausreise eine Gefahr im Zusammenhang mit der Bekämpfung des internationalen Terrorismus oder schwerer grenzübergreifender Straftaten darstellen.

Nach meiner Rechtsauffassung sind die Erwägungen des Gerichts über die Unzulässigkeit der langfristigen anlasslosen Speicherung der Fluggastdaten sämtlicher Passagiere auf die PNR-RL und das FlugDaG übertragbar. Deshalb habe ich sowohl die Bundesregierung als auch gemeinsam mit den anderen europäischen Datenschutzaufsichtsbehörden die Kommission zu Nachbesserungen der Gesetze aufgefordert. Bislang ist hier jedoch wenig Bereitschaft dazu erkennbar.

Inzwischen sind sowohl in Deutschland als auch in anderen EU-Staaten Klagen gegen die Speicherung von Fluggastdaten anhängig. Das belgische Verfassungsgericht hat dem EuGH mehrere Fragen zur Vereinbarkeit von PNR-Regelungen mit der Grundrechtecharta zur Vorabentscheidung vorgelegt. Ich begrüße es, auf diesem Weg eine Klärung herbeizuführen. Es bedarf insbesondere einer Grundsatzentscheidung des EuGH, ob und wie lange eine anlasslose Speicherung von Fluggastdaten zum Zwecke der Verhütung und Verfolgung von terroristischen und sonstigen schweren Straftaten rechtmäßig erfolgen kann.

6.5 Abfragen beim Bundesamt für Verfassungsschutz vor Vergabe von öffentlicher Förderung

Die Bundesministerien befragen bei der Vergabe staatlicher Leistungen an private Dritte das Bundesamt für Verfassungsschutz (BfV), um eine missbräuchliche Inanspruchnahme der Leistungen durch verfassungsfeindliche Organisationen auszuschließen. Für die Einbeziehung des BfV und die damit verbundene Verarbeitung personenbezogener Daten fehlt es an einer hinreichenden gesetzlichen Grundlage.

Zur ganzheitlichen Bekämpfung von extremistischen und terroristischen Organisationen hat das Bundesministerium des Innern, für Bau und Heimat (BMI) mit dem sog. Haber-Diwell-Erlass aus dem Jahr 2017 auch den Bereich der staatlichen Leistungsgewährung als relevant für die innere Sicherheit eingestuft. Bei den ins Auge gefassten Leistungen handelt es sich beispielsweise um Förderprogramme mit jugend-, bildungs-, entwicklungs-, umwelt- oder integrationspolitischer Zielsetzung. Um eine missbräuchliche Inanspruchnahme dieser Leistungen durch verfassungsfeindliche Organisationen zu verhindern, sollen die Bundesministerien Anfragen zum Vorliegen von möglichen verfassungsschutzrelevanten Erkenntnissen an das BfV richten. Nach Überprüfung der in der Anfrage genannten Organisationen, Personen oder Veranstaltungen erteilt das BfV den Bundesministerien Auskunft darüber, ob verfassungsschutzrelevante Erkenntnisse vorliegen oder nicht. Von der Mitteilung hängt maßgeblich ab, ob staatliche Leistungen an die Antragstellenden vergeben werden.

Wegen der tiefgreifenden Auswirkungen für die von der Anfrage Betroffenen und der damit einhergehenden Grundrechtsrelevanz bedarf es für die fraglichen Daten-

verarbeitungen bei der Einbeziehung des BfV einer besonderen gesetzlichen Vorschrift.

Aktuell fehlt eine entsprechende Regelung von Gesetzesrang, die die Einbeziehung des BfV zur Überprüfung von Personen bezüglich des Vorliegens verfassungsschutzrelevanter Erkenntnisse explizit erlaubt, um Missbrauch staatlicher Leistungen zu verhindern. Regelungen ausschließlich in Form eines Erlasses reichen nicht aus.

Sonstige für das BfV einschlägige, allgemeine gesetzliche Regelungen oder Generalklauseln, wie etwa § 8 Absatz 1 Satz 1 oder § 10 Absatz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG), scheiden generell als Ermächtigungsgrundlage aus, weil tatsächliche Anhaltspunkte vorliegen müssen, dass die gesetzliche Aufgabenerfüllung des BfV berührt ist. Zum Zeitpunkt der Anfrage eines Bundesministeriums an das BfV zwecks Überprüfung bestehen aber gerade keine Anhaltspunkte dafür, dass im Zusammenhang mit der jeweiligen Leistungsvergabe die freiheitlich demokratische Grundordnung oder der Bestand und die Sicherheit des Staates tatsächlich gefährdet sind. Das vorgesehene Verfahren liefert allenfalls als Endergebnis und auch nur in Bezug auf einzelne Überprüfte derartige tatsächliche Anhaltspunkte.

Wenn der Gesetzgeber es für erforderlich hält, Erkenntnisse des BfV für die Entscheidung über die Vergabe staatlicher Leistungen zu nutzen, muss er eine entsprechende gesetzliche Grundlage schaffen.

Das BMI sieht entgegen meiner Auffassung keinen gesetzgeberischen Handlungsbedarf und erachtet § 3 BDSG i. V. m. §§ 8 Abs. 1, 17 Abs. 1 und 19 Abs. 1 Satz 2 BVerfSchG als ausreichende Gesetzesgrundlage.

Ich empfehle, für das sogenannte Haber-Verfahren eine ausdrückliche und umfassende gesetzliche Grundlage zu schaffen.

6.6 Beratungs- und Informationsbesuche beim Bundesnachrichtendienst

Der Bundesnachrichtendienst (BND) passt seine technischen Fähigkeiten und Kapazitäten im Rahmen der Strategischen Initiative Technik (SIT) an geänderte Anforderungen an. Dies ist eine Erkenntnis aus meinen diversen Beratungs- und Informationsbesuchen, die ich im Berichtszeitraum bei Nachrichtendiensten durchgeführt habe. Aufgrund der strengen Vorgaben der Verschlusssachenanweisung kann ich an dieser Stelle allerdings nur sehr eingeschränkt hierüber berichten.

Die bereits in den vergangenen Jahren begonnene gemeinsame Betrachtung von Zweck und Funktionsweise neuer IT-Systeme beim BND wurde im Berichtszeitraum mit zwei weiteren Beratungs- und Informationsbesuchen fortgesetzt. Im Fokus der Besuche standen ausgewählte Systeme, die Teil der technischen Neuaufstellung der Fernmeldeaufklärung sind. Dabei konnte ich einen weitreichenden Einblick in die Erfassung und Weiterverarbeitung von personenbezogenen Daten durch den BND gewinnen. Die Durchführung späterer Datenschutzkontrollen kann so vorbereitet und erleichtert werden. Es ist geplant, den Überblick über die IT-Landschaft des BND durch diese Form des Informationsaustauschs auch im kommenden Jahr weiter zu vervollständigen.

6.7 Kontrollen bei Sicherheitsbehörden

6.7.1 Pflichtkontrollen

Immer häufiger sehen sowohl nationale Gesetze als auch EU-Recht turnusmäßige Kontrollen bestimmter Dateien oder Ermittlungsmaßnahmen vor.

In meinem letzten Tätigkeitsbericht habe ich über meine ersten Erfahrungen mit den verschiedenen Pflichtkontrollen berichtet (vgl. 27. TB Nr. 14.3.9). Auch im aktuellen Berichtszeitraum habe ich wieder mehrere Pflichtkontrollen durchgeführt, nämlich die Anti-Terror-Datei (ATD) und die Rechtsextremismus-Datei (RED), die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), die Zulässigkeit von Anfragen an das europäische Visa-Informationssystem (VIS) sowie das europäische Asylsystem European Dactyloscopy (EURODAC).

ATD-/RED-Kontrollen

In 2019 wurden diese Dateien bei fast allen meiner Zuständigkeit unterfallenden Sicherheitsbehörden geprüft. Kontrollen fanden beim Bundeskriminalamt (BKA), der Bundespolizei (BPol), dem Zollkriminalamt (ZKA), dem Bundesnachrichtendienst (BND) und dem Bundesamt für Verfassungsschutz (BfV) statt.

Beim BKA habe ich neben der Kontrolle der ATD auch die ebenfalls vorgesehene Pflichtkontrolle der RED durchgeführt. Beide führten nicht zu Beanstandungen. Wie sich allerdings vor allem bei der ATD zeigte, tauschten die beteiligten Behörden die wesentlichen Informationen außerhalb dieser Datei aus. Insbesondere wurde das BKA durch Informationen anderer Behörden außerhalb der ATD über Sachverhalte informiert, an die

sich dann eigene Ermittlungen anschlossen. Vor diesem Hintergrund tragen diese gemeinsamen Dateien aus meiner Sicht letztlich nicht zu einer effektiveren Aufgabenerledigung des BKA bei.

Bei der BPol habe ich ebenfalls die ATD und die RED kontrolliert. Die Prüfungen bestätigten wie schon die Kontrollen im Jahr 2017, dass beide Dateien zwar als Kommunikationsanbahnungsinstrumente konzipiert sind, die Kommunikation bei aktuellen Verdachtsmomenten jedoch auf anderen Kommunikationswegen geführt wird. Die Kommunikation über ATD bzw. RED ist in Gefahrensituationen für die beteiligten Behörden zu umständlich und zu ineffektiv. Trotzdem werden die Dateien mit großem zeitlichen und personellen Aufwand pflichtgemäß befüllt, um die Informationen auch über diesen Weg den anderen Behörden zugänglich zu machen.

Dass andere Kommunikationswege und Kooperationsformen in der Praxis mehr Bedeutung haben als die ATD, war auch mein Eindruck aus einer weiteren Pflichtkontrolle der ATD beim ZKA. Hinzu kam die Problematik, dass das ZKA einerseits als verantwortliche Stelle in die ATD einspeichert und dementsprechend die Speichervoraussetzungen selbstständig festzustellen hat, andererseits jedoch mangels eigener Federführung in der Terrorismusbekämpfung „tatsächliche Anhaltspunkte“ im Sinne des § 2 ATD-Gesetz in der Regel nur im Zusammenhang mit von anderen Behörden mitgeteilten Erkenntnissen erhält. Die Tatsache, dass eine Person bereits von einer anderen Behörde in der ATD gespeichert ist, ist hier allein nicht ausreichend. Vielmehr müssen entsprechend valide Einzelinformationen anderer Behörden im Rahmen der eigenen Aufgabenerfüllung eingeholt werden oder vorliegen. Ansonsten würden sich Speicherungen schneeballartig ausbreiten. Als Konsequenz muss das ZKA alle ATD-Einträge nochmals überprüfen und solche Einträge löschen, die nur darauf basieren, dass eine andere Stelle die Person auch gespeichert hat.

Die Kontrolle der ATD beim BND aus dem Jahr 2018 konnte 2019 noch nicht abgeschlossen werden. Die kontrollierten Datensätze legten viele Bezüge zu ausländischen Nachrichtendiensten offen. In diesem Bereich gilt die »Third-party-rule«, die eine Konsultation des beteiligten ausländischen Nachrichtendienstes nach sich zieht. Eine Rückmeldung der ausländischen Partnerdienste zu der Frage, ob auch ich Kenntnis von diesen Datensätzen erhalten kann, steht noch aus. Die datenschutzrechtliche Überprüfung solcher Speicherungen gestaltet sich deshalb langwierig, schwierig und ist für mich nur mit großem Aufwand möglich.

Eine weitere Kontrolle der ATD und RED fand beim BfV statt. Dies geschah in mittlerweile bewährter Zusammenarbeit mit der G10-Kommission. Allerdings verwehrt die Bundesregierung – wie bereits bei der entsprechenden Kontrolle des BND im Jahre 2018 – der G10-Kommission die Kenntnisnahme von Daten, bei denen aus ihrer Sicht kein Indiz dafür besteht, dass es sich um Daten aus G 10-Maßnahmen handelt (vgl. 6.7.5). Dadurch wird eine durchgängige und lückenlose Aufsicht über das BfV erschwert. Darüber hinaus – wie auch schon im letzten Tätigkeitsbericht erwähnt (vgl. 27. TB Nr. 9.3.11) – sind die Protokollierungen beider Dateien nach wie vor schwer nutzbar für Datenschutzkontrollzwecke.

Da eine grundlegende Erneuerung der auch von den Sicherheitsbehörden ungeliebten Dateien überfällig ist, aber weiterhin auf sich warten lässt, bleibe ich bei meiner Forderung, die ATD und die RED abzuschaffen. Alternativ fordere ich das BMI als Fachaufsicht sowohl über das BKA als auch über das BfV und die BPol auf, endlich beide Dateien so zu reformieren, dass sie für alle beteiligten Behörden einfacher zu bedienen sind. Derzeit erzeugen nicht nur die Kontrolle, sondern auch die technische und fachliche Pflege einen Aufwand, der in keinem Verhältnis zum fachlichen Mehrwert steht. Zudem könnten die kontrollierenden Stellen ihre Aufgaben effizienter wahrnehmen.

Schengener Informationssystem der zweiten Generation (SIS II)

Bei der BPol habe ich in 2019 eine Folgekontrolle zur 2018er-Kontrolle der präventiv-polizeilichen Personenausschreibungen zur Einreise- und Aufenthaltsverweigerung durchgeführt. Hier hatte ich Defizite bei der Dokumentation der Speichervoraussetzungen festgestellt. Dies betraf insbesondere die erforderlichen Prognoseentscheidungen. Meine diesjährige Kontrolle ergab, dass die Bundespolizei hier aktiv auf eine einheitliche Verwaltungspraxis hinwirkt. An einigen Stellen war die Dokumentation nach wie vor nicht selbsterklärend, so dass ich erneut Nachbesserungen empfohlen habe. Ein anderer Kritikpunkt aus der diesjährigen Kontrolle betraf die Protokolldaten. Die Speicherdauer entsprach nicht in allen Punkten den europäischen Vorgaben. Außerdem waren die Daten nicht kurzfristig für die Datenschutzkontrolle verfügbar, die BPol hat Nachbesserungen zugesagt.

Beim BKA habe ich stichprobenartig die Rechtmäßigkeit von Personenausschreibungen kontrolliert. Die Stichprobe ergab keine Mängel. Auch die Verfahrensvorschriften bei der Eingabe von Ausschreibungen zur Festnahme sowie beim Umgang mit Treffermeldungen

wurden befolgt. Inhalt und Umfang von Treffermeldungen sollen in künftigen Kontrollen noch einmal genauer untersucht werden. Der Hauptkritikpunkt dieser Kontrolle betraf wie auch bei der BPol die Protokollierung. Die Speicherdauer der Protokolldaten zur Historie von Ausschreibungen ist zu kurz und dringend den europäischen Vorgaben anzupassen; das BKA hat Abhilfe zugesagt.

Im Berichtszeitraum habe ich beim BND eine Kontrolle zum SIS II durchgeführt. Die deutschen Nachrichtendienste dürfen das SIS II nur für sogenannte verdeckte Ausschreibungen nach Art. 36 Abs. 3 SIS-Beschluss i. V. m. § 17 Abs. 3 BVerfSchG nutzen, um Reisebewegungen nachzuvollziehen, nicht aber beispielsweise zur Festnahme bei der Einreise. Voraussetzung hierfür ist, dass die dabei gewonnenen Informationen zur Abwehr einer von der betroffenen Person ausgehenden erheblichen Gefährdung oder anderer erheblicher Gefahren für die Sicherheit des Staates erforderlich sind. Die Bewertung der geprüften Stichprobe dauert noch an, allerdings kann ich bereits jetzt festhalten, dass ich die Dokumentation des Verfahrens nicht durchgängig nachvollziehen kann.

Abfrage von Daten aus VIS und EURODAC

Im Jahre 2019 habe ich beim BKA die Rechtmäßigkeit von Recherchen in VIS und EURODAC überprüft. Solche Recherchen dürfen unter bestimmten Voraussetzungen ausschließlich zum Zwecke der Verhütung, Aufdeckung oder Ermittlung terroristischer oder sonstige schwerer Straftaten durchgeführt werden. Ich habe für beide Systeme Stichproben durchgeführt. In allen Fällen war die Rechtmäßigkeit der Abfragen nachvollziehbar, im Bereich der VIS-Abfragen ist die Dokumentation allerdings verbesserungsfähig. Hier habe ich eine entsprechende Empfehlung ausgesprochen.

Bereits im Jahr 2018 hatte ich bei der Bundepolizei eine Kontrolle zur Rechtmäßigkeit von EURODAC-Recherchen begonnen, bei der sich schnell Dokumentationsdefizite abzeichneten. Nach Auswertung ergänzender Unterlagen und Protokolldaten war im Ergebnis nicht in allen Fällen nachvollziehbar dokumentiert, ob die Voraussetzungen für die Zulässigkeit des Abgleiches tatsächlich vorlagen. Dies habe ich in 2019 als Verstoß gegen die aus dem Rechtsstaatsprinzip des Art. 20 Abs. 3 GG abzuleitende Pflicht zur Führung ordnungsgemäßer Akten beanstandet. Infolge der Beanstandung hat die Bundespolizei inzwischen Maßnahmen getroffen, um das vorgefundene Dokumentationsdefizit für die Zukunft abzustellen. Diese erscheinen nach derzeitigem Stand geeignet. In einer künftigen Kontrolle werde ich noch einmal überprüfen, ob die Maßnahmen zum gewünschten Ergebnis geführt haben.

Fazit

Turnusmäßige Pflichtkontrollen leisten einen wichtigen Beitrag zur Einhaltung der jeweiligen datenschutzrechtlichen Vorgaben. Allerdings binden sie auch erhebliche personelle Ressourcen. Mittel- und langfristig darf das nicht dazu führen, dass dies zu Lasten nicht ausdrücklich regulierter Bereiche geht, die sich gegebenenfalls sogar als datenschutzrechtlich problematischer erwiesen haben, als die Bereiche, in denen Pflichtkontrollen vorgeschrieben sind. Im wichtigen Bereich der Aufsicht über sicherheitsbehördliches Handeln müssen die Voraussetzungen für eine ausgewogene Kontrollpraxis stets gegeben bleiben, die vom Bundestag genehmigten zusätzlichen Stellen beim BfDI leisten hierzu einen wichtigen Beitrag.

Querverweise:

6.7.5 Fragmentierung der Aufsichtslandschaft über die Nachrichtendienste

6.7.2 Quellen-Telekommunikationsüberwachung beim BKA

Das Bundeskriminalamt (BKA) hat die datenschutzrechtlichen Anforderungen zur Nachvollziehbarkeit ihrer TKÜ-Überwachungsmaßnahmen verbessert. Bei einer datenschutzrechtlichen Kontrolle habe ich auch Teile des Quellcodes einsehen können.

Bereits in der Vergangenheit habe ich Quellen-TKÜ-Maßnahmen u. a. wegen der technischen Funktionalitäten und Risiken der verwendeten Softwareprodukte kritisiert. Als Ergebnis der Diskussion zwischen Datenschutz- und Sicherheitsbehörden wurde ein strengerer Anforderungskatalog erarbeitet. Bereits damals bestand ich auf der uneingeschränkten Nachvollziehbarkeit der Umsetzung dieser aus den rechtlichen Befugnissen abgeleiteten Anforderungen bis hin zur Offenlegung des Quellcodes des Softwareprodukts. Denn in einer solchen Konstellation ist es generell schwierig, die genaue Funktionsweise einerseits und die Seiteneffekte andererseits zu kennen und zu beherrschen. Bei der seinerzeit eingesetzten Überwachungssoftware bemängelte ich vor diesem Hintergrund die fehlende Dokumentation und praktisch unmögliche Einsichtnahme in den Quellcode zur Überprüfung des Bezugs zu den rechtlichen Vorgaben.

Mittlerweile hat das BKA mit erheblichem Aufwand eine eigene Entwicklung einer Quellen-TKÜ-Software vorangetrieben. Dabei sollte die zuvor bemängelte Intransparenz bei der durchgängigen Umsetzung von Vorgaben in Quellcode beseitigt werden. In einer Kontrolle im Jahr 2019 überprüfte ich daher, ob der Entwicklungsprozess der Software so ausgestaltet ist, dass zu jedem Entwicklungsschritt der Bezug zu den Anforderungen und Rechts-

normen herstellbar und überprüfbar ist. Dazu betrachtete ich für eine spezielle Version der Software, die auf einem überwachten Gerät eingesetzt werden kann, eine Stichprobe der Funktionalität vom abstrakt formulierten Anforderungsmanagement bis in die Details des Quellcodes.

Im Ergebnis konnte ich mich davon überzeugen, dass das BKA die Nachvollziehbarkeit der Anforderungen in den einzelnen Prozessschritten erbringen kann und die rechtskonforme Ausgestaltung dieser speziellen Softwarekomponente des Überwachungssystems grundsätzlich beherrscht. Zuvor hatte ich in einem Anwendungstest festgestellt, dass sich die Software auf die Überwachung der laufenden Telekommunikation beschränkt.

6.7.3 Das Vorgangsbearbeitungssystem beim BKA

Bei einer Kontrolle habe ich das Vorgangsbearbeitungssystem (VBS) und die Aktenführung beim Bundeskriminalamt (BKA) beanstandet. Das VBS unterscheidet nicht ausreichend zwischen den verschiedenen Zwecken, zu denen die Polizeibehörde personenbezogene Daten verarbeitet. Von daher sind auch Zugriffsrechte und Recherchemöglichkeiten zu weit gefasst. Darüber hinaus ist nicht vorgesehen, Daten aus heimlichen Ermittlungsmaßnahmen zu kennzeichnen.

Das VBS dient nach der bislang bestehenden Errichtungsanordnung dazu, zu einzelnen Vorgängen Dokumente zu erstellen und zu bearbeiten. Darüber hinaus soll es ein- und ausgehende Nachrichten, Dokumente und Vorgänge dokumentieren und bereits vorhandene verwalten. Schließlich kann damit auch nach einzelnen Dokumenten und Vorgängen gesucht werden.

Vorgefunden habe ich allerdings ein System, das auf der einen Seite deutlich über diese beschriebenen Funktionen hinausgeht, andererseits aber grundlegende Anforderungen nicht erfüllt. Daher habe ich insgesamt sechs Beanstandungen ausgesprochen:

Das Vorgangsbearbeitungssystem als solches

Das VBS trennt nicht ausreichend zwischen den verschiedenen Zwecken, zu denen das BKA personenbezogene Daten verarbeitet. Die Zweckbindung ist jedoch ein wesentliches Grundprinzip des Datenschutzes. Ausgangspunkt ist der Anlass, weshalb eine Person in polizeilichen Dateien gespeichert ist. Dieser kann sehr unterschiedlich sein. So können etwa Personen erfasst werden, weil sie als Täter überführt sind. Aber auch geschädigte Personen oder Zeugen einer Straftat können erfasst sein. Hier müssen datenschutzrechtlich unterschiedliche Maßstäbe gelten. Deshalb unterscheiden alle Polizeigesetze des Bundes und der Länder drei grundlegende Zwecke, zu denen Polizeibehörden Daten verarbeiten:

1. **Aufgabenerfüllung**: Die Polizeibehörde darf Daten speichern, um eine Aufgabe erfüllen zu können. Dafür darf sie umfangreich Daten erheben, beispielsweise von Zeugen oder Opfern. Andererseits muss der Zugriff auf diese Daten begrenzt sein. Nur diejenigen, die den „Fall" bearbeiten, dürfen die Daten sehen. Deshalb sind Zugriffe in der Regel auf die zuständige Organisationseinheit zu begrenzen. Ist der Vorgang abgeschlossen, gibt es prinzipiell zwei unterschiedliche Gründe, die Daten weiter aufzubewahren.
2. **Vorsorge („polizeiliches Gedächtnis")**: Die Polizei kann die Daten von Personen weiter speichern, die dafür hinreichenden Anlass gegeben haben. So bestimmt das BKA-Gesetz, dass Daten von Beschuldigten und Verdächtigen zu Vorsorgezwecken gespeichert werden dürfen, wenn sich aus einer dokumentierten Negativprognose ergibt, dass von ihnen weitere Straftaten zu erwarten sind. Zeugen und Opfer darf das BKA – von wenigen Ausnahmefällen abgesehen – nicht für diesen Zweck speichern.
3. **Dokumentation**: Diese Datenspeicherung dient der späteren Prüfung, ob die Polizeibehörde rechtmäßig gehandelt hat. Das gilt beispielsweise dann, wenn sich Opfer darüber beklagen, die Polizei sei zu spät eingeschritten oder eine verdächtigte Person meint, sie sei zu Unrecht abgehört worden. Ein ähnlicher damit zusammenhängender Zweck ist die **Vorgangsverwaltung**. Diese dient dazu, Vorgänge und Dokumente wieder aufzufinden.

Das VBS trennt im Ergebnis nicht ausreichend zwischen diesen drei grundlegenden Zwecken. Insbesondere sind die zu Zwecken der Vorgangsverwaltung und Dokumentation verarbeiteten Daten nicht strikt von den Daten zur Aufgabenerfüllung bzw. Bearbeitung getrennt. In den einzelnen Datensätzen konnte ich bei der Kontrolle nicht nachvollziehen, ob das BKA diese gespeichert hatte, um eine konkrete Aufgabe zu erfüllen oder um das polizeiliche Handeln zu dokumentieren. Damit eng zusammen hängt der Mangel, dass die Zugriffsrechte nicht passend zum Verarbeitungszweck vergeben worden waren, was ich ebenfalls beanstandet habe. Zur Aufgabenerfüllung gespeicherte Daten dürfen prinzipiell nur für diejenigen Bearbeiter zum Zugriff stehen, die für die jeweilige Aufgabe zuständig sind. Ausnahmen sind möglich, müssen aber besonders begründet sein. Ansonsten bestünde die Gefahr, dass die Zweckbindung unterlaufen würde. Stehen etwa alle zur Dokumentation gespeicherten Daten der Recherche offen, dann sind auch alle Personen zu finden, die für die Gefahrenvorsorge nicht gespeichert werden dürften. Das wären dann auch Personen, für die keine Negativprognose gestellt werden kann.

Das VBS darf deshalb nicht als umfassendes Recherchesystem genutzt werden. Es enthält jedoch eine Funktion mit dem Namen „Dateienrundlauf". Damit können die Anwendenden alle Informationen im VBS durchsuchen. Ausgenommen sind nur solche Informationen, die als „beschränkt recherchierbar" gekennzeichnet sind. Das betrifft aber nur einen Teil der Daten. Prinzipiell können die Anwenderinnen und Anwender im BKA, die mit kriminalpolizeilicher Arbeit betraut sind, alle polizeilichen Daten recherchieren. Das betrifft auch solche Daten, für deren Bearbeitung die Beschäftigten innerhalb des Hauses nicht zuständig sind. Daneben können sie gleichzeitig auch die weiteren polizeilichen Datenbestände und weitere Register durchsuchen. Das gilt etwa für die im polizeilichen Informationssystem (INPOL) und im Bundeszentralregister (BZR) abgelegten Informationen. Diese Funktion wird häufig genutzt und führt nach meiner Einschätzung unter anderem dazu, dass Personen teilweise nur deshalb im VBS gespeichert werden, um einen Dateienrundlauf überhaupt durchführen zu können. Personen nur deshalb zu speichern, um nach ihnen recherchieren zu können, ist grob datenschutzwidrig. Den Dateienrundlauf habe ich daher auch beanstandet.

Zu klären ist auch, welche Daten überhaupt zur Dokumentation gespeichert werden. So nimmt das BKA in großem Umfang kriminaltaktische Anfragen (KTA) der Länder entgegen. Daran schließen sich vielfach keinerlei weitere Maßnahmen an. Sie werden nur im VBS gespeichert. Es ist zweifelhaft, was damit genau dokumentiert werden soll. Im Ergebnis werden so die Regelungen zur Vorsorgespeicherung umgangen. Eigentlich gehören die KTA in eine Zentralstellendatei, da sie vorsorglich und recherchierbar vorgehalten werden. Dafür müssen aber im Einzelfall die gesetzlichen Voraussetzungen vorliegen.

Sehr uneinheitlich waren die vergebenen Aussonderungsprüffristen. Es besteht innerhalb des BKA kein einheitlicher Maßstab, nach welchen Kriterien diese für das VBS vergeben werden. Das Gesetz schreibt aber ausdrücklich vor, dass nur eine „befristete" Dokumentation zulässig ist. Dies sollte näher konkretisiert werden, weil die Mitarbeitenden des BKA sonst keinen Maßstab haben, nach dem sie handeln können. Dies habe ich ebenfalls beanstandet.

Darüber hinaus fehlte die Möglichkeit, Daten zu kennzeichnen, die mit besonders eingriffsintensiven Maßnahmen erhoben wurden. Auch das habe ich beanstandet. Solche Daten sind schon seit längerem nach den Vorschriften der Strafprozessordnung zu kennzeichnen.

Bei aller Kritik ist aber die Technik des Systems durchaus positiv zu sehen. Es handelt sich um eine Eigenentwicklung des BKA. Dadurch war es dem BKA möglich, etwa die vergebenen Zugriffsrechte und umfangreiche Übersichten über die Datenverteilung in kurzer Zeit für die datenschutzrechtliche Kontrolle vorzulegen. Die Mängel sehe ich daher nicht in der Technik, sondern in den organisatorischen Vorgaben des Hauses.

Die Aktenführung

Die Dokumentation der Rechtmäßigkeit polizeilichen Handelns muss vollständig sein. Das VBS spiegelt jedoch die vorhandenen Vorgänge nur ausschnittweise wieder. Ein Großteil des Schriftverkehrs und der Vermerke sind lediglich als Dateien in den Gruppenlaufwerken gespeichert. Dies stellt aber nicht ausreichend sicher, dass die Akten vollständig und manipulationssicher vorgehalten werden. Es wird auch nicht die Aktenmäßigkeit der Unterlagen gewahrt. Denn dafür müssen Unterlagen zwingend in der richtigen Abfolge gespeichert sein und stets die einzelnen Verfügungswege und die jeweiligen innerbehördlichen Urheber erkennen lassen. Anderenfalls besteht eine Auflösung der Kontextverknüpfung. Eine ordnungsgemäße Dokumentation setzt zudem eine systematische Registrierung der einzelnen Dokumente einschließlich der Vergabe von Aktenzeichen voraus. Auch eine lückenlose Ablage im Referatslaufwerk genügt hier nicht. Dies habe ich als Verstoß gegen die Grundsätze der ordnungsgemäßen Aktenführung beanstandet.

Ich empfehle im Ergebnis, die Funktionalitäten der elektronischen Aktenführung grundlegend neu auszurichten. Insbesondere sollte das Nebeneinander von Aktenführung und Dokumentation polizeilichen Handelns auf ein unumgängliches Mindestmaß beschränkt werden. Eine durchgehende Dokumentation der Rechtmäßigkeit polizeilichen Handelns ist konsequent sicherzustellen.

6.7.4 Datenschutz bei Sicherheitsüberprüfungen

Datenschutzrechtliche Vorgaben sind auch im Bereich des Sicherheitsüberprüfungsrechtes zu beachten.

Im Berichtszeitraum habe ich bei drei Unternehmen kontrolliert, die den Geheimschutz des Bundesministeriums für Wirtschaft und Energie betreuen. Die Unternehmen führen dort im Rahmen des vorbeugenden personellen Geheimschutzes Sicherheitsüberprüfungen durch. Bei allen Unternehmen habe ich bei der Führung der Sicherheitsakten Verstöße festgestellt, die mir bereits bei vergleichbaren Kontrollen in der Vergangenheit aufgefallen sind (27. TB Nr. 9.3.14.). Beispiele sind hier eine unvollständige Aktenführung, das Auffinden von unzulässigen Unterlagen in den Sicherheitsakten oder die Nichteinhaltung der gesetzlichen Vernichtungs- und Löschfristen. Zumeist waren diese Verstöße auf Unkenntnis der zuständigen Sicherheitsbevollmächtigten zurückzuführen. Ich konnte erreichen, dass die Verstöße bei der Aktenführung überwiegend noch vor Ort oder im Nachgang zu meinem Kontrollbesuch behoben wurden. Auf Beanstandungen habe ich daher verzichtet.

Besonders herausstellen möchte ich, dass mit allen geprüften Unternehmen eine konstruktive Zusammenarbeit möglich war. Meine Hinweise vor Ort wurden von den Sicherheitsbevollmächtigten angenommen und deren Umsetzung bzw. das Abstellen der festgestellten Mängel zugesagt.

Ebenfalls im Berichtszeitraum habe ich beim BfV die Führung der Sicherheits- und Sicherheitsüberprüfungsakten zu Personen kontrolliert, die sich für eine Tätigkeit beim BfV beworben haben. Auch hier habe ich verschiedene datenschutzrechtliche Verstöße bei einzelnen Maßnahmen des Sicherheitsüberprüfungsverfahrens, bei der Führung der Sicherheitsakten sowie bei der Einhaltung von Vernichtungs- und Löschfristen festgestellt. Das BfV hat jedoch im Nachgang zu meiner Prüfung die Akten von unzulässig gespeicherten Unterlagen bereinigt sowie die Einhaltung der Vernichtungs- und Löschfristen überprüft. So konnten die Verstöße bei der Aktenführung überwiegend noch vor Ort oder im Nachgang zu meinem Kontrollbesuch behoben werden.

Kritisch sehe ich, wie das BfV seine Möglichkeit ausübt, Einsicht in die Personalakten der Betroffenen zu nehmen. Hierzu bin ich mit dem BfV noch im Gespräch.

6.7.5 Fragmentierung der Aufsicht über die Nachrichtendienste

Die Aufsicht über die Nachrichtendienste in Deutschland ist fragmentiert. Neben meinen wiederholten Appellen an den Gesetzgeber, die Kontrolldichte in diesem Bereich zu erhöhen, versuche ich, durch Gespräche und Kontakte zu anderen Aufsichtsinstanzen in der Praxis möglichst Lücken in der Kontrolle zu vermeiden.

Wie bereits in den letzten Tätigkeitsberichten immer wieder angesprochen, führt die Fragmentierung der Aufsicht über die Nachrichtendienste zu Kontrolllücken, die gesetzlich und tatsächlich behoben werden müssen (vgl. 27. TB Nr. 9.1.5). Ich nehme die Pflicht zur Zusammenarbeit mit anderen Kontrollorganen ernst und führe weiterhin gemeinsam mit der G-10-Kommission Kontrollen der ATD und der RED durch. Diese Verpflichtung ergibt sich aus der verfassungsrechtlichen Rechtsprechung.

Während die Bundesregierung nach der Änderung der Gesetzesbegründung zu § 26a BVerfSchG mir endlich auch die Kenntnisnahme von G-10-Daten zubilligt, wurde der G-10-Kommission bei der ATD-Kontrolle beim BND im Jahre 2018 der Einblick in nicht aus G-10-Maßnahmen stammenden Daten verwehrt. Diese Auffassung hat die Bundesregierung auch in 2019 aufrecht erhalten und verwehrte der Kommission bei der gemeinsamen Kontrolle der RED beim BfV ebenfalls die Einsichtnahme (vgl. 6.7.1). Begründet wurde dies mit dem Hinweis, dass § 15 Abs. 6 Satz 5 G-10 im Gegensatz zu § 26a BVerfSchG gerade keine Änderung erfahren habe. Die Bundesregierung sieht zu einer solchen Änderung offenbar keinen Anlass. Ich hoffe darauf, dass das BVerfG in einer anhängigen Verfassungsbeschwerde eindeutige Aussagen zur Zusammenarbeit von BfDI und G-10-Kommission treffen wird, um so Rechtssicherheit und Klarheit für alle Beteiligten zu schaffen.

Neben der G-10-Kommission gibt es weitere Aufsichtsbehörden über die Nachrichtendiente, z. B. das Unabhängige Gremium, das den BND im Bereich der Ausland-Ausland-Fernmeldeaufklärung kontrolliert. Auch hier ergeben sich aus meiner Sicht Anknüpfungspunkte für eine Zusammenarbeit, um Kontrolllücken zu vermeiden.

Ich habe mich daher mit dem Unabhängigen Gremium zu einem ersten Austausch getroffen und ihm meine Sichtweise dargelegt. Das Unabhängige Gremium sieht sich strengen Verschwiegenheitspflichten unterworfen. Nach meiner Auffassung wäre hier eine gesetzliche Änderung hin zu einem aktiven Austausch nicht nur wünschenswert, sondern im Lichte der verfassungsgerichtlichen Rechtsprechung sogar notwendig, um den BND im Bereich der Fernmeldeaufklärung und der sich daran anschließenden ggf. weiteren Verarbeitung personenbezogener Daten lückenlos kontrollieren zu können.

Meine Behörde verfügt gerade wegen der Aufsicht über die Nachrichtendienste, Sicherheitsbehörden, öffentliche Stellen und private Unternehmen unter einem Dach über eine umfassende Fach- und Methodenkompetenz im Bereich der Datenschutzkontrolle. Der Haushaltsgesetzgeber hat die Notwendigkeit einer starken Datenschutzaufsicht im Bereich der Sicherheitsbehörden (Polizei wie Nachrichtendienste) erkannt und durch einen großzügigen Stellenzuwachs unterstrichen. Diese gebündelte Kompetenz kann in Zusammenarbeit mit den anderen Kontrollorganen und deren Zuständigkeiten und Fähigkeiten zu einer adäquaten Kontrolle führen.

Querverweis:

6.7.1 Pflichtkontrollen

7 Bundestag

7.1 Das Hausausweis- und Zutrittssystem im Deutschen Bundestag

Der Ältestenrat des Deutschen Bundestages hat 2018 beschlossen, für Besucher und Mitarbeiter des Deutschen Bundestages einen elektronischen Hausausweis einzuführen, der zum Betreten der Liegenschaften des Deutschen Bundestags berechtigt. Dieser Hausausweis enthält einen RFID-Chip, der an den Pforten der jeweiligen Liegenschaften kontaktlos gelesen wird.

Das Hausausweissystem ist seit Anfang 2019 in Betrieb. Es basiert auf einem Umsetzungskonzept, in dem meine Empfehlungen übernommen worden sind. Im März 2019 habe ich einen Informations- und Kontrollbesuch zu diesem System durchgeführt.

Auf dem Hausausweis wird nur eine Kartennummer (AccessID) gespeichert. Er wird an den Pforten der Liegenschaften des Deutschen Bundestags kontaktlos eingelesen, um den zugehörigen Datensatz aus einer zentral gespeicherten Datei abrufen zu können. Ausschließlich zur Überprüfung der Identität des Ausweisinhabers werden dem Pfortenpersonal diejenigen Daten angezeigt, die einschließlich des Lichtbilds auch auf dem Ausweis abgedruckt sind. Für den RFID-Chip wird ein eigenes kryptografisches Modul verwendet, um den Hausausweis gegen unbefugte Zugriffe abzusichern.

Auf Basis der mir vorgelegten Unterlagen, der geführten Gespräche sowie der Kontrolle vor Ort habe ich den Eindruck gewonnen, dass das Hausausweis- und Zutrittssystem mit Blick auf den Schutz personenbezogener Daten nach dem Stand der Technik gestaltet wurde. Die organisatorischen Regelungen zum Umgang mit den Betroffenenrechten sind ausreichend und die Maßnahmen zur Information der Betroffenen im erforderlichen Maß umfassend. Mit Blick auf das Prinzip der Datensparsamkeit sind die erhobenen Daten für den Zweck der Gewährung eines Zugangs zu den Liegenschaften des Deutschen Bundestags erforderlich und die vorgesehenen Löschfristen sind angemessen. Insbesondere wird der Zugang nicht protokolliert, so dass eine Erstellung von Bewegungshistorien nicht möglich ist.

7.2 Kontrolle der Bundestagspolizei

In meinem 25. TB (Nr. 21.1) hatte ich bereits den Erlass einer ausreichenden formellen Rechtsgrundlage für die Polizei beim Deutschen Bundestag gefordert. Trotz sachgerechter Arbeit habe ich die polizeiliche Datenverarbeitung durch die Bundestagspolizei beanstandet, weil es ihr auch weiterhin an einer entsprechenden Rechtgrundlage fehlt.

Im Januar 2019 habe ich bei der Polizei des Deutschen Bundestages einen Beratungs- und Kontrollbesuch durchgeführt. Kontrollgegenstand war dabei im Wesentlichen der Abgleich personenbezogener Daten bei der Einlasskontrolle zu den Liegenschaften und Gebäuden des Deutschen Bundestages sowie der Vergabe von Hausausweisen. Für beides greift die Bundestagspolizei auf das beim Bundeskriminalamt (BKA) geführte polizeiliche Informationssystem (INPOL) und auf das Bundeszentralregister (BZR) zu. Ihre Vorgehensweise insbesondere bei der Einlasskontrolle ist sachgerecht und grundsätzlich nicht zu beanstanden. Sie orientiert sich dabei am Schutzgut des geordneten Parlamentsbetriebes und dem Schutz der daran beteiligten Verfassungsorgane.

Gleichwohl fehlt nach wie vor eine formelle Ermächtigung für die Ausübung dieser polizeilichen Befugnisse. Das in Art. 40 Abs. 2 GG geregelte Hausrecht des Bundestagspräsidenten ist meines Erachtens keine ausreichende Rechtsgrundlage für die Ausübung polizeilicher Befugnisse, die in das Grundrecht auf informationelle Selbstbestimmung eingreifen. Hierfür bedarf es meines Erachtens einer verfassungskonformen gesetzlichen Ermächtigungsgrundlage, die bestimmt genug ist und auch die JI-Richtlinie umsetzt. Daher habe ich die polizeiliche Datenverarbeitung formell gegenüber dem Präsidenten des Deutschen Bundestages beanstandet. Erfreulicherweise hat mir der Bundestagspräsident zwischenzeitlich mitgeteilt, dass er die Bundestagsverwaltung mit der Erarbeitung eines Gesetzesentwurfes beauftragt hat, der auch im Bereich des Datenschutzes die gesetzlichen Grundlagen für die Arbeit der Bundestagspolizei präzisieren soll.

8 Weitere Einzelthemen

8.1 Drittstaatentransfers

Die Globalisierung führt zu einer zunehmenden länderübergreifenden Verarbeitung und Übermittlung in Drittstaaten von personenbezogenen Daten. Im vorangegangenen Jahr standen insbesondere die Diskussionen zu den Auswirkungen des Brexit auf den Datenverkehr zwischen den EU-Mitgliedstaaten und dem Vereinigten Königreich im Fokus. Daneben blieb die Übermittlung von personenbezogenen Daten aus der EU in die USA ein Dauerthema.

8.1.1 Brexit – Folgen für den Datentransfer

Der Austritt des Vereinigten Königreichs aus der EU hat auch Auswirkungen auf den Datenverkehr zwischen den EU-Mitgliedstaaten und dem Vereinigten Königreich, das dadurch datenschutzrechtlich zu einem Drittland wurde.

Ich habe bereits frühzeitig darauf hingewiesen, dass Verantwortliche und Auftragsverarbeiter auch im Bereich Datenschutz Vorkehrungen für den Brexit treffen sollten. Auch wenn inzwischen feststeht, dass das Vereinigte Königreich auf der Grundlage eines Austrittsabkommen aus der EU austreten wird, sollten Verantwortliche und Auftragsverarbeiter weiterhin aufmerksam bleiben.

Das Vereinigte Königreich wird datenschutzrechtlich bereits mit dem Austritt zum 31. Januar 2020 zu einem Drittland. Dennoch wird die DSGVO bis zum 31. Dezember 2020 im Vereinigten Königreich wirksam bleiben. Es bedarf daher in diesem Übergangszeitraum keiner besonderen Schutzmaßnahmen, wenn Daten in das Vereinigte Königreich übermittelt werden. So lange profitieren Unternehmen mit Sitz im Vereinigten Königreich außerdem vom One-Stop-Shop.

In der politischen Erklärung zu den weiteren Beziehungen zwischen dem Vereinigten Königreich und der EU nach dem EU-Austritt wird angestrebt, möglichst bis Ende 2020 die notwendigen Angemessenheitsbeschlüsse zu fassen, auf deren Grundlage weiterhin ein freier Datenfluss erfolgen könnte. Sofern dies nicht gelingt und auch keine Verlängerung der vorgesehenen Übergangszeit beschlossen wird, würde das Vereinigte Königreich sofort zu einem Drittland werden, in dem die DSGVO nicht mehr gilt. Verantwortliche und Auftragsverarbeiter, die personenbezogene Daten an Partner im Vereinigten Königreich übermitteln wollen, müssten ab diesem Zeitpunkt ihre Datentransfers mit den besonderen Schutzmaßnahmen nach Kapitel V der DSGVO absichern.

Ich werde weiterhin über die jeweils aktuelle Situation in Sachen Brexit unter www.bfdi.bund.de/brexit informieren.

8.1.2 Das Schrems II-Verfahren

Standardvertragsklauseln sind eine Grundlage für Datenübermittlungen in die USA. Darüber wird der EuGH im sog. Schrems II-Verfahren in der ersten Jahreshälfte 2020 entscheiden.

Es war ein Paukenschlag, als der EuGH im Oktober 2015 in der sog. Schrems-Entscheidung (Rechtssache C-362/14) das Safe Harbor-Abkommen für ungültig erklärte. Ein neues Abkommen mit den USA wurde notwendig, das Privacy Shield entstand. Nun entscheidet der EuGH im sog. Schrems II-Verfahren erneut über die Datenübermittlung innerhalb des Facebook-Konzerns. Diese Entscheidung könnte noch sehr viel weitergehende Konsequenzen haben. Denn dieses Mal geht es darum, ob die geltenden Standardvertragsklauseln für die Übermittlung von personenbezogenen Daten in die USA ausreichen. Standardvertragsklauseln sind das in der Praxis meistverwendete Instrument, um die für eine Übermittlung in einen Drittstaat notwendigen geeigneten Garantien nachzuweisen. Die Bedeutung des Falles zeigte auch die achtstündige mündliche Verhandlung vor der Großen Kammer des EuGH. Zu dieser wurde erstmals auch der EDSA geladen, der dabei durch die Ausschussvorsitzende und einen Mitarbeiter meiner Behörde vertreten worden ist.

Sollte der EuGH entscheiden, dass die umfangreichen Befugnisse der US-amerikanischen Nachrichtendienste oder die unbefriedigenden Rechtschutzmöglichkeiten

von EU-Bürgerinnen und Bürgern der Verwendung der geltenden Standardvertragsklauseln entgegenstehen, könnten diese als geeignete Garantien wegfallen. Das hätte massive Auswirkungen für Datenübermittlungen in die USA, aber voraussichtlich auch für Übermittlungen in andere Drittstaaten. Nach der mündlichen Verhandlung im Schrems II-Verfahren ist auch nicht ausgeschlossen, dass der EuGH zugleich über die Wirksamkeit des Privacy Shield entscheidet. Denn an die Feststellungen, die die Europäische Kommission im Privacy Shield zum US-Recht getroffen hat, könnten die Datenschutzbehörden auch bei einer Entscheidung über die Rechtmäßigkeit von Übermittlungen gebunden sein, die auf Standardvertragsklauseln beruhen. Sie dürften keine Maßnahmen treffen, so deutete der EuGH in der mündlichen Verhandlung an, die im Widerspruch zu den Feststellungen der Kommission stehen.

Der EuGH hat angekündigt in der ersten Jahreshälfte 2020 seine Entscheidung zu treffen. Ein erster Anhaltspunkt, wie das Gericht entscheiden könnte, ist der Schlussantrag des Generalanwalts vom 19. Dezember 2019. Darin empfiehlt der Generalanwalt, dass die Standardvertragsklauseln weiterhin gültig bleiben sollen. Diese böten als Transferinstrument ausreichende Schutzmaßnahmen für personenbezogene Daten. Unternehmen seien dennoch angehalten die Übermittlung von Daten in Drittstaaten auszusetzen, wenn das Recht des Drittstaates die Erfüllung der vertraglichen Pflichten unmöglich macht. Die Datenschutzbehörden wären dann außerdem verpflichtet solche Übermittlungen zu untersagen.

Die Frage, ob das Privacy Shield rechtmäßig ist, muss aus Sicht des Generalanwalts in diesem Verfahren nicht entschieden werden. Für den Fall, dass der EuGH abweichend von seiner Empfehlung auch hierzu eine Entscheidung treffen will, erklärte er jedoch vorsorglich seine Zweifel an der Rechtmäßigkeit des Übereinkommens.

8.1.3 Entwicklungen beim EU-US Privacy Shield

Das EU-US Datenschutzabkommen Privacy Shield wird inzwischen besser durch die US-Administration umgesetzt. Gleichwohl gibt es immer noch wesentliche Kritikpunkte.

Das „EU-US Privacy Shield“ (Privacy Shield) wurde im Berichtszeitraum einer weiteren gemeinsamen Überprüfung unterzogen, an der einer meiner Mitarbeiter als Teil der EDSA-Delegation mitgewirkt hat. Dabei konnten auch positive Entwicklungen auf US-Seite konstatiert werden. So ist das wichtige Aufsichtsgremium Privacy and Civil Liberties Oversight Board wieder voll besetzt. Dieses Gremium berät den Präsidenten und die Exekutive zum Schutz von Bürgerrechten bei Maßnahmen der Terrorabwehr und hat zur Erfüllung der Aufgabe weitgehende Einsichtsrechte. Daneben wurde eine neue Ombudsperson, die sich Beschwerden von europäischen Bürgerinnen und Bürgern über den Zugriff von U.S.-Sicherheitsbehörden auf ihre personenbezogenen Daten annehmen soll, für das Privacy Shield benannt.

Diesen ersten Schritten zu einer besseren Aufsicht über die Sicherheitsbehörden in den USA müssen aus Sicht des EDSA allerdings weitere Schritte folgen. So hat der EDSA das Privacy and Civil Liberties Oversight Board aufgefordert, ihm weitere Berichte über den Zugriff von US-Sicherheitsbehörden auf personenbezogene Daten von europäischen Bürgerinnen und Bürgern zur Verfügung zu stellen. Zudem fehlt es weiterhin an Nachprüfungen durch die US-Behörden, ob die nach dem Privacy Shield zertifizierten US-Unternehmen dessen Vorgaben tatsächlich befolgen.

Auch die Frage, ob die Ombudsperson tatsächlich einen wirksamen Rechtsschutz im Sinne von Art. 47 der EU-Grundrechtecharta gewährleisten kann, ist weiterhin offen und liegt dem Europäischen Gerichtshof im Rahmen des sogenannten Schrems II-Verfahrens (vgl. Nr. 8.1.2) zur Klärung vor.

Dieses und die beim Europäischen Gericht anhängigen Verfahren gegen das Privacy Shield werden verdeutlichen, welche Rahmenbedingungen die EU-Grundrechtecharta für den transatlantischen Datenverkehr setzt.

Querverweis:

8.1.2 Schrems II

8.2 Das Onlinezugangsgesetz

Die Bundesregierung arbeitet intensiv an der Umsetzung des Onlinezugangsgesetzes (OZG). Dessen Umsetzungskatalog umfasst derzeit 575 Verwaltungsdienstleistungen, die bis Ende 2022 von Bund, Ländern und Kommunen vollständig digital angeboten werden sollen.

Wie bereits in meinem 27. Tätigkeitsbericht (Nr. 9.2.2) dargestellt, sollen Bürgerinnen und Bürger sowie Unternehmen bei einem Verwaltungsportal ihrer Wahl Zugang zu den online angebotenen Verwaltungsdienstleistungen erhalten, ohne sich dazu mehr als einmal identifizieren zu müssen (Once-Only-Prinzip). Wichtig ist für die Nutzung, in welcher Form sie sich bei den Nutzerkonten identifizieren können. Dies richtet sich nach dem jeweiligen Schutzniveau der Verwaltungsdienstleistung. Die eIDAS-Verordnung der Europäischen Union unterscheidet die drei Vertrauensniveaus „niedrig“, „substanziell“ und „hoch“. Online angeboten werden bisher Verwaltungsdienstleistungen für die Schutzniveaus „niedrig“ (Registrierung anhand Benutzername und Passwort) und „hoch“ (Registrierung anhand der Online-Funktion

des Personalausweises und des elektronisches Aufenthaltstitels). Die Identifizierungsdaten dürfen nur nach Einwilligung der Nutzerinnen und Nutzer dauerhaft im Nutzerkonto gespeichert werden.

Das OZG legt zur Umsetzung des Once-Only-Prinzips die zur Identifizierung einer natürlichen oder juristischen Person erforderlichen Daten, d. h. den hierfür notwendigen Kerndatensatz, fest. Dieser ist das Bindeglied für behördenübergreifende Verwaltungsverfahren. Auf der Basis dieses Identitätsmanagements ist eine zuverlässige Verknüpfung der bei unterschiedlichen Behörden vorliegenden Angaben möglich.

Die bereichsübergreifende Identifizierung ist datenschutzkonform auszugestalten. Insoweit bestehen neue Herausforderungen. Auch im Rahmen der Umsetzung des Once-Only-Prinzips wird teilweise dafür plädiert, pauschal eine einheitliche Personenkennziffer (PKZ) einzuführen oder die Steuer-Identifikationsnummer als PKZ zu verwenden. Dies würde aber eine Nachverfolgung der betroffenen Person durch alle Bereiche des öffentlichen Lebens sowie eine umfassende und detaillierte Profilbildung der Betroffenen ermöglichen. Derart umfassende Profilbildungen sind nach Auffassung des Bundesverfassungsgerichts verfassungswidrig. Außerdem erhöht eine PKZ bei Datenlecks und Cyberangriffen die Gefahr, dass diese Daten in Händen Unbefugter den Bürgerinnen und Bürgern zugeordnet werden können.

Bei der Nutzung von Diensten nach dem OZG muss sichergestellt werden, dass die Bürgerinnen und Bürger jederzeit und umfassend die Kontrolle über ihre Daten be- und erhalten. Wenn beispielsweise eine staatliche Leistung beantragt werden soll, für die bislang analog mehrere Einzelanträge bei verschiedenen Stellen ausgefüllt oder Auskünfte abgefragt werden müssen, könnte dies künftig zusammen mit nur einem Mausklick erledigt werden. Dieser würde dann nach einmaliger Authentifizierung des Beantragenden automatisiert die erforderlichen Prozesse auslösen. Ein aktuelles Beispiel ist das Digitalisierungsprojekt ELFE (Einfache Leistungen für Eltern), dessen Zielsetzung es ist, u. a. eine kombinierte Beantragung von Kindergeld und Elterngeld zu ermöglichen.

Diese nutzerfreundliche Antragsstellung darf aber aus datenschutzrechtlicher Sicht nicht dazu führen, dass die einzelnen Datenverarbeitungsvorgänge für den Antragstellenden in einer Black Box verschwinden. Um hier Transparenz zu schaffen gibt es zwei verschiedene Konzepte:

Eine Alternative wäre, die Beantragung weiterhin dem Antragstellenden Schritt für Schritt über eine App oder den Web-Browser anzuzeigen. Die Formulare würden nacheinander angezeigt, müssten allerdings nicht mehr selbst befüllt werden, da sich das System die erforderlichen Daten aus den relevanten Quellen herauszieht. Die hierbei laufenden Prozesse könnten unmittelbar beim „Ausfüllen“ erklärt werden. Den Bürgerinnen und Bürgern würde dadurch eine Kontrollmöglichkeit eröffnet, bevor sie letztverantwortlich nur noch das Absenden der Formulare per Klick bestätigen.

Alternativ käme ein sogenanntes Datenschutzcockpit in Betracht, mit welchem für Bürgerinnen und Bürger auf einer eigens dafür geschaffenen Web-Seite, ähnlich den sogenannten Privacy-Panels sozialer Netze, Transparenz geschaffen wird. Hier würden alle Teilprozesse des Antrags tatsächlich mit einem Klick ausgelöst. An dieser Stelle ist zum einen auf die datenschutzkonforme Einwilligung zum Datenaustausch zu achten und zum anderen sind die Antragstellenden genauestens über den sie betreffenden Datenaustausch zu informieren. Dies könnte beim Datenschutzcockpit lediglich im Nachhinein über eine Darstellung und Erläuterung der im Hintergrund abgelaufenen Einzelprozesse erfolgen.

Beide Alternativen sorgen für eine hinreichende Transparenz, um die Verwendung der Daten durch die Behörden einzusehen und die personenbezogenen Datenaustausche zwischen Behörden darzustellen. Ein wesentlicher Unterschied liegt lediglich in der Steuerungsmöglichkeit der Antragstellenden. Während die Alternative des Datencockpits die Antragstellung schneller und einfacher macht, behalten Bürgerinnen und Bürger bei der Schritt-für-Schritt Beantragung mehr Kontrolle.

Unabhängig davon, welche Methode letztendlich die erforderliche Transparenz gewährleisten soll, werde ich bei der Erarbeitung der hierfür notwendigen gesetzlichen Grundlagen darauf achten, dass die Entlastung der Bürgerinnen und Bürger sowie der Unternehmen durch die Vereinfachung und nutzerfreundlichere Gestaltung nicht zu Defiziten beim Schutz der personenbezogenen Daten führt.

Im Rahmen der Umsetzung des OZG plant die Bundesregierung unter Federführung des Bundesministeriums des Innern, für Bau und Heimat den Betrieb eines eigenen Portals mit der Bezeichnung „Bundesportal“. Eine erste Version dieses Portals wurde unter hohem Zeitdruck noch im Berichtszeitraum in Betrieb genommen. Dabei kam es teilweise zu sehr kurzen Fristen für die Prüfung der vorgelegten Dokumente, die daher von mir noch nicht abgeschlossen werden konnte. Hier wünsche ich mir, dass ich so frühzeitig eingebunden werde, dass ich meine Aufgaben mit der gebotenen Sorgfalt erfüllen kann.

Ich empfehle, den Bürgerinnen und Bürgern im Zusammenhang mit Diensten nach dem Onlinezugangsgesetz eine nutzerfreundliche Möglichkeit einzuräumen, um die stattfindenden Datenverarbeitungsprozesse nachvollziehen und kontrollieren zu können.

8.3 Unverschlüsselter E-Mail-Versand

Die sichere Verarbeitung personenbezogener Daten ist eine Grundvoraussetzung. Selbst mögliche Einwilligungen betroffener Personen zum unverschlüsselten E-Mail-Versand können Verantwortliche daher nicht von ihrer Pflicht entbinden, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbefugter Offenbarung zu treffen.

Der Umgang mit Daten muss sowohl in der analogen Welt als auch der digitalen Welt sicher gestaltet werden. Meine Prüfungspraxis und die Beschwerden von Bürgerinnen und Bürgern zeigen mir aber, dass der Datenschutz leidet, weil hier unterschiedliche Standards verwendet werden. So versenden verschiedene öffentliche Stellen und Unternehmen per unverschlüsselter E-Mail auch sensible Daten der Bürgerinnen und Bürger. Besonders kritisch ist dies zu bewerten, wenn diese Praxis gemäß Art. 9 DSGVO besonders zu schützende Gesundheitsdaten betrifft. Die fehlende Vertraulichkeit einer unverschlüsselten E-Mail-Kommunikation ist allseits bekannt. Unverschlüsselte E-Mails entsprechen im Hinblick auf den Schutz der Vertraulichkeit in der analogen Welt einem Versand per Postkarte. Wer Informationen also beim Postversand nicht per Postkarte, sondern nur in einem verschlossenen Umschlag verschickt, sollte sie beim elektronischen Versand auch in einer verschlüsselten E-Mail versenden.

Verschlüsselung als „geeignete technische Maßnahme“!

Gem. Art. 5 Abs. 1 lit. f DSGVO sind personenbezogene Daten so zu verarbeiten, dass eine angemessene Sicherheit dieser Daten gewährleistet ist. Das umfasst den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung sowie unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“). Welche technischen und organisatorischen Maßnahmen im Einzelnen getroffen werden müssen, hängt dabei vom Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen ab. Je sensibler die Daten (als besonders sensibel gelten die in Art. 9 DSGVO genannten besonderen Kategorien von personenbezogenen Daten, wie etwa Gesundheitsdaten), desto höher sind die Anforderungen an die zu treffenden Schutzmaßnahmen.

Zwar muss nicht zwangsläufig jede Übermittlung personenbezogener Daten auf elektronischem Wege per Ende-zu-Ende verschlüsselter E-Mail erfolgen. Dieses Verfahren ist eine mögliche - bei Datenübermittlungen sogar wesentliche - Maßnahme, um ein angemessenes Schutzniveau zu gewährleisten. Eine andere Möglichkeit ist beispielsweise der E-Mail-Versand von Dokumenten in passwortgeschützten Archiven. Dabei ist aber darauf zu achten, dass die verwendete Verschlüsselungstechnik ausreichend sicher ist und entsprechend sichere Passwörter verwendet werden. Das zum Entschlüsseln notwendige Passwort muss zudem auf sichere Art und Weise übermittelt werden. Das setzt in der Regel einen separaten Kommunikationsweg voraus. Eine unverschlüsselte E-Mail und erst recht der Text der E-Mail selbst, an die das verschlüsselte Archiv angehängt ist, gewährleisten keinerlei Sicherheit. Im geeigneten Kontext kann auch mittels lückenloser Verschlüsselung des Transportweges ein angemessenes Schutzniveau erreicht werden. Ein Online-Abruf von schützenswerten Daten über eine verschlüsselte Verbindung ermöglicht für Absender und Empfänger ein bekanntes und praktikables Verfahren. Die notwendigen Zugangsmerkmale (Login, Passwort) sind, wie bereits zuvor beschrieben, über einen anderen und sicheren Kommunikationsweg zu übermitteln. In vielen Fällen ist die Sicherheit von E-Mails besonders gering, da sie vielfach nicht einmal mit einer Transportverschlüsselung über das Internet versandt werden. Dies wäre technisch umsetzbar, wurde jedoch von einigen Providern in den letzten Jahren nicht verfolgt. Innerhalb der deutschen Netzlandschaft besteht daher ein Nachholbedarf.

Da das Schutzniveau auch nach der Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen zu bestimmen ist, sind in Ausnahmefällen sogar Fallkonstellationen denkbar, in denen eine unverschlüsselte Kommunikation per E-Mail zulässig ist. Das gilt beispielsweise für elektronische Benachrichtigungen durch eine unverschlüsselte E-Mail über die Bereitstellung von sensiblen Daten in einer geschützten Umgebung (z. B. über Login und Passwort zu einem bestehenden Account).

Im Bewusstsein der Gefahren für die Vertraulichkeit der Übermittlung wird daher vielfach versucht, über Zustimmungen/Einwilligungen der betroffenen Personen diese Art der „unverschlossenen" Datenübermittlung faktisch zu legitimieren.

Zwar sieht die DSGVO als mögliche Rechtsgrundlage einer datenschutzkonformen Datenverarbeitung eine Einwilligung vor. Diese kann sich nach Art. 6 Abs. 1 DSGVO aber nur auf die Zulässigkeit der Verarbeitung personenbezogener Daten, nicht hingegen auf die gesetzliche Verpflichtung zur Einhaltung der notwendigen technischen und organisatorischen Maßnahmen durch Verantwortliche beziehen. Es wäre ein Verstoß gegen das Rechtsstaatsgebot des Art. 20 Abs. 3 GG, wenn öffentlichen Stellen erlaubt würde, auf die Einhaltung gesetzlicher Verpflichtungen aufgrund einer „freiwilligen" Entscheidung des Betroffenen zu verzichten.

Zudem ist fraglich, ob das Merkmal einer freiwilligen Einwilligung überhaupt vorliegt, wenn eine Behörde von einer Bürgerin oder einem Bürger verlangt, einer bestimmten Datenverarbeitungsweise die Einwilligung zu erteilen.

Ich halte eine solche Einwilligung weder für freiwillig erteilt noch für datenschutzkonform. Sie kann in keinem Fall die unverschlüsselte Übermittlung personenbezogener Daten legitimieren.

Absenkung des Datenschutzniveaus per Gesetz?

Trotz meiner im Rahmen des Gesetzgebungsverfahrens zum Ausdruck gebrachten Bedenken wurde die Abgabenordnung mit Wirkung zum 18. Dezember 2019 dahingehend geändert, es Finanzbehörden zu gestatten, auch Daten, die dem Steuergeheimnis unterliegen, per unverschlüsselter E-Mail an Bürgerinnen oder Bürgern zu übermitteln. Voraussetzung hierfür soll die Einwilligung aller betroffenen Personen sein.

In Stellungnahmen an die Bundesregierung und den Finanzausschuss habe ich darauf hingewiesen, dass diese Regelung gegen europarechtliche Vorgaben verstoßen würde, weil die DSGVO im Hinblick auf die Sicherheit der Verarbeitung keine nationalen Ausnahmen zulässt.

Ich empfehle den öffentlichen Stellen des Bundes, personenbezogene Daten grundsätzlich nur verschlüsselt per E-Mail zu versenden.

8.4 Datenmissbrauch in der Jobbörse der Bundesagentur für Arbeit

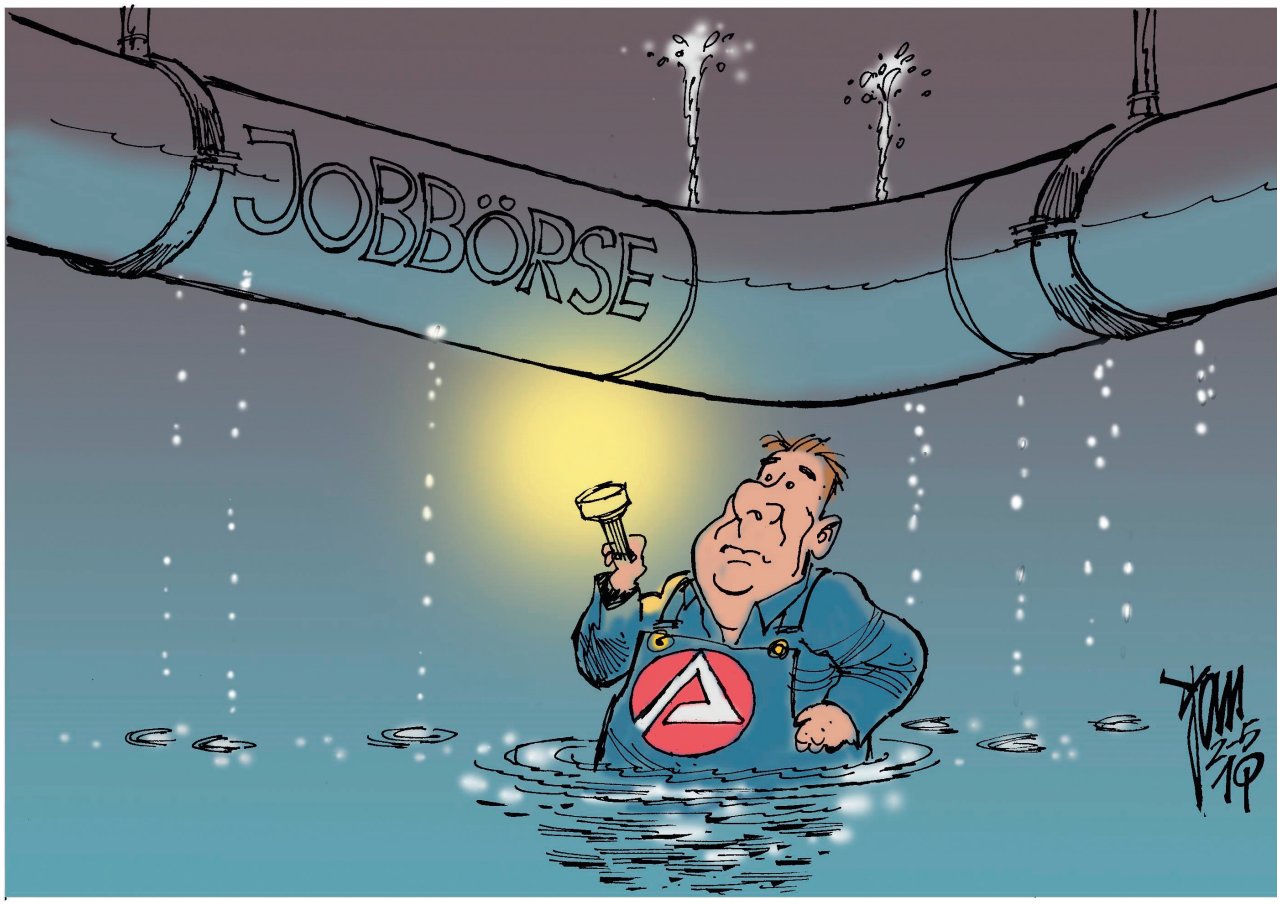
In der Jobbörse der Bundesagentur für Arbeit können auch private Arbeitsvermittler freie Stellen anbieten. Es muss allerdings eine tatsächlich zu besetzende Stelle geben. Ein allgemeines Stellenangebot zum Erhalt von Bewerberdaten und zum Aufbau eines Bewerberpools ist nicht zulässig. Dies ist aber im Berichtszeitraum durch missbräuchliche Nutzung der Jobbörse geschehen.

Durch einen Bericht des Südwestrundfunk (SWR) vom 2. Mai 2019 wurde ich darüber informiert, dass die Jobbörse durch mehrere „private Arbeitsvermittler" missbraucht wurde, um an Bewerberdaten der Nutzer der Jobbörse zu gelangen. Hierzu wurden in großem Maße Stellenangebote veröffentlicht, denen keine tatsächlich zu besetzende Stelle zugrunde lag. Haben sich betroffene Personen mit ihren Unterlagen hierauf beworben, wurden sie im weiteren Verlauf durch den „privaten Arbeitsvermittler" angeschrieben und um Einwilligung zur Weitergabe ihrer Daten an andere potentielle Arbeitgeber gebeten. Nach erfolgter Einwilligung wurden die Daten an Dritte verkauft.

Nach Bekanntwerden der Vorwürfe und eigener Sachverhaltsermittlung hat die Bundesagentur für Arbeit 46 verdächtige „Arbeitgeber-Accounts" deaktiviert. Darüber hinaus haben sowohl die Bundesagentur für Arbeit als auch ich Strafanzeige gegen einen der missbräuchlich handelnden „privaten Arbeitsvermittler" gestellt.

Darüber hinaus hat die Bundesagentur in Abstimmung mit mir Maßnahmen ergriffen, um die Daten der Nutzer besser zu schützen. Seit Mitte August 2019 ist nun die Jobbörse so konfiguriert, dass Anzeigen privater Vermittler nur noch bei zielgerichteter Aktivierung durch die jeweiligen Nutzerinnen und Nutzer angezeigt werden. Diese sehen zudem neuerdings, ob ein Stellenangebot von der Bundesagentur für Arbeit unterstützt wird.

Alle in die Jobbörse eingestellten Stellenangebote werden automatisiert überprüft. Der dabei eingesetzte Algorithmus berücksichtigt bereits das identifizierte missbräuchliche Handlungsmuster und wird stetig weiterentwickelt. Zehn Prozent der Stellenangebote werden zusätzlich manuell geprüft. Der Zugang zur Jobbörse ist nun für Arbeitgeber/Stellenanbieter schwieriger geworden. Mittlerweile ist nicht nur eine Betriebsnummer zur Nutzung erforderlich, sondern die Bundesagentur für Arbeit kann noch weitere Unterlagen von Unternehmen anfordern, die die Jobbörse nutzen möchten.



EIN LECK, EIN LECK, EIN DATENLECK! ERST EINS, DANN ZWEI, DANN…

Die Jobbörse der Bundesagentur für Arbeit soll den Arbeitssuchenden und den Arbeitgebern auf möglichst einfachem Weg eine Stellen- und Mitarbeitersuche ermöglichen. Es liegt nicht im Interesse der Nutzerinnen und Nutzer, wenn sich Betriebe aufgrund hoher bürokratischer Hürden und aufwendiger Authentifizierungsverfahren gegen eine Stellenausschreibung in der Jobbörse entscheiden und damit weniger Stellen angeboten werden. Selbstverständlich muss die Bundesagentur für Arbeit alle Möglichkeiten ausschöpfen, die Daten der Nutzer der Jobbörse zu schützen. Hierbei werde ich die Bundesagentur für Arbeit auch weiterhin unterstützen. Allerdings sollten alle Betroffenen bei der Verarbeitung ihrer Daten wachsam sein. Sobald weitere Einwilligungen gefordert werden oder eine nicht nachvollziehbare Weitergabe der Daten an Dritte ansteht, sollten sich betroffene Personen unmittelbar an die Bundesagentur für Arbeit wenden. Diese prüft entsprechende Verdachtsfälle und löscht die Arbeitgeber-Accounts, die gegen die Nutzungsbedingungen der Jobbörse verstoßen.

8.5 Ausländer- und Asylrecht

Auch in diesem Berichtszeitraum gab es wieder zahlreiche Änderungen auf diesem Rechtsgebiet. Ich habe in den Ressortberatungen und im Rahmen einer Anhörung vor dem Bundestagsausschuss für Inneres und Heimat Stellung genommen.

Unter den zahlreichen Gesetzgebungsverfahren ist das Zweite Datenaustauschverbesserungsgesetz von besonderer Bedeutung. Ich habe hierzu in einer öffentlichen Anhörung des Ausschusses für Inneres und Heimat eine kritische Position bezogen. Eine weitere schriftliche Stellungnahme hat auch die Datenschutzkonferenz des Bundes und der Länder gegenüber dem Ausschuss abgegeben.

Mit dem Gesetz wurden erneut die Möglichkeiten zum Datenabruf aus dem Ausländerzentralregister (AZR) erweitert. Kritisch sehe ich in diesem Zusammenhang beispielsweise den erweiterten Datenabrufmöglichkeiten durch das Zollkriminalamt. Die Notwendigkeit eines

Zugriffs auf diese Daten im Zusammenhang mit der Zollfahndung kann ich nicht hinreichend erkennen. Zudem wurde u. a. mit der Polizei beim Deutschen Bundestag eine weitere Behörde zum automatisierten Abruf aus dem AZR berechtigt. Die Notwendigkeit für diese Form der Auskunft aus dem Register sehe ich nach wie vor nicht. Als besonders kritisch habe ich erneut die weitere Ausweitung der Nutzung der AZR-Nummer zur eindeutigen Zuordnung von Datensätzen bewertet. Auf der Grundlage dieser Ausweitung sehe ich die Gefahr der unzulässigen Bildung eines einheitlichen Personenkennzeichens.

Im parlamentarischen Verfahren wurde als Ausgleich für die Vereinfachung der Zugriffsmöglichkeiten auf das AZR die Pflicht zur Erstellung eines Berechtigungskonzepts durch die abrufenden Stellen in das AZR-Gesetz eingefügt. Von der Umsetzung dieser Verpflichtung werde ich mich bei künftigen Kontrollen der zum Abruf berechtigten Stellen überzeugen.

Die Zahl der Beschwerden auf dem Gebiet des Ausländer- und Asylrechts verbleibt auf einem relativ niedrigen Niveau. Zumeist begehren die Bürgerinnen und Bürger, die sich an mich wenden, Unterstützung im Zusammenhang mit einer teilweise verweigerten Auskunft aus dem AZR. Als Ursachen für die vergleichsweise geringen Zahlen kommen wohl unzureichende Bekanntheit der bestehenden Beschwerdemöglichkeiten und vor allem die verbreitete Unsicherheit bei der Beschreitung dieses Weges in Betracht. Vorhandene Missstände werden teilweise jedoch nur auf diesem Weg erkannt und können erst dann behoben werden. Meine Mitarbeiterinnen und Mitarbeiter haben daher auf einer Veranstaltung von Flüchtlingsverbänden hierauf hingewiesen und für die verstärkte Einbindung der Datenschutzaufsichtsbehörden bei Problemen geworben.

8.6 Facebook-Fanpages

Mehrere Gerichtsurteile verdeutlichen, dass ein datenschutzkonformer Betrieb sogenannter Facebook-Fanpages derzeit nicht möglich ist.

Fanpages erfreuen sich bei Unternehmen und Bundesbehörden weiterhin großer Beliebtheit. Den meisten Betreibern dürfte aber inzwischen klar sein, dass sie durch den Betrieb einer Fanpage Facebook viele Daten ihrer Besucher zuliefern. Um welche Daten es sich dabei genau handelt und was mit ihnen passiert, ist nur schwer herauszufinden.

Die DSK hat im April 2019 die „Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit“ beschlossen. Darin wird erneut dargelegt, dass die bislang von Facebook zur Verfügung gestellten Informationen nicht ausreichen. Fanpagebetreiber stehen datenschutzrechtlich in einer gemeinsamen Verantwortung mit Facebook und haben daher nach der DSGVO eine Rechenschaftspflicht gegenüber den Nutzerinnen und Nutzern. Dieser Verantwortung können sie ohne nähere Informationen von Facebook nicht nachkommen. Ein datenschutzkonformer Betrieb ist so nicht möglich. Mit mehreren Rundschreiben habe ich die Unternehmen und Bundesbehörden, die meiner Aufsicht unterstehen, auf diese Rechtslage hingewiesen und sie aufgefordert, die notwendigen Informationen bei Facebook einzufordern.

Ende Oktober 2019 hat Facebook schließlich neue Informationen zur Datenverarbeitung im Internet veröffentlicht. Diese Informationen werden derzeit in den Gremien der DSK ausgewertet.

Die Bundesbehörden sehe ich in einer Vorbildfunktion, sich datenschutzkonform zu verhalten. Für die Bundesregierung hat das Bundespresseamt stellvertretend die Kommunikation mit Facebook übernommen und mir mitgeteilt, dass mehrere Gespräche mit Facebook stattfanden. Das Ergebnis ist allerdings ernüchternd: auch das Bundespresseamt als Vertreter der Bundesregierung erhielt von Facebook lediglich Anfang November die allgemeinen im Internet zugänglichen Informationen. Durch diese Haltung von Facebook bleibt das Problem auf der Tagesordnung.

Die DSK wird beraten, wie künftig einheitlich vorgegangen werden kann. In jedem Fall sehen sich die Aufsichtsbehörden durch das Urteil des Bundesverwaltungsgerichts vom 11. September 2019 (Az. 6 C 15.18) gestärkt. Das Gericht hat bestätigt, dass die deutschen Aufsichtsbehörden unmittelbar gegen Fanpagebetreiber vorgehen und damit auch den Betrieb einer Fanpage untersagen dürfen. Die Behörden müssen insbesondere nicht eine Entscheidung der federführend zuständigen irischen Datenschutzbehörde abwarten.

Ich habe auch den Austausch mit anderen europäischen Aufsichtsbehörden zum Thema intensiviert, um eine möglichst einheitliche Aufsichtspraxis in der EU zu gewährleisten.

8.7 Datenschutz im Kraftfahrzeug

Weiterentwicklungen der Digitalisierung bis hin zum automatisierten und autonomen Fahren bringen nicht nur technische, sondern auch datenschutzrechtliche Herausforderungen.

Die an der Entwicklung automatisierter und vernetzter Autos beteiligten Unternehmen versprechen, den Straßenverkehr sicherer zu machen und den Fahrkomfort zu erhöhen. Die Einhaltung dieser Versprechen darf aber die persönlichen Rechte und Freiheiten von Haltern, Fahrern und Beifahrern in Bezug auf ihre dabei erhobenen personenbezogenen Daten nicht unzulässig einschränken.

Position der Datenschutzkonferenz

Nach Auffassung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder sind im Prozess der technischen Entwicklung der neuen Fahrzeuge insbesondere folgende Punkte zu beachten:

- Alle beim Betrieb von Fahrzeugen anfallenden Daten werden durch den individuellen Gebrauch des Fahrzeugs beeinflusst und sind deshalb personenbezogen. Es gibt keine Daten, die von vornherein datenschutzrechtlich irrelevant sind.
- Die Automobilindustrie trägt die Verantwortung dafür, ihre Produkte datenschutzgerecht zu gestalten. Sie ist auch gehalten, entsprechend auf Zulieferer und Anbieter von Zusatzdiensten einzuwirken, die die technische Autoinfrastruktur nutzen. Sie hat insbesondere die datenschutzrechtlichen Grundsätze von Privacy by Design und Privacy by Default zu beachten.
- Die Nutzerinnen und Nutzer der Fahrzeuge haben einen Anspruch auf umfassende Transparenz über die im Fahrzeug stattfindenden Datenerhebungs- und -verarbeitungsvorgänge.
- Datensicherheit und Datenintegrität müssen durch geeignete technische und organisatorische Maßnahmen nach dem aktuellen Stand der Technik sichergestellt werden. Dies betrifft insbesondere die Datenkommunikation aus dem Fahrzeug heraus.
- Die Verarbeitung personenbezogener Daten muss wann immer möglich im Fahrzeug selbst erfolgen. Bei vernetzten Fahrzeugen darf ein Zugriff auf Fahrzeugdaten und im Fahrzeug generierte Daten nur unter der vollständigen Kontrolle der Betroffenen stattfinden.

Dialog mit dem Verband der Automobilindustrie

Die Datenschutzbehörden von Bund und Ländern führen seit Dezember 2014 einen stetigen Dialog mit dem Verband der Automobilindustrie (VDA). Am 26. Januar 2016 erzielten beide Seiten ein wichtiges Ergebnis zu den datenschutzrechtlichen Aspekten bei der Nutzung von Kraftfahrzeugen (abrufbar unter www.bfdi.bund.de/entschließungen). Damit bekennen sich die durch den VDA vertretenen Hersteller und Zulieferer zu den Grundsätzen des Datenschutzes. Sie erkennen insbesondere an, dass Fahrzeugdaten immer 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 bei der Bewältigung der zunehmenden und vielfältigen Datenströmen nachkommen. Ich werde auch sehr genau darauf achten, ob die Fahrzeugdaten tatsächlich nur mit Einwilligung der Halter und gegebenenfalls auch der Insassen des Fahrzeugs erhoben und verarbeitet werden. Derartige Daten können beispielsweise weitreichende Aufschlüsse über das Fahrverhalten der Fahrzeugnutzer geben. Die Hoheit über die Fahrzeugdaten muss daher vollständig in deren Händen verbleiben.

Im Berichtszeitraum habe ich gegenüber dem VDA insbesondere die für die Entwicklung des automatisierten und autonomen Fahrens erforderliche Verarbeitung von Video- und Audiosignalen in der Umgebung eines Fahrzeugs angesprochen. Hierbei spielen selbstlernende Systeme eine Rolle, die mit großen Mengen an Echtdaten (Video- und Audiodaten) trainiert werden müssen, damit die Systeme in allen Verkehrssituationen hinreichend sicher agieren können. Das hat zur Konsequenz, dass es zur Vermeidung von Gefahren für Leib und Leben bei der Entwicklung des autonomen und hochautomatisierten Fahrens auf der Basis selbstlernender Systeme technisch bedingt erforderlich sein kann, große Mengen an Video- und Audiodaten zu verarbeiten. Zusammen mit meinen Kolleginnen und Kollegen aus den Ländern setzte ich mich im Rahmen des Dialogs mit dem VDA dafür ein, dass bei der Entwicklung des hochautomatisierten und autonomen Fahrens die datenschutzrechtlichen Vorgaben eingehalten werden. Die bisherigen Gespräche mit den Herstellern zu diesem Thema verlaufen konstruktiv. Wir arbeiten gegenwärtig an einer gemeinsamen Erklärung, in der die datenschutzrechtlichen Vorgaben und Leitlinien festgeschrieben werden.

Automatisiertes und vernetztes Fahren

Mit der zunehmenden Digitalisierung im Automobil- und Verkehrssektor werden Cybersicherheit und Datenschutz auch in diesen Bereichen immer bedeutsamer. So berate ich den vom BMVI eingerichteten „Runden Tisch Automatisiertes und Vernetztes Fahren", der Industrie, Wissenschaft, Versicherer und Verbraucherschützer an einem Tisch versammelt. Hier werden Antworten auf Fragen formuliert, die sich durch technische Entwicklungen ergeben und die automatisierte sowie vernetzte Fahrsysteme möglich machen sollen. Schon jetzt zeichnet sich ab, dass solche Systeme die Erhebung und Verarbeitung einer derzeit noch nicht überschaubaren Anzahl an personenbezogenen Daten notwendig machen werden. Die dafür erforderlichen Vorkehrungen sind in rechtlicher und technischer Hinsicht frühzeitig zu entwickeln, insbesondere auch unter Berücksichtigung der datenschutzrechtlichen Vorgabe von Privacy by Design. Hier hat die Bundesregierung im Energiebereich mit dem Gesetz zur Digitalisierung der Energiewende Maßstäbe festgelegt, die auch im Automobil- und Verkehrssektor zur Anwendung kommen sollten. Ein Beispiel dafür ist der Einsatz obligatorisch sicherheitszertifizierter Kommunikationskomponenten, mit denen der Stand der Technik zum Schutz vor Cyberangriffen und unkontrollierten Datenabflüssen verbessert wird. Auch vernetzte Fahrzeuge sollten nur über solche Komponenten mit anderen Fahrzeugen, den Backend-Systemen der Hersteller oder Dritten kommunizieren können. Diese sollen nach dem Vorbild des Smart-Meter-Gateways für die Energiewirtschaft in einer fahrzeugtechnischen Vorschrift festgelegten Mindestanforderungen an die Cybersicherheit und den Datenschutz erfüllen. In diesem Zusammenhang unterstütze ich ausdrücklich die Bestrebungen der Europäischen Kommission, einen diskriminierungsfreien Zugriff auf Fahrzeugdaten und im Fahrzeug generierte Daten über eine sichere Telematikplattform im Fahrzeug, etwa nach dem Vorbild von Smart-Meter-Gateways, zum Standard zu machen.

Car-to-Car-Kommunikation

Ein wesentlicher Aspekt des künftigen Individualverkehrs betrifft die sogenannte Car-to-Car-Kommunikation. Es handelt sich hierbei um eine Technologie, die es Fahrzeugen ermöglicht, über spezielle Funkverbindungen Fahr- und Umgebungsdaten auszutauschen, um sich z. B. gegenseitig vor Gefahrenstellen zu warnen oder selbstständig Kollisionen in Kreuzungsbereichen zu vermeiden. Nach den mir vorliegenden Informationen sehe ich die Gefahr, dass bei der Entwicklung der Kommunikationsstandards und der Festlegung von Art und Umfang der zu übermittelnden Datenkategorien die Grundsätze von Datensparsamkeit und Datenvermeidung nicht ausreichend beachtet werden. Ich kann bislang keine ausreichenden Vorkehrungen dagegen erkennen, dass im Car-to-Car-Netz befindliche Fahrzeuge nicht doch verfolgbar sind und auf Basis der ausgetauschten Fahrdaten keine personenbezogenen Bewegungsprofile erstellt werden können. Auch bei dieser Form der Online-Kommunikation von Fahrzeugen lassen sich Datenschutz- und 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 Kolleginnen und Kollegen habe ich deshalb an die Europäische Kommission appelliert, bei der Regulierung intelligenter Verkehrssysteme den Anforderungen der DSGVO Rechnung zu tragen.

Ausblick

Neuartige Systeme, für deren Funktionalität eine Vielzahl an Daten, die beim Fahrbetrieb entstehen, verarbeitet werden müssen, sind mit Blick auf die Verkehrssicherheit für die auf Mobilität angewiesene Gesellschaft ein Vorteil. Das rechtfertigt aber nicht, datenschutzrechtliche Vorgaben für derartige Systeme zu vernachlässigen. Beide Zielvorgaben sind gleichzeitig erreichbar. Wichtig sind Transparenz, Datensparsamkeit und weitestgehende Erhaltung der Datensouveränität der Betroffenen.

Positiv ist, dass in vielen neu zugelassenen Fahrzeugtypen mit Online-Diensten meine datenschutzrechtlichen Empfehlungen umgesetzt wurden. So können Fahrzeugnutzer 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. Kundinnen und 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 auch daran messen.

Ich empfehle einen diskriminierungsfreien Zugriff auf Fahrzeugdaten und im Fahrzeug generierte Daten über eine sichere Telematikplattform im Fahrzeug, etwa nach dem Vorbild von Smart-Meter-Gateways.

8.8 Datenschutz bei Postdiensten

Der Wandel hin zu digitalisierten Prozessen bei Postdienstleistungen kann nur unter Beachtung datenschutzrechtlicher Vorschriften gelingen. Der nationale Gesetzgeber trägt durch die Anpassung der gesetzlichen Vorgaben zur Rechtsklarheit in dem sich wandelnden Postmarkt bei.

Durch die Verkündung des 2. Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU) Ende November 2019 wurde der Datenschutz bei Postdienstleistungen vom nationalen Gesetzgeber an die Vorgaben der DSGVO angepasst. Ich habe meine Vorschläge im Rahmen des Gesetzgebungsverfahrens eingebracht. Die bis dahin bestehenden bereichsspezifischen Datenschutzregelungen der Postdienste-Datenschutzverordnung wurden, sofern ergänzend zur DSGVO noch erforderlich, in das Postgesetz (PostG) aufgenommen. Dabei blieb das verfassungsrechtlich geschützte Postgeheimnis in § 39 PostG unangetastet.

Betrachtet man den Postmarkt, so setzt sich der Trend hin zu einer Digitalisierung von Prozessen fort. Beispiele sind das Produkt „Digitale Kopie“ der Deutsche Post AG (vgl. 8.8.1) sowie die Steckfolgensortierung zur Effizienzsteigerung in der Zustellung (vgl. 8.8.2).

8.8.1 Digitale Kopie

Briefsendungen werden bei der Deutsche Post AG jetzt auch digital zugestellt. Der hybride Empfang von Nachrichten ist heute grundsätzlich möglich – er muss aber datenschutzrechtlich angemessen gestaltet werden.

Die Deutsche Post AG bietet einen entsprechenden Service unter dem Namen „Digitale Kopie“ an. Großversender wie Banken, Versicherungen oder auch Behörden können auf diese Weise ihre Briefe parallel zur Papiersendung auch elektronisch zur Versendung übermitteln. Die Deutsche Post AG prüft dann, ob diese Sendung per E-POST digital an den Empfänger zugestellt werden kann. Ist der Empfänger registrierter E-POST-Nutzer, wird das Schreiben zugleich elektronisch zugestellt. Ich setze mich seit über anderthalb Jahren dafür ein, dass dieses Verfahren in einem datenschutzrechtlich zulässigen Rahmen erfolgt. Besonderer Fokus liegt dabei auf den technischen und organisatorischen Maßnahmen. Diese müssen gewährleisten, dass digital vorliegende Schreiben mit möglicherweise sensiblen Einzelinformationen ausschließlich zur elektronischen Zustellung genutzt werden.

Bei der „Digitalen Kopie“ handelt es sich wie bei dem Dienst E-POST zunächst um einen Telekommunikationsdienst. Daher sind bei der datenschutzrechtlichen Bewertung die Vorschriften der DSGVO, des Postgesetzes sowie des Telekommunikationsgesetzes zu beachten.

Während der Beratung der Deutsche Post AG habe ich zwar ein grundsätzlich positives Bild gewonnen, doch besteht an verschiedenen Stellen noch datenschutzrechtlicher Anpassungsbedarf. Dazu gehört u. a. die Reduzierung der Speicherdauer von „Digitalen Kopien“ im Verantwortungsbereich der Deutsche Post AG. Diese sollte auf die Dauer begrenzt werden, die zur Erbringung der Dienstleistung wirklich erforderlich ist.

Weitere Nachbesserungen sind zudem im Bereich der technischen und organisatorischen Maßnahmen erforderlich. So darf z. B. ein Zugriff auf die „Digitalen Kopien“ nur in zuvor festgelegten, eng begrenzten Fällen möglich sein. Auch sollte zur Gewährleistung der Vertraulichkeit der Kommunikation und des verfassungsrechtlich geschützten Fernmeldegeheimnisses eine Ende-zu-Ende Verschlüsselung als Standard etabliert werden. Die verschlüsselte Kommunikation ist derzeit lediglich als Zusatzoption vorgesehen.

Auswertung von Sendungsströmen

Die Deutsche Post AG beabsichtigt, im Rahmen ihres Angebots „Digitale Kopie“ Sendungsströme E-POST-fähiger Sendungen auszuwerten, um potentielle neue E-POST-Kunden auszumachen und anschließend anzuwerben. Dazu wurden zunächst alle Haushalte in Mikrozellen aufgeteilt – durchschnittlich befinden sich 6,6 Haushalte in einer Mikrozelle. Auf Ebene dieser Mikrozellen sollen E-POST-fähige Briefsendungen (oder: Sendungsströme) gezählt werden. Bei Erreichen einer bestimmten Sendungsmenge sollen die in dieser Mikrozelle befindlichen Haushalte mit Werbeschreiben angesprochen werden. An der rechtlichen Zulässigkeit dieser Verarbeitung auf Grundlage eines berechtigten Interesses der Deutsche Post AG bestehen erhebliche Zweifel. Die Deutsche Post AG hat aufgrund meiner Bedenken bisher auf eine Durchführung dieser Zählung von Sendungen verzichtet.

8.8.2 Steckfolgensortierung zur Zustellverbesserung

Briefsendungen werden längst größtenteils von Maschinen sortiert. Neu ist dabei allerdings, dass die maschinengestützte Sortierung auch die Position des Briefkastens innerhalb einer Briefkastenanlage berücksichtigt.

Große Briefkastenanlagen mit vielen einzelnen Briefkästen stellen Zustellkräfte in der Praxis vor erhebliche Herausforderungen. Die teilweise unübersichtliche und uneinheitliche Anordnung von Briefkästen erfordert einen genauen Abgleich von Namen, um Falschzustellungen zu vermeiden , die auch selbst datenschutzrechtlich problematisch sein können. Dies ist nicht nur zeitintensiv, sondern auch mühsam – insbesondere für Zustellkräfte, die mit den örtlichen Gegebenheiten nicht vertraut sind.

Um den Anteil an Fehleinwürfen so gering wie möglich zu halten und die Zustellkräfte zu unterstützen, hat die Deutsche Post AG – zunächst pilotweise – die Position der Briefkästen innerhalb einer Anlage (z. B. dritter Kasten in Reihe vier) erfasst, um diese anschließend

mit dem Namen und der Adresse der dort wohnhaften Personen zu verknüpfen. Diese Informationen ermöglichen im weiteren Verlauf eine sogenannte Steckfolgensortierung, wonach die Briefsendungen in der Tasche des Zustellers bereits auf die Reihenfolge der Briefkästen in der Briefkastenanlage angepasst sind.

Die Verarbeitung berücksichtigt zuerst die berechtigten Interessen des Postdienstleisters. Natürliche Personen, deren „Briefkasten-Daten" erfasst wurden, wurden im Rahmen der Informationspflichten der DSGVO schriftlich informiert. Sofern Betroffene mit der Verarbeitung nicht einverstanden sind, steht ihnen ein Recht auf Widerspruch gegen die Verarbeitung zu.

Das Projekt wurde mir von der Deutsche Post AG frühzeitig vorgestellt, sodass ich bereits am Anfang Verbesserungsbedarf aufzeigen konnte. So konnte ich Einfluss nehmen auf die Auswahl der korrekten Rechtsgrundlage, essentielle Aspekte der technischen und organisatorischen Maßnahmen, die Ausgestaltung der Information an die Betroffenen sowie auf den Umgang mit den Rechten der Betroffenen. Bis zur Ausweitung des Pilotprojekts wurden meine Anregungen von der Deutsche Post AG aufgenommen und umgesetzt.

8.9 Datenschutzbehörden legen Bußgeldkonzept vor

Die DSK hat ein gemeinsames Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen veröffentlicht, das einerseits die Schwere des Verstoßes und zum anderen die Größe des Unternehmens berücksichtigt, damit Geldbußen wirksam, verhältnismäßig und abschreckend sind. Zugleich arbeiten die deutschen Datenschutzbehörden mit den europäischen Aufsichtsbehörden an europaweiten Leitlinien.

DSGVO läutet neues Zeitalter ein

Die DSGVO sieht erstmals europaweit einheitliche Abhilfebefugnisse vor. Dabei fügt sich die Bußgeldbefugnis in ein Gesamtsystem an differenzierten Abhilfemaßnahmen der Datenschutzbehörden zur Rechtsdurchsetzung ein. Diese reichen von bloßen Warnungen und Verwarnungen über Anordnungen bis hin zur Verhängung von Geldbußen. Die Datenschutzbehörden können im Rahmen ihres Ermessens zwischen verschiedenen Abhilfemaßnahmen wählen oder mehrere kumulativ anwenden.

Nach Art. 58 Abs. 2 lit. i i. V. m. Art. 83 Abs. 4 bis 6 DSGVO sind für formelle Verstöße Geldbußen von bis zu 10.000.000 Euro oder zwei Prozent des weltweiten Jahresgesamtumsatzes des vorangegangenen Geschäftsjahres und für materielle Verstöße bis zu 20.000.000 Euro oder vier Prozent des weltweiten Jahresgesamtumsatzes des vorangegangenen Geschäftsjahres möglich. Abweichend von der bisherigen deutschen Rechtstradition gilt dabei die darüber hinausgehende, europäische unmittelbare Verbandshaftung innerhalb eines Konzerns. Damit hat die EU den Verstößen gegen das europäische Datenschutzrecht die gleiche Bedeutung und Tragweite zuerkannt wie für Verstöße gegen das europäische Wettbewerbsrecht.

Europäische Prinzipien und Leitlinien

Für eine effektive Anwendungspraxis hat der europäische Gesetzgeber den Datenschutzbehörden drei aus dem Wettbewerbsrecht bekannte Sanktionsprinzipien verbindlich ins Durchsetzungsprogramm geschrieben: Wirksamkeit, Verhältnismäßigkeit und Abschreckung. Zusätzlich sieht Art. 83 Abs. 2 DSGVO eine Reihe von Ermessenserwägungen vor, die die Datenschutzbehörden sowohl bei der Frage des „Ob" als auch des „Wie hoch" prüfen müssen.

Um eine europaweit einheitliche Anwendung zu gewährleisten, wurde der EDSA in Art. 70 Abs. 1 lit. k DSGVO mit der Aufgabe betraut, anhand dieser Prinzipien Leitlinien für die Festsetzung von Geldbußen nach Art. 83 DSGVO zu entwickeln. Einen ersten Schritt hierzu verwirklichte der EDSA in seiner ersten Plenarsitzung am 25. Mai 2018, in welcher er die Leitlinien für die Anwendung und Festsetzung von Geldbußen bestätigte, die seine Vorgängerin, die Artikel-29-Gruppe, bereits mit Blick auf die DSGVO vorbereitet hatte. Diese Leitlinien vom 03. Oktober 2017 (zu finden unter: http://www.bfdi.bund.de/guidelines) legen zunächst eine einheitliche Auslegung der Bestimmungen von Art. 83 DSGVO fest und umreißen ein einheitliches Konzept zu den Grundsätzen bei der Bußgeldfestsetzung. So wurde unter anderem klargestellt, dass für den Begriff des Unternehmens entsprechend Erwägungsgrund 150 auf den Unternehmensbegriff der Art. 101 und 102 AEUV abzustellen ist. Der Begriff des Unternehmens umfasst demnach jede Einrichtung, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung. Diese kann aus mehreren natürlichen oder juristischen Personen bestehen – eine wesentliche Neuerung zur vormaligen deutschen Rechtstradition.

Die Konkretisierung der Festsetzungsmethodik bzgl. der zu erhebenden Bußgelder bleibt späteren Leitlinien des EDSA vorbehalten, die derzeit beraten werden.

Deutsches Bußgeldkonzept

Um in der Übergangszeit bis zum Erlass entsprechender Leitlinien eine einheitliche Anwendung innerhalb Deutschlands sicherzustellen, hat die DSK ein gemeinsames Konzept zur Bußgeldzumessung in Verfahren

gegen Unternehmen erarbeitet, das am 16. Oktober 2019 veröffentlicht wurde (zu finden unter: www.bfdi.bund.de/beschlüsse-positionspapiere). Es entfaltet keine Bindungswirkung in sogenannten grenzüberschreitenden Fällen, da hier eine Abstimmung mit den europäischen Aufsichtsbehörden erforderlich ist und das deutsche Bußgeldkonzept für diese keine verbindliche Anwendung finden kann, sondern ist ausdrücklich auf sogenannte inländische Fälle beschränkt.

Mit ihrem Konzept passen die Datenschutzbehörden ihre Aufsichtspraxis zugleich an die gesetzgeberische Entscheidung eines im Vergleich zur alten Rechtslage erhöhten Bußgeldrahmens an. Dabei haben die Datenschutzbehörden unter anderem den besonderen wirtschaftlichen Situationen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen (KMU) Rechnung getragen, um sie nicht den gleichen Bußgeldhöhen auszusetzen wie große Unternehmen. Vereine und natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit sind zudem von dem Konzept ausgeschlossen.

Das Konzept sieht eine Bußgeldzumessung in Verfahren gegen Unternehmen in fünf Schritten vor, in denen zunächst unternehmensgrößenabhängig ein Grundbetrag ermittelt (Schritte 1 bis 3) wird, der sodann aufgrund tat- und täterbezogener sowie sonstiger Umstände (Schritte 4 und 5) des Einzelfalls angepasst wird. Im letzten Schritt können auch Besonderheiten des Unternehmens ggf. mindernd berücksichtigt werden, wie z. B. drohende Insolvenz oder ein hoher Umsatz aber eine geringe Gewinnmarge, sofern die Umsatzhöhe nicht auf einem datengetriebenen Geschäftsmodell beruht.

Im schrittweisen Verfahren sind alle Ermessensfaktoren des Art. 83 Abs. 2 DSGVO durch die Datenschutzbehörden zu berücksichtigen. Das Konzept kombiniert – unter Anwendung aller Faktoren des Art. 83 Abs. 2 DSGVO – dabei letztlich zwei wesentliche Gesichtspunkte: zum einen die Schwere des Verstoßes und zum anderen die Größe des Unternehmens. So wird sichergestellt, dass die Geldbuße im Hinblick auf den konkreten Verstoß und gegenüber dem Unternehmen angemessen ist. In Kombination werden so die vom Gesetzgeber vorgegebenen Sanktionsprinzipien der Wirksamkeit, Verhältnismäßigkeit und Abschreckung verwirklicht. Die Datenschutzbehörden werden regelmäßig evaluieren, ob das Konzept diese Prinzipien in der Anwendungspraxis effektiv erreicht oder ob das europäische Effektivitätsgebot (effet utile) eine Nachbesserung erfordert.

Fazit und Ausblick

Das gemeinsame Konzept der DSK zur Bußgeldzumessung in Verfahren gegen Unternehmen zeigt, wie auch in einem föderalen Aufsichtssystem eine einheitliche Anwendung und Durchsetzung des Datenschutzrechts gelingen kann. Das Konzept ist ein erster wichtiger Baustein für eine gemeinsame und einheitliche Rechtsdurchsetzungsstrategie, die jedoch dringend um weitere Bausteine ergänzt werden muss. Insbesondere ist eine gemeinsame Rechtsdurchsetzungsstrategie gerade auch mit Blick auf die anderen möglichen Abhilfebefugnisse gefragt, die bereits jetzt anstelle oder zusätzlich zu Geldbußen angewendet werden und eine kohärente Anwendung erfordern.

Deutsche Unternehmen, Datenschutzbehörden und Gerichte müssen sich auf das neue europäische Sanktionsregime einstellen. Das deutsche Bußgeldkonzept ist ein erster Schritt in diese Richtung. Die europaweite Harmonisierung erfordert eine möglichst rasche Verabschiedung europäischer Leitlinien.

8.10 Akkreditierungsverfahren können starten

Die DSGVO sieht vor, dass die Einhaltung ihrer Vorgaben über Datenschutzzertifizierungen nachgewiesen werden kann. Damit diese Zertifikate auch tatsächlich für eine entsprechende Güte stehen, sieht Art. 43 DSGVO die Akkreditierung von Zertifizierungsstellen vor.

Die DSGVO ermöglicht eine freiwillige Überprüfung der Einhaltung ihrer Vorgaben, die in einem Zertifikat bzw. einem Datenschutzsiegel münden kann. Sie gibt dafür einen grundsätzlichen rechtlichen Rahmen in den Art. 42 und 43 vor. Diese Bestimmungen sollen die Transparenz erhöhen und die Einhaltung der datenschutzrechtlichen Vorgaben verbessern. Jedoch dürfen nur solche Stellen Zertifizierungen gemäß Art. 42 DSGVO erteilen, die auf ihre Eignung zur Durchführung von Zertifizierungsverfahren überprüft und förmlich akkreditiert worden sind. Dieses Verfahren ist eine wesentliche Grundlage für einen gestärkten europaweit einheitlichen Datenschutz. Die konkrete Ausgestaltung des Akkreditierungsverfahrens mit seinen in der DSGVO eher allgemein skizzierten Regelungen obliegt den Mitgliedsstaaten. Auf diese Weise soll den nationalen Besonderheiten Raum gegeben werden. Deutschland hat mit der Regelung von § 39 BDSG hiervon Gebrauch gemacht.

Nationale Umsetzung

Um einen möglichst hohen Qualitätsstandard für die Zertifizierung sicherzustellen, sieht die DSGVO in Art. 43 zunächst eine Akkreditierung von Zertifizierungsstellen vor, die dem Zweck der Konformitätsprüfung dient. Für die Datenschutzaufsichtsbehörden, die in diesem Akkreditierungsprozess eine wichtige Rolle spielen, hat sich damit ein neuer Aufgabenbereich ergeben. Nach § 39 BDSG erfolgt die Entscheidung, ob jemand

als Zertifizierungsstelle agieren darf, durch die jeweils zuständige Datenschutzaufsichtsbehörde auf Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS). Detailregelungen dazu enthält das Akkreditierungsstellengesetz (AkkStelleG). Dort ist etwa festlegt, dass stets die sogenannte „befugniserteilende" Datenschutzaufsichtsbehörde gemeinsam mit der DAkkS das jeweilige Akkreditierungsverfahren bearbeitet. Bei der Durchführung des Akkreditierungsprozesses im Bereich Datenschutz sind sechs Phasen vorgesehen:

1. Antragsphase – Programmprüfung
2. Programmprüfung und Genehmigung der Kriterien
3. Antragsphase Akkreditierung/Befugniserteilung
4. Begutachtungsphase
5. Akkreditierungsphase/Befugniserteilung
6. Überwachungsphase

Die Datenschutzaufsichtsbehörden des Bundes und der Länder befassen sich im Rahmen der nationalen Gremien derzeit intensiv mit der Umsetzung der Vorgaben der DSGVO in das nationale Akkreditierungsverfahren. Sie haben u. a. ein Konzept entwickelt, das ergänzende Anforderungen zur DIN EN ISO/IEC 17065 enthält. Diese Norm wird explizit in der DSGVO erwähnt. Sie befasst sich bereits detailliert mit Fragen der Konformitätsbewertung und wird durch das Papier der Aufsichtsbehörden um datenschutzspezifische Aspekte bei den Anforderungen an Strukturen, Ressourcen und Prozesse oder etwa an das Managementsystem der zu akkreditierenden Stellen, ergänzt (https://www.datenschutzkonferenz-online.de/anwendungshinweise.html). Aktuell werden hier letzte Anpassungen im Rahmen der Datenschutzkonferenz, dem Gremium der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), vorgenommen. Anschließend durchläuft das Papier noch die erforderlichen Genehmigungsprozesse auf europäischer Ebene.

Darüber hinaus wurde auf der nationalen Ebene z. B. auch eine Vereinbarung zwischen den Datenschutzaufsichtsbehörden des Bundes und der Länder und der DAkkS über die Akkreditierungsaufgaben geschlossen, die klare Regelungen im Hinblick auf die Zuständigkeiten und Verantwortlichkeiten enthält und so letztlich die Vorgaben aus BDSG und AkkStelleG konkretisiert. Dies ist nur ein Beispiel, das zeigt, in welchem Ausmaß und Detailgrad die neue Aufgabe der datenschutzrechtlichen Akkreditierung Regelungen und Absprachen auf der nationalen Ebene erfordert. Die Verhandlungen zwischen den beteiligten Akteuren und die Ausarbeitung der einzelnen Verfahrensschritte hat mehr Zeit in Anspruch genommen, als ursprünglich erwartet. Auch auf der europäischen Ebene sind Anpassungen erforderlich, für die es bisher keine Erfahrungswerte gibt.

Der Europäische Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) hat im vergangenen Jahr Leitlinien mit Hinweisen veröffentlicht, welche Aspekte innerhalb des Akkreditierungsverfahrens besonders zu berücksichtigen sind (die Leitlinie vom 14. Dezember 2018 finden Sie unter: http://www.bfdi.bund.de/guidelines). Ergänzend hierzu arbeiten die Gremien auf europäischer Ebene auch an einer konkreten Ausgestaltung entsprechender Verfahren zur Umsetzung der Akkreditierungs- und Zertifizierungsmechanismen innerhalb der Strukturen des EDSA.

Der EDSA muss künftig etwa gewährleisten, dass er Stellungnahmen zu Entwürfen der Aufsichtsbehörden der Mitgliedstaaten abgeben kann, die sich darauf beziehen, Anforderungen für die Akkreditierung einer Zertifizierung gem. Art. 43 Abs. 3 DSGVO zu erlassen oder die in Art. 42 Abs. 5 DSGVO genannten Zertifizierungskriterien zu genehmigen (Art. 64 Abs. 1 lit. c DSGVO). Außerdem besteht gem. Art. 42 Abs. 5 DSGVO (Art. 70 Abs. 1 lit. o DSGVO) die Erfordernis, EU-weite Zertifizierungskriterien zu genehmigen, die die Voraussetzung für ein europäisches Datenschutzsiegel bilden können. Konsistente Verfahren auf der europäischen Ebene sind eine unerlässliche Voraussetzung dafür, dass die Mitgliedstaaten ihre Aktivitäten im Zusammenhang mit der nationalen und EU-weiten Zertifizierung aufnehmen können. Der größte Teil der Prozessschritte wurde zwischenzeitlich im Plenum des EDSA verabschiedet, weitere Details werden nach und nach konkretisiert und verabschiedet.

Erste Akkreditierungsverfahren starten 2020

Die neue Aufgabe der Akkreditierung bringt für alle beteiligten Akteure eine Vielzahl an neuen Herausforderungen mit sich. Die Festlegung entsprechender Verfahren und Prozesse wurde – sowohl auf europäischer als auch auf nationaler Ebene – intensiv diskutiert. 2020 laufen jetzt die ersten Akkreditierungsverfahren an.

Mein Ziel war und ist es, durch ein belastbares, transparentes und zuverlässiges Akkreditierungsverfahren dazu beizutragen, dass Datenschutzzertifizierungen glaubhaft sind. Denn nur so können sie sich zu einem wichtigen Vertrauensanker entwickeln, der echte Mehrwerte schafft.

Produkte und Dienstleistungen mit Datenschutzzertifizierung werden es vor allem kleineren Unternehmen erleichtern sicherzustellen, datenschutzkonform zu handeln.

8.11 Datenschutzberatung bei der IT-Konsolidierung Bund

Das Projekt „IT-Konsolidierung Bund“ hat zum Ziel, die digitale Arbeitsfähigkeit der Bundesregierung für die nächsten Jahre sicherzustellen und einen effizienten Betrieb zu gewährleisten. Die Einhaltung des Datenschutzes ist dabei eine grundlegende Anforderung. Daher berate ich einzelne Teilprojekte der IT-Konsolidierung Bund.

Am 6. November 2019 hat das Bundeskabinett die Neuorganisation der IT-Konsolidierung Bund verabschiedet. Zukünftig wird die Betriebskonsolidierung vom Bundesministerium der Finanzen (BMF) verantwortet, während die Dienstekonsolidierung beim BMI verbleibt. Eine weitere Änderung im Dienstleisterverbund führte dazu, dass viele Teilprojekte der IT-Konsolidierung verzögert wurden.

Nach wie vor bezieht sich meine Beratungsaufgabe im Projekt hauptsächlich auf das Teilprojekt 6 „Dienstekonsolidierung“. Dieses Teilprojekt beinhaltet mehrere Maßnahmen wie den „Bundesclient“, die „Bundescloud“, das „Identity and Access Management“ und den „multifunktionalen elektronischen Dienstausweis“. Auch die Maßnahme „Identity and Access Management“ konnte aufgrund der Änderung im Dienstleisterverbund nicht fortgesetzt werden, wodurch sich die Maßnahmen „Bundescloud“ und „Bundesclient“ verzögerten.

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 und stellt für einige Pilotbehörden bereits Dienste bereit. Derzeitige Aufgabe ist die Zulassung der Bearbeitung von VS-NfD-Dokumenten in der Bundescloud. Es wird zu meinen fortlaufenden Aufgaben gehören, zu oben genannten Themen und dem in der Bundescloud betriebenem Dienste-Portfolio zu beraten.

Bei der Maßnahme „Bundesclient“ geht es um die Bereitstellung bundesweit einheitlicher Arbeitsplätze bis Ende 2025 mit standardisiertem Betriebssystem sowie Basis- und Querschnittsdiensten, wie z. B. E-Mail und Anwendungen zur Dokumentenbearbeitung. Derzeit wird der Bundesclient durch das ITZ Bund getestet. Diese Tests begleite ich entsprechend, um Fragen zum Datenschutz zu beantworten.

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.

Zusammenfassend nehme ich eine gute Zusammenarbeit mit allen Beteiligten, einschließlich dem IT-Dienstleister des Bundes, wahr, sodass ich meiner Aufgabe, die Einhaltung des Datenschutzes bei der Umsetzung der IT-Konsolidierung Bund zu überwachen und die beteiligten Akteure zu beraten, nachkommen kann.

8.12 Datenschutz bei Windows 10

Die Übermittlung von Telemetriedaten von Windows 10 Betriebssystemen an Microsoft stellt ein datenschutzrechtliches Problem für alle beaufsichtigten Stellen dar. Insbesondere im Bereich der öffentlichen Verwaltung ist es deshalb wichtig, die „Digitale Souveränität“ zu stärken, um bei Hard- und Software-Plattformen nicht von einzelnen Herstellern abhängig zu sein.

Ende 2018 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Ergebnisse der sogenannten SiSyPHuS-Studie zu Windows 10. Hierbei wurde vor allem untersucht, inwieweit sogenannte „Telemetriedaten“ des Betriebssystems über das Internet an Microsoft übermittelt werden.

Anfang des Jahres erhielt ich zudem die Ergebnisse einer Untersuchung der Verbindungen zwischen vorhandenen Windows 10 Clients in den Netzwerken der Bundesverwaltung und Telemetrie-Servern bei Microsoft, die ergeben hatte, dass im Zeitraum von Oktober 2018 bis Januar 2019 Datenübertragungen in signifikantem Umfang stattgefunden haben.

Grundlage für die Telemetriedatenverarbeitung ist die Erhebung von Daten in Form von Systemereignissen, wie das Drücken einer Taste oder das Auslösen eines Druckauftrags. Diese Systemereignisse werden mit Nutzeridentifikatoren versehen, die es Microsoft ermöglichen, einen individuellen Nutzer auf einem individuellen Gerät und dessen Nutzungsmuster (wieder) zu erkennen. Diese Markierung (und damit der Personenbezug) erfolgt immer, d. h. in jeder Version von Windows 10 und in jedem Telemetrielevel (Einstellung zu Umfang der übertragenen Daten). Welche dieser markierten Ereignisse durch sogenannte Messpunkte gesammelt und zu Microsoft übertragen werden, hängt grundsätzlich vom Telemetrielevel ab. Allerdings gibt es einen weiteren wichtigen Faktor: das Nutzerverhalten. Denn die Telemetrie wird über eine Konfigurationsdatei gesteuert, die regelmäßig von Microsoft aktualisiert wird und in Abhängigkeit vom Nutzerverhalten die Messpunkte und somit den Inhalt der Telemetriedaten anpasst.

Durch die „Individualisierung“ der Telemetrie jedes einzelnen Systems ist es nicht möglich, allgemeingültige Aussagen darüber zu treffen, welche Telemetriedaten erhoben und zum Hersteller übertragen werden. Der Test eines einzelnen Systems stellt immer nur eine Momentaufnahme dar. In Abhängigkeit vom Nutzerverhalten kann sich der Umfang der übertragenen Telemetriedaten im nächsten Moment bereits ändern. Was sich ebenfalls nicht „messen“ lässt, ist die sekundäre Telemetrie, bei der Microsoft auf ein Windows 10 System zugreift und Dateien und Funktionen, wie z. B. das Auslesen des Hauptspeichers, ausführt. Bisher ist unklar, welches Nutzerverhalten die Änderungen in der Telemetrie auslöst.

Das hat auch Auswirkungen auf die datenschutzrechtliche Bewertung des Einsatzes von Windows 10. Um eine solche einheitlich vorzunehmen, hat die Datenschutzkonferenz (DSK) eine Arbeitsgruppe eingesetzt, an der ich mich aktiv beteilige. Ziel der Gruppe ist es, eine datenschutzrechtliche Positionierung zu Windows 10 zu erarbeiten, die vor allem Rechtssicherheit für Anwenderinnen und Anwender schaffen soll.

Auch wenn aufgrund der vorab dargestellten technischen Komplexität der Prozesse bei der Verarbeitung von Telemetriedaten bei Redaktionsschluss noch keine abschließende Positionierung vorlag, ist es unstrittig, dass die Telemetriedatenverarbeitung datenschutzrechtlich kritisch zu sehen ist. Fraglich ist vor allem, auf welcher Rechtsgrundlage die Verarbeitung personenbezogener Daten durch Microsoft im vorliegenden Fall gestützt werden kann.

Die von Microsoft in der Datenschutzerklärung angegebenen Zwecke der Telemetriedatenverarbeitung können nach meinem Verständnis auch mit Daten ohne Personenbezug erfüllt werden. Demnach wäre der Personenbezug zur Wahrung der Interessen von Microsoft grundsätzlich nicht erforderlich. Daher habe ich Microsoft vorgeschlagen, den Personenbezug zu entfernen, indem statt Nutzeridentifikatoren z. B. Zufallszahlen verwendet werden; eine Variante die bereits andere Anbieter vergleichbarer Produkte anwenden. Microsoft hat zugesagt, den Vorschlag zu prüfen.

Eine Lösung für einen datenschutzkonformen Betrieb von Windows 10 scheint die Trennung des Betriebssystemsfunktionen vom Internet zu sein, wie sie künftig im Rahmen des Bundesclients in der Bundesverwaltung umgesetzt werden soll. Das funktioniert allerdings nur, solange Windows 10 als eine lokal auf dem Arbeitsplatz zu betreibende Lösung genutzt werden kann. Sollte Microsoft, wie bereits angekündigt, Windows nur noch als Cloud-Service anbieten, würde diese Lösung ausscheiden.

Als eine Handreichung für all diejenigen, die mit Windows 10 (auch) personenbezogene Daten verarbeiten wollen, hat die Arbeitsgruppe der DSK ein Prüfschema entwickelt. Das Prüfschema vom 7. November 2019 finden Sie unter: https://www.bfdi.bund.de/beschlüsse-positionspapiere.

Bei einem Test von Windows 10, den im Dezember das Bayerische Landesamt für Datenschutzaufsicht zusammen mit Microsoft im Beisein von Mitarbeitern meiner Behörde durchgeführt hatte, wurde auf einem System über ein Skript (Invoke-UserSimulator) Nutzeraktivität erzeugt und der Netzwerkverkehr aufgezeichnet. Dabei wurde keine Telemetriedatenübermittlung festgestellt. Dieses Vorgehen stellt allerdings nur eine Momentaufnahme dar, da sich in Abhängigkeit vom Nutzerverhalten der Umfang der übertragenen Telemetriedaten im nächsten Moment bereits ändern könnte. Aus diesem Grund sind weitere Untersuchungen des BSI, deren Ergebnisse bei Redaktionsschluss noch nicht vorlagen, abzuwarten. Nur so können die Zusagen von Microsoft, durch Änderungen an Windows 10 sicherzustellen, dass nur für den Betrieb notwendige Daten übertragen werden und alle übertragenen Daten für den Anwender ersichtlich sind, überprüft werden.

Ich werde aber auf jeden Fall weiterhin mit Microsoft im Gespräch bleiben – allein in diesem Jahr habe ich mehrere Gespräche mit Vertretern von Microsoft geführt – um eine Lösung zu finden, die für alle Seiten tragbar ist.

Stärkung der Digitalen Souveränität

Die Problematik bei Windows 10 zeigt, wie wichtig es ist, bei der Wahl von Hard- und Software-Plattformen über Alternativen zu verfügen. Aus diesem Grund begrüße ich die Initiative der Bundesregierung zur Digitalen Souveränität. Im Rahmen dieses Vorhabens wollen Bund, Länder und Kommunen gemeinsam Maßnahmen ergreifen, um die Abhängigkeit von einzelnen Herstellern kontinuierlich zu reduzieren. Nur so ist es möglich, nachhaltig Produkte zu beschaffen, die die Anforderungen an Sicherheit und Datenschutz erfüllen. Bis dahin muss darauf hingearbeitet werden, Fachanwendungen von Hardware- und Software-Plattformen zu entkoppeln, in dem diese z. B. Standardschnittstellen zu Datenbanken verwenden. Ich werde dieses Thema in den entsprechenden Gremien verstärkt ansprechen.

9 BfDI intern

9.1 Personelle Entwicklung und Hausorganisation

Die Bewilligung weiterer Planstellen stärkt die Beratungs-, Kontroll- und Kooperationsmöglichkeiten. Die Erfüllung stetig wachsender Aufgaben sowie der damit einhergehende Personalzuwachs hat die Neuausrichtung der Organisationsstruktur meiner Dienststelle erforderlich gemacht.

Seit der Selbständigkeit des BfDI am1. Januar 2016 hat sich die Personalsituation der Dienststelle deutlich verbessert. Bis zum Jahr 2019 konnte ich einen Stellenzuwachs auf insgesamt 253,5 Planstellen verzeichnen. Neben der Einrichtung der notwendigen Behördenstrukturen waren diese Stellen unter anderem für die Erledigung der zusätzlich – insbesondere durch die DSGVO – übertragenen Aufgaben (z. B. Justitiariat, Bußgeldstelle, Zentrale Anlaufstelle, Datenschutzaufsicht über die Finanzbehörden, kommunale Steuerämter und Jobcenter) sowie als Reaktion auf geänderte Verfahrensweisen (z. B. förmliches Beschwerdeverfahren, Vertretung im europäischen Datenschutzausschuss) notwendig.

Für das Jahr 2020 hat der Haushaltsgesetzgeber weitere 67 Planstellen zugesprochen. Ein großer Teil der Planstellen wird dabei für die Datenschutzaufsicht über die Sicherheitsbehörden eingesetzt, um die vom Bundesverfassungsgericht geforderte Kompensation sicherzustellen. Zusätzlich erhält der BfDI 4,4 Planstellen von der Bundesnetzagentur (BNetzA) nach § 50 BHO. Diese stehen im Zusammenhang mit der Verschiebung datenschutzrechtlicher Zuständigkeiten von der BNetzA auf den BfDI, über die im 27. TB (Nr. 15.1.4) berichtet wurde.

Diese fortschreitende positive Entwicklung begrüße ich sehr, da sie die Möglichkeiten zur Beratung der beaufsichtigten Stellen, des Bundestages und der Öffentlichkeit stärkt, eine bessere Kontrolle gewährleistet und Ressourcen für verstärkte internationale Kooperation und damit Harmonisierung beim Datenschutz schafft.

Der schnelle personelle Aufwuchs und neue Aufgaben machten eine Neuausrichtung der organisatorischen Strukturen meiner Dienststelle erforderlich. Diese wurde mit Wirkung zum 1. August 2019 vollzogen. Es wurden zwei neue Referatsgruppen eingerichtet und die bisher noch als Arbeitsgruppen geführten Organisationseinheiten in eigenständige Referate umgewandelt.

Die Referatsgruppe „Zentrale Aufgaben“, die sich in vier Referate gliedert, nimmt alle Verwaltungsaufgaben für die Dienststelle wie Personalangelegenheiten, Organisation, Haushalt, Innerer Dienst, Beschaffungen sowie die Betreuung der Informations- und Kommunikationstechnik gebündelt wahr.

Zudem machte der stetige Aufgabenzuwachs im Sicherheitsbereich die Einrichtung einer eigenen Referatsgruppe „Polizei und Nachrichtendienste“ mit vier Fachreferaten erforderlich. Der künftig fortschreitende Ausbau der Sicherheitsbehörden und die vom Bundesverfassungsgericht im Gegenzug als Kompensation geforderte Schaffung einer effizienten Datenschutzaufsicht werden auch weiterhin zu einem Aufgaben- und Stellenzuwachs in diesem Bereich führen müssen.

Durch die Neustrukturierung meiner Dienststelle sehe ich den BfDI gut aufgestellt, um auch in Zukunft eine effektive Datenschutzaufsicht sicherstellen zu können.

9.2 Öffentlichkeitsarbeit

Auch im Jahr 2019 blieb der Informationsbedarf der Öffentlichkeit zum Thema DSGVO weiterhin groß. Zudem habe ich ein neues Corporate Design eingeführt. Die Abkehr vom bislang verwendeten Design der Bundesregierung soll die Unabhängigkeit meiner Behörde auch visuell noch einmal unterstreichen.

Corporate Design

Mit der Veröffentlichung meines 27. Tätigkeitsberichts zum Datenschutz habe ich ein neues Corporate Design für meine Behörde eingeführt. Hierdurch wird die Unabhängigkeit meiner Behörde nun auch visuell klarer erkennbar. Die Umstellung sämtlicher Medien meiner Außenkommunikation auf das neue Design konnte im Berichtszeitraum weitgehend abgeschlossen werden. Vor der Neuauflage der Druckpublikationen wurden Restbestände aufgebraucht. Neben der Neuauflage einiger Flyer und Broschüren steht noch ein Relaunch der Website aus, der voraussichtlich im Jahr 2020 abgeschlossen wird.

Veranstaltungen

Im vergangenen Jahr habe ich in Berlin ein Symposium unter dem Titel „Chancen und Risiken für den datenschutzgerechten Einsatz von Künstlicher Intelligenz“ ausgerichtet. Mit dieser Veranstaltung konnte ich mehr als 150 Teilnehmerinnen und Teilnehmer eine Diskussionsplattform zu Datenschutz und Künstlicher Intelligenz bieten. Außerdem konnte ich gemeinsam mit dem Europäischen Datenschutzbeauftragten über 300 Gäste bei unserer Podiumsdiskussion über die Herausforderungen für Datenschutz und Wettbewerbsfähigkeit im digitalen Zeitalter begrüßen. Vergleichbare Veranstaltungen sind auch für die Zukunft geplant.

Besuchergruppen

Meine Mitarbeiterinnen und Mitarbeiter betreuten im Jahr 2019 insgesamt 15 Besuchergruppen mit bis zu 50 Teilnehmerinnen und Teilnehmern. Zwölf dieser Besuchergruppen kamen von Mitgliedern des Bundestages.

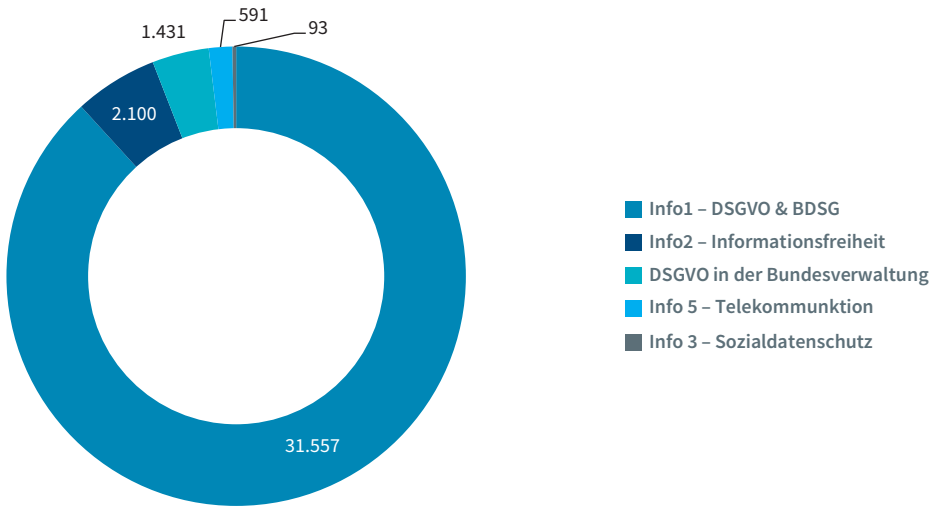
Informationsmaterial

Ein wichtiger Bestandteil meiner Öffentlichkeitsarbeit ist die Veröffentlichung von Flyern und Broschüren. Die Informationsbroschüren wenden sich an Leserinnen und Leser, die sich vertieft mit einem Themengebiet beschäftigen möchten. Die „Info“-Broschüren enthalten neben Beiträgen zur Rechtsmaterie auch die einschlägigen Gesetze. Die knapperen und handlicheren Flyer sollen vor allem Bürgerinnen und Bürger ansprechen. Diese Publikationen enthalten kurze Informationen und klare Handreichungen zum Datenschutz.

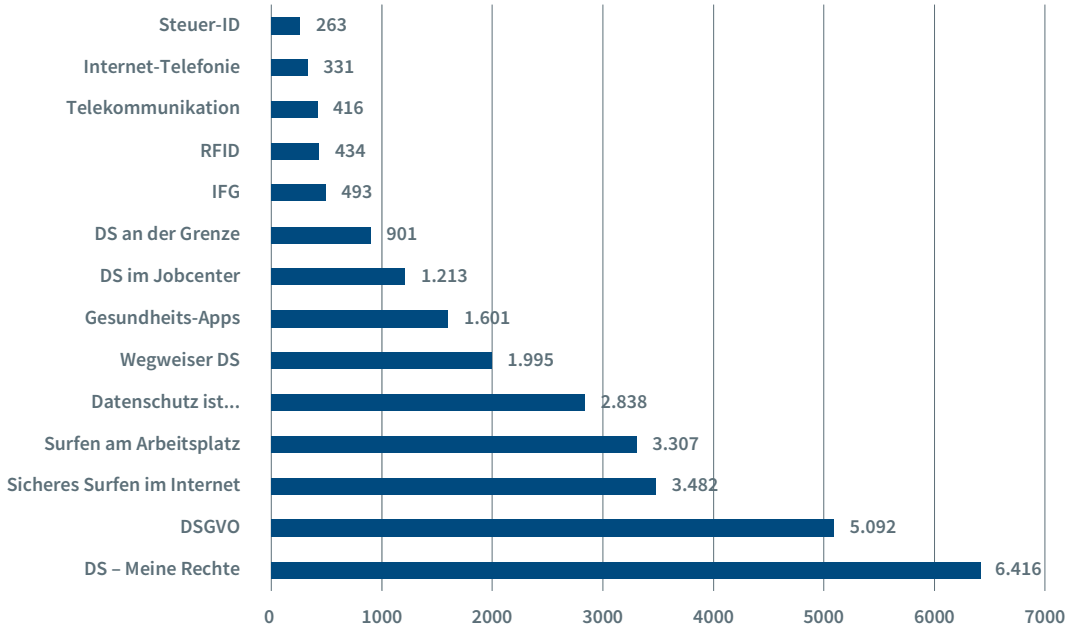
Alle Informationsbroschüren erfreuen sich großer Beliebtheit (siehe Grafiken).

Alle aktuellen Publikationen können unter www.bfdi.bund.de/informationsmaterial bestellt oder als PDF-Dokument heruntergeladen werden.

Abgegebene Broschüren



Abgegebene Flyer



9.3 Die Arbeit des BfDI in Zahlen

Neben meiner Aufgabe als datenschutzrechtliche Aufsichts- und Kontrollinstanz liegt der Schwerpunkt meiner Tätigkeit auf der Beratung von Bürgerinnen und Bürger, dem Deutschen Bundestag und den meiner Aufsicht unterstehenden datenverarbeitenden Stellen. Auch im ersten vollständigen Kalenderjahr unter der DSGVO besteht weiterhin ein großer Bedarf an der Expertise meiner Behörde.

Beschwerden und allgemeine Anfragen

Mich erreichten von Seiten der Bürgerinnen und Bürger viele Beschwerden über Datenschutzverstöße. Eine Anfrage ist dann eine Beschwerde, wenn die betroffene Person annimmt, sie sei bei der Erhebung, Verarbeitung oder Nutzung ihrer persönlichen Daten in ihren Rechten verletzt worden. Das Beschwerderecht ist sowohl in der DSGVO als auch in Spezialgesetzen geregelt.

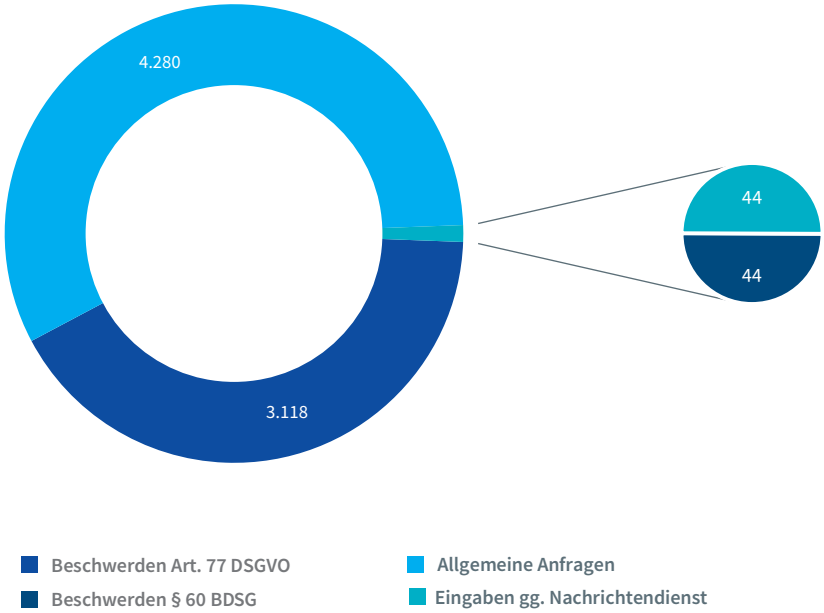
Im Jahr 2019 erreichten mich 3.118 Beschwerden nach Art. 77 DSGVO (Recht auf Beschwerde bei einer Aufsichtsbehörde). Darüber hinaus verzeichnete ich 44 Beschwerden nach § 60 BDSG (Anrufung des Bundesbeauftragten) und 44 Eingaben gegen Nachrichtendienste. Ebenso gingen 3 Beschwerden nach Art. 89 DSGVO ein.

Beratung und Kontrolle

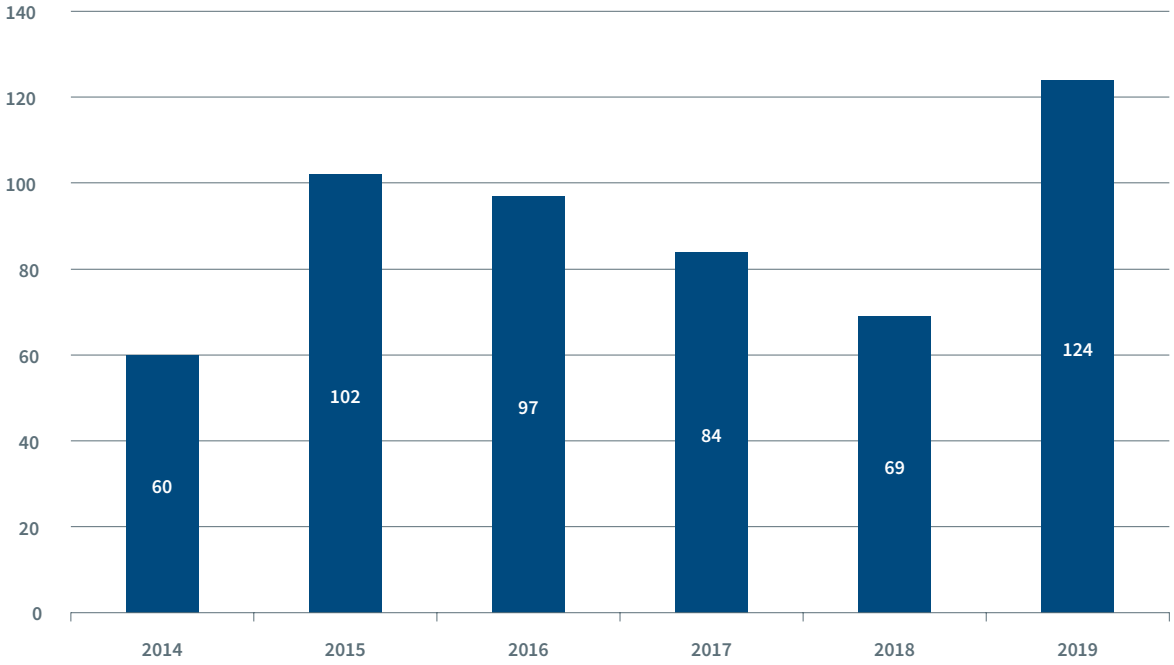
Ein wichtiger Teil meiner Arbeit ist die Beratung von verantwortlichen Stellen und betroffenen Personen. So gingen in meinem Haus 4.280 schriftliche allgemeine Anfragen von Bürgerinnen und Bürgern ein. Darüber hinaus konnte ich in 6.939 Fällen telefonisch beraten.

Bei datenverarbeitenden Stellen meines Zuständigkeitsbereichs habe ich insgesamt 124 Vor-Ort-Termine durchgeführt. Davon waren 51 reine Informations- und Beratungsbesuche. In 73 Fällen waren die Beratungen auch mit einer datenschutzrechtlichen Kontrolle verbunden. Neben diesen Vor-Ort-Terminen haben meine Kolleginnen und Kollegen die meiner Aufsicht unterstehenden Stellen auch wieder regelmäßig schriftlich und telefonisch datenschutzrechtlich beraten.

Beschwerden und Anfragen



Information-, Beratungs- und Kontrollbesuche



Meldungen von Datenschutzverletzungen

Sämtliche öffentlichen und nicht-öffentlichen Stellen müssen gegenüber der zuständigen Aufsichtsbehörde Datenschutzverletzungen melden. Der BfDI hat im Berichtszeitraum fast 15.000 entsprechende Meldungen erhalten.

Meldungen von Datenschutzverstößen	2019
Art. 33 DSGVO	14.649
§ 65 BDSG	0
§ 109 a Absatz 1 TKG	40

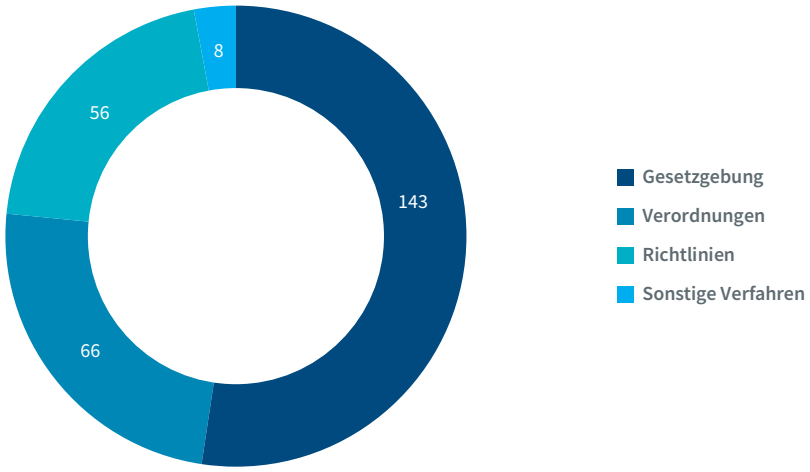
Abhilfemaßnahmen

Im Berichtszeitraum habe ich sechs Verwarnungen nach Art. 58 DSGVO und acht Beanstandungen nach § 16 BDSG ausgesprochen. Außerdem habe ich zwei Geldbußen gemäß Art. 83 DSGVO verhängt.

Förmliche Begleitung bei 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 143 Gesetzgebungsverfahren, 66 Verordnungsverfahren und 56 Richtlinien sowie acht übrige Vorhaben, bei denen ich nach § 21 GGO einzubinden war, geprüft und begleitet.

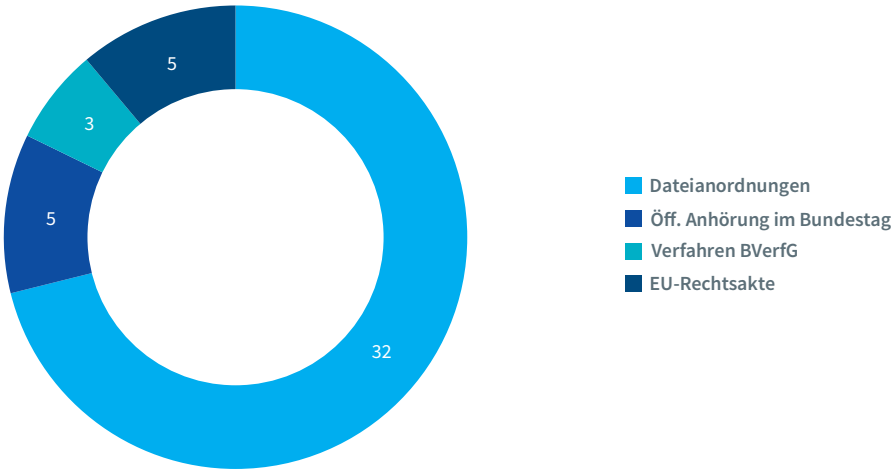
Beteiligungen nach § 21 GGO



Weitere Verfahren mit Beteiligung des BfDI

Darüber hinaus habe ich zu 32 Dateianordnungen, drei Verfahren des Bundesverfassungsgerichts und fünf EU-Rechtsakten Stellung genommen. Außerdem habe ich bei fünf öffentlichen Anhörungen im Deutschen Bundestag meine Expertise einbringen können.

Weitere Verfahren mit Beteiligung des BfDI



Sonstiges

Im vergangenen Jahr wurden 25 Rechtsbehelfe gegen Entscheidungen des BfDI eingelegt. Von den hieraus resultierenden gerichtlichen Verfahren ergingen erstinstanzlich drei Entscheidungen zu Gunsten meiner Behörde. Diese sind noch nicht rechtskräftig geworden. In drei weiteren Fällen wurden zunächst eingelegte Rechtsbehelfe auf Hinweis der Gerichte von der Gegenseite zurückgenommen. Die übrigen 19 Verfahren waren im Berichtszeitraum noch nicht abgeschlossen.

Querverweis:

10.2 Statistischer Überblick über die Verfahren der Zentralen Anlaufstelle (ZASt)

10 BfDI als Zentrale Anlaufstelle (ZASt)

10.1 Die Zusammenarbeit der nationalen Aufsichtsbehörden zu europäischen Themen

Nach Art. 51 Abs. 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. Die auf Ebene des EDSA vereinbarten Geschäftsprozesse werden von der ZASt auf das föderale deutsche System angepasst.

Das Tagesgeschäft der ZASt besteht aus der Koordinierung des Informationsflusses zwischen den europäischen Aufsichtsbehörden bzw. dem Europäischen Datenschutzausschuss (EDSA) einerseits und den Aufsichtsbehörden des Bundes und der Länder andererseits.

Daneben nimmt die gestaltende Tätigkeit einen vergleichsweise großen Raum ein. Diese Tätigkeit besteht darin, die auf Ebene des EDSA vereinbarten Prozesse zur europäischen Zusammenarbeit auf die föderal geprägte Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Deutschland anzupassen. Trotz der föderal aufgeteilten Datenschutzaufsicht soll die Zusammenarbeit mit den europäischen Aufsichtsbehörden und dem EDSA schnell und effektiv sein.

Die DSGVO regelt lediglich die Grundzüge der europäischen Zusammenarbeit und überlässt die weitere Ausgestaltung dem EDSA. Der EDSA macht hiervon umfänglich Gebrauch mit dem Ziel, die gesetzlichen Verfahren besser handhabbar zu machen. Die innerstaatliche Verwaltungsorganisation verbleibt jedoch bei den Mitgliedstaaten und muss für Deutschland entsprechend realisiert werden. Das Zusammenwirken der Prozesse zur Zusammenarbeit auf europäischer und nationaler Ebene soll anhand zweier Beispiele veranschaulicht werden:

Bevor Aufsichtsbehörden verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCRs) von Unternehmen genehmigen dürfen, müssen sie eine Stellungnahme des EDSA beantragen (Art. 64 Abs. 1 lit. f DSGVO). Das Verfahren nach der DSGVO ist sehr formal und unterliegt engen Entscheidungsfristen. Der Beantragung einer Stellungnahme des EDSA gehen meist mehrere Jahre intensiver Abstimmungsarbeit zwischen dem Unternehmen, der federführenden Aufsichtsbehörde (in der Regel diejenige Aufsichtsbehörde, in deren Land das Unternehmen seinen Hauptsitz in der EU hat) und regelmäßig zwei anderen Aufsichtsbehörden (sog. Co-Prüfer) voraus.

Diese komplexen, iterativen Arbeiten können in dem formellen Verfahren vor dem EDSA nach der DSGVO nicht abgebildet werden. Daher wurde ein informelles Vorverfahren zwischen den Aufsichtsbehörden vor Einholung der Stellungnahme etabliert. In diesem Verfahren werden alle europäischen Aufsichtsbehörden bei der Arbeit an den BCRs eingebunden, so dass etwaige Anmerkungen oder Kommentare der einzelnen Aufsichtsbehörden schon vor der Befassung im EDSA berücksichtigt werden können. Die Aufgabe der ZASt ist es, auf nationaler Ebene die Zusammenarbeit aller deutschen Aufsichtsbehörden zu koordinieren, um eine einheitliche deutsche Auffassung zu den einzelnen BCRs herauszuarbeiten und diese auf internationaler Ebene einzubringen. Die ZASt hat hierfür einen ersten Geschäftsprozess entworfen, der mit den Aufsichtsbehörden des Bundes und der Länder abgestimmt wird.

Die DSGVO enthält zudem nur wenige Vorgaben für Beschlussfassungen des EDSA. Der EDSA hat sich deshalb ergänzende Regelungen in seiner Geschäftsordnung gegeben. Dort ist auch ein schriftliches Abstimmungsverfahren vorgesehen, um gegebenenfalls außerhalb der Sitzungstermine Entscheidungen treffen zu können.

Schriftliche Abstimmungsverfahren werden in der Regel binnen einer Frist von einer Woche durchgeführt. Innerhalb dieser kurz bemessenen Frist muss die ZASt die 18 Aufsichtsbehörden des Bundes und der Länder über das Abstimmungsverfahren informieren und die nationalen Willensbildungsprozesse anstoßen. Auch hier gilt der allgemeine Abstimmungsgrundsatz, dass Deutschland trotz mehrerer Aufsichtsbehörden im EDSA nur mit einer Stimme stimmberechtigt ist. Besteht kein Einvernehmen, ist noch innerhalb der Abstimmungsfrist ein gemeinsamer Standpunkt im „streitigen" Verfahren nach § 18 Abs. 2 BDSG herzustellen, damit Deutschland im EDSA fristgerecht abstimmen kann. Hierzu hat die ZASt bereits einen vorläufigen Geschäftsprozess etabliert, der die Sprechfähigkeit der deutschen Datenschutzaufsicht auf europäischer Ebene absichert.

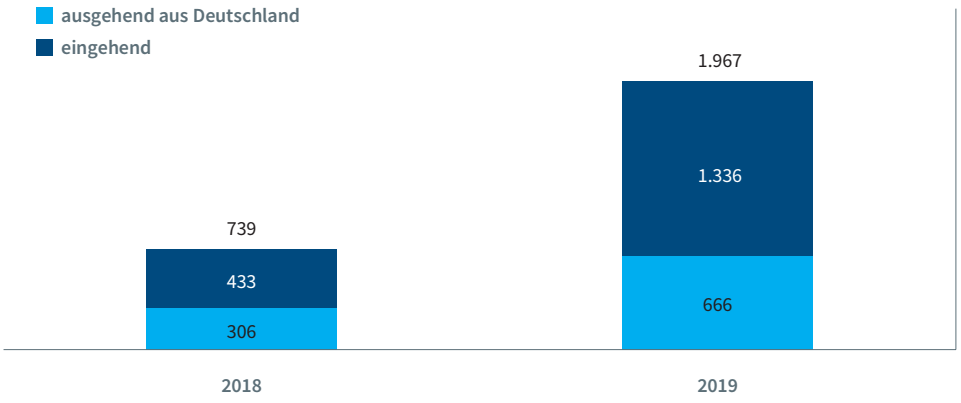
Durch die fortschreitende Abstimmung der europäischen Zusammenarbeit bleiben die Entwicklung und Weiterentwicklung von Prozessen eine Daueraufgabe für die ZASt.

10.2 Statistischer Überblick über die Verfahren der Zusammenarbeit und Kohärenz auf europäischer Ebene aus Sicht der ZASt

Die Zentrale Anlaufstelle (ZASt) als Bindeglied aus und nach Europa ist weiterhin gefordert. Sie koordiniert den Informationsfluss zwischen den europäischen Aufsichtsbehörden bzw. dem Europäischen Datenschutzausschuss (EDSA) einerseits und den Aufsichtsbehörden des Bundes und der Länder andererseits.

Der Koordinationsumfang hat sich im Berichtszeitraum im Gegensatz zum Vorjahr deutlich vervielfacht, wie die Zunahme der einzelnen Verfahren im Binnenmarkt-Informationssystem (IMI) zeigt. Sowohl die Zahl der Verfahren insgesamt als auch die Zahl der Verfahren mit deutscher Beteiligung haben sich von 2018 auf 2019 mehr als verdoppelt:

Verfahren mit deutscher Beteiligung



Wie aus umseitiger Statistik ersichtlich, arbeiten die Aufsichtsbehörden in Europa immer effektiver zusammen. Während im Jahr 2018 noch die initiale Ermittlung der zuständigen/betroffenen Aufsichtsbehörden im Vordergrund stand (Art. 56-Verfahren), startet nun vermehrt die eigentliche Fallbearbeitung. Über informelle Konsultationen nach Art. 60 DSGVO sowie Amtshilfeverfahren nach Art. 61 DSGVO tauschen die Aufsichtsbehörden Informationen zur Fallbearbeitung aus. Ist der Erlass eines Beschlusses (im deutschen Recht Verwaltungsakt) beabsichtigt, wird dieser den betroffenen Aufsichtsbehörden vorab als Entwurf zur Stellungnahme vorgelegt (Art. 60-Verfahren – Entwurf eines Beschlusses/Überarbeiteter Entwurf eines Beschlusses). Nach Erlass wird der Beschluss den anderen Aufsichtsbehörden zur Kenntnis gegeben (Art. 60-Verfahren – Endgültiger Beschluss). Die Zahl der erlassenen endgültigen Beschlüsse ist nicht gleichbedeutend mit der Zahl der insgesamt abgeschlossenen Verfahren, weil viele Verfahren, bei denen kein weiterer Handlungsbedarf besteht, formlos beendet werden können.

Nicht nur die Zusammenarbeit bei der Fallbearbeitung, sondern auch die Arbeit im EDSA haben sich zwischenzeitlich eingespielt. Die Zahl der nach Art. 64 DSGVO ein-

geholten EDSA-Stellungnahmen ging zurück (31 Verfahren vom 25. Mai 2018 bis 31. Dezember 2018 gegenüber 30 im gesamten Jahr 2019), was darin begründet liegt, dass die in der DSGVO vorgesehenen Pflichtaufgaben (z. B. Erlass einer Liste von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist) zu einem großen Teil umgesetzt sind. Der EDSA widmet sich jetzt verstärkt den freiwilligen Aufgaben, insbesondere den Stellungnahmen und Leitlinien (Art. 70 DSGVO), um hier aus eigener Initiative datenschutzrechtliche Akzente zu setzen (vgl. Nr. 3.2.1).

Generell ist der Bedarf an Koordinierung durch die ZASt gestiegen. Dies belegt die Zahl der internen Konsultationen in IMI, die von 43 im Jahr 2018 auf 62 im 2019 zugenommen hat. Interne Konsultationen werden von der ZASt angelegt und dienen der Vorbereitung einer gesamtdeutschen Antwort gegenüber dem EDSA oder anderen an IMI angeschlossenen Aufsichtsbehörden.

Querverweise:

3.2 Europäischer Datenschutzausschuss

Kooperationsverfahren im Berichtsjahr

Verfahren	Insgesamt	Ausgehend von deutschen AB	Anmerkung
Artikel 56 – Identifizierung LSA und CSA	906	261	
Artikel 56 – Local Case Request	5	3	Nur Verfahren mit deutscher Beteiligung
Artikel 60 – Draft Decision	95	20	Nur Verfahren mit deutscher Beteiligung
Artikel 60 – Revised Draft Decision	9	3	Nur Verfahren mit deutscher Beteiligung
Artikel 60 – Final Decision	81	11	Nur Verfahren mit deutscher Beteiligung
Artikel 60 – Informal Consultation	188	29	Nur Verfahren mit deutscher Beteiligung
Artikel 61 – Gegenseitige Amtshilfe	25	17	Nur Anfragen von und nach Deutschland
Artikel 61 – Freiwillige Amtshilfe	601	260	Nur Anfragen von und nach Deutschland
Artikel 64 – Opinion by the EDPB	30	0	Eingang bei ZASt, Verteilung über Interne Konsultation; beinhaltet nur veröffentlichte Verfahren
Artikel 64 – Final EDPB Opinion	0	0	Eingang bei ZASt, Verteilung über Interne Konsultation; Request vom Sekretariat
Interne Konsultation	62		Zentral initiiert durch die ZASt zur nationalen Abstimmung
Gesamt	**2.002**	**666**	

Themenzuordnung nach Bundestagsausschüssen

Ausschuss für Arbeit und Soziales

- 4.3 Datenminimierung
- 4.6 Das Gutachten der Datenethikkommission
- 8.3 Unverschlüsselter E-Mail-Versand
- 8.4 Datenmissbrauch in der Jobbörse der Bundesagentur für Arbeit

Auswärtiger Ausschuss

- 3.3 Datenschutz-Ausschuss des Europarats
- 3.4 Internationale Datenschutzkonferenz
- 8.1.1 Brexit – Folgen für den Datentransfer
- 8.1.3 Entwicklungen beim EU-US Privacy Shield

Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

- 4.2.2 Das Implantateregister
- 4.4 Künstliche Intelligenz
- 4.5.1 Einwilligung in der Forschung
- 4.6 Das Gutachten der Datenethikkommission

Ausschuss für Digitale Agenda

- 3.1 Konferenz der der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)
- 3.2 Europäischer Datenschutzausschuss
- 3.3 Datenschutz-Ausschuss des Europarats
- 3.4 Internationale Datenschutzkonferenz
- 4.1 Evaluierung der Datenschutz-Grundverordnung
- 4.2 Digitalisierung im Gesundheitswesen
- 4.2.1 Die Telematikinfrastruktur mit ihren Anwendungen
- 4.4 Künstliche Intelligenz
- 4.5.2 Tracking und Cookies
- 4.6 Das Gutachten der Datenethikkommission
- 5.1 Das Omnibusgesetz zur Datenschutz-Grundverordnung
- 5.2 Anpassung des Telekommunikationsgesetzes steht aus
- 5.4 Der Zensus 2021
- 5.5 Registermodernisierung in Deutschland
- 6.2 Pilotprojekt zur intelligenten Videoüberwachung am Bahnhof Berlin-Südkreuz
- 7.1 Das Hausausweis- und Zutrittssystem im Deutschen Bundestag
- 8.1.2 Das Schrems II-Verfahren
- 8.2 Das Onlinezugangsgesetz
- 8.3 Unverschlüsselter E-Mail-Versand
- 8.6 Facebook-Fanpages
- 8.7 Datenschutz im Kraftfahrzeug
- 8.8.1 Digitale Kopie
- 8.11 Datenschutzberatung bei der IT-Konsolidierung Bund
- 8.12 Datenschutz bei Windows 10

Ausschuss für Angelegenheiten der Europäischen Union

- 3.2 Europäischer Datenschutzausschuss
- 8.1.3 Entwicklungen beim EU-US Privacy Shield

Ausschuss für Familie, Senioren, Frauen und Jugend

4.6 Das Gutachten der Datenethikkommission

Finanzausschuss

3.1 Konferenz der der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

5.3.3 Darknet

6.7.1 Pflichtkontrollen

8.3 Unverschlüsselter E-Mail-Versand

8.11 Datenschutzberatung bei der IT-Konsolidierung Bund

Ausschuss für Gesundheit

4.2 Digitalisierung im Gesundheitswesen

4.2.1 Die Telematikinfrastruktur mit ihren Anwendungen

4.2.2 Das Implantateregister

4.3 Datenminimierung

4.5.1 Einwilligung in der Forschung

5.6 Gesetzgebung im Gesundheits- und Sozialwesen

8.3 Unverschlüsselter E-Mail-Versand

Haushaltsausschuss

8.11 Datenschutzberatung bei der IT-Konsolidierung Bund

9.1 Personelle Entwicklung und Hausorganisation

Ausschuss für Inneres und Heimat

3.1 Konferenz der der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

3.2 Europäischer Datenschutzausschuss

4.1 Evaluierung der Datenschutz-Grundverordnung

4.6 Das Gutachten der Datenethikkommission

5.1 Das Omnibusgesetz zur Datenschutz-Grundverordnung

5.3.3 Darknet

5.4 Der Zensus 2021

5.5 Registermodernisierung in Deutschland

6.1.1 CLOUD Act

6.1.2 Die e-Evidence-Verordnung

6.1.3 Cybercrime-Konvention

6.2 Pilotprojekt zur intelligenten Videoüberwachung am Bahnhof Berlin-Südkreuz

6.3 Polizei 2020

6.4 Speicherung von Fluggastdaten

6.5 Abfragen beim Bundesamt für Verfassungsschutz vor Vergabe von öffentlicher Förderung

6.6 Beratungs- und Informationsbesuche beim Bundesnachrichtendienst

6.7.1 Pflichtkontrollen

6.7.2 Quellen-Telekommunikationsüberwachung beim BKA

6.7.3 Das Vorgangsbearbeitungssystem beim BKA

6.7.4 Datenschutz bei Sicherheitsüberprüfungen

6.7.5 Fragmentierung der Aufsichtslandschaft über die Nachrichtendienste

8.1.2 Das Schrems II-Verfahren

8.2 Das Onlinezugangsgesetz

8.5 Ausländer- und Asylrecht

8.7 Datenschutz im Kraftfahrzeug

8.9 Datenschutzbehörden legen Bußgeldkonzept vor

8.11 Datenschutzberatung bei der IT-Konsolidierung Bund

8.12 Datenschutz bei Windows 10

Ausschuss für Recht und Verbraucherschutz

3.1 Konferenz der der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

4.1 Evaluierung der Datenschutz-Grundverordnung

4.3 Datenminimierung

4.4 Künstliche Intelligenz

4.6 Das Gutachten der Datenethikkommission

5.1 Das Omnibusgesetz zur Datenschutz-Grundverordnung

5.2 Anpassung des Telekommunikationsgesetzes steht aus

5.3.3 Darknet

5.4 Der Zensus 2021

6.1.1 CLOUD Act

6.1.2 Die e-Evidence-Verordnung

6.1.3 Cybercrime-Konvention

8.3 Unverschlüsselter E-Mail-Versand

Ausschuss für Verkehr und digitale Infrastruktur

4.4 Künstliche Intelligenz

8.7 Datenschutz im Kraftfahrzeug

Ausschuss für Wirtschaft und Energie

3.1 Konferenz der der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

4.4 Künstliche Intelligenz

4.5.2 Tracking und Cookies

4.6 Das Gutachten der Datenethikkommission

5.1 Das Omnibusgesetz zur Datenschutz-Grundverordnung

5.2 Anpassung des Telekommunikationsgesetzes steht aus

8.1.1 Brexit – Folgen für den Datentransfer

8.1.2 Das Schrems II-Verfahren

8.1.3 Entwicklungen beim EU-US Privacy Shield

8.6 Facebook-Fanpages

8.8.1 Digitale Kopie

8.8.2 Steckfolgensortierung zur Zustellverbesserung

8.9 Datenschutzbehörden legen Bußgeldkonzept vor

8.10 Akkreditierungsverfahren können starten

Ältestenrat

7.1 Das Hausausweis- und Zutrittssystem im Deutschen Bundestag

7.2 Kontrolle der Bundestagspolizei

Anlagen

Anlage 1

Übersicht über die durchgeführten Kontrollen, Beratungs und Informationsbesuche

Alexander von Humboldt-Stiftung

Bayerisches Landesamt für Steuern – Informationsbesuch

Bayerisches Staatsministerium der Finanzen und für Heimat – Beratungs- und Informationsbesuch

BG Holz und Metall

BKK Daimler

BKK Linde

BKK mhplus

BKK mobil oil

Bundesagentur für Arbeit – Informationsbesuch

Bundesagentur für Arbeit bzw. IAB – Informationsbesuch

Bundesamt für Migration und Flüchtlinge

Bundesamt für den Militärischen Abschirmdienst

Bundesamt für Güterverkehr

Bundesamt für Verfassungsschutz

Bundesanstalt für Finanzdienstleistungen

Bundesanstalt für Gewässerkunde

Bundeskriminalamt

Bundesministerium der Verteidigung

Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit

Bundesministerium für Wirtschaft und Energie

Bundesnachrichtendienst – Informationsbesuch

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bundespolizei

Bundestagspolizei

Bundesverwaltungsamt – Informationsbesuch

City Brief Bote

DekaBank Deutsche Girozentrale

Deutsche Bundesbank – Informationsbesuch

Deutsche Flugsicherung GmbH

Deutscher Bundestag

Die Beauftragte der Bundesregierung für Kultur und Medien – Informationsbesuch

DRV Bund, Reha-Zentrum Schömberg

Finanzamt in NRW (Brühl)

Finanzämter in Bayern (Ingolstadt, Bad Kissingen)

Helmholtz-Institut – Helmholtz-Zentrum für Infektionsforschung Braunschweig

Jobcenter Bremerhaven

Jobcenter (Erding)

Jobcenter (Freising)

Jobcenter Weimar

Jobst DSL

Julius-Kühn-Institut

KBS – Regionaldirektion Cottbus (Rentenzweig)

KBS Saar-Klinikum Püttlingen (KBS = DRV Knappschaft Bahn See)

Kraftfahrt-Bundesamt

Ministerium der Finanzen des Landes Nordrhein-Westfalen – Informationsbesuch

M-net Telekommunikations GmbH

Mobilcom debitel GmbH

Primcall GmbH

Oberfinanzdirektion Nordrhein-Westfalen Informationsbesuch

Regionaldirektion Düsseldorf der Bundesagentur für Arbeit – Informationsbesuch

Reisestelle des Bundesministeriums des Innern/ BVA – Informationsbesuch

Statistisches Bundesamt, Wiesbaden – Informationsbesuche

Techniker Krankenkasse

Kontrollen von drei Unternehmen im Rahmen des Sicherheitsüberprüfungsgesetz

Vodafone GmbH

Wasserstraßen- und Schifffahrtsamt Duisburg-Meiderich

Zollkriminalamt

Anlage 2

Übersicht über Beanstandungen, Verwarnungen, Geldbußen

Jobcenter Bremen

Verwarnung, unbefugter Zugriff auf das Postfach des behördlichen Datenschutzbeauftragten

Bundestagspolizei

Beanstandung wegen fehlender Rechtsgrundlage

Bundespolizei

Beanstandung, weil bei der Nutzung von Eurodac die vollständige Dokumentation nicht sichergestellt war.
Beanstandung wegen der fehlenden Rechtsverordnung zum „Geschützten Grenzfahndungsbestand“

Bundeskriminalamt

Beanstandungen wegen des Vorgangsbearbeitungs-systems

1&1 Telecom GmbH

Geldbuße wegen Verstoßes gegen Art. 83 Abs. 4 Buchst. a) i. V. m. Art. 32 Abs. 1 DSGVO durch Unterlassen der Implementierung von Prozessen zur hinreichenden Authentifizierung von Anrufern im Kundenservice (zum Veröffentlichungszeitpunkt noch nicht rechtskräftig)

Rapidata GmbH

Geldbuße wegen Verstoßes gegen Art. 83 Abs. 4 Buchst. a) i. V. m. Art. 37 Abs. 1 Buchst. b) und Abs. 7 DSGVO durch Unterlassen der Benennung einer oder eines betrieblichen Datenschutzbeauftragten und fehlende Veröffentlichung und Mitteilung der Kontaktdaten gegenüber betroffenen Personen und Aufsichtsbehörde (rechtskräftig)

Schlagwortverzeichnis

Als Fundstelle ist die Nummer des Beitrags angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis

Abs.	Absatz
AEUV	Der Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AK	Arbeitskreis
AkkStelleG	Gesetz über die Akkreditierungsstelle
AMS	Asservatensystem
App(s)	Applikation(en)
AO	Abgabenordnung
Art.	Artikel
ATD	Anti-Terror-Datei
Az	Aktenzeichen
AZR	Ausländerzentralregister
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BDSG a. F.	Bundesdatenschutzgesetz alte Fassung
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGBL	Bundesgesetzblatt
BHO	Bundeshaltsordnung
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVI	Bundesministerium für Verkehr und Infrastruktur
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Bundestags-Drucksache
BTLE	Borders, Travel, Law Enforcement
BVerfSchG	Bundesverfassungsschutzgesetz
BvR	Aktenzeichen einer Verfassungsbeschwerde beim Bundesverfassungsgericht
BZR	Bundeszentralregister
bzw.	beziehungsweise
CSC	Coordinated Supervsion Committee
DAkkS	Deutsche Akkreditierungsstelle
DEK	Datenethikkommission
d. h.	das heißt
DiGA	Digitale Gesundheitsanwendungen
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DIN	Deutsches Institut für Normung
DNA	Desoxyribonukleinsäure
DPMA	Deutsches Patent- und Markenamt
DSAnpUG-EU	Datenschutz-Anpassungs- und Umsetzungsgesetz EU
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DVG	Digitale-Versorgungs-Gesetz
EDPS	Europäischer Datenschutzbeauftragter
EDSA	Europäischer Datenschutzausschuss
EES	Ein- und Ausreiseregister
eFBS	Einheitliches Fallbearbeitungssystem
eIDAS	Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen
EIRD	Gesetz zur Errichtung eines Implantateregisters Deutschland
EG	Europäische Gemeinschaft
ELFE	Erleichterte Leistungen für Eltern
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EURODAC	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
EWG	Europäische Wirtschaftsgemeinschaft
ff.	fortfolgende
FlugDaG	Gesetz über die Verarbeitung von Fluggastdaten
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GKV	Gesetzliche Krankenversicherung
GKV-Spitzenverband	Spitzenverband Bund der Krankenkassen
GKV-FKG	Gesetz für eine faire Kassenwahl in der gesetzlichen Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung

GPA	Global Privacy Assembly
GRCh	Charta der Grundrechte der Europäischen Union
h. E.	hiesigen Erachtens
ITZ Bund	Informationstechnikzentrum Bund
i. S. d.	im Sinne des
i. V. d.	in Verbindung des
i. v. m.	in Verbindung mit
ICDPPC	Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre
IMSI	International Mobile Subscriber Identity
IMI	Binnenmarkt-Informationssystem
INPOL-Z	Informationssystem der Polizei
IT	Informationstechnik
IP	Internet Protocol
JI-RL	Richtlinie zum Datenschutz bei Polizei und Justiz
Kap.	Kapitel
Kfz	Kraftfahrzeug
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KTA	kriminaltaktische Anfragen
LIBE (Ausschuss)	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des EU-Parlaments
lit.	Litera
LKA	Landeskriminalamt
MarkenG	Gesetz über den Schutz von Marken und sonstigen Kennzeichen
MarkenV	Verordnung zur Ausführung des Markengesetzes
MDK	Medizinische Dienste der Krankenkassen
m. E.	meines Erachtens
Nr.	Nummer
OZG	Onlinezugangsgesetz
ÖPNV	Öffentlicher Personennahverkehr
PIAV	polizeilicher Informations- und Analyseverbund
PIN	Persönliche Identifikationsnummer
PIMS	Personal Information Management Systems
PIU	Passenger Information Unit
PKZ	Personenkennziffer
PMT	Privacy Management Tools
PNR-Daten	Fluggastdatensätze
PNR-RL	Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen
PostG	Postgesetz
PSWG	Policy Strategy Working Group
RED	Rechtsextremismus-Datei
RFID	radio-frequency identification
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
SIS II	Schengener Informationssystems der zweiten Generation
SIT	Strategischen Initiative Technik
sog.	so genannte
SSl	Secure Sockets Layer
Steuer-ID	Steuer-Identifikationsnummer
StPO	Strafprozessordnung
SWR	Südwestrundfunk
s.	siehe
TB	Tätigkeitsbericht
TI	Telematikinfrastruktur
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
u. a.	unter anderem
U. S.	United States
USA	United States of America
VBS	Vorgangsbearbeitungssystem
VDA	Verband der Automobilindustrie
vgl.	vergleiche
VIS	Visa-Informationssystem
VSDM	Versichertenstammdatenmanagement
VS-NfD	Verschlusssache nur für den Dienstgebrauch
WLAN	Wireless Lan
z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZensG 2021	Gesetz zur Durchführung des Zensus im Jahr 2021
ZfDG	Gesetz über das Zollkriminalamt und die Zollfahndungsämter
ZKA	Zollkriminalamt

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Graurheindorfer Str. 153
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 2020

Dieser Bericht ist als Bundestagsdrucksache 19/19900 erschienen.

Druck:
Silber Druck oHG
Am Waldstrauch 1
34266 Niestetal