

# Tätigkeitsbericht 2020

29. Tätigkeitsbericht  
für den Datenschutz und  
die Informationsfreiheit



# BfDI

Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit



29

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

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

# Unterrichtung

durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht für das Jahr 2020

– 29. Tätigkeitsbericht –

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung .....</b>	<b>6</b>
<b>2</b>	<b>Empfehlungen.....</b>	<b>8</b>
2.1	Zusammenfassung der Empfehlungen für den 29. Tätigkeitsbericht.....	8
2.2	Empfehlungen aus dem 28. Datenschutz-Tätigkeitsbericht und dem 7. Informationsfreiheit-Tätigkeitsbericht – Stand der Umsetzung .....	9
2.3	Wichtige Empfehlungen aus früheren Tätigkeitsberichten – Stand der Umsetzung .....	12
<b>3</b>	<b>Gremien.....</b>	<b>16</b>
3.1	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).....	16
3.1.1	Entschießung zum Patientendaten-Schutz-Gesetz .....	16
3.1.2	Registermodernisierung verfassungskonform umsetzen .....	16
3.1.3	Datensouveränität.....	17
3.1.4	Orientierungshilfe Videoüberwachung.....	17
3.1.5	Anforderungen an eine sichere Email-Kommunikation .....	18
3.1.6	Initiative DSK 2.0.....	18
3.2	Europäischer Datenschutzausschuss.....	19
3.2.1	Bericht aus der Key Provisions Expert Subgroup .....	21
3.2.2	Evaluierung der DSGVO: Die erste Runde ist abgeschlossen .....	22
3.2.3	Gesichtserkennung – Nutzen und Grenzen .....	23
3.2.4	Genehmigung und Veröffentlichung der (deutschen) Akkreditierungskriterien zu Überwachungsstellen nach Art. 41 DSGVO .....	23
3.3	Global Privacy Assembly.....	24
<b>4</b>	<b>Schwerpunktthemen .....</b>	<b>26</b>
4.1	Corona .....	26
4.1.1	Die Corona-Warn-App der Bundesregierung .....	26
4.1.2	Die Datenspende-App.....	27
4.1.3	Corona-Maßnahmen und -Projekte .....	28
4.1.4	Änderungen des Infektionsschutzgesetzes.....	30
4.1.5	Schutzmaske nur gegen Daten? .....	31
4.1.6	Messenger und Videokonferenzsysteme – Fluch und Segen in Corona-Zeiten .....	32
4.1.7	Zustellung von Paketen unter Pandemie-bedingungen .....	34
4.1.8	Programme für Sofort- bzw. Überbrückungshilfen des Bundes im Zusammenhang mit der Corona-Pandemie .....	34
4.1.9	Coronabedingte Änderungen in der Arbeitsverwaltung .....	35
4.2	Das Patientendaten-Schutz-Gesetz .....	35
4.3	Umsetzung der Schrems II-Entscheidung des Europäischen Gerichtshofes.....	42

<b>5</b>	<b>Gesetzgebung</b>	44
5.1	Registermodernisierung	44
5.2	Die Digitalisierung der Verwaltung schreitet voran	45
5.3	IT-Sicherheitsgesetz 2.0	46
5.4	Novellierung des Gesetzes über den Bundesnachrichtendienst	47
5.5	Gesetzgebungsverfahren zur Änderung des Verfassungsschutzrechts	49
5.6	Die Verordnung zu den „Apps auf Rezept“	49
5.7	Datentransparenzverordnung	50
5.8	Die Grundrente kommt - aber auch datenschutzgerecht ?	51
5.9	Das Digitale Familienleistungen-Gesetz	52
5.10	Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich	53
<b>6</b>	<b>Sicherheitsbereich</b>	55
6.1	Polizei 2020	55
6.2	Einheitliches Fallbearbeitungssystem	57
6.3	Das Urteil des Bundesverfassungsgerichts zur strategischen Ausland-Ausland-Fernmeldeaufklärung	57
6.4	Das Haber-Verfahren	59
6.5	Sicherheitsüberprüfung von Bewerberinnen und Bewerbern der Nachrichtendienste	60
6.6	Passenger Name Records - Wie viel Datensammlung ist zur Terrorismusbekämpfung gerechtfertigt?	60
6.7	JI-Richtlinie nach wie vor nicht vollständig umgesetzt	62
6.8	Neugestaltung des Informationsverbundes FIU 2.0	63
6.9	Datenschutzverstoß im Bereich der Zollfahndung	64
6.10	Beschäftigtendatenschutz in der Zollverwaltung	64
6.11	Datenschutzverstöße bei der Bundespolizei	66
6.12	Geschützter Grenzfahndungsbestand	66
<b>7</b>	<b>Weitere Einzelthemen</b>	67
7.1	Datenschutzaufsicht im parlamentarischen Bereich	67
7.2	Interdisziplinärer Beirat Beschäftigtendatenschutz	68
7.3	Register im Gesundheitsbereich	68
7.4	Nachbessern, aber bitte richtig – der zweite Beschluss des Bundesverfassungsgerichts zur Bestandsdatenauskunft	69
7.5	Anonymisierung – Eine Standortbestimmung zwischen der DSGVO und dem TKG	71
7.6	Unverschlüsselte Steuerdaten	72
7.7	IT-Konsolidierung Bund	73
7.8	Microsoft, der Datenschutz und die digitale Souveränität	74
7.9	Künstliche Intelligenz – Fortschritte	75
7.10	Zertifizierung und Akkreditierung – erste Verfahren starten	76
7.11	Videoidentverfahren: Aktuelle Grundsatzentscheidung des BfDI mit Ausstrahlungswirkung für viele Bereiche	77
7.12	Folgen des Brexit	78
7.13	Neue Entwicklungen in der Forschung mit Gesundheitsdaten	78
7.14	Berichtigung von Diagnosedaten	79
7.15	Das Krankengeldfallmanagement – Kein Konsens über den Umfang der Datenerhebungsbefugnisse der Krankenkassen	80
7.16	Zuständigkeitsaufteilung im Bereich Telekommunikation	80
7.17	Cyber-Angriff auf die Bundesanstalt für Immobilienaufgaben	81

<b>8 Informationsfreiheitsgesetz</b>	82
8.1 Einzelthemen	82
8.1.1 Informationsfreiheit in der Pandemie	82
8.1.2 Was ist eigentlich ein Geschäftsgeheimnis?	83
8.1.3 Zugang zum Verzeichnis von Verarbeitungstätigkeiten	84
8.1.4 Informationsfreiheitsgesetz des Bundes gilt nicht für der Deutschen Städtetag	85
8.2 Rechtsprechung	85
8.2.1 Streit um die Veröffentlichung einer Stellungnahme zu Glyphosat: Berechtigter Schutz geistigen Eigentums oder Zensur?	85
8.2.2 Was gilt? Das Parteiengesetz oder das Informationsfreiheitsgesetz?	86
8.2.3 Social-Media und die Informationsfreiheit	86
8.3 Statistik zur Informationsfreiheit	87
<b>9 Kontrollen und Auswirkungen</b>	89
9.1 Fragebogenkontrolle zur Authentifizierung bei Call-Centern	89
9.2 Fragebogenkontrolle Handscanner	90
9.3 Änderung der Organisation des behördlichen Datenschutzes im Bundesministerium der Verteidigung ..	90
9.4 Beratungs- und Kontrollbesuche zur Anwendung des Informationsfreiheitsgesetzes	91
9.5 Kontrollen im Sicherheitsbereich	91
9.5.1 Kontrollen und Beanstandungen im Bereich des Bundesamtes für Verfassungsschutz	91
9.5.2 Kontrolle der Anti-Terror Datei	92
9.5.3 Das Vorgangsbearbeitungssystem beim BKA	93
9.5.4 Datenübermittlungen des BKA im internationalen Bereich	94
9.5.5 Allgemeiner Beitrag über die durchgeführten SÜG-Kontrollen	95
<b>10 BfDI intern</b>	96
10.1 Handlungsmöglichkeiten des BfDI bei europarechtswidriger Gesetzgebung	96
10.2 Urteil des Landgerichts Bonn bestätigt Rechtsauffassung des BfDI	96
10.3 Personalentwicklung im Jahr 2020	98
10.4 Die neue Liegenschaft	99
10.5 Presse- und Öffentlichkeitsarbeit	99
10.6 BfDI in Zahlen	101
<b>11 BfDI als zentrale Anlaufstelle (ZAST)</b>	104
11.1 Stärkung der Zentralen Anlaufstelle	104
11.2 Statistischer Einblick in die Arbeit der ZAST im Rahmen der Verfahren der Zusammenarbeit und Kohärenz auf europäischer Ebene	105
<b>12 Und dann war da noch</b>	109
12.1 Die Sache mit den Memes	109
<b>Themenzuordnung nach Bundestagsausschüssen</b>	112
<b>Anlagen</b>	115
Anlage 1 Kontrollen, Beratungs- und Informationsbesuche	115
Anlage 2 Übersicht über Anweisungen, Beanstandungen, Verwarnungen, Geldbußen	117
Abkürzungsverzeichnis	119
Schlagwortverzeichnis	122
<b>Impressum</b>	124

# 1 Einleitung

2020 – was für ein Jahr! Das Corona-Virus und seine Folgen überlagerten alle Lebensbereiche, bestimmten die politische Agenda genauso wie die wirtschaftliche, führten uns in zwei so noch nie dagewesene Lockdowns und in Videokonferenzen ohne Ende. Einige Grundrechte, darunter auch der Datenschutz, wurden zugunsten der Pandemiebekämpfung eingeschränkt.

Abstand halten, Kontakte minimieren, im Homeoffice arbeiten, die Kinder beim Homeschooling betreuen oder anders beschäftigen und gleichzeitig die „normale“ Arbeit bewältigen: All dies wurde im Jahr 2020 von vielen Beschäftigten gefordert und umgesetzt. Auch in meinem Haus wurde Homeoffice der Normalfall und Dank dem bereits 2019 vollzogenen Austausch fast aller Desktop-PCs durch Laptops sowie der Umstellung des Behördenbetriebs auf die e-Akte konnten wir unsere Arbeit abgesehen von den Vor-Ort-Kontrollen so gut wie uneingeschränkt fortsetzen.

Dies war auch dringend notwendig, denn die Bundesregierung steigerte ihre schon im Vorjahr hohe Zahl von Gesetzentwürfen weiter. Insbesondere im Gesundheitsbereich wurden neben dem ohnehin schon sehr beratungsintensiven sogenannten Patientendaten-Schutz-Gesetz (PDSG) gleich drei Pandemiebekämpfungsgesetze auf den Weg gebracht, die zum Teil kaum Zeit zur Prüfung und Beratung ließen.

Das PDSG regelt insbesondere die schon lange geplante elektronische Patientenakte (ePA) und die Einführung von elektronischen Rezepten. Trotz langer und intensiver Beratungen mit dem Bundesgesundheitsministerium ist es leider nicht gelungen, die ePA für alle gesetzlich Versicherten so auszugestalten, dass diese vom ersten Tag an sowohl die gesundheitlichen Vorteile als auch die von der Datenschutz-Grundverordnung (DSGVO) geforderten Maßgaben erfüllt (s. 4.2). Gerade weil die ePA viele, besonders sensible Patientendaten enthalten soll, ist der Schutz dieser Daten besonders wichtig. Ich muss hier auf weitere Nachbesserungen im Sinne der DSGVO bestehen.

Ähnlich beratungsintensiv und am Ende unbefriedigend war die Begleitung des Registermodernisierungsgesetzes, das Ende 2020 in den Bundestag eingebracht wurde. Das Gesetz sieht vor, die Steuer-Identifikationsnummer zukünftig als Personenkennzeichen für über 50 Datenbanken und Register von Bund und Ländern zu nutzen. Aus datenschutzrechtlicher Sicht sinnvollere, die Funktionalität ebenfalls vollumfänglich gewährleistende Alternativen wie beispielsweise bereichsspezifische Personenkenncodierungen wurden nur ungenügend oder gar nicht geprüft. Gerade weil das Bundesverfassungsgericht die Einführung von Personenkenncodierungen in den letzten Jahren immer wieder für verfassungswidrig erklärt hat, vermute ich, dass die aktuellen Pläne einer Verfassungsbeschwerde nicht standhalten werden. Das unterstützenswerte Vorhaben einer Bürokratieentlastung für die Bürgerinnen und Bürger ebenso wie für die Verwaltung läuft damit Gefahr, weiter in die Zukunft verschoben zu werden (s. 5.1 und 5.2).

Nicht in die Zukunft verschoben werden können die Auswirkungen des Urteils des Europäischen Gerichtshofs (EuGH) zum internationalen Datenverkehr vom Juli 2020. Mit seiner sogenannten Schrems II-Entscheidung erklärte das Gericht nicht nur die Regelungen des „Privacy Shields“ für unwirksam. Es stellte auch noch einmal klar, dass grundsätzlich ein der EU gleichwertiges Datenschutzniveau für Datentransfers in Drittstaaten bestehen muss. Insofern müssen beispielsweise Standarddatenschutzklauseln unter anderem dann um „zusätzliche Maßnahmen“ ergänzt werden, wenn im Empfängerland Sicherheitsbehörden einen umfassenden Zugriff auf die übermittelten Daten nehmen können (s. 4.3). Zur Unterstützung der von der unmittelbaren Wirksamkeit des Urteils betroffenen datenverarbeitenden Stellen hat der Europäische Datenschutzausschuss unverzüglich erste Handlungsempfehlungen und Hilfestellungen zur Verfügung gestellt. Aufgrund der Gravität und Reichweite der Auswirkungen des Urteils werden seine Folgen uns aber sicherlich auch noch in den nächsten Jahren beschäftigen.

Ein Thema, dass uns hoffentlich nicht über die nächsten Jahre beschäftigen wird, ist die Corona-Warn-App (CWA). Zum einen, weil zu hoffen bleibt, dass wir Corona schnellstmöglich in den Griff bekommen, zum anderen, weil die in 2020 in dieses Projekt investierte Arbeit immer wieder unter hohem Zeitdruck geschehen musste. Deshalb freut es mich auch, dass die CWA als positives Beispiel dafür dienen kann, wie durch die konsequente Einbindung einer Datenschutzaufsichtsbehörde im gesamten Entwicklungsprozess ein aus datenschutzrechtlicher Sicht hervorragendes Produkt an den Markt gebracht werden konnte (s. 4.1.1). Nicht zuletzt aufgrund der datenschutzfreundlichen Ausgestaltung trifft die CWA in der Bevölkerung auf eine hohe Akzeptanz und wurde bis Ende des Jahres 2020 bereits mehr als 24 Millionen Mal heruntergeladen.

Gerade deshalb verwundert und irritiert mich die aktuelle Diskussion über angeblich fehlende Funktionalitäten der App. Vor allem die von vielen Stellen vorgebrachten Behauptungen, strenge Datenschutzvorgaben würden eine sinnvolle Weiterentwicklung der CWA verhindern, sind schlichtweg falsch und basieren nicht selten auf mangelndem Verständnis der Funktionsweise und technischen Möglichkeiten der App. Fakt ist, dass bislang keine der in die Diskussion eingebrachten, geeigneten und technisch umsetzbaren Vorschläge am Datenschutz gescheitert ist. Ich wünschte mir daher hier eine differenziertere und vor allem informiertere Debatte, die die sinnvolle und effektive Weiterentwicklung unterstützt. Denn auch wenn die CWA nicht die alleinige Lösung darstellen kann, bietet sie hervorragende Voraussetzungen, Infektionsketten schneller zu unterbinden und damit wesentlich zur Bekämpfung der Pandemie beizutragen.

Auch jenseits von Corona war der BfDI in 2020 mit vielen Themen befasst, deren Auswirkungen nicht nur spezielle Bereiche und rechtliche Fragen umfassen, wie z. B. die Novellierung des Bundesnachrichtendienstgesetzes (s. 5.4), die notwendige Datenschutzordnung des Bundestages (s. 6.1) oder Entwicklungen im Bereich der Künstlichen Intelligenz (s. 6.9). Eine ganze Reihe von Fragestellungen betreffen auch Themen, die unmittelbar spürbare Auswirkungen für einzelne Bürgerinnen und Bürger haben können, wie etwa Verfahren zum Krankengeldfallmanagement (s. 6.14), der unverschlüsselte E-Mailversand von sensiblen

Daten (s. 6.6) oder Vorgaben zur datenschutzkonformen Umsetzung privater Videoüberwachung (s. 3.1.4).

Ein weiterer wichtiger Bereich meiner Arbeit ist dieses Jahr zum ersten Mal gemeinsam mit dem Datenschutz in diesem Bericht vertreten: Die Informationsfreiheit. Auch hier nahm Corona Einfluss auf meine Arbeit: Die Modalitäten und die Kosten der Rückholung von deutschen Staatsbürgerinnen und Staatsbürgern während des ersten Lockdowns war Gegenstand zahlreicher Anfragen. Viele Menschen richteten Fragen zum Pandemiemanagement an das Robert Koch-Institut oder das Bundesministerium für Gesundheit, bei denen ich um Vermittlung gebeten worden war.

Letztendlich belegt auch der diesjährige Tätigkeitsbericht wieder eindrucksvoll, dass Datenschutz und Informationsfreiheit Querschnittsthemen sind, die in fast allen Lebensbereichen mehr oder weniger Bedeutung entfalten. Vor allem zeigt sich, dass die Arbeit zur Unterstützung der Bürgerinnen und Bürger bei der Wahrung und Durchsetzung ihres Grundrechts auf informationelle Selbstbestimmung nach wie vor weiter zunimmt. Erfreulicherweise konnte durch den Stellenaufwuchs in den letzten drei Jahren unter anderem die Beratung und Information der von mir beaufsichtigten Stellen weiter intensiviert werden. Damit konnten ich die in der DSGVO und im Bundesdatenschutzgesetz festgelegten Arbeitsaufträge „sensibilisieren, beraten, kontrollieren“ besser als zuvor umsetzen. Und daher gibt es neben den im Tätigkeitsbericht erwähnten Positivbeispielen, bei denen die Beratung zu datenschutzfreundlichen Lösungen und einer guten Umsetzung des Anspruchs auf Informationsfreiheit geführt hat, noch viele weitere Fälle, bei denen unsere Empfehlungen von Unternehmen und Behörden aufgegriffen und umgesetzt wurden.

Diese Arbeit mache ich nicht allein, sondern kann mich auf ein starkes, motiviertes und engagiertes Team aus – Stand Ende 2020 – 251 Mitarbeiterinnen und Mitarbeiter verlassen. Ihnen möchte ich an dieser Stelle meine aufrichtige Anerkennung für die geleistete (Mehr)Arbeit aussprechen und mich für die großartige Zusammenarbeit auch und gerade unter den in diesem Jahr erschwerten Bedingungen bedanken.

Prof. Ulrich Kelber

## 2 Empfehlungen

### 2.1 Zusammenfassung der Empfehlungen für den 29. Tätigkeitsbericht

Ich empfehle den meiner Aufsicht unterliegenden Stellen, mich auch bei zeitkritischen Projekten frühzeitig einzubinden. Dadurch kann dem Datenschutz und damit auch dem Schutz der Betroffenenrechte von Anfang an ausreichend Rechnung getragen werden. (Nr. 4.1.4, 4.1.8, 4.1.9)

Ich empfehle dem Bundesrat, eine Stellvertreterin bzw. einen Stellvertreter des gemeinsamen Vertreters nach § 17 Abs. 1 BDSG zu wählen. (Nr. 11.1)

Ich empfehle, bei der Registermodernisierung statt auf eine einheitliche Personenkennziffer auf mehrere bereichsspezifische Identifikatoren zurückzugreifen. Zumindest sollte das 4-Corner-Modell für jede Datenübermittlung eingesetzt und eine strenge Zweckbindung für die Verwendung der ID-Nr. festgelegt werden. Das Datencockpit sollte zeitnah zu einer echten Bestandsdatenauskunft weiterentwickelt werden. (Nr.5.1)

Ich empfehle, dass die meiner Aufsicht unterliegenden Stellen ihre Datenübermittlungen an Drittländer im Hinblick auf die Anforderungen des Schrems II-Urteils des

EuGH sorgfältig überprüfen und erforderliche Anpassungen vornehmen. (Nr. 4.3)

Ich empfehle, die Gesetze, Projekte und Maßnahmen, die im Rahmen der Corona-Pandemie unter hohem Druck und innerhalb kürzester Fristen entwickelt und umgesetzt wurden, nach Ende der Pandemielage bewusst und sorgfältig zu evaluieren. (Nr. 4.1.3, 4.1.4)

Ich empfehle, „digitale Gesundheitsanwendungen“ in der sicheren Telematikinfrastruktur oder auf maschinenlesbaren Datenträgern an die Nutzer zu übermitteln. Zudem sollte für die Bereitstellung der „digitalen Gesundheitsanwendungen“ in der Telematikinfrastruktur ein App-Store neu geschaffen und von schweigepflichtigen Akteuren des Gesundheitssystems betrieben werden. (Nr. 5.6)

Ich empfehle klarzustellen, dass die Ausübung von Datenschutzrechten nicht zu Strafschärfungen in Disziplinarverfahren führen darf. (Nr. 6.10)

Ich empfehle, das europäische Datenschutzrecht umgehend und vollständig umzusetzen. Dies sollte nicht als Vorwand dafür dienen, umstrittene Regelungen mit neuen Eingriffsbefugnissen für die Sicherheitsbehörden einzuführen. (Nr. 6.7)






## 2.2 Empfehlungen aus dem 28. Datenschutz-Tätigkeitsbericht und dem 7. Informationsfreiheit-Tätigkeitsbericht – Stand der Umsetzung

Empfehlung	Stand der Umsetzung
 Ich empfehle, bei der vielfältigen Umsetzung der KI die sieben datenschutzrechtlichen Anforderungen der „Hambacher Erklärung zur Künstlichen Intelligenz“ zu beachten. (Nr. 3.1 des 28. TB)	KI entwickelt sich rasant. Es ist gut, dass der (öffentliche) Diskurs um die rechtlichen, wirtschaftlichen und gesellschaftlichen Implikationen von KI in vollem Gange ist. Datenschutz ist hierbei ein wichtiger Erfolgsfaktor. Ich werde die Entwicklungen in diesem Bereich weiter aufmerksam verfolgen und mich weiter für eine datenschutzkonforme KI einsetzen, die dem Menschen dient.
 Ich empfehle, im Rahmen der Evaluation der DSGVO die Position der nationalen Datenschutz-Aufsichtsbehörden 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 des 28. TB)	Bericht der Kommission zur Evaluierung liegt vor (MITTEILUNG DER KOMMISSION COM(2020) 264 final).  Die Bundesregierung hat sich im Rat bei der Evaluierung intensiv eingebracht. Unmittelbare Maßnahmen zur Änderung der DSGVO hat die KOM im Ergebnis nicht erwogen.
 Ich empfehle, bei der elektronischen Patientenakte von Beginn an ein differenziertes Rollen- und Rechtemanagement zu implementieren. (Nr. 4.2.1 des 28. TB)	Zwar ist das Patienten-Daten-Schutzgesetz mit seinen zahlreichen Regelungen zur TI und der elektronischen Patientenakte (ePA) in Kraft getreten. Allerdings startet die ePA zum 1.1.2021 ohne die Möglichkeit, dokumentengenau den Zugriff zu steuern. Erst ab dem 1.1.2022 können sogenannte Front-End-Nutzer dokumentengenau steuern, alle anderen Versicherten sollen dauerhaft die Zugriffsberechtigungen nur über Dokumentenkategorien steuern können.
 Ich empfehle, statt einer Verlagerung von Registern ins Bundesinstitut für Arzneimittel und Medizinprodukte eine eigenständige unabhängige Registerbehörde im Gesundheitsbereich zu schaffen. (Nr. 4.2.2 des 28. TB)	Diese Empfehlung wurde bisher nicht aufgegriffen.
 Ich empfehle, die Vorschläge der Datenethikkommission gesetzlich zu verankern. (Nr. 4.6)	Soweit ersichtlich, ist bislang kein Umsetzungsschritt erfolgt. Ein erster Versuch, im TTDSG-E ein PIMS einzuführen, ist bereits im Ansatz wieder zurückgezogen worden.
 Ich empfehle, das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) an die DSGVO anzupassen. (Nr. 5.2 des 28. TB)	Die Bundesregierung hat Ende 2020 einen Gesetzentwurf zur Modernisierung des Telekommunikations- sowie des Telemedienrechts vorgelegt.
 Ich empfehle, ein Sicherheitsgesetz-Moratorium auszusprechen und einen Evaluationsprozess der sicherheitsbehördlichen Eingriffskompetenzen einzuleiten, um mögliche Vollzugsdefizite zu identifizieren. (Nr. 5.3 des 28. TB)	Diese Empfehlung wurde bisher nicht aufgegriffen.
 Ich empfehle, bei der Registermodernisierung statt auf eine einheitliche Personenkennziffer auf mehrere bereichsspezifische Identifikatoren zurückzugreifen. (Nr. 5.5 des 28. TB)	Im noch laufenden Gesetzgebungsverfahren wurden meine Bedenken weitgehend nicht berücksichtigt. Die Empfehlung wird daher auch durch eine neue Empfehlung aktualisiert und konkretisiert (siehe oben).

	Empfehlung	Stand der Umsetzung
	Ich empfehle, auf eine Videoüberwachung mit biometrischer Gesichtserkennung im öffentlichen Raum zu verzichten. (Nr. 6.2 des 28. TB)	Bisher wurde eine entsprechende Regelung nicht ins BPolG aufgenommen.
	Ich empfehle, für das sogenannte Haber-Verfahren eine ausdrückliche und umfassende gesetzliche Grundlage zu schaffen. (Nr. 6.5 des 28. TB)	Diese Empfehlung wurde bisher nicht aufgegriffen.
	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 des 28. TB)	Im Entwurf des Registermodernisierungsgesetzes ist ein Datencockpit vorgesehen, das eine Transparenz bezüglich der Übermittlungen zwischen den vom RegMoG erfassten Registern vorsieht. Ich setze mich darüber hinaus dafür ein, das Datencockpit zu einer echten Bestandsdatenauskunft auszubauen.
	Ich empfehle den meiner Aufsicht unterstehenden Stellen, personenbezogene Daten grundsätzlich nur verschlüsselt per E-Mail zu versenden. (Nr. 8.3 des 28. TB)	Leider wird immer noch viel zu wenig auf verschlüsselte E-Mail-Kommunikation gesetzt. Insbesondere führte meine Kritik an einer diesbezüglichen Regelung in der Abgabenordnung zu keiner Verbesserung.
	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. (Nr. 8.7 des 28. TB)	Diese Empfehlung wurde bisher nicht aufgegriffen.
	<p>Ich empfehle dem Gesetzgeber die Weiterentwicklung des Informationsfreiheitsgesetzes in Richtung eines Transparenzgesetzes.</p> <p>a) Dieses Transparenzgesetz sollte die Behörden deutlich stärker und umfangreicher zu proaktiven Veröffentlichungen verpflichten.</p> <p>b) Mit einem Transparenzgesetz sollte die Bundesregierung auch zur Einrichtung und zum Betrieb eines zentralen Portals des Bundes für die gebündelte proaktive Informationsbereitstellung verpflichtet werden. Hier sollten bisher nicht veröffentlichte Informationen ebenso wie geeignete, auf Antrag hin einzelnen Interessenten bereitgestellte Informationen für alle verfügbar gemacht werden (sog. „access for one – access for all“ - Prinzip).</p> <p>c) Zudem sollte das Portal die Möglichkeit für eine einfache elektronische Antragstellung und Bescheidung eröffnen. Dies sollte das Auffinden von Informationen erleichtern und gleichzeitig den Aufwand in den Verwaltungen reduzieren.</p>	<p>Der Bundesgesetzgeber hat meine Empfehlung, das Informationsfreiheitsgesetz zu einem Transparenzgesetz weiterzuentwickeln, bisher nicht aufgegriffen.</p> <p>Allerdings gibt es Initiativen im Bereich offener Daten: Im Dezember 2020 haben BMI und BMWi den Referentenentwurf zum Zweiten Open-Data-Gesetz und Datennutzungsgesetz vorgelegt<sup>1</sup>.</p> <p>Mit dem Gesetzentwurf soll zum einen die Open-Data-Regelung des Bundes (§ 12a E-Government-Gesetz) ausgeweitet werden. Mehr öffentliche Verwaltungsdaten sollen über den zentralen Zugangspunkt GovData und dort zu hinterlegende Metadaten auffindbar werden.</p> <p>Zum anderen soll das Datennutzungsgesetz die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors in nationales Recht umsetzen. Das weitere Gesetzgebungsverfahren bleibt abzuwarten.</p>

<sup>1</sup> Entwurf eines Gesetzes zur Änderung des E-Government-Gesetzes und zur Einführung des Gesetzes für die Nutzung von Daten des öffentlichen Sektors, Quelle: <https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/referentenentwurf-zweites-open-data-gesetz-und-datennutzungsgesetz.pdf>






Empfehlung	Stand der Umsetzung
<p> Ich empfehle dem Gesetzgeber, meine Funktion als Bundesbeauftragter für die Informationsfreiheit auszubauen.</p> <p>a) Dabei sollte mir die Möglichkeit für verbindliche Anordnungen und weitere Sanktionen analog zu meinen datenschutzrechtlichen Befugnissen gegeben werden. Damit wären Antragstellerinnen und Antragsteller nicht mehr nur auf den – oft zeit- und kostenintensiven – Weg des gerichtlichen Rechtsschutzes angewiesen.</p> <p> b) Wie schon meine Vorgänger empfehle ich dem Gesetzgeber die Erweiterung meiner Aufgaben und Befugnisse insbesondere im Hinblick auf das Umwelt- und das Verbraucherinformationsrecht. Auf diese Weise könnte ich den zweifelsohne auch hier bestehenden Bedarf für die Beratung und Unterstützung der Antragstellerinnen und Antragsteller wie auch der Behörden decken.</p>	<p>Meine Anordnungs- und Sanktionsbefugnisse im Informationsfreiheitsrecht wurden bisher nicht entsprechend meiner datenschutzrechtlichen Befugnisse ausgeweitet.</p> <p>Ein entsprechendes Gesetzgebungsverfahren wurde eingeleitet.</p> <p>Zwischenzeitlich liegt ein Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Änderung des Umweltschadensgesetzes, des Umweltinformationsgesetzes und weiterer umweltrechtlicher Vorschriften“ vom 11.11.2020 vor<sup>2</sup>:</p> <p>Das Umweltbundesamt hat im Dezember 2020 die Studie „Evaluation des Umweltinformationsgesetzes (UIG) - Analyse der Anwendung der Regelungen des UIG und Erschließung von Optimierungspotentialen für einen ungehinderten und einfachen Zugang zu Umweltinformationen“ veröffentlicht<sup>3</sup>. Dem Gutachten lässt sich entnehmen, dass die Erweiterung der Ombuds- und Kontrollkompetenzen des BfDI auf das UIG (vgl. S. 159 f. der Studie) sowie der Überwachungsaufgaben auf den BfDI (vgl. S. 167) empfohlen wurde.</p>
<p> Ich empfehle dem Gesetzgeber die kritische Prüfung der Ausnahmetatbestände des Informationsfreiheitsgesetzes auf Redundanz und weiter bestehende Notwendigkeit.</p>	<p>Die gebotene Prüfung steht noch aus.</p>







2 Quelle: BT-Drucks. 19/24230: <https://www.bmu.de/gesetz/entwurf-eines-gesetzes-zur-aenderung-des-umweltschadensgesetzes-des-umweltinformationsgesetzes-und-w/>


3 Quelle: <https://www.umweltbundesamt.de/publikationen/evaluation-des-umweltinformationsgesetzes-uig>

## 2.3 Wichtige Empfehlungen aus früheren Tätigkeitsberichten – 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 mir vorliegenden Entwurf für ein neues BPolG sind Abhilfebefugnisse des BfDI vorgesehen. 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)	Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.
 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)	Der Gesetzgeber lehnt dies ab. Wir beobachten daher Fälle, wo Datenschutzverstöße bewusst begangen wurden, um einen wirtschaftlichen Vorteil zu erreichen.
 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)	Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.
 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)	Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.
 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)	Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.
 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)	Erfreulicherweise wird das Muster zunehmend in größerem Umfang eingesetzt.

Empfehlung	Stand der Umsetzung
 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. Allerdings haben meine Folgekontrollen hier noch immer Defizite aufgezeigt, die es seitens der verantwortlichen Stellen noch zu verbessern gilt. Ich werde die Umsetzung der Dokumentationsverbesserung weiterhin kritisch begleiten.
 Ich empfehle dem Gesetzgeber angesichts des festgestellten geringen Nutzwerts von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen. (Nr. 9.3.5 im 27. TB)	Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.
 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)	Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.
 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)	Im Rat der EU konnte auch unter der deutschen Ratspräsidentschaft kein Fortschritt und damit nach wie vor keine allgemeine Ausrichtung herbeigeführt werden.
 Ich rate den öffentlichen Stellen des Bundes, 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)	Im aktuellen Berichtszeitraum konnten keine Verbesserungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.

Empfehlung	Stand der Umsetzung
 Ich empfehle den Bundesbehörden, die eine Fanpage betreiben, zu prüfen, ob der Betrieb einer Facebook-Fanpage zur Erfüllung ihrer Aufgaben unbedingt erforderlich ist oder sie sich nicht – zumindest bis zur rechtlichen Klärung der Situation – datenschutzfreundlichere Kommunikationskanäle nutzen können. (Nr. 15.2.8 im 27. TB)	<p>Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.</p>
 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 im 27. TB)	<p>Mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz sowie dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz hat der Gesetzgeber eine weitgehende Umsetzung der Regelungsaufträge und Regelungsspielräume aus der DSGVO vorgenommen. Meinen Empfehlungen hat der Gesetzgeber in beiden Gesetzen zum Teil entsprochen. Einige Regelungen beurteile ich jedoch weiterhin kritisch, wie etwa die Beschränkung der Aufsichtsbefugnisse bei Berufsgeheimnisträgern, die zum Teil europarechtswidrigen Regelungen zur Videoüberwachung oder punktuell zu weitgehenden Beschränkungen der Betroffenenrechte. Diese Punkte sollten bei der anstehenden Evaluierung des BDSG in den Fokus genommen werden</p>
 Für die Zukunft empfehle ich dem Deutschen Bundestag, sich eine eigene Datenschutzordnung unter Beachtung der Vorgaben der DSGVO zu geben. (Nr. 14.1.1 im 27. TB)	<p>Der Bundestag prüft derzeit die Schaffung einer eigenen Datenschutzordnung.</p>
 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)	<p>Im Sommer 2020 hat das BMAS den interdisziplinären Beirat Beschäftigtendatenschutz einberufen. Die Beiratstätigkeit dauert aktuell noch an. Die Empfehlungen des Beirats sind für die erste Jahreshälfte 2021 geplant. Mit der Beiratstätigkeit wurde der erste Schritt in Richtung eines Beschäftigtendatenschutzgesetzes gegangen.</p>
 Ich empfehle dem Gesetzgeber, die Rechtsgrundlagen für die Eingriffsbefugnisse der Sicherheitsbehörden und der Nachrichtendienste entsprechend der Vorgaben des Bundesverfassungsgerichtes zum BKAG verfassungskonform auszugestalten, d. h. auch geltende Regelungen entsprechend zu ändern. (Nr. 1.3 im 26. TB)	<p>Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.</p>
 Ich empfehle dem Gesetzgeber, gesetzliche Regelungen für das Einführen von Mortalitätsregistern für Forschungszwecke zu schaffen. (Nr. 9.2.3 im 26. TB)	<p>Im aktuellen Berichtszeitraum konnten keine Änderungen festgestellt werden. Zum aktuellen Sachstand wird auf die Ausführungen im letzten TB verwiesen.</p>

Empfehlung	Stand der Umsetzung
 <p>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)</p>	<p>Das IT-Sicherheitsgesetz 2.0 wurde am 16.12.2020 vom Kabinett beschlossen und liegt dem Bundestag zur Beratung vor. Auch im weiteren Gesetzgebungsverfahren ist darauf zu achten, dass die Belange des Datenschutzes bestmögliche Berücksichtigung finden.</p>

## 3 Gremien

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

Die DSK hat die Aufgabe, die Datenschutzgrundrechte zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Den jährlich wechselnden Vorsitz hatte im Jahr 2020 der Sächsische Landesdatenschutzbeauftragte Andreas Schurig.

Coronabedingt fanden alle Vor-, Zwischen- und Hauptkonferenzen der DSK als Videokonferenzen statt. Es wurden neun Entschlüsse zu aktuellen Gesetzgebungsvorhaben und sechs Beschlüsse, z.B. zum Einsatz von Google Analytics verabschiedet. Außerdem wurden aktuelle Orientierungshilfen beispielsweise zu Videokonferenzsystemen sowie Anwendungshinweise zur Akkreditierung und zum Standard-Datenschutzmodell erarbeitet.

#### 3.1.1 Entschlüsselung zum Patientendaten-Schutz-Gesetz

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich mehrfach mit dem Patientendaten-Schutz-Gesetz (PDSG) befasst, mit dem die Digitalisierung im Gesundheitswesen beschleunigt wird. Als Ergebnis ihrer Beratungen hat die DSK eine Entschlüsselung veröffentlicht (s. 4.2).

Obwohl die Begleitung des Gesetzgebungsverfahrens zum PDSG als Bundesgesetz in meinen alleinigen Zuständigkeitsbereich fällt, war die Erarbeitung einer einheitlichen datenschutzrechtlichen Auffassung zum PDSG mit den Landesdatenschutzbeauftragten erforderlich. Denn das PDSG enthält Vorgaben für alle gesetzlichen Krankenkassen, d. h. sowohl für die meiner Aufsicht als auch die den Landesbeauftragten unterstehenden Krankenkassen. Die gemeinsame Positionierung erfolgte auf Arbeitsebene in der Unterarbeitsgruppe eGK

des AK Gesundheit und Soziales sowie durch Abstimmungen auf Behördenleiterenebene. Das Ergebnis dieser Arbeiten habe ich im Rahmen einer Bundespressekonferenz vorgestellt, an der auch drei Landesbeauftragte teilgenommen haben. Im weiteren Verlauf hat die DSK eine Entschlüsselung zum PDSG verabschiedet, in der die datenschutzrechtlich problematischen Regelungen des Gesetzentwurfs angesprochen und Lösungen aufgezeigt wurden. Dadurch sollten notwendige datenschutzrechtliche Verbesserungen des PDSG vor dem letzten Beratungsdurchgang im Bundesrat erwirkt werden, leider ohne Erfolg. Daher müssen die Datenschutzaufsichtsbehörden zur Erfüllung ihrer aufsichtsrechtlichen Verpflichtung nach Inkrafttreten des PDSG, die Verhängung aufsichtsrechtlicher Maßnahmen gegenüber den datenschutzrechtlich Verantwortlichen zur Wahrung bzw. Wiederherstellung der Datenschutzkonformität prüfen.

#### Querverweis:

#### 4.2 Patientendaten-Schutz-Gesetz

#### 3.1.2 Registermodernisierung verfassungskonform umsetzen

Die DSK hat sich deutlich gegen die Zweckentfremdung der Steuer-ID zu einem Personenkennzeichen ausgesprochen.

Mit der Entschlüsselung „Registermodernisierung verfassungskonform umsetzen!“ vom 26. August 2020 positionierte sich die DSK deutlich gegen das Vorhaben der Bundesregierung, die Steuer-ID zu einem registerübergreifenden Ordnungsmerkmal (Personenkennzeichen) auszubauen. Die DSK nahm dabei Bezug auf ihre vorhergehende Entschlüsselung vom 12. September 2019 zu diesem Thema.

Die DSK verweist auf die seit jeher äußerst kritische Bewertung des Bundesverfassungsgerichts gegenüber der Einführung derartiger Personenkennzeichen. Wie das höchste deutsche Gericht sieht auch die DSK die Gefahr eines Missbrauchs als grundrechtsgefährdend an. Der



Entwurf des Registermodernisierungsgesetzes enthält hierfür keinen ausreichenden Ausgleich. Die Möglichkeit einer Zusammenführung von Daten zu einem Persönlichkeitsprofil wird nicht effektiv verhindert und es ist damit zu rechnen, dass die Steuer-ID als Identifikationsnummer nach und nach auch im Wirtschaftsleben verwendet wird.

Die DSK kritisiert, dass wesentlich datenschutzfreundlichere Alternativen, wie „sektorspezifische“ Personenkennzeichen, nicht berücksichtigt werden. Diese Verfahren sind für die Praxis geeignet, werden aber offenbar aus – relativ geringen – wirtschaftlichen Erwägungen und wegen eines selbstgesetzten Eilbedarfs nicht ergriffen.

Die Entschließung vom 26. August 2020 finden Sie unter [www.bfdi.bund.de/entschliessungen](http://www.bfdi.bund.de/entschliessungen).

#### **Querverweis:**

#### **5.1 Registermodernisierung**

##### **3.1.3 Datensouveränität**

Datensouveränität hat sich als ein Leitbegriff der Digitalpolitik etabliert. Er prägt die Debatten um eine künftige Datenstrategie auf europäischer und nationaler Ebene. Doch die Verwendung des Begriffes bleibt weiterhin oft unscharf. Als Alternativbegriff zum Recht auf informationelle Selbstbestimmung des Grundgesetzes eignet er sich nicht. Er sollte auch nicht als Kampfbegriff gegen das bestehende gesetzliche Datenschutzkonzept etabliert werden. Eine Entschließung der DSK definiert, was aus Datenschutzsicht darunter verstanden werden sollte und formuliert konkrete Forderungen.

Der Begriff Datensouveränität hatte zunächst im Zusammenhang mit den kurz nach der Verabschiedung der Datenschutz-Grundverordnung aufkommenden Ideen von einem sog. Dateneigentum an Bedeutung gewonnen (vgl. dazu 27. TB, 1.5., S. 34). Er ist kein Rechtsbegriff, sondern entstammt der politischen Debatte. Inzwischen findet er häufig Verwendung in Diskussionen um europäische und nationale Datenstrategien. Das Eckpunktetpapier der Bundesregierung für eine Datenstrategie sieht in der Gewährleistung verbesserter Zugänge zu Daten die „digitale Souveränität“ gesichert. Datensouveränität bezeichnet damit eher eine auf die Sicherung der Eigenständigkeit und Unabhängigkeit von Institutionen und der europäischen Digitalisierung ausgerichtete Wirtschaftspolitik. Als ein Beispiel wird dabei vor allem das von der Bundesregierung angestoßene, auf eine europäische Cloud-Infrastruktur ausgerichtete Projekt Gaia-X genannt. In diesem Zusammenhang plant das Bundesinnenministerium auch ein Zentrum Digitale

Souveränität (ZenDis), dessen Aufgabe im Schwerpunkt die Thematik Open Source Software in der öffentlichen Verwaltung sein soll.

Dieses auf den Schutz vor einseitigen Abhängigkeiten ausgerichtete institutionelle Verständnis findet auch datenschutzpolitisch Unterstützung. So bekennt sich die Datenschutzkonferenz in einer Entschließung vom September 2020 zur Wahlfreiheit und vollständigen Kontrolle der Verantwortlichen der öffentlichen Verwaltung über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung. Bund, Länder und Kommunen werden aufgefordert, langfristig nur solche Hard- und Software einzusetzen, die den Verantwortlichen der Datenverarbeitung die ausschließliche und vollständige Kontrolle überlässt, Transparenz der Sicherheitsfunktionen gewährleistet und eine Nutzung ohne Profilbildung und missbräuchliche Kenntnisnahme Dritter erlaubt. Bereits kurzfristig müssten Ziele und Kriterien digitaler Souveränität bei allen Beschaffungs- und Vergabeverfahren berücksichtigt werden. Dabei sollen Open Source Produkte bevorzugt sowie Dienstleistungen und Produkte mit Blick auf Privacy by Design, datenschutzfreundliche Voreinstellungen und individuelle Konfigurierbarkeit ausgewählt werden.

Allerdings findet der Begriff nach wie vor auch in der auf individuelle Verbraucherrechte bezogenen Debatte Verwendung. Manchen Interessenvertretern geht es dabei mit Schlagworten wie „Datenspende“ und „Daten als Entgelt“ eher darum, eine wirtschaftliche Verwertungsautonomie des Einzelnen an die Stelle des materiell begründeten Rechts auf informationelle Selbstbestimmung zu setzen. Das dabei zugrunde liegende, eigentumsanaloge Verständnis von Daten und der vermeintlich unteilbaren Herrschaft über die einen selbst betreffenden Daten geht fehl. Denn wirtschaftlich geht es mehr um die Verwertung von Informationen als um Daten, oft sogar um die Verwertung von mehreren Personen betreffenden Kommunikationen und die gezielte Erlangung von Wissen über einzelne Personen oder Personengruppen. Hier gilt mehr denn je, dass diese immateriellen Güter besonderen Schutz benötigen, und dass nur mit einem differenzierten Datenschutzkonzept ein Höchstmaß an Persönlichkeitsschutz zu erreichen ist. Ein von manchen gar befürworteter allgemeiner Wandel des Datenschutzes hin zur Datensouveränität ist daher weder zu erwarten, noch wäre er mit Blick auf den gebotenen Schutz der Rechte der Bürgerinnen und Bürger in der Digitalisierung angemessen.

##### **3.1.4 Orientierungshilfe Videoüberwachung**

Die Datenschutzkonferenz (DSK) legt eine Orientierungshilfe für Fragestellungen bei privater Videoüberwachung vor.

Am 03. September 2020 stellte die DSK eine Orientierungshilfe zur Videoüberwachung durch nicht-öffentliche Stellen vor. Diese Orientierungshilfe lehnt sich weitgehend an die Leitlinien 3/2019 des Europäischen Datenschutzausschusses (EDSA) zu Datenverarbeitungen durch Videoanlagen (vgl. 28. TB Nr. 3.2) an und ergänzt diese um spezifische Verarbeitungssituationen in Deutschland. Hierzu gehören u. a. die Abschnitte zur Videoüberwachung in der Nachbarschaft, die datenschutzrechtliche Bewertung von Tür- und Klingelkameras, Drohnen, Wildkameras und Dashcams.

Die Orientierungshilfe bietet darüber hinaus auch eine umfassende Darstellung der grundlegenden datenschutzrechtlichen Erwägungen zur Videoüberwachung sowie einige praxisnahe Hilfestellungen. So befinden sich im Anhang ein Muster für Hinweisschilder sowie eine Checkliste zu den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung.

Die Orientierungshilfe kann auf meiner Homepage unter [www.bfdi.bund.de/orientierungshilfen](http://www.bfdi.bund.de/orientierungshilfen), hier „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ vom 04.09.2020 abgerufen werden.

### **3.1.5 Anforderungen an eine sichere Email-Kommunikation**

Die vertrauliche Ende-zu-Ende Kommunikation per Email findet leider weiterhin keine große Akzeptanz, da sie immer noch nicht einfach zu handhaben ist. Umso wichtiger ist es, Emails zumindest bereits auf dem Transportweg bei den Diensteanbietern verschlüsselt zu übertragen und somit vor der Einsichtnahme oder Manipulation von Dritten auf Transportabschnitten zu schützen. Hierüber trifft die in 2020 von der DSK erstellte Orientierungshilfe entsprechende Festlegungen zur Kommunikation der Diensteanbieter.

Die Orientierungshilfe zeigt auf, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von Email-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche Email-Diensteanbieter auf dem Transportweg zu erfüllen sind. Risiken, denen ruhenden Daten wie bereits empfangene Emails ausgesetzt sind oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden nicht betrachtet. Diese Anforderungen richten sich nach den Vorgaben des Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DSGVO. Die Orientierungshilfe nimmt den Stand der Technik zum Veröffentlichungszeitpunkt als Ausgangspunkt für die Konkretisierung der Anforderungen. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich mit einer neuen technischen Richtlinie mit der Thematik der verschlüsselten Email-Kommunikation auf Transportebene auseinandergesetzt und Vorgaben

gemacht (BSI TR-03108 Sicherer E-Mail-Transport <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108-1.html>)

Die Erstellung der Orientierungshilfe ist auf meinen Vorschlag hin initiiert worden. Grundgedanke war es, zu einer einheitlichen Auffassung zur Verschlüsselung auf dem Transportweg zu kommen, um den Unternehmen der Telekommunikationsbranche entsprechende einheitliche Vorgaben zu machen. Die Orientierungshilfe spiegelt nun ein abgestimmtes Meinungsbild der Länder und des Bundes bei der Email-Verschlüsselung wider und setzte einen Maßstab für vertrauliche Kommunikation auf Transportebene. Sie kann unter [www.bfdi.bund.de/orientierungshilfen](http://www.bfdi.bund.de/orientierungshilfen) heruntergeladen werden.

### **3.1.6 Initiative DSK 2.0**

Die DSK hat beschlossen, auf Leitungsebene einen „Arbeitskreis DSK 2.0“ einzurichten, der die Zusammenarbeit der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder einschließlich der Arbeitsweise der DSK evaluieren und ggf. Vorschläge für eine Neugestaltung erarbeiten soll.

Der AK DSK 2.0 soll vor dem Hintergrund der politischen Debatte um eine Zentralisierung der Datenschutzaufsicht und aufgrund stetig neuer datenschutzrechtlicher Fragestellungen bei einer sich immer schneller entwickelnden Technik die bisherige Arbeitsweise der DSK und die Zusammenarbeit der Aufsichtsbehörden überprüfen. Er soll Verbesserungspotentiale ermitteln, um die Zusammenarbeit auch weiterhin erfolgreich und eigenbestimmt zu gestalten.

Bürgerinnen und Bürger, Unternehmen und Verbände erwarten zu Recht, dass auch unter der föderalen Struktur der Datenschutzaufsicht in Deutschland vergleichbare Sachverhalte gleich behandelt werden und die Verfahren effizient und transparent ausgestaltet sind.

Ich setze mich deshalb im Rahmen des Arbeitskreises DSK 2.0 dafür ein, dass

- schnellere und effizientere Entscheidungsprozesse der DSK etabliert werden,
- Beschlüsse der DSK verbindlicher werden,
- die Aufsichtspraxis weiter harmonisiert wird und
- die Verbindung zwischen den Arbeitskreisen der DSK und den Arbeitsgruppen des Europäischen Datenschutzausschusses optimiert wird.

Die Arbeiten sollen bis zur 101. Datenschutzkonferenz im Frühjahr 2021 abgeschlossen werden.

## 3.2 Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) hat im Berichtszeitraum seine Arbeit an einer europaweit einheitlichen Anwendung der Datenschutz-Grundverordnung (DSGVO) weiter intensiviert. Hierzu wurden Leitlinien angenommen und Stellungnahmen abgegeben. Auch die grenzüberschreitende Zusammenarbeit wurde weiter verstärkt.

Der EDSA ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten EU beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Diese Aufgaben habe ich bereits in meinen beiden vorangegangenen Tätigkeitsberichten näher erläutert. Als gemeinsamer Vertreter aller deutschen Aufsichtsbehörden bin ich Mitglied des Ausschusses.

Die Arbeit des EDSA wurde nach den beiden ersten Sitzungen im Januar und Februar von den Auswirkungen der COVID-19-Pandemie geprägt. Alle weiteren Sitzungen fanden in Form von Videokonferenzen als „remote-meeting“ statt. Dabei hat der EDSA die Gesamtzahl der Sitzungen deutlich erhöht und insgesamt 27 Mal – zum Teil über zwei Tage – konferiert.

Der Schwerpunkt der Arbeiten lag weiterhin auf der Erarbeitung von Leitlinien nach Art. 70 DSGVO zur einheitlichen Umsetzung der DSGVO in Europa. Daneben hat der Ausschuss auch Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO angenommen und eine erste formale Entscheidung im Streitbeilegungsverfahren zu einem grenzüberschreitenden Beschwerdeverfahren (Kohärenzverfahren) gefasst. Weiterhin hat er sich mit aktuellen datenschutzpolitischen Fragen auf internationaler- und EU-Ebene befasst, u.a. zu Datenverarbeitungen in Folge der COVID-19-Pandemie.

Inhaltlich wurde die Arbeit des EDSA in der zweiten Jahreshälfte erheblich durch die Ergebnisse des Schrems II-Urteils (EuGH, Urteil vom 16. Juli 2020, Az. C-311/18) beeinflusst. Dieses Urteil hat die Anforderungen an Datentransfers in Drittstaaten neu geprägt<sup>4</sup>. (s. 4.3)

Es folgten Ausarbeitungen zu unterschiedlichen Details des Datentransfers. Die **Empfehlungen zum Einsatz zusätzlicher Maßnahmen („supplementary measures“)**<sup>5</sup> enthalten beispielsweise einen Fahrplan der Schritte, die

Datenexporteure gehen müssen, um herauszufinden, ob sie zusätzliche Maßnahmen ergreifen müssen. Das ist die Voraussetzung dafür, in Übereinstimmung mit dem EU-Recht Daten in Länder außerhalb des EWR transferieren zu dürfen.

Der EDSA hat sich zudem für die Jahre 2021 bis 2023 eine Strategie gegeben.

### Leitlinien

Der EDSA hat im Berichtszeitraum zahlreiche Leitlinien verabschiedet, an deren Erarbeitung ich regelmäßig als Berichterstatter oder Mitberichterstatter mitgewirkt habe. Diese wurden zum Teil zur Wahrung von Transparenz und Beteiligung der öffentlichen Konsultation unterzogen.

- Die **Leitlinien 1/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen** verdeutlichen z. B. das Verhältnis zur geplanten E-Privacy-Verordnung und zu Fragen der Verarbeitung von personenbezogenen Daten für neue Zwecke.
- Die **Leitlinien 2/2020 zu Artikel 46 (2) (a) und 46 (3) (b) der Verordnung 2016/679 für die Übermittlung personenbezogener Daten zwischen EWR- und Nicht-EWR-Behörden und -Einrichtungen** befassen sich mit internationalen Datentransfers zwischen öffentlichen Einrichtungen, die zu verschiedenen Zwecken der Verwaltungszusammenarbeit im Rahmen der DSGVO erfolgen. Die Leitlinien gelten aber nicht für Transfers im Bereich der öffentlichen Sicherheit, der Verteidigung oder der Sicherheit des Staates.
- Die **Leitlinien 3/2020 über die Verarbeitung von Gesundheitsdaten zum Zwecke der wissenschaftlichen Forschung im Zusammenhang mit dem Ausbruch von COVID-19** sollen die dringlichsten Fragen in diesem Zusammenhang näher beleuchten, u. a. die Rechtsgrundlage, die Einführung geeigneter Garantien für eine solche Verarbeitung von Gesundheitsdaten und die Ausübung der Rechte betroffener Personen. (s.a. 6.13)
- Die **Leitlinien 4/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19** klären die Bedingungen und Grundsätze

4 Erklärung zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Maximilian Schrems und Facebook Ireland vom 17. Juli 2020 (<https://www.bfdi.bund.de/edsa-stellungnahmen>)

5 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ([https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer\\_de](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_de))

für die verhältnismäßige Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung für zwei konkrete Anwendungen: Diese gelten für die Verwendung von Standortdaten zur Unterstützung der Reaktion auf die Pandemie durch die Modellierung der Verbreitung des Virus, sodass die Wirksamkeit der Beschränkungsmaßnahmen insgesamt beurteilt werden kann. Sie finden ferner Anwendung für die Kontaktnachverfolgung, um Einzelpersonen darüber zu informieren, dass sie sich in unmittelbarer Nähe zu einer Person aufgehalten haben, die zu einem späteren Zeitpunkt als Träger des Virus bestätigt wurde. Das Ziel ist, die Infektionsketten so früh wie möglich zu unterbrechen.

- Die **Leitlinien 5/2020 zur Einwilligung gemäß Verordnung 2016/679** konzentrieren sich auf die durch die DSGVO eingetretenen Änderungen. Sie geben praktische Hinweise für die Einhaltung der Vorgaben der DSGVO zur Einwilligung auf Grundlage der Stellungnahme 15/2011 der Artikel-29-Arbeitsgruppe (Vorgänger des EDSA). Hier bestand u. a. Klärungsbedarf in Bezug auf die Gültigkeit der Einwilligung bei der Interaktion mit so genannten „Cookie-Walls“ und zur Einwilligung beim Scrollen. (s.a. 3.2.2)
- Die **Leitlinien 6/2020 zum Zusammenspiel der zweiten Zahlungsdienste-Richtlinie und der DSGVO** zielen darauf ab, weitere Hinweise zu Datenschutzaspekten im Kontext der PSD2 (Payment Services Directive2) zu geben, insbesondere zum Verhältnis der einschlägigen Bestimmungen der DSGVO und der PSD2. Der inhaltliche Schwerpunkt dieser Richtlinien liegt auf der Verarbeitung personenbezogener Daten durch Anbieter von Kontoinformationsdiensten (Account Information Service Provider) und Anbieter von Zahlungsauslösediensten (Payment Initiation Service Provider).
- Die **Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO** haben das Hauptziel, die Bedeutung der Begriffe zu klären und die verschiedenen Rollen und die Verteilung der Verantwortlichkeiten zwischen diesen Akteuren zu verdeutlichen. (s.a. 3.2.1)
- Die **Leitlinien 8/2020 bezüglich der Zielgruppenansprache von Social-Media-Nutzern** sollen vor dem Hintergrund mehrerer EuGH-Urteile (EuGH, Urteil vom 05. Juni 2018, Az. C-210/16 und Urteil vom 29. Juli 2019, Az. C-40/17) die Verteilung der Rollen und Verantwortlichkeiten zwischen Social-Media-Plattformen und Unternehmen oder anderen Organisationen, die Targeting-Funktionen dieser Social-Media-Plattformen nutzen, klarstellen. Außerdem sollen sie die Auswirkung der jeweiligen Datenverarbei-

tungsvorgänge auf die (Grund-)Rechte und Freiheiten der betroffenen Personen anhand praktischer Beispiele verdeutlichen.

- Die **Leitlinien 9/2020 zu maßgeblichen und begründeten Einwänden gem. Verordnung 2016/679** geben eine Anleitung, was unter einem „maßgeblichen und begründeten Einspruch“ betroffener Aufsichtsbehörden gegen Entscheidungsvorschläge der federführenden Aufsichtsbehörden in grenzüberschreitenden Aufsichtsfällen zu verstehen ist. Sie klären auch, wie zu verfahren und was bei der Beurteilung eines Einspruchs zu berücksichtigen ist.

#### **Stellungnahmen im Kohärenzverfahren / Entscheidung im Kooperationsverfahren**

Im Kohärenzverfahren hat der EDSA 28 Stellungnahmen verfasst. Diese betreffen zum großen Teil durch Mitgliedstaaten vorgelegte verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO), Standardvertragsklauseln (Art. 48 Abs. 8 DSGVO) oder die Akkreditierung von Zertifizierungsstellen (Art. 43 Abs. 3 DSGVO) bzw. Stellen zur Überwachung der Einhaltung von Verhaltensregeln (Art. 41 DSGVO).

In meinem letzten Tätigkeitsbericht habe ich darauf hingewiesen, dass noch in keinem großen grenzüberschreitenden Fall, der weltweit führende Tech-Unternehmen betrifft, ein Entwurf für eine Entscheidung der federführenden nationalen Aufsichtsbehörde ergangen ist. Ein erster solcher Entwurf liegt inzwischen vor und ist bereits zum Gegenstand eines Einspruchsverfahrens nach Art. 60 Abs. 4 DSGVO geworden, an dem sich auch deutsche Aufsichtsbehörden beteiligt haben. Der EDSA hat im November 2020 zum ersten Mal formal über einen solchen Einspruch entschieden.

#### **EDSA-Strategie 2021-2023**

Neben seinem Arbeitsprogramm hat der EDSA eine Strategie für den Zeitraum von 2021 bis 2023 aufgestellt. Diese steht auf vier Säulen: Die erste Säule beinhaltet die **Förderung der Harmonisierung und die Erleichterung der Rechtskonformität (Compliance)**. Dazu strebt der EDSA ein Höchstmaß an Konsistenz bei der Anwendung der Datenschutzvorschriften und eine Begrenzung der Fragmentierung unter den Mitgliedstaaten an. Die zweite Säule zielt auf die **Unterstützung einer effektiven Durchsetzung und einer effizienten Zusammenarbeit zwischen nationalen Aufsichtsbehörden**. Hierfür sollen u. a. interne Prozesse optimiert, Fachwissen gebündelt und eine verbesserte Koordination gefördert werden. Die dritte Säule formuliert einen **grundrechtlichen Ansatz für neue Technologien**. Dies beinhaltet z. B. die Bewertung neuer Technologien wie KI, Biometrie oder Profiling. Die vierte Säule stellt die **globale Dimension**



dar. Der EDSA ist entschlossen, das hohe EU-Datenschutzniveau auch über die Grenzen der EU hinaus bei der Entwicklung globaler Standards zu befördern. Mit meiner Wahl in das Executive Committee der Global Privacy Assembly (GPA) habe ich hierfür bereits die Weichen gestellt.<sup>6</sup> Dementsprechend haben die Vorsitzende des EDSA und mehrere Mitglieder ihre Unterstützung zum Ausdruck gebracht und die Bedeutung einer engen Zusammenarbeit mit der GPA betont.

#### **Querverweise:**

4.3 Schrems II, 3.3 Global Privacy Assembly

#### **3.2.1 Bericht aus der Key Provisions Expert Subgroup**

Die Key Provisions Expert Subgroup (KEYP) des EDSA hat sich auch 2020 mit wichtigen grundsätzlichen Fragestellungen zur Auslegung der DSGVO befasst. Sie konnte die Beratungen der Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ sowie eine Überarbeitung der Leitlinien zur Einwilligung betreffend „Cookie Walls“ und „Scrollen als Zustimmung“ abschließen. Die Arbeit an anderen bedeutenden Dossiers dauert an.

#### **Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“**

Für die Anwendung der DSGVO ist es von zentraler Bedeutung, ob ein Akteur als alleiniger Verantwortlicher, gemeinsamer Verantwortlicher oder als Auftragsverarbeiter tätig ist. Die Leitlinien geben daher wichtige Hinweise, wie diese Begriffe voneinander abzugrenzen sind. Diese Hinweise werden durch praktische Anwendungsfälle ergänzt (Teil 1 der Leitlinien).

Im zweiten Teil der Leitlinien werden die Beziehungen gemeinsamer Verantwortlicher untereinander sowie zwischen Verantwortlichem und Auftragsverarbeiter näher beleuchtet und insbesondere die rechtlichen Auswirkungen dargestellt. Für die Praxis dürfte besonders der Anhang der Leitlinien interessant sein. Dieser enthält ein Flow-Chart, das es den beteiligten Akteuren ermöglichen soll, ihre Rolle zu prüfen.

Die öffentliche Konsultation der Leitlinien endete im Oktober 2020. Mit einer Veröffentlichung des endgültigen Textes wird Anfang 2021 gerechnet.

#### **Aktualisierte Leitlinien 05/2020 zur Einwilligung nach DSGVO**

Der EDSA hat nach entsprechenden Vorarbeiten der KEYP eine in Bezug auf die Einwilligung bei der Nutzung

von Internetseiten überarbeitete Fassung der Leitlinien zur Einwilligung nach DSGVO verabschiedet. Zum einen stellte der EDSA klar, dass das bloße Scrollen oder Weitersurfen auf einer Internetseite in keinem Fall eine wirksame Einwilligung ist. Hier fehlt es an einer eindeutig bestätigenden Handlung. Zum anderen enthalten die Leitlinien nunmehr einen deutlichen Hinweis, dass der Zugang zu einem Online-Service nicht von der Erlaubnis in das Setzen von Cookies (sog. Cookie Walls) abhängig gemacht werden darf. Bei Webseiten, die durch ihren Aufbau den Nutzenden auf diesem Wege Tracking aufzwingen, fehlt es an der Freiwilligkeit der Einwilligung. Ausnahmsweise sind Cookie-Walls dann zulässig, wenn ein vergleichbarer Dienst auch ohne Tracking angeboten wird, beispielsweise als zahlungspflichtiger Dienst.

Als Mitglied des EDSA habe ich der Überarbeitung der Leitlinien zugestimmt und wünsche mir, dass Verantwortliche daraus die richtigen Schlüsse ziehen und endlich datenschutzfreundliche Alternativen anbieten. Die Cookie-Thematik spielt auch bei dem Gesetzgebungsverfahren zur E-Privacy Verordnung eine Rolle (s. 5.10). Die überarbeiteten Leitlinien zur Einwilligung sind in englischer Sprache auf der Webseite des EDSA abrufbar und werden nach der Übersetzung ins Deutsche auch über den Internetauftritt der DSK zu finden sein.

#### **Laufende Arbeiten**

Nach dem Arbeitsplan des EDSA werden in der KEYP Leitlinien zu den Betroffenenrechten erarbeitet. In einem ersten Schritt geht es um das Recht auf Auskunft nach Art. 15 DSGVO. Das Dossier soll Hilfestellung leisten bei den zahlreichen, in der Anwendungspraxis sehr wichtigen Fragestellungen. Das betrifft die Reichweite des Rechts auf Kopie (Art. 15 Abs. 3 DSGVO) sowie Ausnahmen und Grenzen des Auskunftsrechts (Art. 15 Abs. 3 DSGVO, Art. 12 Abs. 5 DSGVO). Im Berichtszeitraum wurden erste Entwürfe beraten und Vorentscheidungen zu einigen Weichenstellungen getroffen. Die Verabschiedung der Leitlinien zu den Betroffenenrechten / Recht auf Auskunft, bei denen ich mich gemeinsam mit der LDI NRW als Co-Berichterstatter einbringe, ist im Jahr 2021 zu erwarten.

Inzwischen hat innerhalb der KEYP auch eine Arbeitsgruppe zur Erstellung der Leitlinie zur Rechtsgrundlage des „berechtigten Interesses“ nach Art. 6 Abs. 1 lit. f) DSGVO ihre Arbeit aufgenommen. Diese Leitlinie erfährt große Aufmerksamkeit in der Fachöffentlichkeit. Die zugrunde liegende Norm der DSGVO wurde weitgehend offen formuliert und zuweilen missverständlich als „Gummiparagraph“ interpretiert. Sie wurde sogar als

6 „BfDI in Executive Committee der Global Privacy Assembly gewählt“, Pressemitteilung vom 16. Oktober 2020 ([www.bfdi.bund.de/pressemitteilungen](http://www.bfdi.bund.de/pressemitteilungen))

vermeintliche Rechtsgrundlage für besonders risikoreiche Datenverarbeitungen herangezogen, was mit dieser Norm allerdings unvereinbar ist. Ich bin gemeinsam mit dem LfDI Baden-Württemberg sowie dem LfDI Mecklenburg-Vorpommern als Co-Berichterstatter an der Ausarbeitung beteiligt. Die Leitlinie zum berechtigten Interesse wird das Working Paper 217 aus dem Jahre 2014 der Artikel 29-Gruppe (Stellungnahme 6/2014) ersetzen. Ich werde mich dafür einsetzen, dass die Leitlinie die vorhandenen Probleme der Praxis möglichst konkret aufgreift und diese Rechtsgrundlage sich nicht als beliebiger Auffangtatbestand für ansonsten nicht haltbare Datenverarbeitungen erweist.

#### **Querverweis:**

5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich, E-Privacy Verordnung

#### **3.2.2 Evaluierung der DSGVO: Die erste Runde ist abgeschlossen**

Zum Stichtag 25. Mai 2020 hatte die Europäische Kommission eine Evaluierung der DSGVO durchzuführen. Hierfür hatte sie den EDSA konsultiert. Insgesamt zieht die Kommission eine positive Bilanz der DSGVO. Gleichwohl erkennt sie Verbesserungsbedarf in der praktischen Umsetzung.

Die Europäische Kommission legte gem. Art. 97 Abs. 1 DSGVO dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung der DSGVO vor. Dazu hatte sie nach Art. 97 Abs. 3 DSGVO beim EDSA Informationen angefordert. Die DSK hatte dem EDSA ihren Erfahrungsbericht zur Anwendung der DSGVO, dessen Inhalt ich in meinem letzten Tätigkeitsbericht bereits detailliert vorgestellt habe (vgl. TB Nr. 4.1), zugeleitet.

Am 18. Februar 2020 hat der EDSA den gemeinsamen Antwortbeitrag zur Evaluierung der DSGVO beschlossen. Er betont die Bedeutung der DSGVO für den Schutz und die Stärkung des Grundrechts auf Datenschutz innerhalb der EU. Insgesamt sieht der EDSA in der DSGVO ein gelungenes europaweit einheitliches Regelwerk. Auch wenn er gegenwärtig keinen Bedarf für eine kurzfristige Revision erkennt, zeigt er in verschiedenen Bereichen Verbesserungsbedarf auf. So betont er die Notwendigkeit bürokratischer Erleichterungen für kleine und mittlere Unternehmen (KMU). Er verlangt zudem für eine effektive Durchführung des One-Stop-Shop-Mechanismus die angemessene Ausstattung der Aufsichtsbehörden mit den dazu erforderlichen Ressourcen. Im Hinblick auf den internationalen Datenverkehr hebt der EDSA die Bedeutung der Angemessenheitsbeschlüsse der Europäischen Kommission hervor. Er fordert die Kommission auf, die Beschlüsse über EU-Standardvertragsklauseln

für Datenübermittlungen in Drittstaaten zu überarbeiten.

Die Europäische Kommission bewertet in ihrem Evaluationsbericht vom 24. Juni 2020 die DSGVO insgesamt als Erfolg. Wesentliche Ziele der DSGVO seien erreicht worden. Die Kommission unterstützt die Forderung nach angemessener Ausstattung der Aufsichtsbehörden sowohl in finanzieller als auch in personeller Hinsicht. Die bürokratische Entlastung bei KMU, deren Datenverarbeitungen nicht mit hohen Risiken verbunden sind, soll zumindest geprüft werden. Zudem wird die Ausbaufähigkeit des Rechts auf Datenübertragbarkeit (bis hin zum real-time Datenaustausch) als zentrales Betroffenenrecht hervorgehoben. Die fortbestehende Fragmentierung innerhalb des Geltungsbereichs der DSGVO aufgrund der Nutzung von Öffnungsklauseln durch die nationalen Gesetzgeber sieht die Kommission als problematisch an.

#### **Kein aktueller Änderungsbedarf**

Insgesamt sieht die Europäische Kommission keinen Bedarf, die DSGVO durch konkrete Änderungen anzupassen. Die nächste Evaluierung ist nach Art. 97 Abs. 1 DSGVO für das Jahr 2024 angesetzt. Bis dahin müssen die Aufsichtsbehörden weiterhin ihren Beitrag zur notwendigen datenschutzpolitischen Debatte leisten.

Auch ich halte zum jetzigen Zeitpunkt umfangreiche gesetzliche Änderungen an der DSGVO für verfrüht. Der EDSA erarbeitet Leitlinien zu verschiedenen Thematiken, woran ich mich intensiv beteilige. Hierdurch soll eine einheitliche Rechtsanwendung im Regelungsbereich der DSGVO gewährleistet werden. Ein europäischer Flickenteppich wird dadurch vermieden. Insgesamt ist die DSGVO ein großer Fortschritt für den Datenschutz in Europa. Das neue Regelwerk hat sich auch in Zeiten der Corona-Pandemie bewährt. Auch über die europäischen Grenzen hinweg dient die DSGVO als moderne Grundlage für die Anpassung des Datenschutzrechts. Trotz der großen Fortschritte sehe ich durchaus Bedarf für Verbesserungen bei der praktischen Umsetzung der DSGVO. Das gilt insbesondere im Bereich der Zusammenarbeit der Datenschutzaufsichtsbehörden in grenzüberschreitenden Verfahren. Unterschiede in den nationalen Verwaltungsverfahren dürfen die effektive Durchsetzung der DSGVO gegenüber Datenschutzverstößen international agierenden Unternehmen nicht beeinträchtigen.

### 3.2.3 Gesichtserkennung – Nutzen und Grenzen

Was passiert mit einer Gesellschaft, wenn ihre Mitglieder beim Aufenthalt im öffentlichen Raum regelmäßig von der Polizei kontrolliert werden? An Plätzen, Bahnhöfen und Verkehrsknotenpunkten, jeden Tag? Ohne dafür einen Anlass gegeben zu haben?

Dieses Szenario ist keine Beschreibung der Zustände in fernen, autoritär geführten Ländern. Es betrifft Europa. Es betrifft Deutschland. Sicherheitsbehörden in Europa, im Bund und in den Ländern möchten sich die Vorteile biometrischer Gesichtserkennung zu Nutzen machen. Diskutiert wird, hierfür immer mehr Überwachungskameras einzusetzen. Diese sind bereits jetzt an zahlreichen öffentlichen Plätzen und Bahnhöfen auf die Menschen gerichtet (vgl. 27. TB Nr. 9.3.3 und 28. TB Nr. 6.2).

Für die Sicherheitsbehörden bietet sich die Möglichkeit, Gesichter der Passantinnen und Passanten in Echtzeit, also „live“, mit Fahndungslisten abzugleichen. Sie können Details über die Lebensumstände von Verdächtigen sammeln sowie verdeckte Ermittlungen und Festnahmen durchführen.

Ein solches Vorgehen wirft grundsätzliche Fragen auf. Der geschilderte Live-Abgleich ist das Gleiche wie eine Polizeikontrolle aller Personen, die einen Ort passieren oder sich dort aufhalten. Es wäre dasselbe, wenn jede Person am Eingang eines Bahnhofs ihren Fingerabdruck abgeben müsste, um diesen mit polizeilichen Listen abzugleichen. Dann ist jede Person verdächtig. Die Entlastung gelingt ihr nur über einen Nicht-Treffer beim Abgleich mit den Listen. Die vom Bundesverfassungsgericht verbürgte Vermutung, dass Bürgerinnen und Bürger grundsätzlich rechtschaffen sind, wird in ihr Gegenteil verkehrt.

Die Anwendung einer solchen Technologie betrifft unmittelbar die Privatsphäre des Individuums. Die Technologie bedroht aber auch die Funktionsweise der Demokratie. Denn die Annahme, sich im öffentlichen Raum anonym bewegen zu können, ist für viele Menschen Grundvoraussetzung für eine Teilnahme an Demonstrationen, politisches Engagement und die Bildung von Opposition. Das Wissen, regelmäßig staatlich erfasst zu werden, hat einen einschüchternden und entmutigenden Effekt. Darunter leiden Selbstbestimmung und Vielfalt. Diese sind aber grundlegende Voraussetzungen für das Funktionieren eines auf Pluralität und Mitwirkungsfähigkeit seiner Bürgerinnen und Bürger begründeten freiheitlichen demokratischen Gemeinwesens.

#### EDSA-Richtlinien

Ich begrüße den Entschluss des EDSA, Richtlinien zur Nutzung von Gesichtserkennungstechnologie durch

Strafverfolgungsbehörden zu erarbeiten. Hiervon ist nicht nur die voran genannte Live-Überwachung umfasst, sondern auch andere Anwendungen. Ich freue mich, an den Richtlinien als einer der Berichtersteller maßgeblich mitwirken zu können.

#### Stellungnahme zu Clearview AI

Zur Identifizierung von Personen bietet sich für Strafverfolgungsbehörden auch die Durchforstung des Internets an. Hierauf spezialisierte Unternehmen analysieren mit ihrer Gesichtserkennungssoftware riesige Mengen an Fotos, die Menschen z. B. in sozialen Netzwerken geteilt haben. Aber auch Fotos auf Webseiten des Arbeitgebers sind betroffen. Zahlreiche Sicherheitsbehörden weltweit haben bereits derartige Leistungen in Anspruch genommen.

Die Vorgänge um das Unternehmen Clearview AI führten zu einer Anfrage von mehreren Mitgliedern des EU-Parlaments. Im EDSA wurde daraufhin eine gemeinsame Stellungnahme erarbeitet, an der ich als Berichtersteller mitgewirkt habe.

Der EDSA verweist in seiner Stellungnahme darauf, dass sich eine solche Datenverarbeitung wesentlich von behörden-internen Bildabgleichen unterscheidet. Private Unternehmen führen hier - quasi als Hilfspersonen - den Datenabgleich durch. Unklar ist auch die Art und Weise der Erstellung der Datenpools und deren Rechtmäßigkeit. Die Verarbeitung der so gewonnenen Daten in einem Drittstaat, wie den USA, sehe ich kritisch.

Der EDSA verlangt eine politische Auseinandersetzung über die Rolle von Technologien wie der Gesichtserkennung, insbesondere deren Auswirkungen auf die Grundrechte. Dieser Einschätzung schließe ich mich mit Nachdruck an.

### 3.2.4 Genehmigung und Veröffentlichung der (deutschen) Akkreditierungskriterien zu Überwachungsstellen nach Art. 41 DSGVO

Die deutschen Akkreditierungskriterien für Überwachungsstellen eines Codes of Conduct sind vom EDSA gebilligt und auf der Webseite der DSK veröffentlicht worden.

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 von Verhaltensregeln gem. Art. 41 DSGVO, sogenannte Codes of Conduct, abfassen und veröffentlichen. Zuvor müssen diese gem. Art. 64 Abs. 1 S. 2 lit. c i. V. m. Art. 41 Abs. 3 DSGVO im Rahmen eines Kohärenzverfahrens vom EDSA gebilligt werden. Codes of Conduct „präzisieren“ die DSGVO, die teilweise sehr abstrakte Regelungen und eine Vielzahl von General-

klauseln enthält. Codes of Conduct können hier als Auslegungshilfen herangezogen werden.

Das Kohärenzverfahren und die damit verbundene Stellungnahme des EDSA zu dem nationalen Entwurf von Akkreditierungsanforderungen dienen gem. Art. 63 DSGVO der einheitlichen Anwendung der Art. 40 und 41 DSGVO durch alle Mitgliedstaaten der EU.

Ich hatte bereits die europäischen „Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679“ mit entwickelt. Diese Leitlinien sollen praktische Hinweise und Auslegungshilfen zur Anwendung der Art. 40 und 41 der DSGVO geben und die Vorschriften und das Verfahren zur Einreichung, Genehmigung und Veröffentlichung von Codes of Conduct auf nationaler und europäischer Ebene erläutern. Die Leitlinien sehen u. a. 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 vom EDSA gebilligt. Sie sind auf der Webseite der DSK veröffentlicht.

Ich habe zudem an den Stellungnahmen des EDSA zu den Akkreditierungskriterien für Überwachungsstellen von Codes of Conduct von zehn weiteren EU-Mitgliedstaaten mitgewirkt.

### 3.3 Global Privacy Assembly

Die Global Privacy Assembly (GPA), bis 2019 „International Conference of Data Protection and Privacy Commissioners“, hat sich 2020 u.a. mit den Herausforderungen der COVID-19-Pandemie für den Datenschutz beschäftigt. Erstmals wurde mit dem BfDI ein deutscher Vertreter in das „Executive Committee“ der GPA gewählt.

Wie viele andere internationale Organisationen oder Vereinigungen wurde auch die GPA mit ihren mehr als 120 Datenschutzbehörden aus aller Welt von der COVID-19-Pandemie in Mitleidenschaft gezogen. Dies zeigte sich bei der Arbeitsweise der GPA selbst wie auch bei der Behandlung von Fachthemen. Bereits im Frühjahr 2020 war klar geworden, dass die für den Herbst geplante Konferenz in Mexiko-Stadt nicht wie geplant stattfinden kann. Mit Unterstützung des Sekretariats und insbesondere unter Leitung des GPA-Vorsitzes meiner britischen Kollegin, Elizabeth Denham, ist es der GPA jedoch gelungen, zügig und mit Erfolg auf die daten-

schutzpolitischen Herausforderungen der Pandemie zu reagieren.

Das Executive Committee hat zwei Statements zur Gewährleistung des Datenschutzes auch unter den Bedingungen der Pandemie herausgegeben. Das sind eine allgemeine Erklärung vom März 2020 sowie ein Statement zur datenschutzgerechten Kontaktnachverfolgung vom Mai 2020. Darüber hinaus hat das Executive Committee als Steuerungsgremium der GPA eine COVID-19-Taskforce eingesetzt, die sich im Verlauf des Jahres mit der Sicherstellung des Datenschutzes unter den besonderen Bedingungen der Pandemie beschäftigt hat.

Gerne habe ich in dieser Taskforce mitgewirkt und dabei besonders meine Erfahrungen aus der datenschutzrechtlichen Begleitung der deutschen Corona-Warn-App eingebracht. Im Rahmen der Bekämpfung der COVID-19-Pandemie war bereits recht früh, zuerst in asiatischen Ländern wie Singapur, Südkorea und Taiwan, aufgefallen, dass Applikationen für Mobilfunkgeräte als geeignete Hilfsinstrumente für die Kontaktnachverfolgung in Frage kommen könnten. Mit der Entwicklung entsprechender Software-Anwendungen wurde dann unverzüglich begonnen. Die gesammelte Expertise der COVID-19-Taskforce floss schließlich in ein umfassendes „Best Practice Compendium“ ein, das den Mitgliedern der GPA zur Verfügung gestellt wurde.

Ich freue mich, dass unser jährliches Treffen der GPA-Mitglieder im Herbst 2020 dank der Bemühungen des Vorsitzes und des Sekretariats der GPA noch als gemeinsame Videokonferenz stattfinden konnte. Das erste Treffen dieser Art hatte 1979 in Bonn unter der Bezeichnung Internationale Datenschutzkonferenz stattgefunden.

Die Vorbereitung einer solchen digitalen globalen Veranstaltung begegnet erheblichen praktischen Schwierigkeiten. So muss eine für Teilnehmer von Chile im Westen bis Neuseeland im Osten geeignete Uhrzeit gefunden werden, denn irgendwo ist es immer schon sehr früh oder sehr spät.

Das virtuelle Jahrestreffen 2020 hat sich nicht nur mit der COVID-19-Pandemie befasst. Es wurden auch Entschlüsse zu wichtigen Zukunftsthemen angenommen, z. B. zur KI (Artificial Intelligence/AI) oder zur Gesichtserkennung (Facial Recognition). In beiden Fällen verlangt die GPA, dass für die Betroffenen Transparenz über Art und Umfang der Verarbeitung personenbezogener Daten gewährleistet sein muss. Es darf auch keine rein maschinellen Entscheidungen über Menschen geben. Das ist nicht allein zum Schutz der personenbezogenen Daten wichtig, sondern auch zur Vermeidung systemimmanenter Diskriminierungen.



Die GPA hat ihren Weg hin zu einer besser strukturierten Organisationsform fortgesetzt. Ihre Mitglieder haben es dem Executive Committee erlaubt, künftig auch außerhalb des jährlichen Treffens Beschlüsse oder Entschlüsse zur Annahme vorzulegen. Dadurch soll die GPA als Organisation auf aktuelle datenschutzrechtlich relevante Themen und Ereignisse besser reagieren können.

Als erstes deutsches Mitglied wurde ich auf dem Treffen in das Executive Committee der GPA gewählt. Für die breite Unterstützung, die ich bei dieser einstimmigen Wahl aus den Reihen meiner Kolleginnen und Kollegen in der GPA erfahren durfte, danke ich ausdrücklich. In den kommenden zwei Jahren werde ich sowohl die breit gefächerte Erfahrung deutscher Datenschutzbehörden einbringen und eine Verknüpfung des GPA Executive

Committee mit dem EDSA anstreben. Auf diese Weise möchte ich zu einer weiteren Harmonisierung des Datenschutzes auch auf globaler Ebene beitragen.

Die Konferenz 2021 soll nach aktueller Planung in Mexiko als Präsenzveranstaltung stattfinden. Ich danke meinem Kollegen in Mexiko für seine Bereitschaft, die GPA-Konferenz auch ein Jahr später als Gastgeber auszurichten.

Die Statements, Entschlüsse und weitere Dokumente der GPA finden sich unter [www.globalprivacyassembly.org](http://www.globalprivacyassembly.org).

#### **Querverweise:**

3.2 EDSA, 4.1.1 Corona-Warn-App

## 4

## Schwerpunktt Themen

### 4.1 Corona

Die Corona-Pandemie prägte das ganze Jahr 2020 – auch im Datenschutz. Beratung und Information waren nicht nur im Zusammenhang mit der Entwicklung von Apps notwendig und zeitaufwändig, sondern auch für die datenschutzkonforme Ausgestaltung von Gesetzen und Verordnungen oder die Nutzung von Videokonferenzsystemen. Nachfolgend sind einige der Beratungspunkte rund um die Pandemiebekämpfung dargestellt.

#### 4.1.1 Die Corona-Warn-App der Bundesregierung

Die Corona-Warn-App (CWA) der Bundesregierung wurde am 16. Juni 2020, nach etwas mehr als zwei Monaten Entwicklungszeit, durch das Robert Koch-Institut (RKI) veröffentlicht. Als Contact-Tracing-App ermöglicht sie die datenschutzfreundliche Erfassung von möglicherweise infektionsrelevanten Begegnungen

zwischen Nutzerinnen und Nutzern der App unter Verwendung des Bluetooth-Standards. Bei einem positiven COVID-19-Testbefund können Nutzerinnen und Nutzer sehr schnell ihre Kontakte über die Corona-Warn-App warnen, ohne dabei ihre Identität offenlegen zu müssen. Die so gewarnten Kontaktpersonen haben dann die Möglichkeit, sich an Ärzte und Gesundheitsämter zu wenden und sich selbst testen zu lassen. Durch ihr umsichtiges Verhalten leisten die gewarnten Kontaktpersonen einen effektiven Beitrag zur Vermeidung weiterer Infektionen.

Das Projekt CWA habe ich von Beginn an in beratender Funktion begleitet und nehme auch die Datenschutzaufsicht über das Projekt des RKI wahr.

#### Datenschutz als Erfolgsfaktor

Um effektiv wirken zu können, ist die CWA auf die Unterstützung durch große Teile der Bevölkerung angewie-



sen. Der Datenschutz ist ein wesentlicher Faktor für die Akzeptanz bei solchen digitalen Lösungen. Die vergleichsweise hohe Zahl von gut 25 Millionen Downloads zeigt, dass dies auch bei der CWA der Fall ist. So gilt das französische Pendant, das einen weniger datenschutzfreundlichen Ansatz mit zentraler Datenverarbeitung verfolgt, mit nur rund 2 Millionen Downloads bei noch geringerer Nutzung bereits als gescheitert.

Ein solcher zentraler Ansatz wie z.B. in Frankreich wurde zuerst auch in Deutschland und weiteren Staaten durch die multinationale Initiative PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) diskutiert. Nach kritischer Bewertung von Seiten der Wissenschaft, Zivilgesellschaft und Datenschützern wurde die Umsetzung dieses Ansatzes aber Ende April 2020 durch die Bundesregierung schließlich verworfen. Stattdessen wurde ab diesem Zeitpunkt der nun verwendete dezentrale Ansatz konsequent umgesetzt. Das Vorhaben wurde dabei durch sinnvolle Maßnahmen, wie die Entwicklung in einem überaus transparenten Open-Source-Verfahren, flankiert. Die allgemeine Kritik an der Verwendung des von Apple und Google bereitgestellten Protokolls Google/Apple Exposure Notifications, insbesondere der Vorwurf eines unberechtigten Abgreifens von Daten, wurde bislang nicht durch nachvollziehbare Belege untermauert. In der Gesamtschau lässt sich festhalten, dass mit der CWA eine grundsätzlich datenschutzfreundliche Umsetzung des dezentralen Contact-Tracing-Ansatzes gelungen ist.

### **Problematischer Medienbruch**

Dem positiven Eindruck der Kernanwendung in Form der CWA gegenüber steht leider das problembeladene, aber für deren praktischen Einsatz unabdingbare Betriebsumfeld. So war bereits zum Start der CWA klar, dass mangels der hierfür erforderlichen technischen Ausstattung längst nicht alle beteiligten Labore in der Lage sein würden, ihre Testergebnisse für die Nutzerinnen und Nutzer der App bereitzustellen.

So konnten die Nutzerinnen und Nutzer, deren Tests von diesen Laboren ausgewertet wurden, den datenschutzfreundlichen Workflow zur Ergebnisbereitstellung in der CWA nicht nutzen und ihre Kontakte bei einem positiven Befund nicht direkt warnen. Stattdessen musste für diese Fälle ein alternativer Prozess unter Verwendung sogenannter „Tele-TANs“ etabliert werden. Um diese Tele-TAN zu erhalten, müssen sich die positiv getesteten Nutzerinnen und Nutzer an eine Freischalt-Hotline wenden.

Dieser unerwünschte Medienbruch bei der App-Nutzung stellt ein Datenschutzrisiko dar, insbesondere da bei der Hotline kurzzeitig personenbezogene Daten vorgehalten

werden, die eine Identifikation der Anruferinnen und Anrufer ermöglichen.

Im Rahmen der Datenschutzaufsicht habe ich daher besonderes Augenmerk auf die frühzeitige Prüfung dieser Hotline gelegt. Dabei stellte ich geringe Mängel bei der Zutrittskontrolle fest.

Erfreulicherweise ist es dem RKI gelungen, diese Mängel zeitnah zu beheben. Das Problem der fehlenden Laboranbindungen ist aber auch jetzt noch nicht gelöst. Der aus Sicht des Datenschutzes problematische Medienbruch besteht weiter fort.

### **Ein Blick in die Zukunft**

Zum Redaktionsschluss war noch kein Ende der COVID-19-Pandemie absehbar. Zuletzt laut gewordene Kritik an mangelnden Fähigkeiten und Funktionen der CWA war teils berechtigt, oft aber auch auf Unwissenheit über die bewusst gewählte Zielsetzung und die Grenzen der technischen Möglichkeiten des gewählten Ansatzes zurückzuführen. So wurde die CWA zum Beispiel ganz bewusst für den Zweck des datensparsamen Contact-Tracing (Rückverfolgung) entwickelt. Deshalb wurde ein Contact-Tracking (Verfolgung) nicht geplant und ist technisch in dieser App nicht möglich.

Ungeachtet dessen besteht selbstverständlich Potenzial für eine Weiterentwicklung der CWA. Ideen wie eine Clustererkennung sind sinnvoll und möglich. Schade ist nur, dass ich als zuständige Datenschutzaufsicht von vielen dieser Überlegungen erst spät aus der Presse erfuhr. Hier wäre eine zeitnahe Einbindung seitens der Verantwortlichen in die Planungen geeigneter.

Mit dem Ende der COVID-19-Pandemie wird auch der Einsatz der CWA enden. Die dabei gewonnenen Erkenntnisse, wie derartige Lösungen auf freiwilliger Basis effektiv und datenschutzfreundlich umsetzbar sind, sollten bei eventuellen zukünftigen Projekten Berücksichtigung finden.

Weitere Informationen zum Thema finden Sie auch in der Guideline des EDSA vom 21. April 2020, die Sie unter [www.bfdi.bund.de/guidelines](http://www.bfdi.bund.de/guidelines) abrufen können.

#### **4.1.2 Die Datenspende-App**

Mit der App Corona-Datenspende analysiert das Robert Koch-Institut (RKI) freiwillig bereitgestellte Daten aus Fitness-Trackern von inzwischen mehr als 500.000 Bürgerinnen und Bürgern. Dazu verarbeitet das RKI insbesondere auch Gesundheitsdaten, die als besondere Kategorie personenbezogener Daten gelten. Mit den Erkenntnissen aus der Analyse dieser Daten beabsichtigt das RKI, die Vorhersage von Erkrankungen wie COVID-19 zu optimieren. Dadurch soll eine bessere

Steuerung von Eindämmungsmaßnahmen gegen die derzeitige Pandemie ermöglicht werden.

Inmitten der Diskussion über die Einführung einer Corona-Tracing-App veröffentlichte das RKI am 7. April 2020 die Corona-Datenspende-App. Mit der überraschenden Veröffentlichung dieser zusätzlichen App sorgte das RKI nicht nur in der breiten Öffentlichkeit für Verwirrung.

Auch ich wurde mit nur wenigen Tagen Vorlaufzeit sehr kurzfristig eingebunden. In meiner Ersteinschätzung konnte ich das RKI zu einigen, für den Datenschutz wesentlichen Aspekten, beraten. Eine fertige Version der Corona-Datenspende-App lag aber auch mir bis zu deren Veröffentlichung im April nicht vor.

Mit der Veröffentlichung dieser ersten staatlichen Corona-App stieß das RKI auf breite Resonanz in der Zivilgesellschaft. Deren Engagement, wie zum Beispiel die Untersuchung durch den Chaos Computer Club (CCC), begrüße ich ausdrücklich. Dabei aufgezeigte Mängel dienen immer der Verbesserung und liefern nicht zuletzt zusätzliche Erkenntnisse für die Arbeit der Datenschutzaufsicht.

Bis heute begleite ich das RKI bei diesem Projekt im Rahmen meiner Datenschutzaufsicht. Dabei wurden verschiedene Aspekte der Datenverarbeitung geprüft. Festgestellte Mängel wurden umgehend mit dem RKI diskutiert und oft sehr kurzfristig abgestellt. Abhilfemaßnahmen nach Art. 58 DSGVO waren bis Redaktionsschluss nicht erforderlich.

Wie bereits bei meiner Ersteinschätzung hat auch die weitere Analyse und Bewertung gezeigt, dass die Schnittstelle zwischen den Systemen des RKI und den Fitness-Tracker-Anbietern das größte Problem aus Sicht des Datenschutzes darstellt. So stellte die datenschutzkonforme Erhebung der Fitness-Tracker-Daten aus den Systemen der unterschiedlichen Anbieter das RKI teils vor große Herausforderungen hinsichtlich der Datenminimierung. Diese ist aber unbedingt erforderlich, um das zentrale Versprechen der Pseudonymität von Nutzerinnen und Nutzern der Corona-Datenspende einhalten zu können.

Unabhängig von konkreten Mängeln stellt sich bei einem solchen Projekt mit experimentellem Charakter immer die Frage, ob die Datenverarbeitung ihren eigentlichen Zweck auch tatsächlich erfüllt. Tut sie das nicht, muss die Verarbeitung beendet werden. Daher hatte ich bereits bei der Veröffentlichung darauf hingewiesen, dass ich eine regelmäßige Evaluierung erwarte. Die mir hierzu bislang vorliegenden Stellungnahmen des RKI lassen eine diesbezügliche endgültige Bewertung aktuell noch nicht zu.

#### 4.1.3 Corona-Maßnahmen und -Projekte

**Datenschutz in Zeiten von Corona: Wie lässt sich verhindern, dass der Datenschutz zum prominenten Opfer der Pandemie wird? Vertrauen ist für die Akzeptanz der Nutzer digitaler Anwendungen elementar. Deshalb berate ich bei der Entwicklung und Entstehung solcher Anwendungen, bin allerdings keine Genehmigungsbehörde.**

Zur Bewältigung der Corona-Pandemie hat das Bundesministerium für Gesundheit (BMG) eine Vielzahl von Projekten entwickelt und gefördert. Bereits im Frühjahr kam der im BMG zuständige Projektmanager auf mich zu und bat um meine Unterstützung. Da ich ein großes Interesse daran habe, dass angesichts der besonderen Umstände und des hohen Zeitdrucks der Schutz personenbezogener Daten im Blick bleibt, habe ich gerne zugesagt, mich mit den jeweiligen Maßnahmen und Projekten bevorzugt zu befassen.

##### Symptom-Tagebuch

Eines der Projekte war das sog. Symptom-Tagebuch, eine webbasierte Anwendung, die den Gesundheitsämtern das Management der Kontaktpersonen erleichtern und ihnen vom BMG unentgeltlich zur Verfügung gestellt werden soll. Die Kontaktpersonen in Quarantäne erhalten dabei täglich einen Link und füllen dann selbst den Online-Fragebogen zu ihren Symptomen aus, so dass das aufwendige Telefonieren entfällt. Ich habe das BMG beraten und auf eine Nachbesserung der Unterlagen hingewirkt. So wurde auf eine zusätzliche Berichtsfunktion verzichtet, die statistische Auswertungen der erfassten Daten erzeugt, nachdem ich Zweifel an der Wirksamkeit der dafür vorgesehenen Anonymisierung angemeldet und entsprechende Absicherungen gefordert hatte.

Einer abschließenden oder verbindlichen Einschätzung stand jedoch entgegen, dass es auch auf die konkrete Anbindung in die IT-Struktur ankam. Zudem sind für die Datenverarbeitung in den kommunalen Gesundheitsämtern die jeweiligen Landesdatenschutzbeauftragten zuständig. Dem – nicht nur hier – geäußerten dringenden Wunsch, eine „Freigabe“ zu erteilen, konnte ich aber auch deshalb nicht nachkommen, da dies nicht zu meinen gesetzlichen Aufgaben und Rechten gehört: Der BfDI ist keine Genehmigungsbehörde, dies würde nämlich z.B. auch eine technische Durchprüfung aller verwendeten Bausteine einer Lösung notwendig machen.

##### DEMIS-SARS-CoV-2

Beraten habe ich das BMG und das Robert Koch-Institut (RKI) beim Start des Deutschen Elektronischen Melde- und Informationssystems für den Infektionsschutz (DEMIS) in einer ersten Ausbaustufe (DEMIS-SARS-CoV-2). Ich hatte diese Software bereits in den Anfängen

ihrer Entwicklung in den Jahren 2013/2014 eng begleitet. DEMIS soll der rein elektronischen Abwicklung der im Infektionsschutzgesetz (IfSG) vorgesehenen Meldepflichten dienen, sieht aber auch weitere Funktionen mit zentraler Datenspeicherung und Zugriffsmöglichkeiten der jeweiligen Behörden vor. Die gesetzliche Grundlage für DEMIS ist § 14 IfSG. Allerdings liegt die hier vorgesehene Verordnung mit näheren Bestimmungen zur Umsetzung noch nicht vor. DEMIS ist daher bislang noch nicht im vollen Umfang im Einsatz. Durch bestimmte Funktionen dürften Bereiche mit gemeinsamer datenschutzrechtlicher Verantwortung entstehen, die besondere Vereinbarungen erfordern. Um in der Pandemie-Lage möglichst schnell einen sicheren Übertragungsweg für die Meldung der vielen Infizierten nutzen zu können, wurde das System allerdings vorab - mit begrenztem Umfang - in Betrieb gesetzt. Für diese Funktionalitäten können die datenschutzrechtlichen Verantwortlichkeiten leichter zugeordnet werden. So können die Daten verschlüsselt von den Laboren zu den Gesundheitsämtern und weiter zum RKI übermittelt werden. Nach vorgegebener Struktur werden die Testergebnisse und weitere Angaben erfasst, im System dem zuständigen Gesundheitsamt zugeordnet und dann nach dort gemeldet. Dabei wird ein besonderes Pseudonymisierungsverfahren eingesetzt, das die Identifizierung von Doppelmeldungen ermöglicht. Das ist ein wesentlicher Fortschritt gegenüber der zuvor praktizierten Übermittlung per Fax, sowohl was die Geschwindigkeit betrifft als auch den Datenschutz. Die im IfSG zunächst eingeführte Pflicht zur Meldung der Negativ-Getesteten hätte ebenfalls über DEMIS erfüllt werden sollen. Ich hatte das RKI bereits darauf hingewiesen, dass ich die Meldungen für nicht zulässig halte. Noch vor dem Betrieb von DEMIS-SARS-CoV-2 wurde die Pflicht im Gesetz vernünftigerweise wieder gestrichen.

#### **SORMAS@DEMIS**

Im Zusammenhang mit DEMIS steht auch die Beratung von BMG und RKI zu der Software SORMAS mit verschiedenen Modulen. SORMAS steht für Surveillance Outbreak Response Management und Analysis System und wurde vom Helmholtz-Zentrum für Infektionsforschung (HZI) zur Erfassung der Fälle und Kontaktpersonen entwickelt. Das BMG wollte den Gesundheitsämtern diese Software kostenfrei zur Verfügung stellen, um deren Arbeit zu unterstützen. Die Version SORMAS-ÖGD wurde auch vorher schon in einigen Gesundheitsämtern angewandt, um die Fälle zu verwalten – SORMAS –L (für local). Es enthält neben einer Berichtsfunktion- auch eine Schnittstelle für eine Tagebuchfunktion für die Quarantäne. Die Anbindung von SORMAS an DEMIS erleichtert mit einem effizienten Kontaktpersonenmanagement die Ermittlung von Kontaktketten, auch über

die kommunalen Grenzen hinweg, da die Gesundheitsämter auch untereinander vernetzt sind – SORMAS X (für eXchange). Ein weiteres Modul dient der übergreifenden Datenanalyse - SORMAS XL (für eXtra Laxer), ist aber bei Redaktionsschluss noch nicht im Einsatz, da ich wegen der ungeklärten Rechtsgrundlage Bedenken angemeldet hatte. Dass die Anwendungen beim Informationstechnikzentrum des Bundes (ITZBund) gehostet werden, begrüße ich, da dies etwaige Bedenken an einer Datenhaltung durch Privatunternehmen ausräumt. Um die rechtlichen Anforderungen zu erfüllen, müssen nun die jeweiligen Gesundheitsämter Auftragsvereinbarungen mit dem ITZBund schließen.

Auch bei dieser Beratung bestand die Problematik, dass ich für die Bewertung der Software im konkreten Einsatz in den Gesundheitsämtern rechtlich nicht zuständig bin. In diesem Fall habe ich in Absprache mit BMG und HZI die Landesdatenschutzbeauftragten in die Beratung eingebunden und eine gemeinsame datenschutzrechtliche Einschätzung der zuständigen Datenschutzaufsichtsbehörden in den Ländern koordiniert. Letztlich war ich gemeinsam mit den Landesdatenschutzbehörden mit einem Betriebsbeginn „unter Vorbehalt“ einverstanden, da das BMG versichert hatte, auch während des Betriebs nötige datenschutzrechtliche Verbesserungen zu veranlassen. Zudem war die bisherige Praxis der Fallbearbeitung in den Gesundheitsämtern oft weder effizient noch datenschutzkonform, und es bestand hoher politischer Druck, das neue System einzusetzen.

#### **Forschungsprojekt KaDoIn**

Eine weitere Beratungsbitte des BMG bezog sich auf KaDoIn, eine von der Medizinischen Hochschule Hannover (MHH) konzipierte Anwendung zur kartenbasierten Dokumentation von Indexpatienten. KaDoIn dient dazu, die Standortdaten aus dem Smartphone eines infizierten Indexpatienten auszulesen, mittels Googlemaps zu visualisieren, strukturiert aufzubereiten und mit den Standortdaten möglicher Kontaktpersonen abzugleichen. Die MHH erforschte im Rahmen einer vom BMG geförderten Studie, wie hiermit die Kontaktpersonennachverfolgung der Gesundheitsämter unterstützt werden kann. Die Sorge vor einem unzulässigen Tracking konnte rasch ausgeräumt werden, da die Daten lokal im Browser aufbereitet und strukturiert angeboten werden. Der Nutzer – also der Indexpatient – entscheidet selbst, welche Daten er auswählt und dem Gesundheitsamt übermittelt. Die Teilnahme an der Studie war freiwillig, daher sah ich keine wesentlichen datenschutzrechtlichen Hindernisse.

#### **Querverweis:**

##### **4.1.4 Änderungen des Infektionsschutzgesetzes**



#### 4.1.4 Änderungen des Infektionsschutzgesetzes

In drei „Etappen“ wurde das Infektionsschutzgesetz (IfSG) aufgrund der Pandemie-Lage geändert. Dabei wurde durch die Ausweitung sowohl der Gründe als auch des Umfangs von Meldepflichten für Erkrankungen und Krankheitserreger erheblich in das Grundrecht auf informationelle Selbstbestimmung eingegriffen. Transparente Begründungen und eine Auseinandersetzung mit den datenschutzrechtlichen Anforderungen wären nötig gewesen, fehlten jedoch immer wieder. Die unzureichend begründete Meldepflicht der Negativ-Getesteten wurde vernünftigerweise wieder gestrichen.

Nachdem bereits im Januar 2020 die Meldepflicht für Erkrankungen und Krankheitserreger nach dem Infektionsschutzgesetz durch Verordnung auf COVID-19 und SARS-CoV-2 ausgedehnt worden war, wurde das Infektionsschutzgesetz im März, April und November geändert. Die fachlichen Abstimmungen und die politischen Beschlüsse wurden in kürzesten Zeitspannen getroffen. Nicht nur die Anzahl der Gesetze und Verordnungen, die das Bundesministerium für Gesundheit (BMG) bearbeitet hat, stieg durch die Pandemie in rekordverdächtige Höhen. Auch die zur Befassung gewährten Zeitspannen für die Beratung waren extrem kurz. Dabei gestand das BMG auch bei den vielen übrigen, nicht durch „Corona“ begründeten Gesetzen und Verordnungen ohne erkennbaren Grund nicht die in der Gemeinsamen Geschäftsordnung der Bundesministerien vorgesehenen Beteiligungsfristen zu.

##### Erstes Pandemie-Schutz-Gesetz

Zum (Ersten) Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite gab es am Freitagnachmittag eine Vorwarnung, dass der Entwurf am Samstag, dem 21. März 2020, mit einer Frist zur Stellungnahme von vier (!) Stunden vorgelegt wurde. Neben weitreichenden Eingriffs- und Verordnungsbefugnissen für das BMG waren Pflichten für Beförderungsternehmer und Fluggesellschaften vorgesehen. Ich habe erhebliche Zweifel an der Verfassungsmäßigkeit geltend gemacht, insbesondere hinsichtlich der Geeignetheit einiger Maßnahmen. Auch während einer Pandemie sind Grundrechte nicht außer Kraft gesetzt. Leider wurden meine Bedenken überwiegend nicht berücksichtigt. Weder die erforderliche Nachbesserung der Begründung oder die von mir geforderte Evaluation, noch die nötigen Löschvorgaben oder die zielführende datenschutzrechtliche Begleitung landesübergreifender Forschungsvorhaben zentral durch mich wurden vorgesehen.

Mit dem Gesetz wurde auch das Gesetz zur Durchführung der Internationalen Gesundheitsvorschriften geändert. Die darin nunmehr vorgesehenen Abfragen beim Fluggastdaten-Informationssystem verstoßen gegen die EU-Richtlinie über PNR-Daten.<sup>7</sup> Nachdem der Bundestag das Gesetz am 25. März 2020 beschlossen und der Bundesrat am 27. März zugestimmt hatte, trat es am 28. März 2020 in Kraft. (s. meine Stellungnahme vom 3. April 2020 [www.bfdi.bund.de/stellungnahmen](http://www.bfdi.bund.de/stellungnahmen))

##### Zweites Änderungsgesetz

Der Entwurf des Zweiten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite wurde am Nachmittag des 20. April 2020 versandt mit der Bitte um Stellungnahme bis zum 22. April 2020. Auch in diesem Gesetzentwurf waren weitgehende Veränderungen des IfSG enthalten. Nicht alle waren eilbedürftig: Ohne Bezug zur aktuellen Lage wurde die namentliche Meldepflicht bei neuen, bislang unbekannten Erkrankungen bereits auf den Verdachtsfall ausgeweitet. Konkret auf SARS-CoV-2 und SARS-CoV bezogen wurde dagegen die neu eingeführte Meldepflicht bei negativem Testergebnis an das Robert Koch-Institut (RKI). Die Begründung dafür enthielt jedoch ausschließlich statistische Erwägungen. Dass die Meldungen an das RKI pseudonymisiert abgegeben werden sollten und daher die Vorgaben der DSGVO einzuhalten waren, wurde im Gesetz und seiner Begründung nicht berücksichtigt. Das Infektionsschutzgesetz dient der Gefahrenabwehr, konkret dem Schutz vor Ansteckung mit einer infektiösen Krankheit. Die Negativ-Getesteten sind jedoch nicht ansteckend. Ich hielt die Meldungen in dieser Form daher für nicht erforderlich und damit für unzulässig. Leider blieb die Regelung dennoch zunächst im Gesetz. Keinen Eingang ins Gesetz fand der Immunitätspass. Ein Immunitätspass würde eine gesundheitsbezogene Angabe enthalten, die ärztliche Bewertung der Immunität. Damit würde er sich wesentlich vom Impfpass unterscheiden, der die Tatsache der Impfung dokumentiert. Für den Impfpass gilt, dass nur in bestimmten Fällen eine Einsicht verlangt werden darf. Da im April die Immunität bezüglich SARS-CoV-2 wissenschaftlich noch nicht geklärt war, wurde die Regelung wieder zurückgezogen. In meinen Augen wäre es mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren, sollte ein Immunitätsnachweis allgemein als „Eintrittskarte“ eingesetzt werden. Das würde umgekehrt zu einer Diskriminierung derjenigen führen, die einen derartigen Nachweis nicht erbringen können. Dieses Gesetz trat am 23. Mai 2020 in Kraft.

<sup>7</sup> Art. 1 Abs. 2 der RL (EU)2016/681 vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

Der Ablauf dieses Gesetzgebungsvorhabens zeigte, dass die pandemische Lage auch bei der Regierung große Unsicherheit ausgelöst hat. Es fehlten belastbare wissenschaftliche Erkenntnisse zu Infektionswegen und -gefahren, zur Erkrankungswahrscheinlichkeit und Wiederansteckungsgefahr und zu zielführender medikamentöser Behandlung. Dieser Unsicherheit sollte offenbar mit umfassender, gesetzlich verpflichtender bundesweiter staatlicher Erhebung von personenbezogenen Gesundheitsdaten begegnet werden. Ob auch regionale Erhebungen oder Erhebungen auf Basis einer Einwilligung im Rahmen von klinischen und wissenschaftlichen Forschungsvorhaben zu hinreichenden Erkenntnissen hätten führen können, wurde nicht diskutiert.

### **Drittes Pandemie-Schutz-Gesetz**

Das Dritte Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Bedeutung wurde am Abend des 14. Oktober 2020 mit Frist zur Stellungnahme bis zum 16. Oktober 2020 vorgelegt. Eine veränderte und teilweise ergänzte Fassung wurde am Freitag, den 23. Oktober morgens, mit Frist bis zum gleichen Tag 18.00 Uhr übersandt. Diese extrem kurzen Fristen erschwerten die sachgerechte Bearbeitung. Da die Pandemie-Lage zu diesem Zeitpunkt bereits seit mehreren Monaten bestand, war diese Eile aus meiner Sicht nicht angemessen, hätte aber zumindest mit einer Einbindung in die Überlegungen auch vor Erstellung eines abgestimmten Entwurfs gemindert werden können. Erneut wurden verschiedene Meldepflichten und Übermittlungen personenbezogener Daten eingeführt oder erweitert. Hierbei wurde nicht berücksichtigt, dass die Verarbeitung von Gesundheitsdaten, also besonders geschützten personenbezogenen Daten, einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Diese sind daher sorgfältig zu begründen und zu rechtfertigen und es sind besondere flankierende Maßnahmen zum Schutz der sensiblen Daten vorzusehen. Insbesondere wurde eine Verfeinerung der Angaben zum Wohnort der Infizierten vorgesehen, ohne zu berücksichtigen, dass dadurch das Re-Identifikationsrisiko steigt. Denn diese Regelung gilt nicht nur für COVID-19, sondern auch für andere, seltenere Erreger. Zudem wurde ohne ausreichende Begründung vorgesehen, dass pseudonyme Meldungen zur Impfung und zu Impffolgen nun an zwei verschiedene Stellen zu adressieren sind: an das Robert Koch-Institut und das Paul-Ehrlich-Institut. Das führt zu einer Verdoppelung der Datenmenge, die ich kritisch sehe. Ausgeweitet wurden auch die Pflichten bei der Einreise: Statt der sogenannten Aussteigekarte, die auf Grundlage der internationalen Gesundheitsvorschriften von den Passagieren auszufüllen und dann dem zuständigen Gesundheitsamt zuzuleiten ist, wird nun eine Digitale Einreiseanmeldung vorgesehen, in der auch

Individualreisende Angaben zu Person und Aufenthalt machen müssen.

Interessant ist auch der Vergleich der Formulierungen der bisherigen Aussteigekarte und derjenigen für COVID-19: In der bisherigen gibt es Erläuterungen zu Grundlagen der Datenverarbeitung. Dann werden Daten zu Person, Mitreisenden und Aufenthaltsorten erfragt. Die COVID-19-Fassung weist dagegen drastisch auf die Ausfüllpflicht und das drohende Bußgeld bei Falschangaben hin. Dann werden zusätzlich Gesundheitsinformationen abgefragt, nämlich Symptome und Testung. Dadurch waren erhöhte Anforderungen an die Sicherheit der Verarbeitung der Daten zu erfüllen, die ich bei der Beratung zur technischen Umsetzung beim digitalen Versand der Aussteigekarten zu berücksichtigen hatte.

Problematisch waren auch im Dritten Pandemie-Schutz-Gesetz wieder die Regelungen, die Pflichten und Befugnisse für Beförderungsunternehmen und Bundespolizei im Zusammenhang mit der Einreise betreffen. Durch Verordnung kann vorgesehen werden, dass den Beförderern Nachweise über Meldepflichten, Impfungen und Gesundheitszustand vorzulegen sind und dass die Beförderer ihrerseits Daten der Passagiere übermitteln müssen. Die Bundespolizei soll die Erfüllung der Pflichten aus der Verordnung überwachen und Verstöße melden. Die Begründung blieb hier erneut deutlich hinter den Anforderungen der Gemeinsamen Geschäftsordnung der Bundesministerien zurück. Die Grundrechtseingriffe werden nicht ausreichend abgewogen und gerechtfertigt. Insbesondere Geeignetheit und Erforderlichkeit der Maßnahmen werden nicht dargelegt. Im Kontext der EU bedarf eine Unterscheidung zwischen grenzüberschreitenden und innerdeutschen Reisen einer besonderen Begründung. Die nach Artikel 9 Absatz DSGVO für die Verarbeitung von Gesundheitsdaten notwendigen besonderen Schutzmaßnahmen werden nicht erwähnt. Weitere Vorgaben für die Beförderer, also private Unternehmen, fehlen. Dabei ist zu regeln, ob und wie sie die Daten erheben und wie lange, in welchem Umfang und mit welchen Schutzvorkehrungen sie sie speichern dürfen. Als Erfolg konnte ich jedoch verbuchen, dass mit diesem Gesetz die Meldepflicht der Negativ-Getesteten wieder gestrichen wurde, bevor mit ihrer Umsetzung begonnen wurde.

#### **4.1.5 Schutzmaske nur gegen Daten?**

Kurz vor Weihnachten wollte der Bundesgesundheitsminister Gutes tun und per Verordnung an besonders Gefährdete kostenfrei Schutzmasken über Apotheken verteilen lassen. Einige Apotheker sahen dies als Chance, auch für andere Zwecke an die Daten Ihrer Kunden zu kommen.

Anfang Dezember erließ das Bundesministerium für Gesundheit (BMG) die „Verordnung zum Anspruch auf Schutzmasken zur Vermeidung einer Infektion mit dem Coronavirus SARS-CoV-2 - Coronavirus-Schutzmasken-Verordnung (SchutzmV)“, mit der Personen, die das 60. Lebensjahr vollendet haben, sowie Personen, bei denen bestimmte Erkrankungen oder bestimmte Risikofaktoren für einen schweren Verlauf der COVID-19-Erkrankung vorliegen, Anspruch auf drei FFP2-Schutzmasken oder ähnlicher Qualität erhalten. Die Verteilung erfolgt über die Apotheken. Für die Verteilung sieht § 4 Absatz 1 Satz 1 SchutzmV vor, dass die Anspruchsberechtigten ihr Alter durch „Vorlage des Personalausweises“ nachweisen sollen. Wie ich einigen Beschwerden Betroffener entnehmen konnte, haben manche Apothekerinnen und Apotheker in diesem Zusammenhang den Ausweis ihrer Kunden gleich kopiert. Dafür existiert keinerlei Berechtigung oder Rechtsgrundlage. Einige Apothekerinnen und Apotheker wollten zudem nur dann eine eigentlich kostenlos abzugebende Schutzmaske aushändigen, wenn die Betroffenen zuvor einen Antrag für eine Kundenkarte ausgefüllt und sich bereit erklärt haben, dass deren Daten (für Werbezwecke) an Dritte übermitteln werden dürfen. Die nach dem Willen des BMG eigentlich kostenlosen Schutzmasken sollten also mit den Daten der Anspruchsberechtigten bezahlt werden.

Ich habe das BMG gebeten, einzuschreiten und die Apotheken aufzufordern, sich entsprechend der Verordnung zu verhalten. Da ich für die Apotheken nicht die zuständige Datenschutzaufsichtsbehörde bin, habe ich die konkreten Beschwerden an meine Kolleginnen und Kollegen in den Ländern mit dem Hinweis weitergegeben, zu prüfen, ob hier nicht Bußgelder nach der DSGVO zu verhängen sind.

#### **4.1.6 Messenger und Videokonferenzssysteme - Fluch und Segen in Corona-Zeiten**

Videokonferenzsysteme und Messenger-Apps haben seit Beginn der Corona-Pandemie einen enormen Zuwachs in ihrer Bedeutung erfahren, denn Konferenzen, Homeoffice und mobiles Arbeiten wären ohne sie sehr viel schwieriger umzusetzen. Leider sind nicht alle Systeme mit Blick auf den Datenschutz unbedenklich.

Homeoffice und mobiles Arbeiten können wichtige Beiträge dazu leisten, in Situationen wie der Corona-Pandemie die Anzahl und Dauer direkter Kontakte zu verringern und so die Ansteckungsgefahr zu reduzieren. Die breite Verfügbarkeit leistungsfähiger Mobilfunk- oder Festnetzverbindungen ermöglicht es, einen großen Teil der Besprechungen und Veranstaltungen, die in der Vergangenheit als Präsenzveranstaltungen durchgeführt wurden, stattdessen virtuell abzuhalten. Dabei müssen

jedoch die Grundsätze des Datenschutzes beachtet werden, was sich bei so mancher technischen Lösung als problematisch erweist.

#### **Anfänglich große Unsicherheit**

Zu Beginn der Kontaktbeschränkungen im Frühjahr 2020 waren viele Firmen und Behörden gezwungen, schnell eine funktionierende Kommunikationsinfrastruktur zu schaffen, um Homeoffice und mobiles Arbeiten in einem Umfang zu ermöglichen, der zuvor kaum vorstellbar war. Gerade in dieser Phase gab es neben den rein praktischen Herausforderungen eine große Unsicherheit, welche der verfügbaren Lösungen Firmen und Behörden einsetzen können. Es durfte keine Vernachlässigung des Schutzes der personenbezogenen Daten der Beschäftigten und von Kundinnen und Kunden erfolgen. Andererseits war eine erhöhte Bereitschaft erkennbar, diesen Schutz - entweder bewusst oder unbewusst - erst einmal hintanzustellen.

#### **Chancen und Risiken beim Einsatz von Videokonferenzsystemen**

Gerade in einer Situation wie der Corona-Pandemie bieten Videokonferenzsysteme die Chance, Anzahl und Dauer direkter Kontakte deutlich zu reduzieren, wenn Beschäftigte vermehrt mobil bzw. aus dem Homeoffice arbeiten oder wenn Dienstreisen zu Vor-Ort-Terminen durch Videokonferenzen ersetzt werden. Diesem Nutzen stehen allerdings auch eine Reihe von Risiken gegenüber. Diese betreffen sowohl die Personen, die an einer Videokonferenz teilnehmen, als auch Personen, über die personenbezogene Daten, etwa mittels Messenger, ausgetauscht oder im Rahmen einer Videokonferenz gesprochen wird. Hier gilt es die Privatsphäre von Beschäftigten (sowie gegebenenfalls ihrer Familien) zu schützen, die aus dem Homeoffice an Videokonferenzen teilnehmen, und auch dafür Sorge zu tragen, dass sensitive Inhalte gleichermaßen geschützt werden, wie es bei einem Präsenztreffen möglich ist. Wird ein System genutzt, das der datenschutzrechtlich Verantwortliche nicht selbst betreibt, sondern das von einem Dienstleister betrieben wird, der eventuell seinen Sitz außerhalb Europas hat, muss außerdem beachtet werden, dass etwaige „Datensammlungen“ durch den Dienstleister die in Europa geltenden datenschutzrechtlichen Vorgaben berücksichtigen.

#### **Hinweise zur Auswahl und zum Betrieb**

Anfang April 2020 habe ich auf meiner Website Hinweise zur Auswahl und zum sicheren Betrieb von Messenger- und Videokonferenzdiensten veröffentlicht. Dabei habe ich besonderen Wert auf die Aspekte Transparenz, Sicherheit und Steuerbarkeit gelegt. Die Verantwortung für die datenschutzkonforme Nutzung eines Dienstes



liegt auch dann weitgehend bei den Nutzern, wenn ein von einem Anbieter zentral betriebener Dienst zum Einsatz kommt. Auch habe ich den Anwenderinnen und Anwendern eine Reihe von Leitfragen an die Hand gegeben, die ihnen bei der Beurteilung und Auswahl entsprechender Angebote helfen.

### **Orientierungshilfe der Datenschutzkonferenz**

Im Verlauf des Jahres hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Orientierungshilfe zum Einsatz von Videokonferenzsystemen erarbeitet, die im Oktober 2020 veröffentlicht wurde. Diese Orientierungshilfe wird durch eine Checkliste ergänzt, die Verantwortliche dabei unterstützt, bei der Auswahl und Nutzung von Videokonferenzsystemen keine relevanten Aspekte außer Acht zu lassen. Die Orientierungshilfe adressiert ausdrücklich den Beschäftigtendatenschutz, der gerade beim Einsatz von Videokonferenzsystemen im Homeoffice oder bei mobiler Arbeit eine wichtige Rolle spielt.

### **Rundschreiben an die Bundesverwaltung zu WhatsApp**

Nachdem mich zu Anfang der Corona-Krise einzelne Hinweise erreicht haben, die den Einsatz von WhatsApp durch Stellen der Bundesverwaltung bemängelten, habe ich im April 2020 in einem Rundschreiben an alle obersten Bundesbehörden klargestellt, dass Bundesbehörden auf den Einsatz von WhatsApp verzichten sollten. Die Übermittlung von Metadaten an WhatsApp und, in einem zweiten Schritt, auch an Facebook, liefert stets einen Beitrag zur Profilbildung durch Facebook. Dies ist für Behörden, die in besonderem Maß an die Einhaltung von Recht und Gesetz gebunden sind und denen in diesem Zusammenhang eine Vorbildfunktion zukommt, nicht tragbar.



### **Nutzung eines öffentlich verfügbaren Dienstes oder Eigenbetrieb?**

Eine zentrale Frage bei der Nutzung von Videokonferenz- oder Messengersystemen ist die Wahl zwischen der Nutzung eines kommerziellen, öffentlich verfügbaren Dienstes und dem Eigenbetrieb eines entsprechenden Systems. Während der Eigenbetrieb eines Systems den Verantwortlichen einerseits die volle Kontrolle über praktisch alle datenschutzrelevanten Parameter gibt, bürdet er ihnen andererseits die komplette Verantwortung für den sicheren und performanten Betrieb auf. Der technische und organisatorische Aufwand für den Aufbau und den Betrieb eines Dienstes in Eigenregie ist groß. Die Nutzung öffentlich verfügbarer, kommerzieller Angebote ist demgegenüber oft schneller zu realisieren und mit weniger Aufwand verbunden.

Gerade solche Angebote, die besonders schnell und einfach genutzt werden können, sind jedoch oft besonders problematisch. Für diese zentral betriebenen Dienste ist nur die Installation einer App auf einem Mobilgerät oder einer Client-Anwendung auf einem Notebook erforderlich. Es könnten vom entsprechenden Anbietern möglicherweise aber auch Nutzungsdaten erhoben werden, woraus sich Profile bilden lassen, die gegebenenfalls für eigene Zwecke genutzt werden sollen. Hier sind die Anbieter zu mehr Transparenz aufgefordert. Bietet ein Dienst die Möglichkeit zum Teilen von Dateien oder zur Aufzeichnung von Gesprächen oder Sitzungen, so ist dies immer dann problematisch, wenn die entsprechenden Inhalte auf der Infrastruktur des Anbieters gegebenenfalls unverschlüsselt gespeichert werden. Auch über die Frage, ob bzw. wie die Datenströme auf dem Weg von den Clients zum Server geschützt werden, muss transparent informiert werden.

#### **4.1.7 Zustellung von Paketen unter Pandemiebedingungen**

Die Corona-Pandemie hat das Sendungsvolumen im Paketbereich stark erhöht. Mit dem Erfordernis der kontaktlosen Zustellung kollidierten in der Anfangszeit einige Varianten der Übergabedokumentation mit den Vorgaben des Datenschutzes.

Auch die Zustellung von Paketen, deren Volumen durch die Schließungen des Einzelhandels sprunghaft angestiegen war, musste an die gebotenen Abstandsregeln angepasst werden. Zustellungen mit dem Unterschreiben auf dem Handscanner und der zugehörige Austausch des Geräts und des Stifts mussten ersetzt werden. Die Paketdienstleistungsfirmen in Deutschland haben daher im Frühjahr ihre Prozesse angepasst: Statt die Sendungen durch Unterschriften quittieren zu lassen, sollten die Zustellenden fortan beispielsweise die Unterschrift der empfangenden Person auf dem Paket abfotografieren.

Mehrere Bürgerinnen und Bürger berichteten mir, dass neben ihrer Unterschrift auf dem Paket auch ihr Ausweis im Rahmen der Zustellung fotografiert wurde. In Einzelfällen fotografierten Mitarbeitende der Paketdienstleistungsfirmen die empfangende Person mit ihrem Paket zu Dokumentationszwecken und übertrugen diese Bilder in die firmeneigenen Systeme.

Die mir gemeldeten Vorfälle wurden in der Regel bei der Sachverhaltsaufklärung von den betreffenden Paketdienstleistungsfirmen bestätigt, selbstverständlich verbunden mit der Bestätigung der Löschung der zu Unrecht erhobenen personenbezogenen Daten. Ausweisfotografien oder Bilder von empfangenden Personen gehen zweifellos weit über das gesetzlich Erlaubte hinaus. Sie zu erheben und zu speichern, stellt einen klaren Verstoß gegen die DSGVO dar.

Auch für Postdienstleistende gilt: Eine entsprechende Einarbeitung und Sensibilisierung der Mitarbeitenden hinsichtlich der gesetzlichen Vorgaben beugt Datenschutzverstößen vor.

#### **4.1.8 Programme für Sofort- bzw. Überbrückungshilfen des Bundes im Zusammenhang mit der Corona-Pandemie**

In die Umsetzung der Programme der Bundesregierung zur Überwindung der negativen wirtschaftlichen Auswirkungen der Corona-Pandemie wurde ich zu unterschiedlichen Zeitpunkten einbezogen. Dabei hat sich gezeigt, wie wichtig die frühzeitige Einbeziehung meines Hauses in datenschutzrechtlichen Fragen ist.

Die Bundesregierung hat auf die wirtschaftlichen Folgen der Corona-Pandemie schnell mit finanziellen Stabilisierungsmaßnahmen für die Wirtschaft reagiert. Hierzu

wurden bereits bestehende Mechanismen erweitert oder neue Programme aufgelegt, wie die Stabilisierungsmaßnahmen aus dem Großbürgerschafts-Programm und dem Wirtschaftsstabilisierungsfonds. Zusätzlich wurde ein Programm mit Überbrückungshilfen für kleine und mittelständische Unternehmen aufgelegt, die ihren Geschäftsbetrieb im Zuge der Corona-Krise ganz oder zu wesentlichen Teilen einstellen mussten. All diese Programme eint, dass während der entsprechenden Antragsverfahren regelmäßig personenbezogene Daten von verschiedensten an den Verfahren beteiligten Personen verarbeitet werden.

Gerade aufgrund des Bedarfs für eine schnelle Umsetzung und der dabei zu beachtenden komplexen datenschutzrechtlichen Fragen hätte ich mir eine frühzeitige Einbindung in diese Projekte gewünscht, damit die Verfahren auf eine solide datenschutzrechtliche Basis gestellt werden können. Dies war jedoch nicht durchgängig der Fall.

Als Positivbeispiel möchte ich das neue Programm zur Überbrückungshilfe für kleine und mittelständische Unternehmen, die ihren Geschäftsbetrieb im Zuge der Corona-Krise ganz oder zu wesentlichen Teilen einstellen mussten, hervorheben. Hier ist das Bundesministerium für Wirtschaft und Energie (BMWi) schon im Stadium erster Überlegungen auf mich zugekommen, um bei den angedachten Prozessschritten meine Expertise einzuholen. Der Verwaltungsvollzug dieses Programmes sollte bürgernah durch die Länder erfolgen. Daher habe ich meine Kolleginnen und Kollegen in den Ländern regelmäßig über das Programm informiert, so dass eine komplette Begleitung durch die zuständigen Datenschutzbehörden sichergestellt werden konnte. Außerdem konnte ich das BMWi neben datenschutzrechtlichen Fragen im Zusammenhang mit der Beteiligung von Finanzverwaltung und Wirtschaftsprüfern auch zu der eingerichteten Verfahrensplattform „Onlineantrag Überbrückungshilfe“ beraten. Das BMWi hat hierzu ein umfassendes Datenschutzkonzept, ein Verzeichnis von Verarbeitungstätigkeiten sowie eine Datenschutz-Folgeabschätzung vorgelegt, in denen sich eine erfreuliche Sensibilisierung hinsichtlich der Berücksichtigung notwendiger datenschutzrechtlicher Aspekte gezeigt hat.

Von den Stabilisierungsmaßnahmen aus dem Großbürgerschafts-Programm und dem Wirtschaftsstabilisierungsfonds habe ich dagegen erst Kenntnis erlangt, als sie sich beim BMWi bereits in der Umsetzung befanden. Insbesondere zu der Einbindung von Drittparteien als Mandatar in die durchzuführenden Antragsprozesse hätte ich gerne von Anfang an Stellung nehmen können. Die hier gewählte Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten, die von der Entscheidungsbefugnis der einzelnen Akteure im Antragsverfahren abweicht,

erschließt sich mir nicht. Gerade für eine effektive Wahrnehmung der Betroffenenrechte ist eine klare Zuordnung der Verantwortlichkeiten jedoch besonders wichtig. Daher befinde ich mich zu diesem Punkt noch in weiteren Abstimmungsgesprächen mit dem BMWi.

#### **4.1.9 Coronabedingte Änderungen in der Arbeitsverwaltung**

Ein übereiltes Gesetzgebungsverfahren bezüglich des vereinfachten Zugangs zu Leistungen nach dem Sozialgesetzbuch Zweites Buch (SGB II; Sozialschutzpaket I) führt zu Unsicherheit in Datenschutzfragen.

Um die sozialen und wirtschaftlichen Folgen der Maßnahmen zur Eindämmung des Coronavirus im Frühjahr 2020 abzufedern, wurden durch das Sozialschutzpaket I Regelungen zum erleichterten Zugang zu Leistungen der Grundsicherung nach dem SGB II mit Geltung für Bewilligungszeiträume ab dem 01.03.2020 eingeführt. Ziel des Gesetzes war nach der Gesetzesbegründung (BT-Drucksache 19/18107), die Leistungen in einem vereinfachten Verfahren schnell und unbürokratisch zugänglich zu machen, um die Betroffenen zeitnah unterstützen zu können. Niemand sollte aufgrund der wirtschaftlichen Auswirkungen dieser Krise in existenzielle Not geraten. Das vereinfachte Verfahren sei zur Unterstützung der Arbeitsfähigkeit der Jobcenter erforderlich. Das Gesetzgebungsverfahren erfolgte im Eilverfahren. Die normalerweise im Gesetzgebungsverfahren vorgesehene Verbändeanhörung erfolgte nicht; ich wurde zwar beteiligt, jedoch mit einer derart kurzen Frist, dass mir eine umfassende Prüfung des Gesetzesentwurfs nicht möglich war. Obwohl ich die Eilbedürftigkeit des Gesetzesvorhabens in einer Krisensituation anerkenne, bin ich der Auffassung, dass mit diesem Eilverfahren rechtsstaatliche Grundsätze überdehnt wurden, insbesondere da auch in solchen Fällen eine vorzeitige und damit parallele Beteiligung erfolgen könnte. Ich verweise auf die kritische Stellungnahme des Deutschen Sozialgerichtstags vom 25. März 2020 zum Gesetzesentwurf, der ich mich in diesem Punkt anschließe.

Mit dem Sozialschutzpaket I wurde unter anderem geregelt, dass Vermögen für die Dauer von sechs Monaten nicht berücksichtigt wird, nicht jedoch, wenn das Vermögen erheblich ist. Es wird vermutet, dass kein erhebliches Vermögen vorhanden ist, wenn die Antragstellerin oder der Antragsteller dies im Antrag erklärt. Inwieweit aus der gesetzlichen Regelung, dass kein Vermögen anzurechnen ist, folgt, dass insgesamt überhaupt keine Vermögensprüfung stattfinden soll, bleibt unklar. Auch aus der Gesetzesbegründung lässt sich keine Konkretisierung ableiten. Ziel des Gesetzgebungsvorhabens war es, die oftmals aufwendige und zeitintensive Vermögens-

prüfung schnell und unbürokratisch zu gestalten, ohne von einer Vermögensprüfung generell abzusehen.

Diese an sich leistungsrechtliche Frage hat schwerwiegende Auswirkungen auf das Datenschutzrecht. Die Regelung führte bei einigen Antragstellenden zu Unsicherheiten, da einige Jobcenter ungeachtet dessen weiterhin zur Prüfung des Vorhandenseins von Einkommen und Vermögen erforderliche Unterlagen anforderten. Insbesondere wurde wie bisher die Vorlage von Kontoauszügen der letzten Monate verlangt. Wenn jedoch eine Vermögensprüfung grundsätzlich unzulässig ist, ist auch das regelhafte Anfordern von Kontoauszügen nicht mit dem datenschutzrechtlichen Grundsatz der Datensparsamkeit vereinbar. Die Jobcenter dürfen nur Daten verarbeiten, die zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind.

Dies führte zu einer erheblichen Verunsicherung und einem erhöhten Aufkommen von Anfragen bei mir. Die Informationen aus dem Internetauftritt des Bundesministeriums für Arbeit und Soziales (BMAS) waren nicht geeignet, diese Verunsicherung zu beseitigen. Im Grundsatz haben die Jobcenter nach meiner Auffassung zu Recht die Vorlage von anspruchsbegründenden Unterlagen, wie den Kontoauszügen der letzten drei Monate, verlangt. Sinn und Zweck der durch das Sozialpaket vorgenommenen Gesetzesänderung ist nicht, die Vermögensprüfung als solche generell auszuschließen. Es geht lediglich darum, dass Verwaltungsverfahren vereinfacht werden, damit die Leistungen schneller ausgezahlt werden können. Die Sichtung von Kontoauszügen der letzten drei Monate verzögert das Verwaltungsverfahren nicht wesentlich. Zudem ist diese erforderlich, um trotz der vereinfachten Vermögensprüfung wenigstens in geringem Umfang die im Antragsverfahren gemachten Angaben überprüfen zu können. Außerdem werden die Kontoauszüge nicht nur zur Prüfung des Vermögens benötigt, sondern auch als Nachweis, welche Einkünfte den Antragstellenden zugeflossen sind. Zwar wird durch die Bundesagentur für Arbeit auf die Pflicht zur Vorlage der Kontoauszüge trotz der Erleichterungen hingewiesen (<https://www.arbeitsagentur.de/corona-faq-grundsicherung-arbeitslosengeld-2>). Eine klarere gesetzliche Regelung sowie eine ausführlichere Erläuterung der Regelungen durch das BMAS oder die Bundesagentur für Arbeit und die Jobcenter hätten dazu beitragen können, diese Unsicherheiten zu vermeiden.

## **4.2 Das Patientendaten-Schutz-Gesetz**

Das Patientendaten-Schutz-Gesetz (PDSG) ist am 20. Oktober 2020 in Kraft getreten. Es enthält umfängliche

Regelungen zur elektronischen Patientenakte (ePA) und verstößt mit den konkreten Ausgestaltungen zum Zugriffsmanagement gegen die Datenschutz-Grundverordnung (DSGVO). Kritisch sind auch der alternative Zugriff auf die ePA mittels mobiler Geräte (Smartphone etc.), d.h. ohne Verwendung der elektronischen Gesundheitskarte (eGK), sowie die Vorschriften zur elektronischen ärztlichen Verordnung (E-Rezept). Das E-Rezept ist die erste sogenannte Pflichtanwendung, d.h. das PDSG enthält Vorgaben, die zwingend für alle gesetzlich Versicherten gelten. Eine weitere wichtige Regelung im PDSG ermöglicht den Versicherten die Freigabe der Daten in der ePA für die Forschung. Vor diesem Hintergrund fehlen wichtige Festlegungen, die vom Gesetzgeber – und nicht in nachgelagerten Prozessen – getroffen werden müssen.

Mit dem PDSG wird die Digitalisierung im Gesundheitswesen weiter vorangetrieben. Das hierfür entwickelte Konzept der Telematikinfrastruktur (TI) soll Datenschutz und Datensicherheit gewährleisten. Der Gesetzgeber hat zu Recht in der Begründung des PDSG die Wahrung der Patientensouveränität als eine der wichtigsten Vorgaben betont. Trotz dieser zentralen Prämisse des PDSG wird das Ziel einer informationellen Selbstbestimmung der Versicherten vor allem im wohl größten Projekt des Gesetzes, der ePA, verfehlt.



Die Telematikinfrastruktur (TI) vernetzt alle Akteure des Gesundheitswesens im Bereich der gesetzlichen Krankenversicherung und gewährleistet den sektoren- und systemübergreifenden sowie sicheren Austausch von Informationen. Sie ist ein geschlossenes Netz, zu dem nur registrierte Nutzer (Personen oder Institutionen) mit einem elektronischen Heilberufs- und Praxisausweis Zugang erhalten. Um allen Datenschutzanforderungen gerecht zu werden und insbesondere die medizinischen Daten von Patienten zu schützen, wird in der Telematikinfrastruktur auf starke Informationssicherheitsmechanismen gesetzt.

### Gesetz legt datenschutzrechtliche Verantwortung fest

Anwendungen und Komponenten der TI werden von einer Vielzahl von Mitwirkenden geplant, entwickelt und betrieben. Deshalb ist es wichtig, die datenschutzrechtliche Verantwortung klar aufzuteilen. Nur so können Betroffene ihre Rechte wahrnehmen und Behörden ihre Aufsicht effizient ausüben. Deshalb hat bereits im September 2019 die Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern (DSK) einen Beschluss zu ihrer Auffassung der daten-

schutzrechtlichen Verantwortung in der TI gefasst (vgl. 28. TB Nr. 4.2.1). Danach trägt die gematik als zentrale und planende Stelle der TI die datenschutzrechtliche Alleinverantwortung für die zentrale Zone der TI und eine Mitverantwortung für die dezentrale Zone. Das PDSG regelt nunmehr explizit die Verantwortlichkeiten. Im Gegensatz zur Auffassung der DSK beschränkt der Gesetzgeber jedoch die Verantwortlichkeit der gematik (s. § 307 Absatz 5 SGB-V). Die gematik ist datenschutzrechtlich nur verantwortlich, soweit sie die Mittel der Verarbeitung personenbezogener Daten bestimmt und keine Verantwortlichkeit der anderen – allein verantwortlichen – Akteure (vgl. § 307 Absätze 1 bis 4 SGB-V) besteht. Die gematik muss eine koordinierende Stelle einrichten, die Betroffenen Auskünfte zu den Verantwortlichkeiten erteilt. Die Normierung einer lückenlosen datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitungen in der TI und die Einrichtung einer koordinierenden Stelle zur Erteilung von Informationen und Auskünften an die Betroffenen sind grundsätzlich zu begrüßen. Allerdings birgt die gesetzlich geregelte Alleinverantwortlichkeit der Anbieter von Anwendungen auch Probleme, wie das Beispiel der ePA zeigt.



### Elektronische Patientenakte verstößt gegen die DSGVO

Das im PDSG normierte Zugriffsmanagement der ePA verstößt gegen die DSGVO und die Grundrechte der



Versicherten. So erhalten die Versicherten zum Start der ePA am 1. Januar 2021 nicht die volle Hoheit über ihre eigenen Gesundheitsdaten. Das bedeutet z.B., dass im Jahr 2021 kein Versicherter den Zugriff seines Arztes auf einzelne, für die Behandlung notwendige Dokumente, beschränken kann. Der Versicherte hat lediglich die Wahl, Leistungserbringern (z.B. seinen Ärzten) entweder die Berechtigung für den Zugriff auf alle gespeicherten Daten (Befunde, Diagnosen, Therapiemaßnahmen etc.) und alle von ihm selbst in die ePA eingestellten Dokumente zu erteilen oder sie ganz zu verweigern. Es gilt also das Alles-oder-Nichts-Prinzip. D.h. jede Person, der Zugriff auf ein ärztliches oder vom Versicherten selbst eingestelltes Dokument gewährt wird, kann jeweils alle Informationen in der ePA einsehen, auch wenn dies für die jeweilige Behandlung nicht erforderlich ist. Erst ab dem Jahr 2022 sieht das PDSG eine Verbesserung vor. Dies gilt aber nur, wenn man ein mobiles Gerät (z.B. Smartphone, Tablet) nutzt. Ab diesem Zeitpunkt könnten dann mittels Smartphone oder Tablet dokumentengenaue Zugriffe erteilt werden.

Die große Gruppe von Menschen, die kein eigenes Gerät besitzen oder keines benutzen wollen, wird hiervon nicht erfasst. Diese Versicherten werden weiterhin in ihrer Patientensouveränität beschränkt. Sie können lediglich beim Leistungserbringer, z.B. in der ärztlichen Praxis, auf Kategorien von Dokumenten beschränkte Zugriffsrechte erteilen. Alternativ können sie einem Vertretenden mit einem geeigneten technischen Gerät Vertretungsrechte einräumen. Nur der Vertretende kann dann für diese Personen dokumentengenaue Berechtigungen erteilen. Dies bedeutet, dass die Versicherten dem Vertretenden alle in ihrer ePA vorhandenen Gesundheitsdaten, d.h. auch intimste Informationen, offenbaren müssen. Zudem hilft die Vertretung nicht denjenigen Versicherten, die z.B. aus Sicherheitsgründen bewusst kein Smartphone oder Tablet für die Verwaltung ihrer ePA einsetzen wollen – und damit auch kein entsprechendes Gerät eines Vertretenden.

Datenschutzrechtlich kritisch zu bewerten ist auch, dass die Vielzahl derjenigen Menschen, die kein eigenes Endgerät haben oder nutzen wollen, auf Dauer auch keinen Einblick in ihre eigene, von ihnen selbst zu führende ePA haben werden. Sie werden also von einer entsprechenden Nutzung der ePA ausgeschlossen. Somit kann diese Personengruppe auch nicht von den Vorteilen einer ePA in der Gesundheitsversorgung profitieren.

Diese gravierenden Einschränkungen der Patientensouveränität stehen in Widerspruch zu elementaren Vorgaben der DSGVO und verstoßen damit gegen in Deutschland unmittelbar geltendes europäisches Recht. Hierauf habe ich frühzeitig und wiederholt – auch im Rahmen des Gesetzgebungsverfahrens – hingewiesen.

Meine Lösungsvorschläge wurden nicht berücksichtigt bzw. im parlamentarischen Verfahren wieder aus dem Gesetzentwurf herausgenommen. Dies betrifft z.B. die Einrichtung von sogenannten Kassenterminals in den Geschäftsstellen der Krankenkassen, mit denen Versicherte ohne eigenes Endgerät und diejenigen, die kein eigenes Endgerät einsetzen wollen, innerhalb der gesicherten TI-Umgebung in ihre ePA hätten Einblick nehmen können.

Durch die Benachteiligung und Ungleichbehandlung dieser großen Gruppe von Versicherten schafft das PDSG eine Zweiklassengesellschaft bei der ePA.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben diese Kritik auch in einer im September 2020 verabschiedeten Entschließung öffentlich zum Ausdruck gebracht.

Ein weiterer zentraler datenschutzrechtlicher Kritikpunkt ist das nicht den Vorgaben der DSGVO entsprechende Authentifizierungsverfahren der ePA mit eigenen Endgeräten. Weil Gesundheitsdaten besonders sensibel sind, bedürfen Zugriffe auf die ePA immer hochsicherer Authentifizierungsverfahren, die stets dem aktuellen Stand der Technik entsprechen müssen. Das Verfahren der „Alternativen Versichertenidentität“, mit dem Versicherte sich auch ohne Einsatz der eGK an ihrer ePA anmelden können, basiert auf einem Signatordienst und erfüllt diese Sicherheitsanforderungen nicht vollständig. Für einen datenschutzkonformen Zustand bedarf es auch bei dieser sogenannten alternativen Authentifizierung der Gewährleistung eines höchstmöglichen Sicherheitsniveaus. Diese Gewährleistung obliegt ebenfalls den Krankenkassen. Auch wegen dieses Mangels sind gegebenenfalls aufsichtsrechtliche Maßnahmen gegen die Krankenkassen zu richten, um die Ablösung durch ein geeigneteres Verfahren sicherzustellen.

In der 2./3. Lesung des PDSG am 3. Juli 2020 hat Bundesgesundheitsminister Spahn im Deutschen Bundestag zutreffend betont: „(...) Datenschutz ist bei so sensiblen Daten wie Gesundheitsdaten wichtig, und zwar Datenschutz auf höchstem Niveau. Es gibt nichts Sensibleres für den Einzelnen, nichts Persönlicheres, Intimeres als die Daten über die eigene Gesundheit und insbesondere eine mögliche Erkrankung. Deswegen legen wir Datenschutzstandards auf höchstem Niveau in diesem Patientendaten-Schutz-Gesetz fest (...)“.

Auch und insbesondere in meiner Funktion als Datenschutzaufsichtsbehörde bin ich verpflichtet, auf die Beseitigung von Verstößen gegen die DSGVO hinzuwirken.

Eine Umsetzung der ePA ausschließlich nach den Vorgaben des PDSG ist europarechtswidrig und erfordert



## Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 01.09.2020

### Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechts-widrig!

Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (ePA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen. Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden.

Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der ePA am 1. Januar 2021 die volle Hoheit über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten ePA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der ePA für alle Versicherten datenschutzgerecht auszugestalten.

Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der ePA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten etc.) in der elektronischen Patientenakte gespeicherten Daten zu einem „alles oder nichts“ gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.

Erst ein Jahr nach dem Start der ePA, d.h. ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre ePA geeignete Endgeräte (Smartphone, Tablet etc.) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (d.h. sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die ePA und die „Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus“. Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (BR-Drs. 164/1/20, s. Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 ff. SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der ePA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der ePA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

daher die Verhängung aufsichtsrechtlicher Maßnahmen. Dementsprechend habe ich den meiner Aufsicht unterfallenden gesetzlichen Krankenkassen im November 2020 eine förmliche Warnung übersandt, ihren Versicherten eine rechtswidrige ePA anzubieten.

Die Krankenkassen stehen aufgrund der ihnen vom Gesetzgeber zugewiesenen Alleinverantwortlichkeit für die ePA in einem Dilemma. Verweigern sie die Umsetzung der ePA gemäß den Vorgaben des PDSG, drohen ihnen hohe, im PDSG gesetzlich festgelegte Strafzahlungen. Setzen sie demgegenüber das europarechtswidrige Gesetz um, d.h. bieten sie ihren Versicherten eine europarechtswidrige ePA an, kommen sie in den Fokus der Aufsichtsbehörden. Abhilfe schaffen kann hier letztlich nur der Gesetzgeber.

### **Die erste Pflichtanwendung: Die elektronische ärztliche Verordnung**

Das PDSG führt mit den Regelungen in §§ 360 und 361 SGB V eine neue Anwendung ein. Ärztliche Verordnungen müssen ab dem 1. Januar 2022 elektronisch über die TI übermittelt werden. Das sogenannte E-Rezept ist damit eine Pflichtanwendung – und zwar die erste medizinische überhaupt.

Rezepte im Rahmen der vertragsärztlichen Versorgung sollen immer in einem zentralen Speicher in der TI abgelegt werden. Patientinnen und Patienten können dann nur wählen, ob sie die Zugangsinformationen dazu in elektronischer Form oder – nach dem Vorbild eines Bahn- oder Flugtickets – als Papiausdruck mit einem Code-Block zur Einlösung in einer Apotheke ausgehändigt bekommen wollen.

Wie bei der ePA wird es auch beim E-Rezept eine Zweiklassengesellschaft geben. Menschen, die nicht die E-Rezept-App nutzen möchten oder können, erhalten keinen unmittelbaren Einblick in die über sie gespeicherten Daten oder erfolgten Zugriffe auf ihre Rezepte.

Zur Authentisierung in der E-Rezept-App gegenüber dem E-Rezept-Server sieht das PDSG nicht vor, ein alternatives Verfahren ohne eGK anzuwenden. Nutzende werden deshalb ihre eGK über Near Field Communication (NFC) mit dem Endgerät verbinden. Hierbei werden die Daten kontaktlos über eine kurze Strecke von wenigen Zentimetern ausgetauscht. Im Rahmen der Einführung der Anwendung E-Rezept wird in der TI dazu ein Identity Provider aufgebaut – ein Dienst der zunächst nur für das E-Rezept – später potentiell für alle Anwendungen der TI – das Authentisieren der Nutzenden übernimmt und die Identifizierung bestätigt. Somit soll das zentrale Thema Authentisierung aus den Anwendungen ausgelagert werden. Dies ist für die Einführung und Sicherheitsbewertung von Authentisierungsmitteln von Vorteil. Um

diese Vorteile datenschutzkonform zu nutzen, fordere ich, dass die Prozesse zur Einführung von Authentisierungsmitteln im Vorfeld für die gesamte TI entwickelt und die Kriterien der Einstufung der Sicherheitsniveaus transparent festgelegt werden. Eine so zentrale Funktionalität für die Sicherheit der TI muss auch übergreifend geregelt werden und darf nicht bloß ein Annex bei der E-Rezept-Entwicklung sein.

Beim E-Rezept findet auch ein weiterer Paradigmenwechsel statt: Die gematik entwickelt die E-Rezept-App und wird sie zur Verfügung stellen. Die Aufgabe der gematik beschränkt sich demnach nicht, wie z.B. bei der ePA, auf die Erstellung von Spezifikationen und Sicherheitsanforderungen, nach denen Hersteller Komponenten oder Dienste der TI anzubieten haben. Die gematik wird selbst zum Hersteller und damit auch datenschutzrechtlich verantwortlich. Dies hat zur Folge, dass die gematik ihre eigenen Entwicklungen zu prüfen und zuzulassen hat. Insoweit besteht zumindest die Gefahr einer potentiellen Befangenheit. Im Rahmen der Gesetzesberatungen konnte ich zumindest erreichen, dass ein externes Sicherheitsgutachten von der gematik zu beauftragen ist und dieses durch das Bundesamt für Sicherheit in der Informationstechnik geprüft und bestätigt werden muss, bevor die App in Betrieb gehen darf.

Die Verfügbarkeitsanforderungen an das E-Rezept sind natürlich sehr hoch und ebenfalls von zentraler Bedeutung. Während der Konzeption hatte ich für eine dezentrale Lösung plädiert. Diese hätte gegen Ausfälle zentraler Dienste robuster ausgestaltet werden können. In der Abwägung – u.a. mit dem Schutz vor Manipulation und Rezepthandel – hat sich letztlich die geltende spezifizierte zentrale Lösung durchgesetzt.

In allen angesprochenen Aspekten zeigt sich die Wichtigkeit meiner wiederholt und frühzeitig geäußerten Forderung, die zentralen Aspekte der Anwendung E-Rezept im Gesetz zu verankern. Der Gesetzgeber muss für eine Pflichtanwendung wie das E-Rezept selbst zentrale Entscheidungen treffen und Leitplanken im Gesetz vorgeben, ohne sich auf eine spezifische Technik festzulegen. Bedauerlicherweise wurde dies nicht umgesetzt, so dass zentrale Fragestellungen nunmehr nachgelagert, insbesondere im Rahmen der technischen Spezifikationen, von der gematik entschieden werden. Im PDSG fehlen u. a. Regelungen zur Zweckbindung, Datenspeicherung und zu technischen Grundsätzen und Kontrollmöglichkeiten für alle Versicherten. Damit – und vor dem Hintergrund der herausragenden Bedeutung der Anwendung für die Versorgungssicherheit – sind die Regelungen zur Einführung der elektronischen Verordnung nicht hinreichend normenklar und ergänzungsbedürftig. Lediglich in Bezug auf die Normierung einer Regelung zur Speicherdauer der E-Rezepte ist der

Gesetzgeber meinem Petition im PDSG gefolgt. Auch die konkrete Gestaltung der Anwendung E-Rezept muss sich an den Vorgaben der Datenschutz-Grundverordnung messen lassen. Prüfungsschwerpunkt wird neben den Maßnahmen zur Sicherheit der Daten auch die Sicherstellung der Verfügbarkeit sein.

#### **Freigabe der ePA-Daten für die Forschung, § 363 SGB V.**

Eine weitere wichtige neue Regelung im PDSG ermöglicht den Versicherten die Freigabe der in ihrer ePA gespeicherten Daten für die medizinische Forschung. Bereits in der Ressortberatung konnte ich hier wesentliche Verbesserungen erreichen, so dass ab 2023 diese wertvollen und begehrten Gesundheitsdaten auf eine datenschutzgerechte Weise genutzt werden können. Die Forschung mit Gesundheitsdaten ist für die Gesellschaft von erheblicher Bedeutung. Andererseits sind diese Daten besonders sensibel. Ihre Verarbeitung unterliegt nach § 363 SGB V besonderen Anforderungen und Schutzmaßnahmen. Zu diesen gehört, dass die Freigabe freiwillig und nur auf Veranlassung des Versicherten sowie mit seiner ausdrücklichen, jederzeit widerruflichen Einwilligung zulässig ist. Auch der Umfang kann frei bestimmt und auf ausgewählte Dokumente beschränkt werden. Zudem werden die Daten zum Schutz der Betroffenen pseudonymisiert und verschlüsselt übermittelt.

Die Regelung enthält zwei verschiedene Wege der Freigabe für die Forschung, die sich hinsichtlich ihrer datenschutzrechtlichen Bewertung unterscheiden: Einerseits ist eine Freigabe an das Forschungsdatenzentrum (FDZ) beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) möglich, das die Daten dann für Forschungswecke zur Verfügung stellt, andererseits ist eine Freigabe direkt an die Forschung vorgesehen.

#### **Forschungsdatenzentrum**

Bei der Freigabe an das FDZ werden die Daten dort gespeichert und nach Prüfung der Voraussetzungen für die Forschung zur Verfügung gestellt. Das Verfahren orientiert sich an den Vorgaben für die Nutzung der Versorgungsdaten, die aufgrund der Datentransparenzvorschriften der §§ 303a ff SGB V beim FDZ vorgehalten werden. Diese Vorschriften wurden durch das Digitale-Versorgung-Gesetz im Dezember 2019 neu gefasst, über das ich in meinem 28. Tätigkeitsbericht (Nr. 5.6, S. 45) berichtet habe.

Daraus folgt ein geregeltes Antragsverfahren mit ausdrücklich benannten Nutzungsberechtigten und konkret benannten zulässigen Zwecken. Das FDZ prüft Geeignetheit und Erforderlichkeit der beantragten Daten nach Umfang und Struktur in Bezug auf den vorgesehenen Zweck. Wichtig für den Schutz der Daten ist dabei

auch, dass die Nutzungsberechtigten zur Geheimhaltung verpflichtet sind und sich bei Verstoß gegen die Vorgaben strafbar machen. Allerdings konnte ich erreichen, dass für die Nutzung der ePA-Daten ein gegenüber der Datentransparenz reduzierter Kreis als nutzungsberechtigt aufgeführt ist: Nur diejenigen, zu deren Aufgaben die Forschung auch tatsächlich gehört.

Auch der Übermittlungsweg der Daten läuft entsprechend den Regelungen der Datentransparenzvorschriften in §§ 303a ff SGB V über eine Vertrauensstelle.

Grundsätzlich entspricht diese Konzeption der Freigabe an das FDZ datenschutzrechtlichen Anforderungen. Leider hat das Bundesministerium für Gesundheit meine bisherigen Hinweise, das FDZ bei einer unabhängigen Stelle anzusiedeln, nicht aufgegriffen. Aufgrund der Bedeutung der medizinischen Forschung und der hohen Sensibilität der betroffenen medizinischen Daten sollte eine unabhängige Stelle mit dieser Aufgabe betraut werden, um auf diese Weise das Vertrauen der Versicherten zu gewinnen.

#### **Direkte Freigabe für die wissenschaftliche Forschung**

Bei der Freigabe direkt an die Forschung sind außer der Einwilligung leider keine weiteren Vorgaben festgelegt. Kritisch aus datenschutzrechtlicher Sicht ist zudem, dass der Begriff der Einwilligung überdehnt wurde. Eine Einwilligung für „bestimmte Bereiche der wissenschaftlichen Forschung“, wie sie in § 363 Absatz 8 SGB V vorgesehen ist, ist nur unter bestimmten Voraussetzungen zulässig. Grundsätzlich kann eine freiwillige Einwilligung nur erteilt werden, wenn der Zweck der Verarbeitung konkret beschrieben wird. Die breite Einwilligung („broad consent“) ist in der DSGVO nur ausnahmsweise vorgesehen, wenn eine genaue Bezeichnung nicht möglich ist. Aber auch dann muss der Zweck so genau wie möglich beschrieben werden. Weitere Ausführungen der DSK zu den Voraussetzungen der breiten Einwilligung finden sich in ihrem Beschluss vom 5. April 2019, über den ich in meinem 28. Tätigkeitsbericht (Nr. 4.5.1, S. 34) berichtet habe. Trotz meiner Hinweise fehlen die erforderlichen Vorgaben jedoch in der gesetzlichen Regelung. Ich werde mich bei den Beratungen zur technischen Umsetzung weiter dafür einsetzen, dass noch Verbesserungen und Maßnahmen zur verfahrensmäßigen Absicherung der Datenübermittlung implementiert werden, um eine datenschutzrechtlich zulässige Freigabe und Nutzung zu erreichen.

#### **Änderung des § 68b SGB V**

Ebenfalls geändert durch das PDSG wurde § 68b SGB V. Diese bereits mit dem Digitale-Versorgungsgesetz (DVG) geschaffene Norm eröffnet den Krankenkassen die Möglichkeit, Versorgungsinnovationen zu fördern.



Dazu dürfen sie die versichertenbezogenen Daten, die sie rechtmäßig erhoben und gespeichert haben, im erforderlichen Umfang auswerten. Zuvor sind die Daten zu pseudonymisieren und - soweit möglich - zu anonymisieren. Eine Datenübermittlung an Dritte ist ausgeschlossen.

Nach der ursprünglichen Fassung des DVG durften die Krankenkassen die Auswertung von Versichertendaten und die Unterbreitung von Informationen und individuellen Angeboten nur vornehmen, wenn der Versicherte zuvor schriftlich oder elektronisch eingewilligt hat. Mit dem PDSG wurde dieses Einwilligungserfordernis nunmehr hinsichtlich der Datenauswertung und der Unterbreitung individueller Versorgungsangebote durch ein Widerspruchsrecht ersetzt, das sich lediglich auf die konkrete Angebotsunterbreitung bezieht.

Diese Änderung bewerte ich äußerst kritisch. Mit der gänzlichen Abschaffung des Einwilligungserfordernisses und der fehlenden Widerspruchsmöglichkeit in Bezug auf die Datenauswertung sind insbesondere vulnerable Gruppen unter den Versicherten den Auswertungen durch die Krankenkasse ausgesetzt. Eine tatsächliche Freiwilligkeit der Teilnahme an den Versorgungsangeboten sollte nach meiner Auffassung damit verbunden sein, dass sich die Versicherten im Vorfeld gegen die Einbeziehung ihrer Daten in die Auswertung zum Zwecke der Angebotsunterbreitung entscheiden können.

Ich hatte im Rahmen des Gesetzgebungsverfahrens zum PDSG keine Möglichkeit, zu der nunmehr geltenden Fassung des § 68b SGB V Stellung zu nehmen. Diese Änderung wurde erst im Nachgang zur Ressortabstimmung in der Endphase des parlamentarischen Verfahrens beschlossen. Deshalb habe ich meine Bedenken nachträglich gegenüber dem BMG geäußert, um in einem der laufenden Gesetzgebungsverfahren eine datenschutzkonforme Anpassung des § 68b SGB V zu erreichen. Des Weiteren behalte ich mir aufsichtsrechtliche Maßnahmen gegenüber den Krankenkassen im Hinblick auf die konkreten Verfahrensumsetzungen vor, soweit diese nicht in Einklang mit der Datenschutz-Grundverordnung stehen.

#### **Informationstexte nach § 343 SGB V – Einvernehmen mit BfDI**

Mit dem PDSG wurde außerdem ein neuer § 343 in das SGB V eingeführt. Dieser verpflichtet die Krankenkassen, bevor sie ihren Versicherten nach § 342 Absatz 1 Satz 1 SGB V eine elektronische Patientenakte anbieten, umfassendes, geeignetes Informationsmaterial in präziser, transparenter, verständlicher und leicht zugänglicher Form, in einer klaren, einfachen Sprache und barrierefrei zur Verfügung zu stellen.

Das Informationsmaterial muss über:

- alle relevanten Umstände der Datenverarbeitung für die Einrichtung der elektronischen Patientenakte
- die Übermittlung von Daten in die elektronische Patientenakte
- die Verarbeitung von Daten in der elektronischen Patientenakte durch Leistungserbringer einschließlich der damit verbundenen Datenverarbeitungsvorgänge in den verschiedenen Bestandteilen der Telematikinfrastruktur
- die für die Datenverarbeitung datenschutzrechtlich Verantwortlichen

informieren.

Der Spitzenverband Bund der Krankenkassen (GKV-SV) ist nach § 343 Absatz 2 SGB V verpflichtet worden, den Krankenkassen bei der Erfüllung ihrer Informationspflichten zu helfen, indem er geeignetes Informationsmaterial – auch in elektronischer Form – erstellt und den Krankenkassen zur verbindlichen Nutzung zur Verfügung stellt. Dieses Informationsmaterial hat er im Einvernehmen mit mir zu erstellen, wobei das Einvernehmen spätestens bis zum 30. November 2020 hergestellt sein muss (§ 343 Absatz 2 SGB V).

Nach intensiven Beratungen hat der GKV-SV eine Version der Informationstexte vorgelegt, zu der ich rechtzeitig vor dem Fristablauf mein Einvernehmen erklärt habe.

#### **Querverweis:**

##### **5.7 Datentransparenzverordnung**

## 4.3 Umsetzung der Schrems II-Entscheidung des Europäischen Gerichtshofes

Das Schrems II-Urteil des Europäischen Gerichtshofs (EuGH) hat für viel Aufsehen gesorgt: Von der Unwirksamkeitserklärung des Privacy Shields über Standardvertragsklauseln, die in der Regel nicht mehr ohne Weiteres anwendbar sein werden, bis zu den sogenannten „zusätzlichen Maßnahmen“. Die massiven Auswirkungen auf internationale Datenübermittlungen an Drittländer sind für Verantwortliche und Auftragsverarbeiter deutlich spürbar und bergen, nicht zuletzt auch für die Aufsichtsbehörden, hohe Anforderungen an die Umsetzung.

### Das Schrems II-Urteil

In meinem letzten Tätigkeitsbericht hatte ich bereits über das laufende sog. Schrems II-Verfahren (EuGH: Rechtssache C-311/18)<sup>8</sup> berichtet. In dem Verfahren ging 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. Außerdem wurde erwartet, dass sich der EuGH zur Wirksamkeit des „Privacy Shields“<sup>9</sup> äußern würde.

Am 16. Juli 2020 hat der EuGH schließlich das wegweisende Schrems II-Urteil verkündet und hierin die Regelungen des „Privacy Shields“ für unwirksam erklärt. Für die Datenübermittlungen in die USA bedeutete der Wegfall des Privacy Shields eine einschneidende Veränderung. Darüber hinaus hat der EuGH noch einmal klargestellt, dass personenbezogene Daten von EU Bürgern nur an Drittländer übermittelt werden dürfen, wenn sie in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Dabei hat der EuGH zwar das Instrument der Standardvertragsklauseln nicht grundsätzlich in Frage gestellt. Allerdings legte das Gericht fest, dass diese gegebenenfalls um sog. „zusätzliche Maßnahmen“ ergänzt werden müssten, damit die Daten im Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Für die USA hat der

EuGH bereits festgestellt, dass die Standardvertragsklauseln ohne zusätzliche Maßnahmen dieses gleichwertige Schutzniveau nicht bieten können. Ebenso dürfen die Auswirkungen des Urteils auf andere Drittländer sowie auf weitere Übermittlungsinstrumente gemäß Art. 46 DSGVO, z. B. verbindliche interne Datenschutzvorschriften - BCR, die durch den europäischen Datenschutzausschuss (EDSA) bereits transparent aufgearbeitet wurden, nicht verkannt werden. Der EDSA wird baldmöglichst – ergänzend zu den bereits erfolgten Veröffentlichungen – weitere Details zu den Auswirkungen des Urteils auf die BCR (Art. 46 (2) (b) DSGVO) und die sogenannten Ad hoc Vertragsklauseln gemäß Art. 46 (3) (a) DSGVO veröffentlichen.<sup>10</sup>

### Umsetzung

Der EuGH hat zudem eine klare Aufgabenzuweisung vorgenommen. Unternehmen sowie öffentliche Stellen sind verpflichtet, eigenhändig die Rechtmäßigkeit ihrer Datentransfers in Drittländer zu überprüfen und gegebenenfalls anzupassen. Hierbei werden sie durch die Aufsichtsbehörden beraten und kontrolliert.

Bereits unmittelbar nach dem Urteil habe ich zusammen mit meinen Kolleginnen und Kollegen auf nationaler und europäischer Ebene begonnen, Hilfestellungen für Verantwortliche und Auftragsverarbeiter (Datenexporteure) zu erarbeiten.

Ferner habe ich am 8. Oktober 2020 ein Informationsschreiben zur „Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer“ an die öffentlichen Stellen des Bundes sowie die meiner Aufsicht unterliegenden Unternehmen adressiert und zusätzlich auf meiner Webseite veröffentlicht.<sup>11</sup> Darin habe ich die Kernaussagen des Urteils zusammengefasst und verdeutlicht, wie mein Haus den Anforderungen des EuGH gerecht werden will. Ich habe die Datenexporteure daher auf ihre Verpflichtung zur Prüfung der Datenübermittlung an Drittländer hingewiesen und zudem darauf aufmerksam gemacht, wann eine Meldepflicht mir gegenüber besteht. Die Reaktionen der meiner Aufsicht unterstehenden Unternehmen und Behörden auf das Informationsschreiben werde ich auswerten und sie im Nachgang gezielt zu direkten Datenübermittlungen in spezifischen Bereichen befragen. Ferner wird die Umset-

<sup>8</sup> Schrems II-Urteil des EuGH vom 16. Juli 2020, Rechtssache C-311/18

<sup>9</sup> Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes.

<sup>10</sup> Empfehlungen Schrems II-des EDSA v. 10. November 2020, abrufbar unter: [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en).

<sup>11</sup> Informationsschreiben des BfDI vom 8. Oktober 2020, abrufbar unter: [www.bfdi.bund.de/rundschreiben](http://www.bfdi.bund.de/rundschreiben).

zung des Schrems II-Urteils regelmäßig Schwerpunkt bei zukünftigen Beratungs- und Kontrollbesuchen sein.

Auf meiner Webseite unterstütze ich zudem Verantwortliche und Auftragsverarbeiter mit aktuellen Informationen zur Thematik, z. B. einer Zusammenfassung der Kernaussagen des Schrems II-Urteils, ein Prüfschema zu Übermittlungen an Drittländer und durch Verlinkungen auf relevante Webseiten (z. B. des EDSA).<sup>12</sup>

Im EDSA konnten unter meiner sowie der Mitarbeit weiterer deutscher Aufsichtsbehörden bereits wenige Tage nach der Urteilsverkündung schnelle Hilfestellungen für die Datenexporteure erarbeitet werden. Es handelt sich dabei zum einen um „FAQs“ - Häufig gestellte Fragen - zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems.<sup>13</sup>

Zum anderen wurden am 10. November 2020 im EDSA die Empfehlungen zu den „zusätzlichen Maßnahmen“ („Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data“)<sup>14</sup> angenommen. Die Empfehlungen sollen die Datenexporteure dabei unterstützen herauszufinden, ob sie ihre Datenübermittlungen durch zusätzliche Maßnahmen ergänzen müssen. Außerdem halten die Empfehlungen praktische Beispiele zu Übermittlungsszenarien bereit.

Mit dem Schrems II-Urteil hat der EuGH die Datenexporteure, aber auch die datenschutzrechtlichen Aufsichtsbehörden, vor keine leichte Aufgabe gestellt. Die Arbeit an der Umsetzung der Schrems II-Anforderungen wird alle auf nationaler und europäischer Ebene voraussichtlich noch einige Zeit in Atem halten. Dabei werde ich mich weiterhin engagieren, die Umsetzung des Schrems II-Urteils des EuGH zu unterstützen und voranzutreiben, gerade auch durch Beratung für Unternehmen und Behörden, die Datentransfers in Drittstaaten vornehmen.

---

12 Informationen auf der BfDI Webseite, abrufbar unter: [https://www.bfdi.bund.de/DE/Europa\\_International/International/Artikel/Auswirkungen-Schrems-II-Urteil.html](https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/Auswirkungen-Schrems-II-Urteil.html).

13 Vom EDSA am 23. Juli 2020 angenommenen FAQ's abrufbar unter: [https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union\\_en](https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_en).

14 Empfehlungen „Schrems II“ des EDSA v. 10. November 2020, abrufbar unter: [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en).

# 5 Gesetzgebung

## 5.1 Registermodernisierung

Die Registermodernisierung ist ein zentraler Baustein für eine zukunfts-gewandte moderne Verwaltung. Die bisher im Entwurf eines Registermodernisierungsgesetzes geplante Nutzung der Steuer-ID als einheitliches und übergreifendes Personenkennzeichen begegnet allerdings erheblichen verfassungsrechtlichen Bedenken und stellt damit das Vorhaben grundlegend in Frage.

Schon in meinen beiden letzten Tätigkeitsberichten habe ich mich zur Registermodernisierung geäußert (siehe 28. TB Nr. 5.5, 27. TB Nr. 9.2.2) und hierbei deutlich gemacht, wie wichtig eine verfassungskonforme Ausgestaltung für die notwendige weitere Digitalisierung der Verwaltung ist. Schließlich profitiert nicht zuletzt auch der Datenschutz von modernen Infrastrukturen und Verfahren.

Mit einem einheitlichen, bereichsübergreifenden Personenkennzeichen wie der Steuer-ID, die im aktuell vom Bundestag beratenen Entwurf eines Registermodernisierungsgesetzes (RegMoG) 2020 so vorgesehen ist, verpasst der Gesetzgeber jedoch die Chance, einen Identifikator so zu gestalten, dass er den Anforderungen einer modernen Verwaltung ebenso genügt wie dem Schutz der Bevölkerung und ihrem verfassungsmäßigen Recht auf informationelle Selbstbestimmung. Statt breiter Zustimmung zu einem möglichen großen Wurf bei der Digitalisierung, wie sie unter anderem durch die sehr frühe Beteiligung der Datenschutzkonferenz und meiner Behörde an der Vorbereitung des Gesetzesentwurfs durchaus greifbar war, trifft das Vorhaben nun von vielen Seiten auf fundamentale Kritik.

Die Datenschutzkonferenz hat in ihren Entschlüssen vom 12. September 2019 und 26. August 2020 ausdrücklich davor gewarnt, die Steuer-ID in dieser Weise als Personenkennzeichen zu verwenden und sie vollständig von ihrer ursprünglichen Zweckbestimmung zu lösen. Auch der Bundesrat (BR Drs. 563/20) und der Wissenschaftliche Dienst des Bundestages (WD 3 - 3000 - 196/20) erkannten die verfassungsrechtliche Gefahr, die vom

vorgelegten Entwurf des RegMoG ausgeht. Selbst die bisherige Verwendung im Steuerbereich wäre nicht mehr gesichert.

In diesem Sinne habe ich in meinen Stellungnahmen zum Gesetzesentwurf (siehe u. a. meine Stellungnahme an den Innenausschuss des Bundestages vom 21. Oktober 2020 [www.bfdi.bund.de/stellungnahmen](http://www.bfdi.bund.de/stellungnahmen)) versucht, das Bewusstsein für die Dringlichkeit einer sicheren und verfassungskonformen Ausgestaltung nochmals zu schärfen. Klar ist: Eine funktionierende Registermodernisierung wird es ohne eine rechtssichere und eindeutige Identifizierung einzelner Personen nicht geben können. Aber ein universeller Identifikator wie die Steuer-ID, der mit dem hohen Risiko behaftet ist, nach einem jahrelangen Prozess vom Bundesverfassungsgericht verworfen zu werden, hat das Potential, die digitale Verwaltung in Deutschland womöglich wieder um Jahre zurückzuwerfen. Selbst wenn er in der einen oder anderen Form Bestand haben sollte: Wie beschädigt wird das Vertrauen in dieses Instrument sein? Dies auch, weil bei der Einführung der Steuer-ID im Jahre 2007 die ausdrückliche Zusicherung gegeben wurde, diese in jedem Fall auf den Steuerbereich zu beschränken und niemals als allgemeines Personenkennzeichen zu verwenden.

### Nachbesserungsbedarf

Deshalb muss aus meiner Sicht der gegenwärtige Entwurf an folgenden Stellen nachgebessert werden:

Der Entwurf muss sich von der Idee eines Ausbaus der Steuer-ID zu einem einheitlichen, bereichsübergreifenden Personenkennzeichen lösen, zumal die Steuer-ID keinen ausreichenden Schutz vor Missbrauch bietet. Mit bereichsspezifischen Kennzeichen oder weiteren kryptographischen Methoden gibt es modernere Alternativen.

Das Gesetz muss überdies eine starke Zweckbindung des Identifikators garantieren: Er darf nur zur Identitätsfeststellung zur Erbringung von digitalen Verwaltungsdienstleistungen verwendet werden. Dies ist im Entwurf bisher nicht sichergestellt, gerade weil nach den allgemeinen Regelungen der DSGVO zweckändernde Verwen-

dungen gefunden werden können und der Identifikator sich so unkontrolliert verbreitet. Erst in der öffentlichen Verwaltung, dann irgendwann auch in der Gesellschaft und Privatwirtschaft.

Der Gesetzentwurf trifft zudem bislang keine ausreichenden Vorkehrungen, den Datenaustausch zwischen verschiedenen Verwaltungsbereichen ausreichend gegen Missbrauch, Identitätsdiebstahl und Profilbildung abzusichern. Das im Entwurf enthaltene sog. „4-Corner-Modell“ ist zwar ein guter Ansatz, der mit verschlüsselten „doppelten Umschlägen“ arbeitet und für die Übermittlungsberechtigung eine dritte Stelle nutzt. Dies allein genügt aber nicht, alle relevanten Risiken adäquat einzudämmen. Das Modell kann in missbräuchlicher Absicht umgangen werden und schützt zudem nicht ausreichend gegen die Zusammenführung personenbezogener Daten durch externe Angreifer. Hinzu kommt, dass das 4-Corner-Modell – entgegen den Ankündigungen aus dem Koalitionsausschuss vom 3. Juni 2020 – unter Missachtung des Stands der Technik allein bei bereichsübergreifender Übermittlung eingesetzt werden soll. Da sich bereits andeutet, dass nur wenige große Verwaltungsbereiche gebildet werden, wird das 4-Corner-Modell für einen großen Teil der Datenübermittlungen also gar nicht zur Anwendung kommen.

Mithin darf auch der Steuerbereich nicht von den notwendigen Sicherheitsmaßnahmen ausgenommen bleiben. Mit Einführung des geplanten Identifikators wird schließlich auch er ein allgemeines Personenkennzeichen verwenden; die singuläre Steuer-ID im bisherigen Sinn hört faktisch auf zu bestehen.

Zuletzt muss mit der Digitalisierung der Verwaltung auch der Datenschutz im Übrigen fortentwickelt werden. Das im Entwurf aufgenommene Datencockpit ist hierbei ein wichtiger und guter erster Schritt bei der Schaffung von Transparenz. Die Weiterentwicklung dieses Instruments sollte aber von Anfang mitgedacht werden, um am Ende Bürgerinnen und Bürger mit dem Staat auf Augenhöhe zu bringen. Wenn der Staat in Sekundenschnelle Daten abrufen kann, dann müssen Betroffene dies nicht nur nachvollziehen, sondern das Heft auch selbst in die Hand nehmen können. Nur die Möglichkeit, selbst die eigenen Daten aus den Registern und Datenbanken des Staates abrufen zu können, schafft letztlich eine Art von Waffengleichheit.

#### **Querverweis:**

3.1.2 Registermodernisierung verfassungskonform umsetzen

## **5.2 Die Digitalisierung der Verwaltung schreitet voran**

**Die Digitalisierung der Verwaltungen in Bund und Ländern wird politisch priorisiert und mit Nachdruck vorangetrieben. Die Corona-Pandemie hat diese Entwicklung weiter beschleunigt.**

Mit dem Gesetz zur Digitalisierung von Verwaltungsvorfahren bei der Gewährung von Familienleistungen (Dig-FamG) wurden auch Änderungen am Onlinezugangsgesetz (OZG) vorgenommen. Diese sollen die Bereitschaft der Bürgerinnen und Bürger sowie der Unternehmen oder sonstigen juristischen Personen steigern, Verwaltungsdienstleistungen künftig nicht mehr wie herkömmlich analog, sondern digital in Anspruch zu nehmen. Die Corona-Pandemie beschleunigt nicht nur diese Entwicklung. Sie zeigt auch, wie wichtig es ist, dieses digitale Angebot zu schaffen.

Bei der Nutzung digitaler Verwaltungsdienstleistungen ist mir wichtig, dass diese weiterhin freiwillig erfolgt, d. h. kein Zwang zur Anwendung besteht. Es muss auch in absehbarer Zukunft noch möglich sein, Verwaltungsgeschäfte analog vor Ort zu erledigen. Die Bürgerinnen und Bürger müssen diesbezüglich die freie Wahl haben. Darüber hinaus müssen sie jederzeit transparent nachverfolgen können, wer, zu welchem Zweck, wie, wo und wie lange ihre personenbezogene Daten verarbeitet. Ein Mittel, das sie hierbei unterstützen könnte, ist das geplante Datenschutzcockpit (vgl. hierzu Nr.5.1 Registermodernisierung).

#### **Interoperabilität der Bürgerkonten**

Die Bundesregierung hat mit dem OZG die Voraussetzungen für eine Vernetzung der Verwaltungsportale des Bundes, der Länder und Kommunen geschaffen. Bürgerinnen und Bürger sollen bei einem Verwaltungsportal ihrer Wahl Zugang zu allen online angebotenen Verwaltungsleistungen erhalten, ohne sich dazu mehr als einmal identifizieren zu müssen (Single Sign-On, SSO). Um die dafür erforderliche Interoperabilität der Angebote des Bundes, der Länder und der Kommunen zu ermöglichen, haben Bund und Länder eine Verwaltungsvereinbarung abgeschlossen, die den Betrieb der für die Interoperabilität erforderlichen Dienste und Komponenten durch eine Stelle beim Freistaat Bayern vorsieht. Auf mein Betreiben und das meiner Kolleginnen und Kollegen in den Ländern umfasst diese Vereinbarung auch Regelungen zur Wahrnehmung der gemeinsamen Verantwortung für die Verarbeitung personenbezogener Daten gemäß Art. 26 DSGVO. Dadurch können z. B. Betroffene zur Wahrnehmung ihrer Betroffenenrechte stets einen Ansprechpartner finden.



Für die Interoperabilität der Nutzerkonten ist ein verbindlicher Rahmen für die Bewertung der Vertrauenswürdigkeit der Identifizierungssysteme erforderlich, die den Zugang zu allen Verwaltungsleistungen des Bundes, der Länder und Kommunen ermöglichen. Dieser Rechtsrahmen wurde auf europäischer Ebene mit der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS-Verordnung) geschaffen. In Übereinstimmung mit der eIDAS-Verordnung sieht das OZG die Verwendung von Identifizierungsmitteln für die Vertrauensstufen „niedrig“, „substantiell“ und „hoch“ vor. Für das Niveau „hoch“ ist bislang nur der Personalausweis mit eID-Funktion geeignet. Daneben wird befristet die Möglichkeit zur Nutzung von ELSTER-Softwarezertifikaten zum Nachweis der Identität in den Nutzerkonten sowohl von natürlichen Personen als auch von Organisationen geschaffen. Bis zum 30. Juni 2023 werden die ELSTER-Softwarezertifikate für das Vertrauensniveau „substantiell“ anerkannt. Erfreulich ist, dass mit dem ELSTER Softwarezertifikat ein Identifizierungsmittel für das Vertrauensniveau „substantiell“ angeboten wird, bislang das Einzige für dieses Vertrauensniveau.

In Übereinstimmung mit der eIDAS-Verordnung wurden außerdem Regelungen zur Identifizierung von Personen und Organisationen aus EU-Mitgliedstaaten sowie zur Identifizierung durch anerkannte private Anbieter getroffen. Im Berichtszeitraum wurde der erste deutsche Anbieter eines Identifizierungssystems von der Bundesregierung anerkannt. Anbieter privatrechtlicher Identifizierungssysteme für SSO-Zwecke bieten ihren Kontoanbietern an, dass diese mit Einwilligung der Nutzer eine pseudonymisierte digitale Werbe-Identität zur persönlichen Ansprache der Kontonutzenden verwenden können. Eine solche digitale Werbe-Identität ist mit den Werbe-IDs von Smartphones vergleichbar und ermöglicht die Nutzerkonto-übergreifende Profilierung des Nutzungsverhaltens. Die Nutzer privatrechtlicher Identifizierungsmittel müssen über die Folgen der Einwilligung in die Generierung einer pseudonymisierten digitalen Identität für die personalisierte Ansprache (Werbung) in klarer und verständlicher Art und Weise aufgeklärt werden.

#### **Bundesportal und Nutzerkonto Bund**

Ich begrüße, dass auf mein Betreiben hin mit dem DigFamG auch die Verantwortlichkeiten für das Bundesportal und das Nutzerkonto Bund im E-Government-Gesetz geregelt sowie Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten im Bundesportal und von Zugriffsrechten geschaffen worden sind. Dies gibt Rechtssicherheit und Klarheit für die Nutzerinnen und Nutzer, z. B. darüber, wo sie ihre Betroffenenrech-

te geltend machen können. Allerdings sehe ich die Notwendigkeit, dass für weitere geplante Funktionen des Bundesportals, wie z. B. eine Antragsübersicht, vor deren Aufnahme in den Produktivbetrieb entsprechende Verarbeitungsbefugnisse normiert werden müssen.

#### **Querverweis:**

##### **5.1 Registermodernisierung**

## **5.3 IT-Sicherheitsgesetz 2.0**

**Die Cyber- und Informationssicherheit sind essentielle Vertrauensanker der Digitalisierung. Das mit der Novelle des IT-Sicherheitsgesetzes verfolgte Ziel eines verbesserten Schutzes von Gesellschaft und Wirtschaft in der digitalen Welt muss aber datenschutzrechtliche Erfordernisse berücksichtigen.**

IT-Sicherheit war und ist neuralgischer Punkt für die Digitalisierung und auch für den Schutz personenbezogener Daten. Datenschutz und IT-Sicherheit sind dabei zwangsläufig miteinander verzahnt. Schließlich soll IT-Sicherheit den Missbrauch, unberechtigten Zugang und die unberechtigte Nutzung personenbezogener Daten ausschließen, so dass IT-Sicherheitsrisiken stets auch Datenschutzrisiken sind.

Ein erster Entwurf eines IT-Sicherheitsgesetzes 2.0 wurde mir bereits im Frühjahr 2019 auf Ressortebene zugeleitet. Ursprünglich geplante, aus meiner Sicht überbordende und deshalb datenschutzrechtlich kritische, Neuregelungen im Straf- und Strafprozessrecht wurden in einem neuen Entwurf nicht mehr verfolgt.

Bei dem Gesetzgebungsverfahren ist mir insgesamt besonders wichtig, dass die gemeinsame Verantwortung und Partnerschaft zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und meinem Haus gestärkt wird. Zentrale Voraussetzung für eine effektive beidseitige Aufgabenerledigung ist in diesem Zusammenhang eine valide Informationsbasis. Deshalb ist es wichtig, dass das BSI, das zu einer wichtigen Informationsdrehscheibe für IT-Sicherheit ausgebaut werden soll, mich auch in Zukunft aktiv über erkannte Sicherheitsrisiken und -vorfälle in der Informationstechnik informiert.

Kritisch im Gesetzentwurf sehe ich u.a. eine Ausweitung der Speicherung von Protokolldaten von drei auf zwölf Monate. Argumentiert wird, diese Ausweitung sei für einen effektiven Schutz und eine effektive Aufklärung von Cyberangriffen unerlässlich. Denn Cyberangriffe würden sich typischerweise über einen längeren Zeitraum erstrecken und nur mit vorhandenen Protokolldaten sei eine Rekonstruktion des Angriffs und eine bestmögliche Schadensbeseitigung möglich. Die Motivation für die



längere Speicherdauer ist nachvollziehbar, sie rechtfertigt aus meiner Sicht aber nicht ihre erhebliche Ausweitung und wirft Fragen der Verhältnismäßigkeit auf. Zudem habe ich an verschiedenen Stellen dafür plädiert, im IT-Sicherheitsgesetz klarer herauszuarbeiten, welche konkreten personenbezogenen Daten für welche Zwecke verarbeitet werden.

Für das BSI ist das IT-Sicherheitsgesetz mit einem erheblichen Verantwortungs- und Aufgabenzuwachs verbunden. Korrespondierend hierzu wird auch der Mehraufwand meines Hauses für die Beratung, Kontrolle und Prüfung datenschutzrechtlicher Vorgaben bei der Umsetzung der neuen Prüf-, Abfrage- und Kontrollbefugnisse des BSI deutlich steigen.

Meine Stellungnahme vom 18. Dezember 2020 finden Sie unter: [www.bfdi.bund.de/stellungnahmen](http://www.bfdi.bund.de/stellungnahmen)

## 5.4 Novellierung des Gesetzes über den Bundesnachrichtendienst

Das Bundesverfassungsgericht (BVerfG) hat den Gesetzgeber verpflichtet, Vorschriften des Gesetzes über den Bundesnachrichtendienst (BNDG) zur sogenannten Ausland-Ausland-Fernmeldeaufklärung bis zum 31. Dezember 2021 zu novellieren (vgl. 6.4). Die Abstimmung des Referentenentwurfs erfolgte in Anbetracht der erheblichen Grundrechtsrelevanz mit unangemessenem Zeitdruck.

In meiner ersten Stellungnahme zum Referentenentwurf habe ich meine Kritik am engen Zeitplan für die Ressortbefassung zum Ausdruck gebracht. Der in der Ressortbesprechung am 7. Oktober 2020 – nur eine gute Woche nach Übersendung des Referentenentwurfs an die Ressorts – vom Bundeskanzleramt erklärte Zeitplan, das BNDG innerhalb nur eines Monats im Kabinett einzubringen, verstieß in eklatanter Weise gegen die Vorgaben der Gemeinsamen Geschäftsordnung der Bundesministerien und das Erfordernis einer frühzeitigen Beteiligung meines Hauses. Es war ausgeschlossen, das komplexe Regelwerk innerhalb einer derart kurzen Zeitspanne mit der gebotenen Sorgfalt und Tiefe zu prüfen. Auch wenn das Bundeskanzleramt seinen Zeitplan später modifizierte und das Kabinett den Entwurf erst am 16. Dezember 2020 angenommen hat, ist eine Gesamtberatungszeit von zusammengerechnet nur drei Monaten für insgesamt vier verschiedene, inhaltlich zum Teil erheblich geänderte Referentenentwürfe mit jeweils wenigen Tagen Kommentierungsfrist schlicht unangemessen. Auch zur Vermeidung verfassungsrechtlicher Risiken wäre hier die Einhaltung des Grundsatzes „Gründlichkeit vor Schnelligkeit“ dringend geboten gewesen. Ich kritisiere auch, dass mir keine Stellung-

nahmen der übrigen beteiligten Ressorts zugänglich gemacht wurden. Eine essentielle Auseinandersetzung mit anderen Beteiligten war so nicht möglich.

### Kritikpunkte

Meine inhaltliche Kritik am Referentenentwurf betrifft die vorgesehenen Veränderungen in der Aufsicht über den BND und verschiedene materiell-rechtliche Regelungen.

Ein wesentlicher materiell-rechtlicher Kritikpunkt liegt in der nicht hinreichenden Umsetzung der vom BVerfG vorgegebenen Beschränkungen für Datenübermittlungen durch den BND an andere in- und ausländische öffentliche und nichtöffentliche Stellen. Meine Bedenken gegen die beabsichtigte Ausgestaltung der Übermittlungsvorschriften wurden vom Bundeskanzleramt zwar teilweise berücksichtigt und die Übermittlungsvorschriften als Korrektiv der umfassenden Datenerhebungen der strategischen Ausland-Fernmeldeaufklärung teilweise verbessert. Dennoch blieben andere wichtige Aspekte zur weiteren Ausgestaltung der Übermittlungsbeschränkungen unberücksichtigt, obwohl die Vorschriften nach den Vorgaben des BVerfG gerade entscheidend sind, ein Gegengewicht zur umfangreichen, anlasslosen Datenerhebung im Rahmen der strategischen Ausland-Fernmeldeaufklärung zu schaffen.

Zu den von mir geäußerten Bedenken gehört auch die im Gesetzentwurf vorgesehene Möglichkeit der Übermittlung von Daten, die vom BND zum Zweck der politischen Unterrichtung der Bundesregierung erhoben werden, an die Inlandsnachrichtendienste oder die Polizeien zum dortigen Erkenntnisgewinn. Derartige Daten sollen nach der Intention des BVerfG-Urteils nur zur politischen Unterrichtung der Bundesregierung erhoben und grundsätzlich auch nur direkt zu diesem Zweck an die Bundesregierung übermittelt werden dürfen. Die vom Bundeskanzleramt vertretene Ansicht, dass die Inlandsnachrichtendienste oder die Polizeien diese Daten zur eigenen Weiterleitung an die Bundesregierung erhalten dürfen, geht aus meiner Sicht zu weit. Diese mit dem zweiten Referentenentwurf eingefügte Ausweitung der Übermittlungsbefugnisse stellt eine Verschlechterung des Datenschutzes im Verhältnis zum ersten Referentenentwurf dar und begegnet erheblichen verfassungsrechtlichen Bedenken.

Die vom Urteil des BVerfG ausgehenden Änderungserfordernisse in anderen nachrichtendienstlichen Gesetzen (z.B. dem BVerfSchG) zu den Übermittlungsvorschriften waren hingegen nicht Gegenstand dieses Gesetzgebungsverfahrens. Ermächtigungsgrundlagen des BND zu Übermittlungen außerhalb des BNDG wurden wie die allgemeinen Übermittlungsvorschriften im BNDG nicht angepasst, was absehbar jedenfalls zu einer

Verfassungswidrigkeit der allgemeinen Übermittlungen im BNDG führen dürfte.

Hervorzuheben ist, dass in anderen Bereichen, wie etwa dem Vertraulichkeitsschutz, meine Anregungen zum Anlass für gesetzliche Verbesserungen genommen wurden. Die Normen zum Vertraulichkeitsschutz bei der strategischen Ausland-Fernmeldeaufklärung und dem Eingriff in informationstechnische Systeme zur Gefahrenfrüherkennung waren zunächst so zu verstehen, dass nur die Berufsträger (z.B. Journalisten, Rechtsanwälte) vom Vertraulichkeitsschutz erfasst wurden, nicht aber die Kommunikationsbeziehung unter Einbeziehung der Gesprächspartner als solche geschützt wurde. Dies wurde im Gesetzentwurf nachgebessert. Es fehlt allerdings eine allgemeine Vorschrift abseits der Spezialregelungen zur strategischen Ausland-Fernmeldeaufklärung und dem Eingriff in informationstechnische Systeme.

Die mit der Gesetzesnovelle erstmals normierte Befugnis des BND für Eingriffe in informationstechnische Systeme im Ausland zur Datenerhebung per „Hacking“ und die Befugnis zur Weiterleitung dieser Daten an die Inlandsdienste sowie Polizei- und Strafverfolgungsbehörden ist ebenfalls verfassungsrechtlich erheblich bedenklich. Meine Bedenken gegen derartige, besonders intensive Eingriffe zur Datenerhebung und die damit verbundenen Übermittlungsvoraussetzungen wurden vom Bundeskanzleramt nicht berücksichtigt.



### Neue Aufsichtsbehörde

Besondere Relevanz haben schlussendlich die Regelungen zur Umsetzung der vom BVerfG gemachten Vorgaben für eine unabhängige objektivrechtliche Kontrolle der Maßnahmen des BND im Bereich der strategischen Ausland-Fernmeldeüberwachung. Obwohl mit meiner Behörde eine völlig unabhängige oberste Datenschutzaufsichtsbehörde in Deutschland existiert, die über eine hohe Kompetenz und langjährige Erfahrung in der Datenschutz- und damit der Nachrichtendienstkontrolle des BND und der Inlandsgeheimdienste des Bundes verfügt, beabsichtigt die Bundesregierung die Schaffung einer neuen obersten Bundesbehörde, den sogenann-

ten Unabhängigen Kontrollrat. Dieser soll einerseits eine mit abschließenden Entscheidungsbefugnissen verbundene gerichtsähnliche Kontrolle sicherstellen, der die wesentlichen Verfahrensschritte der strategischen Ausland-Fernmeldeüberwachung unterliegen. Zudem soll er im Wege der administrativen Kontrolle stichprobenmäßig die Rechtmäßigkeit des gesamten Prozesses der strategischen Überwachung überprüfen. Der Bereich der administrativen Kontrolle überlappt sich dabei mit meiner Aufsichtszuständigkeit, da ich die Datenverarbeitungen des BND im Bereich der strategischen Ausland-Fernmeldeaufklärung bereits vollständig kontrolliere.

Mit der Zusammenführung der gerichtsähnlichen und der administrativen Kontrolle unter das Dach einer neuen obersten Bundesbehörde werden Synergieeffekte nicht genutzt, die entstanden wären, wenn die administrative Rechtskontrolle – wie vom BVerfG als eine Lösungsvariante vorgesehen – mir übertragen worden wäre. Statt in meiner Behörde vorhandene und gerade auch im Bereich der Aufsicht über die Nachrichtendienste des Bundes bewährte Kontrollstrukturen mit erfahrener Personal zu nutzen, soll mit erheblichen Mitteln in kürzester Zeit bis Ende des Jahres 2021 eine in der Detailarbeit funktionierende neue, gleichwohl in der Nachrichtendienstkontrolle aber unerfahrene Aufsichtsbehörde aus dem Boden gestampft werden. Da diese auch noch an den Standorten des BND in Berlin und Pullach angesiedelt werden soll, womöglich unmittelbar auf dessen Liegenschaften, ergeben sich auch Zweifel im Hinblick auf die vom BVerfG geforderte Distanz. Diese Zweifel werden dadurch verstärkt, dass das neue Kontrollorgan die Personalverwaltung auf das Bundeskanzleramt und damit auf die dem BND übergeordnete Behörde übertragen kann, wozu der geplante Unabhängige Kontrollrat aufgrund fehlender eigener Strukturen wohl gezwungen sein dürfte. Im Ergebnis wird durch die Existenz einer weiteren Aufsichtsbehörde die Kontrolllandschaft im Bereich der Nachrichtendienste noch unübersichtlicher. Ohne umfassende Kooperationsbefugnisse der Kontrollstellen untereinander wird die Kontrolle des BND zwangsläufig erschwert. Auch deshalb ist es notwendig, das Kooperationsverhältnis zwischen dem Unabhängigen Kontrollrat und meiner Behörde gesetzlich so auszugestalten, dass ein inhaltlicher Austausch über die konkreten Kontrollen erfolgen darf und muss. Hier erfüllt der Gesetzentwurf noch nicht alle Erwartungen und sollte im parlamentarischen Verfahren dringend nachgebessert werden.

### Querverweis:

#### 6.3 FMA-Urteil

## 5.5 Gesetzgebungsverfahren zur Änderung des Verfassungsschutzrechts

Die bestehende Gesetzeslage im Verfassungsschutzrecht lässt derzeit die Quellen-Telekommunikationsüberwachung im nachrichtendienstlichen Bereich sowie eine Intensivierung der Zusammenarbeit zwischen Verfassungsschutzbehörden und Militärischem Abschirmdienst nicht zu. Dies soll durch eine Gesetzesnovelle geändert werden.

Mit Kabinettsbeschluss vom 21. Oktober 2020 hat die Bundesregierung einen Gesetzesentwurf zur Änderung des Verfassungsschutzrechts in den Deutschen Bundestag eingebracht. Aus datenschutzrechtlicher Sicht habe ich zu dem Entwurf bereits Stellung genommen (Mein Dokument vom 4. November 2020 finden Sie unter: [www.bfdi.bund.de/stellungnahmen](http://www.bfdi.bund.de/stellungnahmen)). Die parlamentarischen Beratungen sind zum Zeitpunkt des Redaktionsschlusses noch nicht abgeschlossen.

Gegenstand des Gesetzgebungsvorhabens ist es insbesondere, den Nachrichtendiensten die Befugnis zur Quellen-Telekommunikationsüberwachung einzuräumen sowie den Informationsaustausch zwischen den Verfassungsschutzbehörden und dem Militärischen Abschirmdienst durch erweiterte Möglichkeiten gemeinsamer Datenhaltung technisch auszubauen.

Nicht zuletzt die im vergangenen Jahr ergangenen verfassungsgerichtlichen Entscheidungen zur Ausland-Ausland-Fernmeldeaufklärung (BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17) und zur Bestandsdatenauskunft (BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13) haben einmal mehr deutlich werden lassen, dass Umfang und Ausmaß des Reformbedarfs im Verfassungsschutzrecht dramatisch sind. Die Regelungssystematik, -dichte und -tiefe der entsprechenden Vorschriften weisen generell nicht die notwendige Konsistenz und Qualität auf, die Nachrichtendienste im Einklang mit den verfassungsrechtlichen Vorgaben zu in Grundrechte eingreifende Maßnahmen zu ermächtigen.

Anstatt an diesen Defiziten etwas zu verbessern, sieht der Gesetzentwurf demgegenüber vor, die ohnehin schon verfassungsrechtlich nicht belastbare Gesetzeslage weiter zu strapazieren. Gerade die Einführung einer so tiefgreifenden und folgenschweren Maßnahme wie der Quellen-Telekommunikationsüberwachung bedarf eines umfassenden, stringenten und belastbaren gesetzlichen Gesamtkonzepts, das alle Vorgaben des Bundesverfassungsgerichts berücksichtigt.

Auch die Intensivierung des Informationsaustauschs zwischen den Verfassungsschutzbehörden und dem

Militärischen Abschirmdienst, die dem Grunde nach sicherlich richtig ist, lässt sich auf Basis des bisherigen Gesetzentwurfs nicht im Einklang mit der Verfassung verwirklichen. Grundvoraussetzung dafür, dass die Zusammenarbeit zwischen den Inlandsgeheimdiensten intensiviert und ausgebaut werden kann, sind verfassungskonforme gesetzliche Übermittlungsregelungen zwischen den betreffenden Behörden. Spätestens nach den Feststellungen des Bundesverfassungsgerichts in der Entscheidung zur Ausland-Ausland-Fernmeldeaufklärung sind die Übermittlungsregelungen des Bundesverfassungsschutzgesetzes und des Gesetzes über den Militärischen Abschirmdienst grundlegend reformbedürftig.

Der Gesetzgeber sollte sich daher derzeit ausschließlich darauf konzentrieren, das Verfassungsschutzrecht entsprechend der verfassungsrechtlichen Anforderungen von Grund auf zu reformieren. Erst nachdem dies vollständig gelungen ist, sollte er auf Basis einer gewissenhaften Evaluation der Notwendigkeit und Wirksamkeit nachrichtendienstlicher Kompetenzen über eine Ausweitung nachrichtendienstlicher Datenverarbeitungen oder gar eine Ausweitung nachrichtendienstlicher Befugnisse nachdenken. Dabei muss er auch besonderes Augenmerk darauf legen, ob etwaige Befugniserweiterungen wirklich erforderlich sind oder ob nicht vielmehr die Polizei- und Strafverfolgungsbehörden mit ihren schon bestehenden Befugnissen die staatlichen Bedürfnisse bereits abdecken.

### Querverweise:

5.3 Novellierung des Gesetzes über den Bundesnachrichtendienst, 6.3 FMA-Urteil

## 5.6 Die Verordnung zu den „Apps auf Rezept“

Patienten erwarten bei verordneten Gesundheitsapps zu Recht, dass ihre Daten vertraulich bleiben. Um dies sicherzustellen, müssen die Regelungen in der Digitale-Gesundheitsanwendungen Verordnung DiGAV nachgebessert werden – eine Selbsterklärung der Hersteller kann hier nicht reichen.

Im April 2020 ist die DiGAV in Kraft getreten. Sie soll die Vorschriften des Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG – siehe hierzu meinen 28. Tätigkeitsbericht Nr. 5.6) zu den Digitalen Gesundheitsanwendungen (DiGAs), insbesondere §§ 33a und 139e Fünftes Buch Sozialgesetzbuch (SGB V), konkretisieren. Eingeführt wurde in § 33a SGB V ein Anspruch der gesetzlich Krankenversicherten auf eine Versorgung mit DiGAs, die

von Ärzten und Psychotherapeuten verordnet werden können und durch die Krankenkasse erstattet werden. Voraussetzung hierfür ist, dass die jeweilige DiGA ein Prüfverfahren beim Bundesamt für Arzneimittel und Medizinprodukte (BfArM) erfolgreich durchlaufen hat und in einem Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen aufgeführt ist. Details zu diesem sog. „Fast-Track-Verfahren“, des schnellen Zugangs von DiGAs zum ersten Gesundheitsmarkt, sind in der DiGAV enthalten.

Meine grundsätzlichen Bedenken gegen die Verfahren zur Sicherstellung eines hinreichenden Datenschutz- und Datensicherheitsniveaus bei den DiGAs habe ich bereits im Gesetzgebungsverfahren zum DVG gegenüber dem Bundesgesundheitsministerium und dem Ausschuss für Gesundheit des Deutschen Bundestages vorgebracht. Leider wurden sie auch in der DiGAV nicht berücksichtigt und gelten uneingeschränkt fort.

So habe ich immer wieder auf datenschutzrechtliche Bedenken hinsichtlich des Vertriebs von Gesundheits-Apps über Plattformen der Unternehmen Apple und Google hingewiesen. Problematisch beim Download der DiGAs über kommerzielle App-Stores ist, dass sensible Gesundheitsdaten an unberechtigte Dritte und auch die App-Store-Betreiber gelangen können (z. B. über den Umstand der Nutzung einer Depressions-App o. ä. - die Metadaten können in diesen Fällen sehr sensibel sein). Die digitalen Gesundheitsanwendungen sollten daher nicht über „öffentlich zugängliche digitale Vertriebsplattformen“ wie die der US-amerikanischen Unternehmen übermittelt werden. Stattdessen sollte ein App-Store in der Telematikinfrastruktur geschaffen werden, der von Akteuren des Gesundheitssystems betrieben wird, die der gesetzlichen Schweigepflicht unterliegen. Natürlich besteht auch während der Nutzung der DiGA die Gefahr, dass die Hersteller der mobilen Endgeräte oder andere Dritte etwa durch die Einbindung von Tracking- oder Analysetools sensible Gesundheitsdaten erhalten und Gesundheitsprofile erstellen.

#### **Vertraulichkeit und Verantwortlichkeit nicht gesichert**

Transparenz für die Nutzenden ist ein ganz wesentlicher Aspekt, insbesondere wenn die freiwillige, informierte, ausdrückliche Einwilligung der Nutzenden die Rechtsgrundlage für die Verwendung der DiGA darstellt. Im DVG, in der DiGAV und erläuternd im Leitfaden des BfArM zum „Fast Track Verfahren“ nach § 139e SGB V wird zwar abstrakt aufgeführt, dass Datenschutz und Datensicherheit einzuhalten sind. Problematisch ist aber, dass nur eine Selbsterklärung der DiGA-Hersteller vorgesehen ist, die jedoch keinerlei rechtliche Verbindlichkeit entfaltet, und somit nicht sicher nachgewiesen werden kann, dass Datenschutzanforderungen, die in

§ 139e SGB V und in der DiGAV gefordert werden, auch tatsächlich eingehalten werden.

Darüber hinaus fehlen klarstellende Regelungen zur datenschutzrechtlichen Verantwortlichkeit. Zu welchen Zwecken und unter welchen Voraussetzungen der Hersteller die mit der DiGA erhobenen Daten verarbeiten darf, wird in § 4 Abs. 2 DiGAV aufgeführt. Allerdings können darüber hinaus noch andere Stellen Zugang zu den sensiblen Gesundheitsdaten erhalten, je nach konkretem Verwendungszusammenhang der DiGA, zum Beispiel Ärzte oder andere Leistungserbringer. Häufig kann ein DiGA-Hersteller in seiner „Datenschutz-Selbsterklärung“ gegenüber dem BfArM vieles nicht verlässlich beantworten. Damit ist eine Transparenz für den Nutzer nicht gewährleistet. Vielmehr wäre eine umfassende Aufklärung der Nutzer darüber, welche Personen/Einrichtungen im Rahmen der DiGA-Nutzung Zugriff auf welche ihrer Gesundheitsdaten erhalten, vorab erforderlich. Leider ist weder im DVG noch in der DiGAV ein Ansprechpartner für Betroffenenrechte vorgesehen, der im konkreten Verwendungszusammenhang umfassend Auskunft geben könnte. Klarstellungen, die ich gefordert hatte, wurden nicht getroffen.

Ich hoffe sehr, dass zukünftige Gesetze und Verordnungen zur weiteren Digitalisierung des Gesundheitswesens diese Defizite beheben.

## **5.7 Datentransparenzverordnung**

**Die Datentransparenzverordnung konkretisiert die Vorgaben im SGB V und trifft nähere Festlegungen für die Datenverarbeitung im Forschungsdatenzentrum. Leider fehlen Regelungen zur Umsetzung des Widerspruchrechts.**

Mit der novellierten Datentransparenzverordnung vom 19. Juni 2020, die am 11. Juli 2020 in Kraft trat, werden die Aufgaben und das Verfahren der Datentransparenz nach §§ 303a bis 303e SGB V konkretisiert. Durch das Digitale-Versorgung-Gesetz vom 9. Dezember 2019, über das ich in meinem 28. Tätigkeitsbericht (Nr. 5.6, S. 45) berichtet habe, hat das Verfahren der Datentransparenz eine Reihe von Änderungen erfahren, so dass auch die Verordnung neu gefasst werden musste. Das Bundesministerium für Gesundheit (BMG) hat mich hier zwar frühzeitig eingebunden, dennoch waren am Ende die mir gesetzten Fristen auch hier wieder sehr kurz bemessen: Der Entwurf selbst wurde schließlich mit einer Frist von lediglich 12 Kalendertagen zur Stellungnahme an die Ressorts versandt.

Insgesamt ließen die Formulierungen des Entwurfs erkennen, dass dem Datenschutz grundsätzlich ein



hoher Stellenwert zugemessen wurde. Dies begrüße ich ausdrücklich, da ein nachweislich sorgsamer Umgang mit den hier betroffenen sensiblen Gesundheitsdaten wesentlich für die Akzeptanz in der Bevölkerung ist. Diese ist nötig, da es sich bei den Datenzulieferungen für das Forschungsdatenzentrum (FDZ) aufgrund der Datentransparenzregelungen um die Abrechnungsdaten der mehr als 70 Mio. gesetzlich Versicherten handelt. Zudem war der Datenumfang durch das DVG erweitert worden. Zur Transparenz gegenüber den Betroffenen trägt bei, dass nunmehr die einzelnen Datenkategorien in der Verordnung genannt sind und sich nicht hinter Verweisen auf andere Normen verstecken.

In dieser Verordnung wird auch festgelegt, dass das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) die Forschungsdatenbank führt und das Robert Koch-Institut als Vertrauensstelle für die Pseudonymisierung der Daten sorgt. Die Forschungsdatenbank ist wegen des Umfangs der Daten und deren Sensibilität von besonderer Bedeutung. Umso wichtiger wäre es gewesen, die Aufgabenzuweisung in diesem Zusammenhang nicht in einer Verordnung, sondern durch Gesetz vorzunehmen. Ich habe daher – bisher leider vergeblich – angeregt, zeitnah eine entsprechende Änderung des § 303a SGB V vorzusehen.

Die Benennung des BfArM als Halterin der Forschungsdatenbank ist problematisch, da das BfArM zugleich zu dem im Gesetz konkret benannten Kreis von Nutzungsberechtigten zählt, die nach Prüfung eines entsprechenden Antrages Daten zur Verfügung gestellt bekommen. So könnte das BfArM über seinen eigenen Antrag entscheiden. Hier fehlt die erforderliche Unabhängigkeit, die für ein geordnetes Verfahren, das auch datenschutzrechtliche Aspekte gebührend beachtet, unabdingbar ist. In der Verordnung wurde diese Unvereinbarkeit gelöst, indem festgelegt wurde, dass das BfArM selbst keine Daten erhalten kann. Diese Regelung sehe ich mit einer gewissen Skepsis, da sie die gesetzlich eingeräumte Nutzungsberechtigung des BfArM konterkariert. Auch deshalb werde ich die Antragsbearbeitung im BfArM zu gegebener Zeit sorgfältig prüfen.

#### **Neue Widerspruchregelung notwendig**

Zudem hatte ich empfohlen, Regelungen zur Umsetzung des Rechts der Betroffenen zum Widerspruch nach Art. 21 Abs. 6 DSGVO vorzusehen, auch wenn die Voraussetzungen nur in wenigen besonderen Fällen tatsächlich vorliegen dürften. Das Recht besteht unabhängig von einer Umsetzungsregelung. Aus Gründen der Rechtsklarheit sollte hier allerdings ein Verfahren vorgegeben werden, da der Widerspruch vernünftigerweise nicht beim FDZ selbst, sondern bereits bei der jeweiligen Krankenkasse zu erklären ist. Diese Empfehlung wurde leider

nicht umgesetzt. Dies ist bedauerlich, hätte dies doch die bei Bürgerinnen und Bürgern bestehende, mir aufgrund verschiedener Eingaben bekannte Besorgnis gegenüber der verpflichtenden staatlichen Datensammlung und -haltung mildern können. Das BMG hat signalisiert, demnächst außerhalb der Datentransparenzverordnung ein geordnetes Widerspruchsverfahren zu etablieren. Den Fortgang dieser Bemühungen werde ich weiter beobachten. Meine Bitte, ein allgemeines Widerspruchsrecht vorzusehen, hat das BMG nicht aufgegriffen.

#### **Querverweis:**

7.3 Register im Gesundheitswesen

## **5.8 Die Grundrente kommt - aber auch datenschutzgerecht ?**

**Die finanzielle Besserstellung durch die Einführung der Grundrente ist gesellschaftlich begrüßenswert. Die geplante Form der Anspruchsprüfung greift allerdings in das Recht auf informationelle Selbstbestimmung ein.**

Wer über viele Jahre hinweg in die gesetzliche Rentenversicherung mit unterdurchschnittlichem Einkommen eingezahlt hat, soll im Alter finanziell besser abgesichert sein. Dies ist Ziel des Gesetzes zur Einführung der Grundrente (Grundrentengesetz) zum 1. Januar 2021.

Am Gesetzgebungsverfahren wurde ich beteiligt. Meine datenschutzrechtlichen Einwände fanden jedoch keine Berücksichtigung.

Das Grundrentengesetz sieht die Nutzung der steuerlichen Identifikationsnummer außerhalb des Besteuerungsverfahrens durch die Träger der gesetzlichen Rentenversicherung vor. Vor dem Hintergrund der verfassungsgerichtlichen Rechtsprechung zur Schaffung eines einheitlichen Personenkennzeichens ist dies verfassungsrechtlich problematisch. Dies gilt umso mehr, als dass aktuell von der Bundesregierung geplant ist, im Zuge der Registermodernisierung ebenfalls die steuerliche Identifikationsnummer als einheitliches Personenkennzeichen für alle Bürgerinnen und Bürger einzuführen (s. 5.1 Registermodernisierung).

Bei der Berechnung der Grundrente ist nicht nur das Einkommen der rentenberechtigten Person, sondern auch das der mit ihr in Ehe oder Lebenspartnerschaft lebenden Person maßgebend. Den Trägern der gesetzlichen Rentenversicherung wird deshalb die Befugnis eingeräumt, auch die steuerliche Identifikationsnummer des Ehegatten oder der Lebenspartnerin beim Bundeszentralamt für Steuern abzufragen und für einen automatisierten Datenabgleich mit den Finanzbehörden bei der Einkommensprüfung zu nutzen. Neben

der beschriebenen Problematik um die Nutzung der steuerlichen Identifikationsnummer außerhalb des Besteuerungsverfahrens verletzt dieser Datenabgleich den datenschutzrechtlichen Ersterhebungsgrundsatz und greift so in die Rechte auf informationelle Selbstbestimmung Dritter ein.

#### Querverweis:

##### 5.1 Registermodernisierung

## 5.9 Das Digitale Familienleistungen-Gesetz

**Digitale Familienleistungen als erster Schritt einer umfassenden Verwaltungsdigitalisierung? Weniger Papierkram nur mit mehr Datenschutz.**

Das Gesetz zur Digitalisierung von Verwaltungsvorfahren bei der Gewährung von Familienleistungen (Digitale-Familienleistungen-Gesetz) vom 3. Dezember 2020 verspricht weniger Papierkram bei wichtigen Familienleistungen wie dem Elterngeld, dem Kindergeld oder dem Kinderzuschlag. Die Digitalisierung dieser Anträge soll den Anfang einer umfassenden Verwaltungsdigitalisierung bilden. Dies begrüße ich grundsätzlich. Allerdings wurde die Verwaltungsdigitalisierung im Schnellverfahren umgesetzt. Enge Zeitpläne waren in diesem ambitionierten Gesetzgebungsverfahren von Beginn an der Tagesordnung. Im Ergebnis ist die Digitalisierung von Elterngeld, Kindergeld oder dem Antrag auf Erteilung einer Geburtsurkunde freiwillig, setzt im Wesentlichen die Einwilligung der Antragsteller voraus und stellt – was auch so bleiben muss – eine Alternative neben der immer noch möglichen Papierantragsstellung dar.

Das Ziel des Digitale-Familienleistungen-Gesetz, der Beginn des digitalen Antragsverfahrens im Sozialrecht zu sein, findet meine uneingeschränkte Unterstützung. Dies gilt auch für die hier gefundene Einwilligungsmöglichkeit. Einwilligung im Sinne der DSGVO bedeutet allerdings „informierte Einwilligung“. Die Bürgerin und der Bürger muss wissen, in welche Datenverarbeitung sie oder er einwilligt. Hierauf wird es bei der Umsetzung des Gesetzes ankommen. Im Sozialrecht gilt in vielen Bereichen zudem der Direkterhebungsgrundsatz, das heißt, Daten sind unmittelbar beim Betroffenen zu erheben. Hiervon wird durch das Gesetz deutlich abgewichen, wenn auch zur Bequemlichkeit der betroffenen Antragsteller. Transparenz und Kontrolle durch die Bürger und Bürgerinnen über ihre eigenen Daten und die jederzeitige Möglichkeit der Einsichtnahme in den

Stand der jeweiligen Verfahren sind daher wesentlich. Daher darf „vertrauensvolle Kommunikation“ zwischen verschiedenen Behörden nicht dazu führen, dass die Behörden durch die Digitalisierung mehr über die Bürgerinnen und Bürger wissen als diesen bewusst ist. Hierbei kommt es vor allem auf die Umsetzung in der Praxis an, die ich weiterhin kritisch begleiten werde.

#### Digitalisierung weiterer Verwaltungsverfahren

Mit dem Gesetz wurden durch Änderungen des Onlinezugangsgesetzes (OZG) und des E-Government-Gesetzes (EGovG) weitere datenschutzrechtliche Regelungen für das Nutzerkonto sowie für die Verarbeitung personenbezogener Daten im Verwaltungsportal des Bundes geschaffen (vgl. hierzu Nr 5.2). Diese Rahmenbedingungen – die auch für die Digitalisierung weiterer Verwaltungsverfahren genutzt werden können – sind ausnahmslos durch eine freiwillige Teilnahme der Bürgerinnen und Bürger und ein hohes Maß an Datensicherheit geprägt. Hier konnte ich im Gesetzgebungsverfahren zahlreiche Impulse setzen, die der Gesetzgeber aufgegriffen hat.

Im Gesetz selbst hatte ich darüber hinaus gefordert, soweit die Übertragungswege und weitere datenschutzrechtlich relevante Aspekte zwischen der Datenstelle der Rentenversicherung (DSRV) und den nach § 12 Absatz 1 des Bundeselterngeld- und Elternzeitgesetzes (BEEG) zuständigen Behörden geregelt werden, auch ein Einvernehmen mit mir vorzusehen (§ 108a Absatz 4 SGB IV). Ich bedauere, dass dieser Anregung nicht gefolgt wurde. Mit dem Gesetz werden die Rechtsgrundlagen für die Datenübermittlungen zur Nutzung des rvBEA-Verfahrens<sup>15</sup> für die Abfrage von Entgeltdaten bei den Arbeitgebern auch für Elterngeld geschaffen (§ 108a SGB IV, § 9 Absatz 2 BEEG). Den zuständigen Elterngeldstellen der Länder wird die Möglichkeit eröffnet, das Datenabfrage- und Übermittlungsverfahren der DSRV zu nutzen. Die Antragsteller müssen daher nicht mehr selbst die erforderlichen Entgeltbescheinigungen ihres Arbeitgebers vorlegen, sondern die DSRV fragt im Auftrag der Elterngeldstellen der Länder die Entgeltdaten elektronisch bei den Arbeitsgebern ab und leitet diese anschließend an die Elterngeldstellen weiter. Hinsichtlich der noch zu vereinbarenden Rahmenvereinbarung, in der die Modalitäten dieser – rechtssystematisch einzigartigen – Auftragserteilung geregelt werden, werde ich meine Beratung anbieten.

Ich begrüße ausdrücklich, dass die zuständige Elterngeldstelle die Abfrage und Übermittlung der Entgeltbescheinigungen nach § 108a SGB IV nur dann beauftragt, wenn die Antragstellerinnen und Antragsteller ihr

<sup>15</sup> „rv“ steht für Rentenversicherung; „BEA“ steht für Bescheinigungen elektronisch anfordern und annehmen.



gegenüber sowohl in die Datenabfrage als auch in die Datenübermittlung ihrer Entgeltbescheinigungsdaten eingewilligt haben.

Das alles zeigt, dass die Digitalisierung komplexer Verwaltungsverfahren, an denen neben den Bürger und Bürgerinnen verschiedene öffentliche und private Stellen aus Bund und Ländern beteiligt sind, keine einfache und schnelle, aber eben auch eine lösbare Aufgabe ist. Verwaltungsdigitalisierung und die damit einhergehende – sehr wünschenswerte – Verwaltungsvereinfachung darf nicht zu Lasten der Rechte, der Mitwirkungs- und Kontrollmöglichkeiten der Bürger und Bürgerinnen gehen. Digitalisierung sollte vielmehr dazu genutzt werden, die Transparenz und Mitwirkungsmöglichkeiten für Bürger und Bürgerinnen zu erhöhen.

Die den in den nächsten Jahren folgenden weiteren Gesetzgebungsvorhaben zur Digitalisierung bei Antragsverfahren im Sozialrecht werde ich konstruktiv begleiten.

## 5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich

Mehrere Gesetze im Telekommunikationsbereich müssen zeitnah an europäisches Recht angepasst werden. Dies wird aber nach derzeitigem Stand nicht fristgerecht erfolgen. Auch die E-Privacy-Verordnung lässt weiter auf sich warten.

Bereits in meinem letzten TB (Nr. 5.2) habe ich moniert, dass zahlreiche Gesetze immer noch nicht an die Datenschutz-Grundverordnung (DSGVO) angepasst worden sind. Auch die E-Privacy-Richtlinie ist seit Jahren nur unzureichend umgesetzt. Insbesondere die Vorgaben zu Cookies entsprechen nicht dem europäischen Recht. Ich habe den Gesetzgeber mehrfach aufgefordert, hier endlich tätig zu werden. Die fortbestehende Rechtsunsicherheit ist für Unternehmen und Aufsichtsbehörden unerträglich. Im Juli 2020 hat die Bundesregierung erstmals einen Entwurf für eine Anpassung des Telemediengesetzes vorgelegt. Dieses soll zukünftig „Telekommunikations-Telemedien-Datenschutz-Gesetz“ (TTDSG) heißen. Es ist erfreulich, dass der Gesetzgeber hier einen ersten Schritt unternommen hat. Leider hat der Entwurf erhebliche Mängel. Ich habe hierzu Stellung genommen und Empfehlungen ausgesprochen.

### Telekommunikationsmodernisierungsgesetz

Mit dem Telekommunikationsmodernisierungsgesetz (TKMoG) werden zahlreiche Vorgaben aus dem europäischen „Kodex elektronische Kommunikation“ in nationalen Vorschriften, insbesondere dem Telekommu-

nikationsgesetz (TKG), umgesetzt. Ziele des Kodex sind der Ausbau und die Nutzung von Netzen mit sehr hoher Kapazität, die Gewährleistung eines nachhaltigen und wirksamen Wettbewerbs sowie die Interoperabilität der Telekommunikationsdienste. Ferner sollen die Zugänglichkeit und die Sicherheit von Netzen und Diensten gewährleistet sowie die Interessen der Endnutzer gefördert werden. Bürgerinnen und Bürgern sollen erschwingliche und hochwertige Telekommunikationsdienste bereitgestellt werden. Im Rahmen der Umsetzung in nationales Recht wird auch der zentrale Begriff des Telekommunikationsdienstes deutlich erweitert. Dieser war bisher in § 3 Nr. 24 TKG (alt) definiert und wird zukünftig in der neuen Vorschrift des § 3 Nr. 55 TKG gesetzlich verankert sein. Daher werden nun auch insbesondere Messenger-Dienste, E-Maildienste und Videokonferenzdienste unter den Begriff des Telekommunikationsdienstes fallen. Somit könnte sich in Zukunft meine Datenschutzaufsicht auch auf diese Dienste erstrecken. Gemäß § 9 Bundesdatenschutzgesetz (BDSG) ist nämlich der BfDI zuständig für die Aufsicht über Unternehmen, soweit diese für die geschäftsmäßige Erbringung von Telekommunikationsdienstleistungen Daten von natürlichen oder juristischen Personen verarbeiten.

Leider ist nicht absehbar, wann die Gesetze in Kraft treten werden.

### E-Privacy-Verordnung

Zur Überarbeitung der E-Privacy-Richtlinie, die durch eine – in den Mitgliedstaaten unmittelbar geltende – 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; 28. TB Nr. 5.2). Während die Europäische Kommission bereits am 10. Januar 2017 den Entwurf der E-Privacy-Verordnung vorgelegt und das Europäische Parlament den Berichtsentwurf des federführenden LIBE-Ausschusses am 26. Oktober 2017 angenommen hat, kamen die Verhandlungen im Rat der EU seit Mitte Januar 2017 nicht entscheidend voran. Das ursprüngliche Ziel, die E-Privacy-Verordnung zeitgleich mit der DSGVO am 25. Mai 2018 in Kraft treten zu lassen, wurde deshalb schon um mehr als zweieinhalb Jahre verfehlt. Die deutsche Ratspräsidentschaft wollte im zweiten Halbjahr 2020 eine „allgemeine Ausrichtung“ des Rates erreichen, damit die zur Verabschiedung notwendigen Trilog-Verhandlungen mit dem Europäischen Parlament und der Europäischen Kommission endlich beginnen können. Jedoch zogen sich die Verhandlungen im Rat auch unter deutscher Präsidentschaft weiter hin, so dass mit einer endgültigen Verabschiedung wohl frühestens im Jahr 2021 zu rechnen sein dürfte.

Ich konnte mich gegenüber dem Bundesministerium für Wirtschaft und Energie erfolgreich dafür einsetzen,

dass Vorschriften zur Vorratsdatenspeicherung sowie zur zweckfremden Weiterverarbeitung von Kommunikationsmetadaten ohne Einwilligung der Endnutzer im Verordnungsentwurf wieder gestrichen wurden. Meine Bedenken zur allgemeinen Absenkung des Datenschutzniveaus blieben hingegen leider ungehört, ebenso wurde meiner Forderung nicht entsprochen, gemäß dem Kommissionsentwurf die Datenschutzaufsicht über

die Einhaltung der E-Privacy-Verordnung verpflichtend den Datenschutzbehörden zu überlassen. So drohen in einigen Mitgliedsstaaten eine Zersplitterung der Aufsichtslandschaft und zusätzliche, unnötig komplexe Abstimmungsmechanismen zwischen den verschiedenen Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA). Dies wird die Durchsetzung von Betroffenenrechten erschweren.

## 6 Sicherheitsbereich

### 6.1 Polizei 2020

Mit dem Projekt „Polizei 2020“ wollen die Polizeibehörden in Bund und Ländern die polizeiliche IT-Landschaft neu gestalten. Das System wird in verschiedene „Domänen“ aufgeteilt, die die gesamte Bandbreite polizeilicher Arbeit abdecken. Sie betreffen sowohl Einzelvorgänge als auch solche Informationen, die die Polizeibehörden für die Zukunft auf Vorrat speichern und für Analysen und Datenabgleiche nutzen wollen. Noch fehlen mir belastbare Unterlagen, auf deren Grundlage ich das System oder einzelne Teilsysteme beurteilen könnte.

Die Projektgruppe Polizei 2020 beim Bundesministeriums des Innern, für Bau und Heimat (BMI) stellte mir im Dezember 2019 den Stand des Projekts mündlich vor. Sie sagte mir zu, mich künftig zu beteiligen. Im Nachgang zu diesem Termin übersandte mir das BMI einen ersten „fachlichen Bebauungsplan“.

Dieses Dokument stellt jedoch keine adäquate Grundlage dar, um eine belastbare datenschutzrechtliche Prüfung vornehmen zu können. Das Projekt ist in verschiedene Teilprojekte gegliedert, die offenbar überwiegend in den Ländern entwickelt und dann später in den beim Bundeskriminalamt (BKA) geführten Informationsverbund überführt werden sollen. In verschiedenen Fällen habe ich erst von Dritten erfahren, dass wesentliche Teile in der Planung fortgeschritten sind, die direkt oder indirekt das Projekt Polizei 2020 oder einen seiner Zwischenschritte betreffen.

Deshalb habe ich nach Rücksprache mit den Landesdatenschutzbeauftragten zunächst mit einem grundsätzlichen Schreiben dem BMI gegenüber Stellung genommen. Die Datenschutzkonferenz hat auf dieser Grundlage eine entsprechende EntschlieÙung gefasst.<sup>16</sup>

Inhaltlich begrüÙe ich, dass der Bebauungsplan den Datenschutz als eines der wesentlichen Ziele benennt. Wie dieses Ziel erreicht werden soll, beschreibt der Plan allerdings nicht näher. Notwendig ist es, zunächst die rechtlichen Grenzen und Möglichkeiten zu definieren, bevor das System als Ganzes und einzelne Teilsysteme in die Entwicklung gegeben werden. Die Konzeption oder Programmierung einzelner Module sollte nicht beginnen, bevor grundlegende datenschutzrechtliche Fragen geklärt sind.

#### **Umfassende Bestandsaufnahme erforderlich**

Dies setzt zunächst eine umfassende datenschutzrechtliche Bestandsaufnahme der bereits vorhandenen Daten, Systeme und Verfahrensweisen voraus. Der „fachliche Bebauungsplan“ orientiert sich an polizeilichen Interessen. Er hat nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Ich schlage vor, dies zunächst in einer unabhängigen Evaluierung nachzuholen.

#### **Rechtliche Leitplanken**

Die bisher vorliegenden Unterlagen gehen nicht auf die rechtlichen Rahmenbedingungen ein. Erwähnt wird lediglich eine Neuerung: der Grundsatz der hypothetischen Datenneuerhebung. Dieser Grundsatz ist in der Tat wichtig. Er ist allerdings bei weitem nicht die einzige zu beachtende rechtliche und verfassungsrechtliche Vorgabe. Das Bundeskriminalamtgesetz und die Polizeigesetze der Länder geben zahlreiche rechtliche Leitplanken vor, die beim Konzept Polizei 2020 zu berücksichtigen sind. Die verantwortlichen Stellen müssen ausreichend prüfen und dokumentieren, ob und wie diese eingehalten sind – und zwar bevor sie ein System im Einzelnen planen und in Auftrag geben. Das ist bislang nicht erfüllt.

<sup>16</sup> Sie finden die EntschlieÙung vom 16. April 2020 unter: [www.bfdi.bund.de/entschlieÙungen](http://www.bfdi.bund.de/entschlieÙungen)

## **Zwecktrennung**

Im „Bebauungsplan“ ist zu lesen: „Im Kern gehen die Vorgangs- und Fallbearbeitung, Auswertung und Analyse sowie die Asservatenverwaltung in eine einheitliche polizeiliche Sachbearbeitung über.“ Aufgrund dieser Aussage ist leider zu befürchten, dass künftig nicht mehr hinreichend zwischen den verschiedenen Zwecken differenziert wird, sondern alle gespeicherten Daten unter den Oberbegriff „polizeiliche Sachbearbeitung“ gefasst werden.

Wichtig ist aber: Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden, der gleichzeitig der Gefahren- bzw. der Strafverfolgungsvorsorge dient. Das ist aber der Fall, wenn alle Daten pauschal in einer Auswerte- und Rechercheplattform genutzt werden. Wie dies in Zukunft konkret technisch abgegrenzt werden soll, ist mir nicht bekannt, für die datenschutzrechtliche Bewertung aber fundamental.

## **Auswertung und Analyse**

Mit dem neuen „Datenhaus“ in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht.

Bislang ist unklar, was genau geplant ist. Auf der einen Seite wurde in der mündlichen Darstellung des fachlichen Bebauungsplans betont, es sei nicht beabsichtigt „Künstliche Intelligenz“ einzusetzen. Auf der anderen Seite sieht der Bebauungsplan eine offenbar recht weitreichende „Domäne 2“ für Auswertung und Analyse vor.

## **Datenschutz-Basismodule**

Darüber hinaus sollte bereits jetzt stärker auf die Chancen für den Datenschutz eingegangen werden, zum Beispiel durch speziell für den Datenschutz entwickelte Basismodule.

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste“ zu implementieren. Notwendig sind z. B. ein „Basisdienst Zwecktrennung“, ein „Basisdienst Datenqualität“ und ein „Basisdienst Aufsicht und Kontrolle“, der insbesondere Protokollierungsdienste enthält.

## **Teilprojekt Proof of Concept (PoC) Datenkonsolidierung:**

Anfang 2019 war ich noch zu einem Teilprojekt von Polizei 2020 - der Erprobung des geplanten Datenhauses - in die AG Recht des Projekts eingeladen worden. Ich habe dem BMI erhebliche datenschutzrechtliche Einwände gegen das Projekt mitgeteilt. Seither wurde ich zu dieser AG nicht mehr eingeladen. Im Dezember 2019 sicherte mir das BMI mündlich eine zukünftige Beteiligung an der AG Recht wieder zu. Eine Einladung oder sonstige Beteiligung habe ich entgegen dieser Zusage bis jetzt nicht erhalten.

Das wundert mich insofern, als in der Antwort der Bundesregierung vom 6. August 2020 auf eine Kleine Anfrage noch dargelegt wurde, BMI, BKA sowie Bund-Länder Gremien stünden mit mir in einem regelmäßigen Austausch zur Planung des PoC Datenkonsolidierung. Meine Hinweise würden sorgfältig geprüft und in die weiteren Überlegungen zum PoC einbezogen werden (BT-Drucksache 19/21510).

Inzwischen teilte mir das Ministerium sowohl mit, es sei nicht mehr für das Projekt zuständig, weil dies reine Ländersache sei, gleichzeitig aber auch, das Projekt werde gegebenenfalls später in Polizei 2020 integriert. Deshalb ist für mich nicht nachvollziehbar, ob und weshalb sich das Ministerium nunmehr aus der Verantwortung zieht.

## **Teilprojekt PIAV-S**

PIAV-S steht für die strategische Nutzung der Daten im polizeilichen Informations- und Analyseverbund (PIAV). PIAV soll den Informations- und Nachrichtenaustausch zwischen den Polizeien des Bundes und der Länder erweitern. Es soll dabei helfen, Schwerpunkte zu setzen und die polizeilichen und politischen Führungs- und Entscheidungsebenen zu beraten. Dafür soll es ausgewählte Personen-, Fall- und Sachdaten aus den Vorgangs- oder Fallsystemen der Polizeibehörden bereitstellen und eine tagesaktuelle, orts- und personenbezogene Zählung von Straftaten ermöglichen. PIAV-S unterscheidet sich damit qualitativ von der Polizeilichen Kriminalstatistik (PKS), die Straftaten erst nach Abschluss der polizeilichen Ermittlung erfasst.

Das BKA spricht von einer Anonymisierung der verarbeiteten Daten. Allerdings handelt es sich nach meiner ersten Einschätzung um pseudonymisierte, also personenbezogene Daten. Zur Klärung dieses Punktes bin ich im Gespräch mit dem BKA. Handelt es sich nur um eine Pseudonymisierung, die nach wie vor die polizeiliche Nutzung der Einzeldaten ermöglicht, so sehe ich im Bundesrecht keine Rechtsgrundlage für die Datenübermittlung der Länder an das BKA sowie die Speicherung

in PIAV-S. Deshalb besteht in der Sache noch erheblicher Klärungsbedarf.

## 6.2 Einheitliches Fallbearbeitungssystem

Das einheitliche Fallbearbeitungssystem (eFBS) beim BKA konsolidiert alle dezentralen Fallbearbeitungssysteme der Bundespolizei (BPOL), des BKA und der Polizeien der Länder. In einem ersten Schritt wurden die Systeme von BPOL, BKA und der Polizeien von Brandenburg, Baden-Württemberg, Hessen und Hamburg auf eine gemeinsame Basis gestellt.

2019 wurde mit einer Interimslösung zu eFBS beim BKA als zentralem IT-Dienstleister begonnen. Mit Aufnahme des Wirkbetriebs erhielt ich erstmals schriftliche Unterlagen, die über eine allgemeine Präsentation hinausgehen; erst kurz vor Redaktionsschluss des Tätigkeitsberichts erreichten mich weitere Unterlagen.

Die mandantenfähige Interimslösung beruht auf den individuellen Fallbearbeitungssystemen von BKA, der Bundespolizei und den Teilnehmern der sogenannten CRIME-Kooperation (Polizeien von Brandenburg, Baden-Württemberg, Hessen und Hamburg). Diese verwenden Systemvarianten ein und desselben Herstellers. Die fertige Lösung, das eFBS, soll perspektivisch eine einheitliche Plattform für alle Teilnehmer werden.

Die mir zugesandten Unterlagen beschreiben jedoch nur die Anforderungen aus Benutzersicht, nicht aber das fertige System, so dass keine datenschutzrechtliche Bewertung möglich ist. Insbesondere fehlt es an einer Dokumentation, die exakt den Zweck und die Rechtsgrundlagen des Systems beschreibt. Deshalb sehe ich derzeit folgende Probleme:

Erstens ist nicht dokumentiert, auf welcher rechtlichen Grundlage und zu welchem Zweck eFBS betrieben wird. Wenn eFBS nicht nur für die Zwecke des Strafverfahrens, sondern auch zur Gefahrenvorsorge betrieben werden soll, hätte das auch weitere Auswirkungen zum Beispiel auf die Zugriffsberechtigung. Die datenschutzrechtlichen Verarbeitungszwecke sind vorliegend zu trennen (siehe dazu Nr. 9.5.3 zum VBS).

Zweitens fehlt immer noch eine Datenschutz-Folgenabschätzung. Weil das eFBS als mandantenfähiges System alle Daten in einem Datawarehouse vereinigt und die dezentrale Datenhaltung in Bund und Ländern aufhebt, potenzieren sich die Risiken beim Datenschutz und der IT-Sicherheit. Immerhin wurde mir die Erstellung der Datenschutz-Folgenabschätzung zugesagt.

Drittens wurde bislang noch kein umfassendes Löschkonzept vorgelegt, das beschreibt, wie sich eine Datenlöschung, zum Beispiel aus der Fallbearbeitung vor Ort, auf das System auf Landesebene und Bundesebene oder umgekehrt auswirkt. Stattdessen wird nur beschrieben, wie ein Benutzer eine Löschung in seinem System durchführt. Ergänzend werden neue Worte wie „anlöschen“ und „Löschvormerkung“ kreiert, statt datenschutzrechtliche Standardbegriffe wie Löschen und Sperren zu verwenden.

### Querverweise:

6.1 Polizei 2020, 9.5.3 Vorgangbearbeitungssystem

## 6.3 Das Urteil des Bundesverfassungsgerichts zur strategischen Ausland-Ausland-Fernmeldeaufklärung

Das Urteil des Bundesverfassungsgerichts (BVerfG) zur Verfassungsmäßigkeit der Regelungen im Gesetz über den Bundesnachrichtendienst (BNDG) zur Ausland-Ausland-Fernmeldeaufklärung wurde mit Spannung erwartet. Ich war im Gerichtsverfahren als Sachverständiger geladen und habe aus meiner Kontrollerfahrung Einblicke in die Datenverarbeitungspraxis des Bundesnachrichtendienstes (BND) geben können. Das Urteil, mit dem die Regelungen zur strategischen Ausland-Ausland-Fernmeldeaufklärung im BNDG für verfassungswidrig erklärt worden sind, enthält zugleich detaillierte Vorgaben für eine verfassungskonforme Ausgestaltung der strategischen Ausland-Fernmeldeaufklärung und klärt den Rahmen für die gebotene unabhängige, objektivrechtliche Kontrolle der Datenverarbeitungsprozesse im BND.

Die Menschenrechtsorganisation Reporters sans frontières und weitere Beschwerdeführer hatten Verfassungsbeschwerde gegen die Neufassung des BNDG aus dem Jahr 2016 und ihnen hierdurch drohende Überwachungsmaßnahmen im Rahmen der strategischen Ausland-Ausland-Fernmeldeüberwachung des BND erhoben. Die Beschwerdeführer machten unter anderem geltend, das Fernmeldegeheimnis des Art. 10 Abs. 1 GG und die Pressefreiheit nach Art. 5 Abs. 1 Satz 2 GG schütze auch im Ausland vor Zugriffen der deutschen Staatsgewalt auf Inhalte und Metadaten elektronischer Kommunikation. Hintergrund war die Sorge der Beschwerdeführer, dass Daten aus besonders schützenswerter Kommunikation, z.B. bei journalistischer Recherchearbeit mit Informanten, vom BND entsprechend gängiger Praxis an andere Nachrichtendienste weltweit weitergegeben werden könnten.



Neben der Frage der Bindung der deutschen Staatsgewalt an die Grundrechte beim Handeln im Ausland gegenüber Ausländern stand das Gericht vor der Aufgabe, die verfassungsrechtlichen Grenzen aufzuzeigen, innerhalb derer die strategische Ausland-Fernmeldeaufklärung als Instrument mit erheblicher Streubreite zulässig und verhältnismäßig sein kann. Dabei hat das Gericht unterstrichen, dass eine globale und unbeschränkte Auslandsaufklärung verfassungsrechtlich unzulässig ist. Als besonders eingriffsintensives Aufklärungsinstrument bedarf es laut BVerfG substantieller Beschränkungen auf hinreichend begrenzte und differenzierte Zwecke, die der Gesetzgeber festzulegen hat. In Betracht kommen danach nur Zwecke, die auf den Schutz hochrangiger Gemeinschaftsgüter gerichtet sind, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte. Wesentlich ist dabei auch die Frage, ob der BND in der Lage ist, die Grenzen einer solchen Erlaubnis technisch umzusetzen. Sich dieses Kenntnis über die technischen Fähigkeiten des BND zu verschaffen, war daher eine der Herausforderungen des Verfahrens, der sich das BVerfG durch Befragung des BND selbst und von unabhängigen

Experten und Sachverständigen stellte. Als solcher hatte auch ich die Gelegenheit, Fragen des Gerichts zu beantworten und meine Eindrücke aus der Kontrollpraxis zu vermitteln.

Ein weiterer Schwerpunkt im Verfahren betraf die Frage, welche verfassungsrechtlichen Anforderungen an die Kontrolle der Überwachungsmaßnahmen im Rahmen der strategischen Ausland-Fernmeldeaufklärung zu stellen sind. Nach meiner Erfahrung wird die Möglichkeit einer lückenlosen Kontrolle sämtlicher Datenverarbeitungsprozesse im BND dadurch erschwert, dass ein uneingeschränkter Austausch zwischen anderen Kontrollorganen, wie der G 10-Kommission, und mir nach derzeitiger Rechtslage nicht möglich ist. Zudem beruft sich der BND mir gegenüber auf die sogenannte Third-Party-Rule und verwehrt die Kontrolle von Daten, die er von ausländischen Partnerdiensten erhalten hat und die er nach Maßgabe informeller Übermittlungsabreden mit diesen Diensten nicht ohne deren Zustimmung an Dritte weitergeben darf. Erfreulicherweise hat das BVerfG allerdings unmissverständlich klargestellt, dass der Gesetzgeber die künftige Kontrolle über den



Die Kernaussagen des Urteils (Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17) können wie folgt zusammengefasst werden:

- Die Schutzbereiche des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG und der Pressefreiheit nach Art. 5 Abs. 1 Satz 2 GG erstrecken sich auch auf Maßnahmen deutscher Behörden gegen Ausländer im Ausland, also auch auf Maßnahmen der strategischen Ausland-Fernmeldeaufklärung des BND.
- Die strategische Ausland-Fernmeldeaufklärung ist eine Ausnahmebefugnis mit erheblicher Streubreite und Eingriffsintensität, die unter Beachtung der vom BVerfG aufgezeigten Kriterien zur Begrenzung der Datenerhebung und -verarbeitung verhältnismäßig und verfassungskonform ausgestaltet werden kann. Nach Darstellung des Gerichts gehören hierzu insbesondere einhergehende Regelungen zum Einsatz von Filtertechniken, zu den zulässigen Überwachungszwecken, zur Gestaltung des Überwachungsverfahrens, zu einem fokussierten Umgang mit Suchbegriffen, zu Grenzen der bevorratenden Verkehrsdatenspeicherung, zu Methoden der Datenauswertung, zum Schutz von Vertraulichkeitsbeziehungen und des Kernbereichs privater Lebensgestaltung sowie die Vorgabe von Löschpflichten, und zu den Anforderungen an eine unabhängige objektivrechtliche Kontrolle.
- Werden Daten aus der strategischen Ausland-Fernmeldeaufklärung durch den BND weiterverarbeitet, dürfen Daten, die den Kernbereich privater Lebensgestaltung betreffen, gar nicht und Daten besonders schutzbedürftiger Personen (z.B. Whistleblowern, Dissidenten) oder aus besonders schützenswerten Kommunikationsbeziehungen (z.B. zwischen Anwalt und Mandant, Journalist und Informant) nur in gesetzlich normierten Ausnahmefällen verarbeitet werden.
- Für die verfassungskonforme Durchführung sämtlicher Datenerhebungen und -verarbeitungen im Rahmen der strategischen Ausland-Fernmeldeaufklärung ist auch eine den verfassungsrechtlichen Grenzen entsprechende Ausgestaltung und Nutzung der Datenverarbeitungssysteme und der weiteren Datenverarbeitungsprozesse erforderlich.



- Die Übermittlung der Daten aus der strategischen Ausland-Fernmeldeaufklärung an andere Behörden im Inland und im Ausland ist an strenge Vorgaben geknüpft. Es müssen in der Regel konkretisierte Gefahrensituationen für konkrete, höherrangige Rechtsgüter tatsachenbasiert erkennbar sein, andernfalls ist eine Weitergabe unzulässig. Die Zwecke, die eine Übermittlung erlauben, sind zu normieren, die Durchführung einer Übermittlung ist der unabhängigen Kontrolle zugänglich zu machen.
- Bei der Übermittlung von Daten an ausländische Nachrichtendienste sind ergänzende Bedingungen zu erfüllen. Nach den Vorgaben des BVerfG ist eine Übermittlung der Daten ins Ausland nur dann erlaubt, wenn durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des menschenrechtlichen Schutzes personenbezogener Daten unterlaufen werden. Erforderlich ist die Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat. Der BND muss diese Rechtsstaatlichkeitsvergewisserung als eigenständige Voraussetzung vor einer Datenübermittlung ins Ausland durchführen.
- Eine Berufung auf die „Third-Party-Rule“ darf die Kontrolle von Datenverarbeitungen des BND mit Bezug zu ausländischen Nachrichtendiensten nicht beschränken. Der Gesetzgeber muss eine unabhängige, kontinuierliche Rechtskontrolle der strategischen Ausland-Fernmeldeaufklärung schaffen, die als gerichtsähnliche Kontrolle den rechtmäßigen Einsatz der strategischen Ausland-Fernmeldeaufklärung und als administrative Kontrolle die Praxis der Datenverarbeitungen kontrolliert.

BND organisatorisch so auszugestalten hat, dass sie nicht durch die „Third Party Rule“ behindert wird.

Das BVerfG hat angeordnet, dass die beanstandeten Vorschriften trotz ihrer Verfassungswidrigkeit vorläufig, längstens aber bis zum 31. Dezember 2021, fortgelten. Der Gesetzgeber ist daher aufgefordert, die Vorschriften mit Bezug zur strategischen Ausland-Fernmeldeaufklärung im BNDG neu zu fassen. Das Bundeskabinett hat am 16. Dezember 2020 einen entsprechenden Entwurf des Bundeskanzleramtes für eine BNDG-Novelle gebilligt (vgl. hierzu 5.4). Auch wenn ich es grundsätzlich begrüße, dass die Bundesregierung mit der Novelle den Versuch unternimmt, die Vorgaben des BVerfG für die strategische Ausland-Fernmeldeaufklärung verfassungskonform umzusetzen, habe ich in Teilbereichen des Gesetzentwurfs erhebliche Zweifel, ob ihr dies gelungen ist.

#### Querverweis:

5.4 Novellierung des Gesetzes über den Bundesnachrichtendienst

## 6.4 Das Haber-Verfahren

Das Bundesministerium des Inneren, für Bau und Heimat (BMI) weigert sich nach wie vor anzuerkennen, dass für die beim so genannten Haber-Verfahren erfolgende Datenverarbeitung eine gesonderte Rechtsgrundlage benötigt wird.

Wie bereits im Tätigkeitsbericht 2019 erörtert (vgl. 28. TB Nr. 6.5), gibt es für die Einbeziehung des Bundesamts für Verfassungsschutz (BfV) bei der Vergabe staatlicher Leistungen zur Verhinderung der missbräuchlichen Inanspruchnahme durch verfassungsfeindliche Organisationen (sog. Haber-Verfahren) keine gesetzliche Grundlage. Das Fehlen einer gesetzlichen Ermächtigung für die vom BfV in diesem Zusammenhang vorgenommenen Datenverarbeitungen habe ich daran anschließend im gegenständlichen Berichtszeitraum gemäß § 16 Abs. 2 Bundesdatenschutzgesetz, § 27 Nr. 1 Bundesverfassungsschutzgesetz formal beanstandet.

Die Weigerung des BMI, Schritte zur Beseitigung des gesetzgeberischen Defizits zu unternehmen, ist nicht hinnehmbar. Ein Ministerium als Organ der Exekutive kann nicht eigenmächtig und in Eigenregie neue Datenverarbeitungsbefugnisse für eine seiner Ressortbehörden im Wege von Erlassvorschriften zu Lasten von Grundrechtsträgern schaffen, so wie es das BMI vorliegend mit dem Haber-Diwell-Erlass getan hat. Dies ist ausschließlich die Aufgabe des hierzu legitimierten Gesetzgebers.

Auch die bundesverfassungsgerichtliche Rechtsprechung aus dem vergangenen Jahr lässt daran keine Zweifel und zwingt den Gesetzgeber gerade im nachrichtendienstlichen Bereich zu umfangreichen Reformen. In seinem Urteil zur strategischen Ausland-Ausland-Fernmeldeaufklärung (vgl. auch 6.3) hat das Bundesverfas-

sungsgericht klargestellt, dass die Geheimhaltungsbedürftigkeit nachrichtendienstlicher Tätigkeit kein Weniger bei Anzahl, Umfang und Qualität gesetzlicher Ermächtigungen rechtfertigt.

#### Querverweis:

6.3 Das Urteil des Bundesverfassungsgerichts zur strategischen Ausland-Ausland-Fernmeldeaufklärung

## 6.5 Sicherheitsüberprüfung von Bewerberinnen und Bewerbern der Nachrichtendienste

Bewerberinnen und Bewerber von Nachrichtendiensten werden nicht über das Ergebnis ihrer Sicherheitsüberprüfung informiert und haben auch vorab kein Anhörungsrecht, wenn sich bei den Sicherheitsermittlungen ein potentiell Sicherheitsrisiko ergibt. Über diese Rechtslage werden sie aber künftig im Vorfeld informiert.

Im Bereich des Sicherheitsüberprüfungsrechts erreichen mich vermehrt Eingaben von Bewerberinnen und Bewerbern der Nachrichtendienste des Bundes. Insbesondere tragen die Betroffenen vor, dass ihnen im Rahmen einer Einstellungsabsage nicht mitgeteilt wird, ob diese im Zusammenhang mit der durchgeführten Sicherheitsüberprüfung steht und bitten mich diesbezüglich um Hilfestellung. Im Rahmen meiner datenschutzrechtlichen Prüfkompetenzen im Sicherheitsüberprüfungsgesetz (SÜG) gehe ich diesen Sachverhalten nach.

Auch wenn es sich dabei nicht um primär datenschutzrechtliche Vorschriften handelt, möchte ich klarstellen, dass nach § 6 Abs. 1 Satz 4 SÜG das Anhörungsrecht für Bewerberinnen und Bewerber der Nachrichtendienste des Bundes im Rahmen der Durchführung der Sicherheitsüberprüfung entfällt und diese gemäß § 14 Abs. 4 Satz 2 SÜG auch nicht über das Ergebnis der Sicherheitsüberprüfung informiert werden müssen. Diese Sondervorschriften für Nachrichtendienste sieht das SÜG ausdrücklich vor.

Hintergrund hierfür ist, dass Ausforschungspraktiken ausländischer Nachrichtendienste hinsichtlich des Erkenntnisstandes und der Einstellungspraxis bei den deutschen Nachrichtendiensten unterbunden werden sollen. Es kommt immer wieder vor, dass ausländische Nachrichtendienste etwaige Bewerberinnen und Bewerber in Einstellungsverfahren einschleusen.

Die Eingaben haben mich dennoch veranlasst, bei den jeweiligen Nachrichtendiensten in Erfahrung zu bringen, ob Bewerberinnen und Bewerber im Vorfeld der Durchführung der Sicherheitsüberprüfung auf die

geltenden Einschränkungen schriftlich oder mündlich hingewiesen werden. Die Rückmeldungen haben aufgezeigt, dass dies nicht immer der Fall ist.

Um mehr Transparenz für Bewerberinnen und Bewerber zu schaffen, habe ich den Nachrichtendiensten empfohlen, im Vorfeld der Durchführung der Sicherheitsüberprüfung schriftlich über die Ausnahmeregelungen im SÜG zu informieren. Erfreulicherweise haben alle Nachrichtendienste meine Empfehlung aufgenommen und umgesetzt

## 6.6 Passenger Name Records - Wie viel Datensammlung ist zur Terrorismusbekämpfung gerechtfertigt?

Während der EuGH in mehreren Verfahren die Vereinbarkeit der Verwendung von Fluggastdaten zur Bekämpfung von Terrorismus und anderen schweren Straftaten mit den europäischen Grundrechten überprüft, hat die Kommission im Sommer eine positive Bilanz gezogen. Der Umfang der zugelassenen Datenverarbeitung lässt jedoch weiter an der Verhältnismäßigkeit zweifeln.

Seit vielen Jahren kritisiere ich in meinen Tätigkeitsberichten den Umfang der Verarbeitung von Fluggastdaten durch Polizeibehörden (vgl. 22. TB Nr. 13.5.4; 26. TB Nr. 2.3.2; 27. TB Nr. 1.3; 28. TB Nr. 6.4). Die Richtlinie (EU) 2016/681 vom 27. April 2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PNR-RL) verpflichtet die Mitgliedstaaten, anlasslos Fluggastdaten von Luftfahrtunternehmen zu erheben, abzugleichen und über fünf Jahre zu speichern, um auch eine rückwirkende Auswertung zu ermöglichen. Dies gilt für alle Fluggäste, auch wenn diese für eine mehrjährige Speicherung in einer polizeilichen Datenbank keinerlei Anlass bieten.

Die EU-Kommission hat in diesem Jahr eine Evaluierung zur Umsetzung der PNR-RL durchgeführt (vgl. Evaluierungsbericht vom 24. Juli 2020, COM(2020) 305 final). Aus ihrer Sicht fällt das Ergebnis insgesamt positiv aus. Die Richtlinie erfüllt ihren Zweck und derzeit sollen keine Änderungen vorgenommen werden. Zunächst soll die Entscheidung des EuGH zur Vereinbarkeit der PNR-RL mit den europäischen Grundrechten abgewartet werden. Dort sind Vorabentscheidungsersuchen von Gerichten aus verschiedenen Mitgliedstaaten anhängig. Auch in Deutschland laufen Klagen gegen Luftfahrtunternehmen und die Fluggastdatenzentralstelle beim BKA, die sich insbesondere gegen die Langzeitspeicherung der Passagierdaten richten.

Nach den statistischen Daten, die die Kommission bei den Mitgliedstaaten erhoben hat, erzielt der automatisierte Sofortabgleich der übermittelten Passagierdaten mit Fahndungsdatenbanken oder Mustern technische Treffer bei 0,59 % der Fluggäste. Nach einer manuellen Überprüfung verbleiben 0,11 % bestätigte Treffer, die an die zuständigen Behörden zwecks näherer Überprüfung übermittelt werden. Nach Auffassung der Kommission zeigt der kleine Prozentsatz, dass das System gezielte Treffer generiert und unbescholtene Reisende hier nichts zu befürchten haben. Übertragen in absolute Zahlen, lässt sich diese Schlussfolgerung jedoch anzweifeln.

So überquerten im Jahr 2018 nach Angaben von Eurostat rund 924 Millionen Fluggäste die Außen- oder Binnengrenzen der EU. Bei einer technischen Trefferquote von 0,59 % wären mehr als 5,4 Millionen Menschen einer manuellen Nachkontrolle zu unterziehen. Bei einer Quote von 0,11 % an bestätigten Treffern wären mehr als eine Million Menschen an die zuständigen Behörden zum Zwecke der Einleitung von Folgemaßnahmen zu melden. Auch wenn die Zahlen derzeit in der Praxis wohl niedriger liegen, da noch nicht in allen Staaten der Vollausbau der Fluggastdatenbanken erreicht ist, wären diese Millionen von Kontrollen in der Zukunft rechtlich abgedeckt.

Demgegenüber präsentiert die Kommission nur eine kleine Zahl von Fallstudien, die die Wirksamkeit und

Effizienz der Nutzung von PNR-Daten belegen soll (vgl. Begleitdokument zum Evaluierungsbericht vom 24. Juli 2020, SWD(2020) 128 final). Selbst wenn diese Fälle nur eine Auswahl darstellen, drängt sich die Frage auf, ob die gewählte Form der Massendatenverarbeitung und Datenvorratshaltung noch verhältnismäßig ist, um die unbestritten legitimen Ziele der Bekämpfung terroristischer und sonstiger schwerer Straftaten zu erreichen. Dies gilt umso mehr im Licht der jüngsten Rechtsprechung des EuGH im Verfahren „La Quadrature de Net“, wonach Gesetze, die eine Datenspeicherung erlauben, immer objektive Kriterien aufstellen müssen, die einen Zusammenhang zwischen den gespeicherten Daten und dem Zweck der Speicherung herstellen.

### Datenschutzbehörden fordern Nachbesserung

Vor diesem Hintergrund habe ich zusammen mit den anderen europäischen Datenschutzaufsichtsbehörden im EDSA die EU-Kommission erneut aufgefordert, Nachbesserungen an der Rechtslage vorzunehmen.

An der Diskrepanz zwischen technischen Treffern und manuell bestätigten Treffern zeigt sich außerdem ein grundsätzliches Problem der Datenqualität. Die von den Luftfahrtunternehmen für ihre Zwecke erhobenen Daten sind oftmals für einen polizeilichen Datenabgleich nicht geeignet, weil wichtige Daten wie Geburtsdatum und Geburtsort fehlen und der Fahndungsabgleich so ins Leere läuft.





In diesem Zusammenhang wird immer wieder auf den positiven Effekt des Zusammenwirkens mit den sogenannten API-Daten verwiesen. Hierbei handelt es sich um eine weitere Form der Übermittlung von Passagierdaten. Rechtsgrundlage ist die Richtlinie 2004/82/EG vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (API-RL). Die Mitgliedstaaten können zu vorab bestimmten Flügen aus Drittstaaten die Übermittlung bestimmter Passagierdaten an ihre Grenzkontrollbehörden verlangen. Im Unterschied zu den PNR-Daten müssen die Luftfahrtunternehmen die API-Daten für diesen Zweck gesondert aus offiziellen Ausweisdokumenten erheben. Deshalb sind diese Daten qualitativ hochwertiger und der Datenkranz ist besser auf polizeiliche Zwecke abgestimmt. Werden sie erhoben, sind sie nach der PNR-RL auch an die Fluggastdatenzentralstellen zu übermitteln und führen dort indirekt zu einer besseren Datenqualität. Dieser positive Effekt sollte aber nicht darüber hinwegtäuschen, dass das Zusammenspiel von API-RL und PNR-RL für die betroffenen Personen eine doppelte Überwachung darstellt und zusätzliche Fragen der Verhältnismäßigkeit aufwirft. Dieser Aspekt sollte in der anstehenden Evaluierung der API-RL dringend berücksichtigt werden.

## 6.7 JI-Richtlinie nach wie vor nicht vollständig umgesetzt

**Die Umsetzung europarechtlicher Vorgaben im Bundespolizeigesetz und im Zollfahndungsdienstgesetz scheitert nach wie vor am politischen Ringen um zusätzliche Eingriffsbefugnisse. Erste Anwendungshilfen für die Praxis habe ich bereits entwickelt.**

Für die Verarbeitung personenbezogener Daten bei Polizei und Justiz müssen seit dem 6. Mai 2018 einheitliche Mindeststandards in allen Mitgliedstaaten der EU umgesetzt sein. Hierüber hatte ich bereits in meinem vorletzten Tätigkeitsbericht informiert (vgl. 27. TB Nr. 1.2). Sind bestimmte Vorgaben in den polizeilichen Fachgesetzen noch nicht umgesetzt, so gelten die Regelungen im ersten und dritten Teil des Bundesdatenschutzgesetzes (BDSG) ergänzend. Einige Vorschriften des BDSG müssen jedoch durch das Fachrecht zwingend spezifisch und normenklar ergänzt werden.

Dies gilt beispielsweise für § 48 BDSG, wonach die Verarbeitung besonderer Kategorien personenbezogener Daten nur zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist und zusätzlich geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen sind. Dies betrifft z.B. genetische oder biometrische Daten.

Die Gesetzesformulierung wirft die Frage auf, ob diese Vorschrift neben dem Fachrecht als eigenständige Rechtsgrundlage gelten soll. Das kommt aber schon deshalb nicht in Betracht, weil sie nicht hinreichend bestimmt und normenklar formuliert ist. Der Gesetzgeber sollte klarstellen, dass § 48 BDSG nur zusätzliche Anforderungen aufstellen will, die neben die – noch detailliert zu regelnden – spezifischen Anforderungen des Fachrechts treten.

In der Praxis wird es auch dort schwierig, wo im Fachrecht noch alte Regelungen bestehen, die nicht oder nicht vollständig zu den Anforderungen der Richtlinie passen. Ein Beispiel hierfür sind die Vorgaben der JI-Richtlinie bzw. des BDSG für Datenübermittlungen in Drittstaaten. Hiernach müssen sich die verantwortlichen Stellen vergewissern, dass im Empfängerstaat ein angemessenes Datenschutzniveau vorhanden ist.

Nach dem (bislang nicht novellierten) Bundespolizeigesetz (BPolG) ist das Datenschutzniveau im Empfängerstaat erst im Rahmen einer Interessenabwägung zwischen dem öffentlichen Interesse an der Übermittlung und dem schutzwürdigen Interesse der betroffenen Person zu berücksichtigen. Dies mag auf den ersten Blick für die Praxis unerheblich erscheinen. Die Vorgaben der Richtlinie räumen der Existenz eines angemessenen Datenschutzniveaus jedoch grundsätzlich ein höheres Gewicht ein, wenn eine Abweichung nur in Ausnahmefällen zulässig sein soll. Dies kann im Einzelfall durchaus zu einem anderen Ergebnis führen.

Vor diesem Hintergrund sehe ich daher die Tatsache kritisch, dass die Umsetzung der Richtlinie sowohl im BPolG als auch im Zollfahndungsdienstgesetz (ZFDG) immer noch nicht vollzogen ist.

Zur Anpassung des BPolG gab es Anfang 2020 bereits einen Referentenentwurf, über den jedoch wegen unterschiedlicher Auffassungen der Koalitionspartner über die Notwendigkeit neuer Eingriffsbefugnisse noch keine Einigung erzielt werden konnte. Dieser Entwurf wurde dann nicht weiter verfolgt. Zum Redaktionsschluss war bekannt, dass die Fraktionen der Regierungskoalition an einem Entwurf für das BPolG arbeiten, der dann von den Fraktionen ins Parlament eingebracht werden soll.

Einen Gesetzentwurf zur Novellierung des ZFDG hatte der Deutsche Bundestag sogar bereits beschlossen (vgl. 28. TB Nr. 5.3.1), allerdings kam es nicht mehr zur Zeichnung und Verkündung des Gesetzes. Hintergrund ist offenbar die Entscheidung des Bundesverfassungsgerichts zur Ausgestaltung der sogenannten Bestandsdatenauskunft (vgl. Nr. 7.4). Danach müssen die polizeilichen Fachgesetze klare Regelungen treffen, welche Behörde bei welchen Anlässen welche Daten abfragen darf und wie die Daten dann genutzt werden dürfen. Das



bereits vor der Entscheidung des BVerfG vom Deutschen Bundestag beschlossene neue ZFdG enthielt jedoch eine Regelung, die diesen Anforderungen, die ich bereits vorher im Gesetzgebungsverfahren vertreten habe, nicht genügt. (vgl. 27. TB Nr. 9.1.4).



Während der Gesetzgeber mit der Umsetzung der JI-Richtlinie weiter in der Pflicht bleibt, habe ich erste Erfahrungen mit der praktischen Anwendung der neuen Regelungen des BDSG ausgewertet, um Anwendungshilfen zu einzelnen Vorschriften des BDSG zu entwickeln. Hiermit möchte ich Justiz-, Polizei- und Ordnungswidrigkeiten-Behörden bei ihrer praktischen Arbeit mit den Datenschutzvorgaben unterstützen.

Zu folgenden Vorschriften finden Sie Materialien auf meiner Website:

- § 53 BDSG: Datengeheimnis (Muster)
- § 67 BDSG: Datenschutzfolgenabschätzung (Muster mit Hinweisen, Methodenvorschlag)
- § 70 BDSG: Verzeichnis von Verarbeitungstätigkeiten (Muster mit Hinweisen)
- (demnächst:) § 76 BDSG: Protokollierung (Hinweise).

#### Querverweis:

7.4 Urteil Bestandsdatenauskunft

## 6.8 Neugestaltung des Informationsverbundes FIU 2.0

Die Zentralstelle für Finanztransaktionsuntersuchungen, auch Financial Intelligence Unit (FIU) genannt, plant die Neugestaltung ihrer IT-Landschaft. Zur Bewältigung der stetig wachsenden Anzahl eingehender Verdachtsmeldungen sollen dabei künftig auch Methoden bzw. Algorithmen aus dem Bereich der Künstlichen Intelligenz (KI) eingesetzt werden. Aufgrund der erheblichen damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen habe ich meine Beteiligung eingefordert. So konnte ich frühzeitig beratend tätig werden und auf datenschutzrechtliche Mängel hinweisen.

Die FIU ist eine eigenständige Organisationseinheit unter dem Dach der Generalzolldirektion beim Zollkriminalamt. Sie ist zuständig für die Entgegennahme,

Sammlung und Auswertung von Meldungen über verdächtige Finanztransaktionen, die im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen können. Stellt sie bei ihrer Analyse fest, dass ein Vermögensgegenstand mit Geldwäsche, Terrorismusfinanzierung oder mit einer sonstigen Straftat in Zusammenhang steht, so übermittelt sie ihr Analyseergebnis sowie alle sachdienlichen Informationen an die zuständigen Strafverfolgungsbehörden.

Bis Ende 2023 plant die FIU die Neugestaltung ihrer IT-Landschaft in Form des sogenannten Informationsverbundes FIU 2.0. Für die datenschutzrechtliche Bewertung und Begleitung des Projektes habe ich meine Beteiligung eingefordert und mir das seitens der FIU erstellte Lastenheft vorlegen lassen. Auf diese Weise konnte ich mir bereits in einem sehr frühen Entwicklungsstadium des IT-Projektes einen ersten Eindruck verschaffen und die technischen und fachlichen Anforderungen an das System mit Blick auf die Einhaltung datenschutzrechtlicher Vorschriften überprüfen.

Leider musste ich zahlreiche datenschutzrechtliche Mängel feststellen, auf die ich die FIU hingewiesen habe.

#### Fehlende Rechtsgrundlagen

Für einige der geplanten Datenverarbeitungen der FIU, wie beispielsweise der systematischen Erhebung und Auswertung personenbezogener Daten aus öffentlichen Quellen, dürfte es bereits an einer entsprechenden Rechtsgrundlagen fehlen. Teilweise konnte ich auch darauf aufmerksam machen, dass die Planungen nicht mehr vom gesetzlichen Auftrag der FIU umfasst sein dürften.

Löschkonzepte sowie technische Verfahrenssicherungen zur Einhaltung von ereignisunabhängigen Aussonderungsprüffristen waren ursprünglich gar nicht vorgesehen.

#### Einsatz von Methoden der Künstlichen Intelligenz (KI)

Aus datenschutzrechtlicher Sicht besonders hervorzuheben ist der geplante Einsatz von KI-Methoden zur Bearbeitung der stetig ansteigenden Zahl eingehender Geldwäscheverdachtsmeldungen.

Um aus der großen Anzahl vorliegender Meldungen die werthaltigen Fälle zu filtern, sollen zukünftig automatisierte Anwendungen und selbstlernende Systeme zum Einsatz kommen. Sie sollen zunächst die Priorisierung von Bearbeitungsvorschlägen und Netzwerkdarstellungen vornehmen.

Perspektivisch ist geplant, die manuelle Analyse sämtlicher gemeldeter Sachverhalte durch eine automatisierte Bewertung zu ersetzen. Die Systeme sollen

vorab entscheiden, welche Meldungen einer Einzelfallbetrachtung durch die menschlichen Analysten der FIU bedürfen.

Die übrigen Meldungen sollen automatisiert dem sog. „Informationspool“ zugeführt werden. Das bedeutet, dass die Meldungen in die zentrale Datenbank der FIU überführt und dort kontinuierlich automatisiert neu bewertet werden. Nur wenn sich, z.B. aufgrund einer neuen Datenlage, zu einem späteren Zeitpunkt eine abweichende Bewertung ergibt, soll eine manuelle Bearbeitung erfolgen. Gegen diese Vorgehensweise habe ich bereits Bedenken geäußert.

### **Datenschutzrechtliche Anforderungen**

§ 54 Abs. 1 BDSG statuiert für eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist, das Erfordernis einer spezifischen Rechtsgrundlage. Eine solche hinreichend bestimmte und normenklare Rechtsgrundlage ist bisher im für die FIU maßgeblichen Geldwäschegesetz nicht ersichtlich.

Der Einsatz automatisierter Systeme kann neben dem intensiven Dateneingriff hohe Risiken für die weiteren Rechte und Freiheiten natürlicher Personen zur Folge haben. Dies gilt insbesondere dann, wenn die Anwendungen automatisierte Entscheidungen treffen oder zumindest vorbereiten sollen. Denn komplexe Systeme sind selbst für Fachleute kaum nachvollziehbar.

Bei der FIU kommt erschwerend hinzu, dass es sich um eine besonders eingriffsintensive Datenverarbeitung handelt. Zum einen ist die FIU keine Strafverfolgungsbehörde. Ihre Tätigkeit hat einen reinen Vorfeldcharakter. Daher liegt der Verdachtsgrad einer Geldwäscheverdachtsmeldung noch unterhalb des strafprozessualen Anfangsverdachts. Zum anderen führt sie die beschriebenen Grundrechtseingriffe heimlich durch, sodass die Betroffenen in der Regel keinerlei Kenntnis von der Verarbeitung ihrer personenbezogenen Daten haben.

Aufgrund dieser besonderen Eingriffsintensität in Grundrechte sollten KI-Anwendungen daher allenfalls restriktiv genutzt werden. Zumindest aber müssen KI-Anwendungen hier einer besonderen Vorabprüfung und laufenden Kontrolle gemäß der Empfehlungen der Datenethik-Kommission unterliegen.

## **6.9 Datenschutzverstoß im Bereich der Zollfahndung**

**Bei der Zollfahndung konnten durch die Meldung eines Datenschutzverstoßes Verbesserungen im Umgang mit sichergestellten Datenträgern erreicht werden.**

Die Zollfahndung meldete mir einen Verlust von Asservaten als Datenschutzverletzung. Es handelte sich um Datenträger, die in einem Strafverfahren sichergestellt wurden. Meine Einbindung war geboten, da derartige Datenspeicher oft eine Vielzahl sensibler personenbezogener Daten enthalten können. So können sich z.B. im Speicher eines Smartphones schnell Fotos, Chatverläufe, Passwörter und viele weitere Informationen ansammeln. Im Rahmen meiner Prüfung habe ich festgestellt, dass die betroffenen Asservate nicht ausreichend gegen unbefugte Kenntnisnahme ihres Inhaltes gesichert waren.

Durch die Aufarbeitung des Sachverhaltes konnte eine erhebliche Verbesserung beim künftigen Umgang mit sichergestellten Datenträgern erreicht werden. Insbesondere wurden die organisatorischen Vorgaben der Zollfahndung zum Umgang mit dieser Art von Asservaten überarbeitet. Die neuen Maßnahmen umfassen insbesondere einen gesicherten Transportweg, eine Verschlüsselung nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik und die Versendung von Datenträgern und Zugangsdaten auf getrennten Wegen. Sie sollen künftig in regelmäßigen Abständen evaluiert und den technischen Entwicklungen angepasst werden.

## **6.10 Beschäftigtendatenschutz in der Zollverwaltung**

**Im Rahmen der Bearbeitung zahlreicher Eingaben im Bereich des Beschäftigtendatenschutzes ließ die Zollverwaltung Kooperationsbereitschaft und Problembewusstsein vielfach vermissen. Meine Aufgabenerfüllung wurde mir hierdurch im Berichtszeitraum erheblich erschwert.**

Auch im Jahr 2020 erreichte mich eine Vielzahl von Eingaben von Beschäftigten der Zollverwaltung. Im Rahmen der Bearbeitung stießen meine Mitarbeiterinnen und Mitarbeiter wiederholt auf Widerstände seitens der Zollverwaltung. Bereits in der Vergangenheit hatte die Generalzolldirektion schriftlich darauf hingewiesen, dass Rückfragen zu Stellungnahmen durch meine Mitarbeiterinnen und Mitarbeiter unerwünscht seien. Dokumente zur Sachverhaltsermittlung wurden mir entgegen Art. 58 Absatz 1 lit. a) DSGVO nicht wie gefordert zur Verfügung gestellt. In einem noch laufenden verwal-

tungsgerichtlichen Verfahren zweifelt die Zollverwaltung meinen Anspruch auf Bereitstellung von Informationen zur Erfüllung meiner Aufgaben gem. Art. 58 Absatz 1 lit. a) DSGVO i.V.m. § 16 Absatz 4 BDSG an.

### **Einleitung eines Disziplinarverfahrens als Reaktion auf meine Einbindung**

In einem Fall wurde gegen einen Mitarbeiter aus der Zollverwaltung ein Disziplinarverfahren eingeleitet, weil er sich an mich gewandt hat. Der Mitarbeiter hatte mich mit eindeutigen Hinweisen über einen unzulässigen Austausch dienstlicher Informationen über den Messengerdienst WhatsApp informiert. Die daraufhin von der Zollverwaltung von mir verlangte Herausgabe des Vorgangs zwecks Verwendung für disziplinarische Ermittlungen habe ich unter Hinweis auf mein Zeugnisverweigerungsrecht gemäß § 13 Absatz 3 BDSG verweigert. Dem Mitarbeiter wurde im Disziplinarverfahren vorgeworfen, den Dienstweg umgangen und einen Ansehensverlust der Zollverwaltung mir gegenüber herbeigeführt zu haben. Der mit der dienstlichen Nutzung des Messengerdienstes WhatsApp möglicherweise begangene Datenschutzverstoß wurde dagegen durch die Zollverwaltung bestritten und bisher nicht in gleicher Weise verfolgt. Die Reaktion der zuständigen Stelle innerhalb der Zollverwaltung lässt aus meiner Sicht auf eine ungenügende Sensibilität für den Datenschutz und das Grundrecht auf informationelle Selbstbestimmung schließen. Die Art und Weise des Umgangs mit Hinweisgebern innerhalb der Zollverwaltung ist nicht mit meinen Vorstellungen einer transparenten, problembewussten, datenschutzsensiblen und fairen Bundesverwaltung vereinbar. Insbesondere darf der Hinweis auf einen potentiellen Datenschutzverstoß auch dann nicht zu Nachteilen für die meldende Person führen, wenn diese nicht unmittelbar vom Verstoß betroffen ist. Andernfalls besteht die Gefahr, dass die im Interesse der Allgemeinheit liegende Bereitschaft, auf potentiell rechtswidrige Datenverarbeitungen hinzuweisen, aus Angst vor möglichen Repressionen insgesamt abnimmt.

### **Verlust von Disziplinarvorgängen**

Ebenfalls im Berichtszeitraum meldete mir die Zollverwaltung den Verlust von zwei Disziplinarvorgängen als Datenschutzverletzung. Im Zuge meiner Ermittlungen teilte ich meine Absicht mit, die Zollverwaltung anzuweisen, Personalvorgänge künftig nur noch von Hand zu Hand oder über zugangsbeschränkte Postverteilräume beziehungsweise abschließbare Postfächer zu verteilen. Die Generalzolldirektion reagierte hierauf mit der Behauptung, dass ein entsprechender Anweisungsbescheid wegen Unmöglichkeit der Umsetzung nichtig sei. Die Generalzolldirektion wurde zwischenzeitlich vom Bundesministerium der Finanzen zur Weitergabe

von Disziplinarvorgängen von Hand zu Hand, über den Botendienst oder über zugangsbeschränkte Posträume und/oder Postfächer angewiesen. Diese Weisung begrüße ich ausdrücklich und danke dem Bundesministerium der Finanzen für die Unterstützung meiner Arbeit und der Stärkung des Datenschutzes innerhalb der Generalzolldirektion.

### **Unzulässiger Betrieb einer Zutrittskontroll- und Alarmanlage**

In einem Zollfahndungsamt wurde seit Jahren eine elektronische Zutrittskontroll- und Alarmanlage betrieben, ohne dass die hierfür erforderlichen datenschutzrechtlichen Voraussetzungen erfüllt waren. Erst im Laufe des Jahres 2019 wurde das vorgesehene Rollen- und Löschkonzept implementiert und mit der für den Betrieb und die Wartung der Anlage beauftragten Firma eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Auch die Löschung der erfassten Zutrittsprotokolldaten erfolgte erstmalig in 2019 und somit mehrere Jahre zu spät. In der Folge habe ich von meinen Abhilfebefugnissen nach der DSGVO Gebrauch gemacht und das Zollfahndungsamt verwarnet sowie zugleich angewiesen, die Informationspflicht bei der Erhebung personenbezogener Daten nach Art. 5 Abs. 1 lit. a und Art. 13 DSGVO endlich zu erfüllen. Meiner Anweisung ist das Zollfahndungsamt nachgekommen.

### **Beratungs- und Kontrollbesuch in der Generalzolldirektion**

Im Rahmen eines von meinen Mitarbeiterinnen und Mitarbeitern bei der Generalzolldirektion durchgeführten Beratungs- und Kontrollbesuchs habe ich das datenschutzkonforme Führen von Personalakten kontrolliert und verschiedene datenschutzrechtliche Verstöße festgestellt. Von der Ergreifung von Maßnahmen habe ich abgesehen. Zum einen wurde der Generalzolldirektion die Zuständigkeit für einen Teil der Personalakten durch die Neuorganisation und Gründung als Bundesoberbehörde im Jahr 2016 erstmals übertragen. Zum anderen konnte ich keine unmittelbar nachteilige Auswirkung der Verstöße auf Rechte von Beschäftigten erkennen. Die mir zugesagte Aufarbeitung der Personalakten werde ich zu gegebener Zeit kontrollieren.

Die Zusammenarbeit war seitens der Zollverwaltung vielfach durch mangelnde Sensibilität für die Belange des Datenschutzes, beharrliches Bestreiten von Vorwürfen, Abtun von Beweisen sowie die Nichtahndung von Verstößen geprägt. Für die Zukunft hoffe ich auf eine von gegenseitigem Respekt geprägte und konstruktive Zusammenarbeit mit der Zollverwaltung.

## 6.11 Datenschutzverstöße bei der Bundespolizei

Durch Anfragen und Beschwerden wurde ich auf datenschutzrechtliche Missstände bei der Bundespolizei (BPol) aufmerksam und konnte Verbesserungen erreichen. Betroffen hiervon war auch die Veröffentlichung von Bildern auf Twitter.

Im Rahmen von Bürgereingaben wurde ich auf datenschutzrechtliche Missstände bei der BPol aufmerksam gemacht. Ein Fall betraf etwa die Grenzabfertigung von Reisebussen. Dort wurden häufig die Grenzübertrittspapiere nicht von den Bundespolizeibediensteten an die Reisenden zurückgegeben, sondern von den Busfahrern. Auf meine Nachfragen hin wurde diese Praxis von der BPol geprüft und eine Änderung der Abläufe zugesagt. Künftig soll die Rückgabe der Papiere nur noch von den hierzu befugten Polizeibeamten und Polizeibeamtinnen erfolgen.

Auch ein Fall, bei dem die Rechtmäßigkeit der Videoüberwachung eines Bahnhofes im Zusammenhang mit der An- und Abreise zu und von einer Demonstration geprüft wurde, sollte künftig zu Verbesserungen beim Datenschutz führen. So werden nun in ähnlich gelagerten Fällen die Videodaten nicht mehr nach maximal 30 Tagen, sondern schnellstmöglich gelöscht. Zudem habe ich darauf aufmerksam gemacht, dass die Prüfung, ob überhaupt eine Videoüberwachung zulässig ist, insbesondere bei Demonstrationen, die regelmäßig im Spannungsfeld von Gefahrenabwehr einerseits und dem Grundrecht auf Versammlungsfreiheit andererseits stehen, umfassender zu erfolgen hat. Im Dezember 2020 wurde zu dieser Videoüberwachung auch Klage vor dem Verwaltungsgericht Berlin erhoben.

Auch bei der Nutzung von Twitter gab es Verbesserungspotential. In drei Fällen verwendete die BPol ein Symbolfoto, auf dem der Reisepass einer echten Person erkennbar war. Dabei war es möglich, die im Pass angegebenen Daten wie etwa Name, persönliche Merkmale und das Passfoto zu erkennen. Hier konnte ich eine rasche Löschung erreichen.

## 6.12 Geschützter Grenzfehndungsbestand

Der „Geschützte Grenzfehndungsbestand“ (GGFB) der Bundespolizei wird weiter ohne ausreichende Rechtsgrundlage geführt.

Die von mir regelmäßig durchgeführte Kontrolle des GGFB fand auch im Jahre 2019 statt. Sie wurde nach abschließender Stellungnahme des BMI im Jahre 2020

beendet. In Bezug auf den Umfang und die Art der Nutzung der Datei durch die Bundespolizei führte die Kontrolle nicht zu einer förmlichen Beanstandung. Insbesondere die Unterscheidung von Fehndungsausschreibungen im GGFB und solchen im Schengener Informationssystem war gut nachvollziehbar. Nur bei einzelnen Ausschreibungen stellte ich Fehler fest. Hier konnte ich bei der Bundespolizei (BPol) eine umgehende Korrektur erreichen. Nachbesserungsbedarf habe ich in Bezug auf die Ausgestaltung der Protokollierung geltend gemacht.

Erneut musste ich beanstanden, dass für den GGFB noch immer keine ausreichende Rechtsgrundlage existiert. Die BPol führt die Datei des GGFB aufgrund der §§ 30 und 31 BPolG. Hiernach ist das BMI gesetzlich verpflichtet, die bloßen Rahmenbedingungen, die das BPolG für den GGFB festlegt, durch eine Rechtsverordnung näher auszugestalten. Es kann und darf diese Aufgabe nicht der ausführenden Behörde, also der BPol, überlassen. Die Führung des GGFB ohne diese Rechtsverordnung ist rechtswidrig.

Bereits im April 2015 hatte ich das BMI auf diesen Umstand hingewiesen. Nachdem das BMI im Jahre 2018 noch immer keine Rechtsverordnung erlassen hatte, beanstandete ich im selben Jahr die fehlende Rechtsgrundlage (vgl. 27. TB Nr. 9.3.9). Auch zum Zeitpunkt der Kontrolle im Jahre 2019 und bis Redaktionsschluss im November 2020 hat das BMI die konstituierende Rechtsverordnung nicht erlassen. Während das BMI zunächst Bereitschaft äußerte, die Rechtsverordnung zu erlassen, stellt es seit 2018 auf die anstehende Novelle des BPolG ab. Diese Novelle ist aber bisher nicht einmal in den Deutschen Bundestag eingebracht worden.

Im GGFB sind regelmäßig mehrere Tausend Personen ausgeschrieben. Für diese können die Ausschreibungen erhebliche Folgen haben wie etwa Ingewahrsamnahme, Ausreiseuntersagung oder grenzpolizeiliche Beobachtung. Auch der Verfassungsschutz kann Ausschreibungen veranlassen.

Das BMI hätte die Möglichkeit, diesen rechtswidrigen Zustand zu beenden. Politische Unwägbarkeiten sollten nicht zu einer weiteren Verlängerung dieses erheblichen Mangels führen.

## 7 Weitere Einzelthemen

### 7.1 Datenschutzaufsicht im parlamentarischen Bereich

Die Aufsicht über Datenverarbeitungen durch den Deutschen Bundestag, seine Fraktionen und Mitglieder wirft schwierige Rechtsfragen auf. Die Fraktionen des Bundestags haben nunmehr meine Empfehlung aufgegriffen, sich eine eigene Datenschutzordnung zu geben. Hierzu haben sie eine Arbeitsgruppe eingerichtet, in deren Beratungen ich eingebunden bin.

Mit Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) zum 25. Mai 2018 stellte sich die Frage, inwieweit diese Vorschriften für den Deutschen Bundestag, die Fraktionen und Ausschüsse sowie einzelne Abgeordnete gelten und ob sie meiner datenschutzrechtlichen Aufsicht unterstehen. Im parlamentarischen Bereich werden personenbezogene Daten zu vielfältigen Zwecken verarbeitet. So werden beispielsweise Daten von Bürgerinnen und Bürgern im Rahmen von Petitionen oder Anfragen (z.B. aus den Wahlkreisen) verarbeitet. Gleiches gilt bei der Öffentlichkeitsarbeit, etwa über die eigene Homepage oder die vielfältigen Aktivitäten von Abgeordneten in sozialen Netzwerken. Nicht zuletzt sind Abgeordnete Arbeitgeberinnen und Arbeitgeber und verarbeiten auch auf diese Weise personenbezogene Daten ihrer Beschäftigten. In meinem 27. TB war ich zunächst von einer entsprechenden Geltung der DSGVO für Datenverarbeitungen von Parlamenten und ihren Untergliederungen ausgegangen. Demzufolge beschränkte ich mich aus verfassungsrechtlichen Gründen darauf, nur meine Beratungsaufgaben wahrzunehmen. Schon zu diesem Zeitpunkt empfahl ich dem Deutschen Bundestag, sich eine eigene Datenschutzordnung unter Beachtung der Vorgaben der DSGVO zu geben (vgl. 27. Tb, Nr. 14.1.1).

Mehrere datenschutzrechtliche Eingaben zu Datenverarbeitungen durch Abgeordnete und Fraktionen des Deutschen Bundestags veranlassten mich, meine Zuständigkeit für die datenschutzrechtliche Kontrolle über die Mitglieder und die Fraktionen des Deutschen Bundestages unter Berücksichtigung der Rechtsprechung des

BVerfG zur Parlamentsautonomie zu prüfen. Im November 2019 teilte ich dem Deutschen Bundestag mit, dass ich beabsichtige, künftig meine datenschutzrechtlichen Aufsichtsbefugnisse in Fällen auszuüben, in denen ich die Parlamentsautonomie nicht tangiert sehe. Seitdem bin ich in Gesprächen mit dem Deutschen Bundestag, wie weit die Parlamentsautonomie im Zusammenhang mit der Verarbeitung personenbezogener Daten durch Abgeordnete reicht bzw. wo es darüber hinaus Bereiche gibt, in denen datenschutzrechtliche Aufsichtsmaßnahmen durch mich zulässig sind, um keine aufsichtsfreien Räume entstehen zu lassen.

Im Sommer 2020 entschied der EuGH (Urteil vom 9. Juli 2020, Az. C-272/19) aufgrund einer Vorlage des VG Wiesbaden, dass der Petitionsausschuss des hessischen Landtags Verantwortlicher im Sinne der DSGVO ist. Der Begründung des Urteils kann zudem entnommen werden, dass der EuGH die DSGVO für unmittelbar anwendbar auch auf Datenverarbeitungen des Parlaments und seiner Mitglieder im Kernbereich parlamentarischer Tätigkeiten hält. Damit unterliegen die Fraktionen und Abgeordneten wie andere öffentliche Stellen des Bundes grundsätzlich meiner datenschutzrechtlichen Aufsicht. Mir ist allerdings bewusst, dass ich bei der Ausübung dieser Aufsicht die besondere Stellung der Mitglieder des Deutschen Bundestags als Teil der Legislative berücksichtigen muss. Hier gilt es, nach Maßgabe der Rechtsprechung des BVerfG den Grundsatz der Gewaltenteilung aus Art. 20 Absatz 2 Satz 2 GG sowie die Freiheit der Mandatsausübung durch ein Mitglied des Deutschen Bundestages (Art. 38 Absatz 1 Satz 2 GG) zu wahren. Die einzelnen Abgeordneten sind nach der verfassungsrechtlichen Rechtsprechung nicht von vornherein jeder exekutiven Kontrolle entzogen. Dies ist aber in erster Linie eine eigene Angelegenheit des Deutschen Bundestages, der dabei im Rahmen seiner Parlamentsautonomie zu handeln hat.

Die Fraktionen des Deutschen Bundestages sind derzeit unter meiner Einbindung im Gespräch, wie eine Datenschutzordnung des Deutschen Bundestags und



wie eine den Besonderheiten des Parlaments und den Bestimmungen der DSGVO Rechnung tragende Regelung der datenschutzrechtlichen Aufsicht aussehen könnte. Vorerst werde ich mich daher weiter auf meine Beratungsaufgabe gegenüber Abgeordneten des Deutschen Bundestages beschränken.

## 7.2 Interdisziplinärer Beirat Beschäftigtendatenschutz

Datenskandale verdeutlichen immer wieder, dass bei der Verarbeitung von Beschäftigtendaten oft wenig Transparenz oder Rechtssicherheit herrscht. Seit vielen Jahren fordern die Datenschutzaufsichtsbehörden von Bund und Ländern deshalb ein Beschäftigtendatenschutzgesetz. Im Sommer 2020 hat der Bundesminister für Arbeit und Soziales nun einen interdisziplinären, wissenschaftlichen Beirat unter der Leitung der ehemaligen Bundesjustizministerin, Prof. Dr. Herta Däubler-Gmelin, berufen, dem auch der BfDI angehört.

In einer zunehmend digitalisierten Arbeitswelt werden durch den Einsatz von Künstlicher Intelligenz und Big Data-Anwendungen immer mehr personenbezogene Daten von Beschäftigten verarbeitet. Damit steigt für Beschäftigte das Risiko, ihre Privatsphäre bis hin zu einer totalen Überwachung einzubüßen. Künstliche Intelligenz in Bewerbungsverfahren, Screening von Beschäftigten, GPS-Tracking oder Videoüberwachung sind nur einige Herausforderungen, bei denen Regelungslücken sichtbar werden. Sie machen einen Schutz von Beschäftigten durch klare gesetzliche Regelungen wichtiger denn je. Seit vielen Jahren fordern die Datenschutzaufsichtsbehörden von Bund und Ländern deshalb ein Beschäftigtendatenschutzgesetz, das spezifische Verarbeitungen sowie den Einsatz neuer Technologien im Beschäftigtenkontext regelt. Dabei geht es insbesondere um Eckpunkte wie beispielsweise ein Verbot der Totalüberwachung, Grenzen einer Verhaltens- und Leistungskontrolle und Beweisverwertungsverbote. In Reaktion auf den im Koalitionsvertrag der 19. Legislaturperiode verankerten Prüfauftrag zum Beschäftigtendatenschutz hat das Bundesministerium für Arbeit und Soziales im Sommer 2020 einen interdisziplinären und unabhängigen Beirat mit der Erarbeitung gemeinsamer Handlungsempfehlungen zu einem eigenständigen Beschäftigtendatenschutzgesetz eingesetzt. Dem Beirat unter der Leitung von Prof. Dr. Herta Däubler-Gmelin gehören namhafte Vertreterinnen und Vertreter aus Wissenschaft, Wirtschaft und Verwaltung an, die die Fragestellungen zum Beschäftigtendatenschutz unter juristischen, ethischen, philosophischen und technischen Aspekten betrachten. Die Beratungen des Beirats

dauerten zum Redaktionsschluss dieses Tätigkeitsberichts noch an.

## 7.3 Register im Gesundheitsbereich

Die Nutzung von Daten zu Forschungszwecken bleibt im Gesundheitsbereich ein aktuelles Thema. Der Trend, auf gesetzlicher Grundlage verpflichtend medizinische Daten zu sammeln, hat sich auch im Jahr 2020 unvermindert fortgesetzt. Die Vorteile für Forschung und Behandlung dürfen nicht zu Lasten des Schutzes der betroffenen Patienten, zum Beispiel vor Missbrauch und Identifizierung gehen. Daher sind sichere Verfahren vorzusehen. Die möglichen „Nebenwirkungen“ müssen im Blick bleiben, wenn das Datensammeln als „Allheilmittel“ aufgefasst wird.

### Implantateregister

Über das neu errichtete bundesweite Implantateregister habe ich bereits in meinem letzten Tätigkeitsbericht unter Nr. 4.2.2 (S. 28/29) ausführlich berichtet. Problematisch erwies sich hier, dass das Bundesministerium für Gesundheit (BMG) das Deutsche Institut für medizinische Dokumentation und Information (DIMDI) auflösen und dessen Aufgaben dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) übertragen wollte. Hier konnte ich erreichen, dass diese Übertragung nicht durch einen Erlass des BMG erfolgte.

Stattdessen gab es ein förmliches Gesetzgebungsverfahren, um die betreffenden Vorschriften durch den Deutschen Bundestag selbst zu ändern. Diese Aufgabenübertragung war von wesentlicher Bedeutung, weil sie dazu führte, dass beim BfArM verschiedene Funktionen zusammenfielen, die bisher bewusst verschiedenen Behörden zugewiesen waren. Für das Implantateregister wurde diese Problematik gelöst, indem die Führung des Registers übergangsweise dem BMG zugeordnet wurde. Dies entspricht leider nicht meiner Empfehlung, eine unabhängige Registerbehörde zu schaffen. Das Register hat den unmittelbaren Wirkbetrieb bislang nicht aufgenommen. Es fehlt noch an einer Rechtsverordnung, die nähere Festlegungen trifft. Da vorgesehen ist, dass verschiedene Berechtigte, u.a. das BfArM, für ihre Aufgaben sowie die Hochschulen für wissenschaftliche Forschung die Registerdaten nutzen können, ist wesentlich, den Zugang zu den Daten durch ein sachgerechtes Verfahren zu regeln. Ein Antrag auf Nutzung muss ordnungsgemäß geprüft werden. Dies ist nur gewährleistet, wenn die entscheidende Stelle – hier die Registerstelle – unabhängig ist und insbesondere keine eigenen Nutzungsinteressen hat. Das Implantateregister wird auf verpflichtender gesetzlicher Grundlage eine enorme

Anzahl von Datensätzen enthalten. Daher müssen hier besondere Vorkehrungen zur Absicherung bei Speicherung und Nutzungszugang getroffen werden.

### **Organspenderregister**

Nach lebhafter politischer Auseinandersetzung wurde am 16. März 2020 das Gesetz zur Stärkung der Entscheidungsbereitschaft bei der Organspende beschlossen, das zum 1. März 2022 in Kraft treten wird. Damit wird ein bundesweites Online-Register für die Dokumentation der Erklärung zur Organspende eingerichtet. Ich habe zunächst das DIMDI, dann das BfArM bei der technischen Umsetzung beraten. Wesentliches Thema war hier eine sichere Authentifizierung, damit gewährleistet ist, dass die dokumentierte Erklärung auch wirklich von der benannten Person stammt. Dies lässt sich am einfachsten mit der Online-Funktion des neuen Personalausweises sicherstellen. Leider nutzen viele Bürger diese Funktion bisher nicht. Daher mussten alternative Möglichkeiten entwickelt werden. Wichtig ist auch, dass im Falle der Möglichkeit zur Transplantation garantiert die richtige Erklärung gefunden wird. Um Verwechslungen auszuschließen, war ich zum Schutz der Betroffenen damit einverstanden, dass die Krankenversicherungsnummer als Unterscheidungskriterium verwendet werden kann. Da die Krankenversicherungsnummer eigentlich nur für Zwecke der Krankenversicherung verwendet werden darf, ist dies eine Ausnahme. Diese Regelung darf nicht dazu führen, die Krankenversicherungsnummer als Personenkennziffer zur Zuordnung oder Identifizierung zu nutzen. Das BfArM wird das Organspenderregister nicht selbst führen, sondern hat die Bundesdruckerei mit der Registerführung beauftragt. Leider hat das BfArM versäumt, mich hierüber frühzeitig zu informieren.

### **Weitere Register im Gesundheitswesen**

Im Berichtszeitraum habe ich mich auch mit der Erweiterung des Umfangs der Daten befasst, die aufgrund der Datentransparenzvorschriften im Forschungsdatenzentrum beim BfArM gespeichert werden. Dies sind die Abrechnungsdaten, die den Krankenkassen zu ihren Versicherten vorliegen. Zu diesen kommen ab dem Jahr 2023 die Daten hinzu, die die Versicherten auf freiwilliger Basis aus ihrer sogenannten elektronischen Patientenakte (EPA) für die Forschung freigeben.

Eine weitere Sammlung von medizinischen Daten soll beim Robert Koch-Institut (RKI) durch eine zentrale Zusammenführung der Daten aus den klinischen Krebsregistern der Länder entstehen. Der Gesetzentwurf hierzu hat mich zum Ende des Jahres erreicht. In den Bundesländern gibt es bereits Krebsregister, die epidemiologische und klinische Daten zu den Krebserkrankungen enthalten. Die klinischen Krebsregister dokumentieren

verlaufsbegleitend die onkologische Versorgung in der stationären und ambulanten Behandlung. In den bundesweit einheitlich vorgegebenen Datensätzen sind viele Angaben zu Person und Behandlung enthalten, einschließlich Operation, Art der Therapie, Arzneimittel und Dosis. Die epidemiologischen Krebsregister dienen der bevölkerungsbezogenen Analyse. Sie geben Auskunft, wie häufig Krebserkrankungen in einer Region und einem bestimmten Alter vorkommen. Ein Teil dieser weitgehend statistischen Angaben wurden bisher bereits im Zentrum für Krebsregisterdaten (ZfKD) beim RKI zusammengeführt. Nun ist beabsichtigt, auch umfangreiche Angaben aus den klinischen Krebsregistern beim ZfKD zusammenzuführen. Dies sehe ich kritisch, da durch die Zusammenführung die Daten weitgehend verdoppelt werden. Dies widerspricht dem Grundsatz der Datensparsamkeit. Die Daten sollen verschiedenen Berechtigten zu Forschungszwecken zur Verfügung gestellt werden können. Die Nutzung von Gesundheitsdaten zu Forschungszwecken ist von gesamtgesellschaftlicher Bedeutung. Wichtig ist deshalb, dass das Verfahren zur Entscheidung über den Antrag datenschutzgerecht ausgestaltet wird und bestmöglichen Schutz für sensible Gesundheitsdaten bietet.

### **Querverweise:**

4.2 Patientendaten-Schutz-Gesetz, 5.7 Datentransparenzverordnung

## **7.4 Nachbessern, aber bitte richtig - der zweite Beschluss des Bundesverfassungsgerichts zur Bestandsdatenauskunft**

Das Bundesverfassungsgericht hat im Mai 2020 die Übermittlungsvorschrift des § 113 Telekommunikationsgesetzes (TKG) sowie eine Reihe mit ihm korrespondierender fachgesetzlicher Abrufregelungen für verfassungswidrig erklärt. Damit hat es seine Rechtsprechung aus dem Bestandsdatenauskunft I-Beschluss von 2012 konkretisiert. Der Gesetzgeber hat jetzt bis zum 31. Dezember 2021 Zeit, um nachzubessern.

Mit Beschluss vom 27. Mai 2020 (1 BvR 1873/13, 1 BvR 2618/13) machte das Bundesverfassungsgericht (BVerfG) neue Vorgaben zur Auskunft von Telekommunikationsdiensteanbietern an Sicherheitsbehörden über die Bestandsdaten ihrer Kundinnen und Kunden. In meinem 24. Tätigkeitsbericht hatte ich bereits ausführlich zum Beschluss „Bestandsdatenauskunft I“ des BVerfGs berichtet (vgl. TB Nr. 6.2).

Damals erklärte das Gericht § 113 Abs. 1 S. 1 TKG bei verfassungskonformer Auslegung noch für mit dem

Grundgesetz vereinbar. Nunmehr erklärte es den – infolge des Beschlusses „Bestandsdatenauskunft I“ geänderten § 113 Abs. 1 TKG – für verfassungswidrig. Insbesondere wegen fehlender Normenklarheit erklärten die Karlsruher Richter eine Reihe weiterer mit § 113 Abs. 1 TKG korrespondierender fachgesetzlicher Abrufregelungen aus dem Bundespolizeigesetz, dem Bundeskriminalamtgesetz, dem Zollfahndungsdienstgesetz, dem Bundesverfassungsschutzgesetz, dem BND-Gesetz und dem MAD-Gesetz für verfassungswidrig. Diese einzelnen Befugnisse zum Datenabruf sind nicht hinreichend begrenzt und missachten die notwendigen Anforderungen an Transparenz, Rechtsschutz und Kontrolle.

Das Gericht verlangt, dass Abrufregelungen die Verwendungszwecke der Daten hinreichend begrenzen müssen. Dabei sind Anlass, Zweck und Umfang des Eingriffs auch für den Datenabruf bereichsspezifisch, präzise und normenklar festzulegen. So ist der Abruf für vielfältige und unbegrenzte Verwendungen im gesamten Aufgabenbereich einer Behörde unzulässig.

Ebenso für verfassungswidrig erklärte das Gericht § 113 Abs. 2 S. 1 TKG, da in der Vorschrift eine Beschränkung auf die Abwehr von Gefahren für Rechtsgüter von hervorgehobenem Gewicht fehlt. Überdies kann eine

Bestandsdatenauskunft auch nach begangenen Ordnungswidrigkeiten erfolgen.

Mit der höchstrichterlichen Entscheidung ist eine Auskunft über gespeicherte Bestandsdaten von Telekommunikationskunden grundsätzlich weiterhin zulässig. Das BVerfG hat allerdings klargestellt, dass der Gesetzgeber verhältnismäßige und hinreichend bestimmte Rechtsgrundlagen für die Telekommunikationsanbieter und für die abfragenden Sicherheitsbehörden schaffen muss.

### Doppeltürenmodell bestätigt

Mit seinem Beschluss hat das Gericht das sog. Doppeltürenmodell aus seiner Entscheidung „Bestandsdatenauskunft I“ bestätigt. Danach darf sowohl die Anfrage durch die Sicherheitsbehörde als auch die Übermittlung der Bestandsdaten durch die Diensteanbieter nur aufgrund einer jeweils eigenständigen Rechtsgrundlage erfolgen. Für eine wirksame Bestandsdatenauskunft müssen also zwei „Türen“ geöffnet werden. Das BVerfG hat weiterhin klargestellt, dass für die Zulässigkeit einer Bestandsdatenanfrage grundsätzlich im Einzelfall eine konkrete Gefahr oder ein Anfangsverdacht einer Straftat vorliegen muss. Andernfalls müssen höherrangige Rechtsgüter betroffen sein.



Betrifft die Bestandsdatenauskunft die Zuordnung einer dynamischen IP-Adresse, hat dieser Eingriff ein höheres Gewicht. Deshalb müssen zusätzlich zur konkreten Gefahr im Einzelfall oder zum Anfangsverdacht einer Straftat hinreichend gewichtige Rechtsgüter betroffen sein. Diese Voraussetzungen erfüllen die angegriffenen Regelungen weitgehend nicht. Der Gesetzgeber muss also bei den Übermittlungsbefugnissen und den Abfrageregulungen für die Sicherheitsbehörden nachbessern. Dafür hat er bis zum 31. Dezember 2021 Zeit. Ich empfehle dem Gesetzgeber jedoch, zur Klarstellung und datenschutzfreundlicheren Ausgestaltung der Rechtslage bereits früher tätig zu werden. Für ein zügiges Tätigwerden des Gesetzgebers habe ich mich auch in Rahmen einer Entschließung zum manuellen Auskunftsverfahren der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 25. November 2020 eingesetzt.

Bereits während der Gesetzesänderungen im TKG in Folge der Entscheidung „Bestandsdatenauskunft I“ hatte ich mich dafür stark gemacht, die grundsätzliche Notwendigkeit und den sehr weit gefassten Umfang der Bestandsdatenauskunft kritisch zu hinterfragen (vgl. 24. TB Nr. 6.3). Insbesondere meine Bedenken zur Verhältnismäßigkeit des neu gefassten § 113 Abs. 1 TKG blieben im damaligen und in weiteren Gesetzgebungsverfahren leider unberücksichtigt.

#### **Recht auf informationelle Selbstbestimmung gestärkt**

Mit seinem Beschluss „Bestandsdatenauskunft II“ hat das BVerfG meine langjährige Kritik bestätigt, das Recht auf informationelle Selbstbestimmung gestärkt und der Bestandsdatenauskunft klare Grenzen gesetzt. Auch in meiner Stellungnahme im Rahmen des Gerichtsverfahrens habe ich die unbestimmte Reichweite und die unklare Zweckbindung vieler Regelungen kritisiert. Das BVerfG griff auch den von mir im Verfahren geltend gemachten Vortrag auf, dass Behörden bisher keine Dokumentationspflichten bei der Zuordnung von IP-Adressen auferlegt werden. Die Dokumentation ermöglicht aber eine datenschutzrechtliche Kontrolle des Abrufs von Bestandsdaten anhand von IP-Adressen und erleichtert die verwaltungsgerichtliche Kontrolle. Laut BVerfG sind die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren im Zusammenhang mit der Zuordnung dynamischer IP-Adressen aktenkundig zu machen.

Zur Auskunft anhand der IP-Adressen hatte ich bereits im Gesetzgebungsverfahren darauf hingewiesen, dass die Vorschrift des § 113 Abs. 1 S. 3 TKG viel zu weit gefasst ist und der vorherigen Entscheidung „Bestandsdatenauskunft I“ widerspricht. Der Gesetzgeber hat diese Verfassungswidrigkeit ignoriert. Um die Wiederho-

lung eines derartigen Fehlers im Rahmen der anstehenden TKG-Novelle zu vermeiden, ist eine verfassungsgemäße Anpassung des § 113 TKG geboten. Darauf habe ich den Gesetzgeber im Rahmen des aktuellen Gesetzgebungsverfahrens ausdrücklich hingewiesen. Das Bundesinnenministerium hat im November 2020 einen Referentenentwurf für ein „Reparaturgesetz“ vorgelegt mit dem Ziel, § 113 TKG und die korrespondierenden fachgesetzlichen Abrufregelungen verfassungsgemäß im Sinne des „Bestandsdatenauskunft II“-Beschlusses auszugestalten. Ich bin der Ansicht, dass die Regelungen des BVerfGs-Beschlusses in dem „Reparaturgesetz“ noch nicht vollumfänglich umgesetzt wurden und habe dies im Gesetzgebungsverfahren bemängelt. Meine Kritik blieb bisher jedoch ungehört.

#### **Querverweis:**

5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich

## **7.5 Anonymisierung – Eine Standortbestimmung zwischen der DSGVO und dem TKG**

Mit meinem Positionspapier zur Anonymisierung – unter besonderer Berücksichtigung der TK-Branche – habe ich das erste öffentliche Konsultationsverfahren meiner Behörde erfolgreich durchgeführt. Trotz diverser Meinungsverschiedenheiten der Beteiligten konnte am Ende eine klare Positionierung erfolgen.

Am 29. Juni 2020 habe ich mein „Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche“ veröffentlicht. Es entstand nach der Durchführung des ersten öffentlichen Konsultationsverfahrens meiner Behörde. Trotz der hohen praktischen Bedeutung der Anonymisierung macht die Datenschutz-Grundverordnung (DSGVO) nur sehr rudimentäre Ausführungen zur Anonymisierung. Diese unklare Rechtslage nahm ich zum Anlass, vom 10. Februar bis zum 23. März 2020 eine öffentliche Konsultation zur Anonymisierung – unter besonderer Berücksichtigung der TK-Branche – durchzuführen. Insgesamt habe ich im Laufe des Verfahrens 41 Stellungnahmen von Landesdatenschutzbehörden, Verbänden, Unternehmen, Forschungseinrichtungen und Privatpersonen erhalten. Nach Auswertung aller Stellungnahmen wurde das Positionspapier zusammen mit denjenigen Stellungnahmen, zu denen mir seitens der Beteiligten eine Einwilligung erteilt wurde, auf meiner Website veröffentlicht. Das Papier soll den aktuellen rechtlichen Rahmen für die Anonymisierung aufzeigen und Verantwortlichen eine Orientierung bei der datenschutz-



rechtlichen Bewertung ihrer Anonymisierungspraktiken bieten. Letztlich soll das Papier damit zur Rechtssicherheit beitragen.

Nach Berücksichtigung der Stellungnahmen sind die Hauptpunkte des Papiers die folgenden: Jede Anonymisierung stellt – aus verschiedenen Gründen – eine Verarbeitung personenbezogener Daten dar und bedarf deshalb einer Rechtsgrundlage. Als Rechtsgrundlage kommt grundsätzlich jeder der in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbestände in Betracht. Praktische Relevanz dürften vor allem die Einwilligung und die Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO in Verbindung mit der ursprünglichen Rechtsgrundlage haben, sofern der neue Zweck mit dem ursprünglichen Verarbeitungszweck vereinbar ist. Dass die ursprüngliche Rechtsgrundlage bei einer Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO Anwendung findet, verdeutlicht auch Erwägungsgrund 50 Satz 2 DSGVO. Der Verarbeitungszweck der jeweiligen Anonymisierung ist das hinter der Anonymisierung stehende tatsächliche Interesse des Verantwortlichen – und nicht etwa die Aufhebung des Personenbezugs.

Speziell für Telekommunikationsdienstleister ist eine Anonymisierung auch für Verkehrs- und Standortdaten möglich. So dürfen zum Beispiel Verkehrsdaten nach § 96 Absatz 1 Satz 2 Alternative 2 Telekommunikationsgesetz (TKG) nur verwendet werden, soweit dies für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich ist. Insofern verpflichtet § 96 Absatz 1 Satz 3 TKG den Diensteanbieter, die anderen Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen. Da die personenbezogenen Daten auch durch deren Anonymisierung gelöscht werden können, entsprechen die Telekommunikationsdienstleister mit der Anonymisierung von Verkehrsdaten der Löschungsverpflichtung von § 96 Absatz 1 Satz 2 Alternative 2 TKG. Nach § 98 Absatz 1 TKG dürfen Standortdaten anonymisiert verarbeitet werden, soweit dies zur Bereitstellung von Diensten mit Zusatznutzen erforderlich ist. Ein typisches Beispiel hierfür sind Ortungsdienste.

Weiterhin stellt jede Anonymisierung einen stetigen Prozess dar und ist nicht mit einem Mal erledigt. Dem Verantwortlichen obliegt insofern die fortwährende Aufgabe, die Validität seiner Anonymisierungsverfahren zu überprüfen. Eine absolute Anonymisierung ist jedoch weder technisch möglich noch datenschutzrechtlich gefordert. Ausreichend ist vielmehr, dass eine Re-Identifizierung der betroffenen Personen praktisch nicht mehr möglich ist.

Im Rahmen der Transparenzpflichten hat der Verantwortliche den Betroffenen gemäß Art. 13 Abs. 1 lit. c) DSGVO bzw. gemäß Art. 14 Abs. 1 lit. c) DSGVO die

Zwecke und die Rechtsgrundlage der Anonymisierung mitzuteilen. Sofern die Anonymisierung eine Weiterverarbeitung für einen anderen Zweck darstellt, greift zusätzlich noch die Transparenzpflicht des Art. 13 Abs. 3 DSGVO. Vor einer Anonymisierung ist grundsätzlich eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DSGVO durchzuführen. Denn bei einer Anonymisierung muss der Verantwortliche regelmäßig davon ausgehen, dass voraussichtlich ein hohes Risiko besteht. Das liegt daran, dass in der Regel eine „Verarbeitung in großem Umfang“ stattfindet und die jeweilige Anonymisierungstechnik dem Begriff der neuen Technologien unterfällt. Außerdem spricht für die Durchführung einer Datenschutz-Folgenabschätzung, dass die Generierung eines anonymen Datenbestandes eine komplexe Aufgabe des Verantwortlichen darstellt und viele Fehlerquellen birgt.

Meine Konsultation geht einher mit Bemühungen des Europäischen Datenschutzausschusses (EDSA), die Vorgaben an mögliche Anonymisierungstechniken weiter zu konkretisieren. Die Technology Subgroup des EDSA plant aktuell die Überarbeitung der Stellungnahme 5/2014 zu Anonymisierungstechniken, um die Stellungnahme noch innovations- und anwenderfreundlicher zu gestalten.

## 7.6 Unverschlüsselte Steuerdaten

Die Kommunikation mit einem Finanzamt per E-Mail erfolgt typischerweise unverschlüsselt, so dass diese durch Dritte mitgelesen oder verändert werden könnte. Manche Finanzämter versenden vorab einen Vordruck, in dem die Bürgerinnen und Bürger einer unverschlüsselten E-Mail-Kommunikation durch das Finanzamt zustimmen können. Mit dieser Einwilligung versuchen die Finanzämter, dem Datenschutzrecht Rechnung zu tragen und das Steuergeheimnis zu wahren. Wie in meinem 28. Tätigkeitsbericht (Nr. 8.3) dargestellt, ist eine wirksame Einwilligung in unverschlüsselten E-Mail-Verkehr gegenüber einer Behörde aber datenschutzrechtlich nicht möglich.

Die Bürgerinnen und Bürger haben ein wachsendes Bedürfnis, ihre Kommunikation mit dem Finanzamt digital zu führen. Dazu stehen derzeit nur eingeschränkte technische Möglichkeiten zur Verfügung. Die Verantwortung, einen sicheren Übertragungsweg anzubieten, liegt bei den Finanzämtern. Möchte ein Finanzamt ein Dokument digital senden, muss es nach Art. 32 Abs. 1 lit. a) Datenschutz-Grundverordnung (DSGVO) dafür sorgen, dass die angewendeten technischen und organisatorischen Maßnahmen ein dem Risiko der Datenübermittlung angepasstes Schutzniveau gewährleisten. Für die Praxis bedeutet das, dass unkritische Daten unverschlüs-



selt per Mail gesendet werden dürfen, weitergehende Informationen müssen verschlüsselt übertragen werden.

Gemäß dem seit 12. Dezember 2019 neu ins Gesetz eingefügten § 87a Absatz 1 Satz 3 2. Halbsatz Abgabenordnung (AO) ist ein unverschlüsselter E-Mail-Verkehr des Finanzamts mit Einwilligung aller Beteiligten zulässig. Ich halte diese Regelung jedoch für unvereinbar mit der DSGVO und damit für EU-rechtswidrig. Eine Einwilligung kann sich nicht auf die gesetzliche Verpflichtung zur Einhaltung der notwendigen technischen und organisatorischen Maßnahmen beziehen. Das liegt daran, dass die vom Verantwortlichen zu treffenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO frei wählbar und damit nicht einwilligungsfähig sind. Ich hatte bereits im Gesetzgebungsverfahren meine Bedenken geäußert und ausdrücklich empfohlen, von der geplanten Neufassung des § 87a Absatz 1 Satz 3 AO abzusehen. Meine Stellungnahme vom 11. Oktober 2019 findet sich auf meiner Internetseite unter der Rubrik Transparenz/Stellungnahmen des BfDI.

Ich habe die Finanzverwaltungen von meiner Haltung in Kenntnis gesetzt. Für den Fall einer unverschlüsselten Datenübermittlung per E-Mail durch ein Finanzamt behalte ich mir die Ausübung meiner Abhilfebefugnisse vor.

Die Interessen der Bürgerinnen und Bürger am Schutz ihrer personenbezogenen Daten und gleichzeitig an einer unkomplizierten Kommunikation mit dem Finanzamt können gewahrt werden, indem die Finanzverwaltung sichere Kommunikationswege bereitstellt, wie dies andere Behörden und Privatunternehmen heute regelmäßig tun. Zurzeit können die Bürgerinnen und Bürger meistens nur zwischen einer unverschlüsselten digitalen Übermittlung und einer Sendung per Brief durch das Finanzamt wählen. Der Staat sollte nicht aus der Pflicht entlassen werden, die notwendigen technisch-organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO zu treffen. Die in § 87a AO vorgesehene Einwilligungslösung ist praktisch ungeeignet, das Problem der unverschlüsselten E-Mail-Kommunikation zu lösen. Die Einwilligung ist von erheblichen Unsicherheiten geprägt, wie etwa von der Frage der Freiwilligkeit bis hin zu möglicherweise betroffenen Rechten Dritter. Das Finanzamt trägt bei der Übermittlung das Risiko, dass eine Einwilligung wirksam erteilt wurde und überhaupt relevant ist.

Bei Anfragen von Bürgerinnen und Bürgern rate ich regelmäßig davon ab, einem Finanzamt eine Einwilligung für unverschlüsselte E-Mail-Kommunikation zu erteilen.

Ich gehe davon aus, dass geplante IT-Verfahren für eine sichere Übermittlung durch die Finanzverwaltung zeitnah und datenschutzkonform umgesetzt werden.

## 7.7 IT-Konsolidierung Bund

**Mit dem Projekt „IT-Konsolidierung Bund“ soll die Arbeitsfähigkeit der Bundesregierung für die nächsten Jahre sichergestellt und ein effizienter IT-Betrieb gewährleistet werden. Die Einhaltung des Datenschutzes ist dabei eine grundlegende Anforderung, bei deren Umsetzung dem BfDI eine große Verantwortung zukommt.**

Am 6. November 2019 hat das Bundeskabinett die Neuorganisation der IT-Konsolidierung Bund verabschiedet und damit die bisherige Bündelung von Betriebskonsolidierung und Dienstekonsolidierung beim Bundesministerium des Inneren, für Bau und Heimat (BMI) aufgehoben. Seitdem wird die Betriebskonsolidierung vom Bundesministerium der Finanzen (BMF) verantwortet, während das BMI für die Dienstekonsolidierung zuständig ist. Zudem ist die BWI GmbH aus dem Dienstleisterverbund ausgeschieden, so dass das ITZ Bund alleiniger Dienstleister der Bundesverwaltung ist. Die BWI kann aber als Unterauftragnehmer eingesetzt werden.

Die Neuorganisation der Betriebskonsolidierung blockierte zunächst den Fortschritt des Gesamtprojekts und führte dazu, dass sich viele Teilprojekte der IT-Konsolidierung verzögerten. Die fehlende Grundsatz-Zertifizierung und Freigabe für Verschlusssachen der Stufe „Nur für den Dienstgebrauch“ zentraler Rechenzentren des ITZ Bundes führten zu Verzögerungen bei Behördenprojekten und IT-Maßnahmen. Die Unsicherheiten hinsichtlich der Zukunft der BWI führten zum fast vollständigen Erliegen der ursprünglich von der BWI übernommenen Aufgaben.

Im Laufe des vergangenen Jahres konnte die Dienstekonsolidierung den Rückstand aufholen und die Betriebskonsolidierung schließt entsprechend auf. Die wichtigsten Projekte der Dienstekonsolidierung, d.h. die E-Akte Bund und die Bundescloud, können bereits durch die Behörden genutzt werden.

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“.

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. Die Bundescloud stellt für einige Pilotbehörden bereits Dienste bereit.

Bei der Maßnahme „Bundesclient“ geht es um die Bereitstellung eines bundesweit einheitlichen PC-Arbeitsplat-

zes bis Ende 2025 mit standardisiertem Betriebssystem sowie Basis- und Querschnittsdiensten, wie z. B. E-Mail und Anwendungen zur Dokumentenbearbeitung. Der Bundesclient wird planmäßig weiterentwickelt und fortlaufend durch das ITZ Bund getestet.

Um die Projektleitungen der IT-Konsolidierung Bund langfristig bei den strategischen Entscheidungen zu unterstützen, war meine Mitarbeit in den entsprechenden Gremien erforderlich, etwa zur Architekturrichtlinie. Darüber hinaus stehe ich im regelmäßigen Austausch mit den Projektleitungen der Betriebskonsolidierung und Dienstekonsolidierung.

## 7.8 Microsoft, der Datenschutz und die digitale Souveränität

Wie passen Windows 10, Microsoft 365, Datenschutz und digitale Souveränität zusammen? Diese Frage wurde von Datenschützern in den letzten Monaten kontrovers diskutiert. Am 14. Januar 2020 endete der Produktsupport für Windows 7. Damit stieg der Druck, auf ein aktuelles Betriebssystem umzusteigen. Immer mehr Bundesbehörden stellen ihre Systeme auf Windows 10 um. Die zentrale Bereitstellung von Infrastrukturen und Diensten wird immer erfolgskritischer, was cloudbasierte Angebote in den Fokus rückt.

### Telemetriedaten kontra Datenschutz

Bereits am 7. November 2019 veröffentlichte die Datenschutzkonferenz (DSK) eine Handreichung zum Datenschutz bei Windows 10 (zu finden unter: [www.bfdi.bund.de/beschluesse-positions-papiere](http://www.bfdi.bund.de/beschluesse-positions-papiere)). Verantwortliche sehen sich beim Einsatz des Betriebssystems insbesondere mit der Frage konfrontiert, wie sich die Übermittlung von Telemetriedaten an Microsoft datenschutzrechtlich rechtfertigen lässt.

Telemetriedaten sind technische Daten, die aus dem System erhoben, an Microsoft übermittelt und analysiert werden. Hiermit will das Unternehmen die Stabilität des Systems überprüfen, Quellen für Fehler leichter ermitteln und dadurch die Funktionalität des Systems verbessern. Telemetriedaten enthalten Identifikatoren, die es Microsoft ermöglichen, einen individuellen Nutzer auf einem individuellen Gerät und dessen Nutzungsmuster wiederzuerkennen. Damit gelten sie als personenbezogene Daten, die vom Datenschutz geschützt sind.

Die einfachste datenschutzrechtliche Lösung für das skizzierte Dilemma bestünde darin, die Verarbeitung und Übermittlung von Telemetriedaten im Betriebssystem schlicht auszuschalten. Microsoft hatte gegenüber den Aufsichtsbehörden erklärt, dass zumindest bei der Nutzung der Telemetriestufe „Security“ keine Teleme-

triedaten übermittelt würden. Diese Telemetriestufe kann aber nur bei bestimmten Versionen von Windows 10 eingestellt werden, konkret bei den Enterprise- und Education-Editionen.

Aktuelle Untersuchungen der DSK und die SiSyPHuS-Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) kamen aber zu dem Ergebnis, dass auch eine entsprechende Konfiguration des Systems nicht sicher zu einem kompletten und vor allem dauerhaften Ausschluss der Datenübermittlung führt.

Die Aufsichtsbehörden sehen daher aktuell keine andere Möglichkeit, als den für den Einsatz von Windows 10 Verantwortlichen aufzuerlegen, Maßnahmen zu ergreifen, um eine Telemetriedatenübermittlung sicher zu unterbinden. Hierzu hat die DSK am 26. November 2020 einen entsprechenden Beschluss gefasst (ebenfalls zu finden unter: [www.bfdi.bund.de/beschluesse-positions-papiere](http://www.bfdi.bund.de/beschluesse-positions-papiere)). Konkret bedeutet dies, Verantwortliche müssen neben der Telemetriestufe Security zusätzlich mittels vertraglicher, technischer oder organisatorischer Maßnahmen (z. B. durch eine Filterung der Internetzugriffe von Windows-10-Systemen über eine entsprechende Infrastruktur) sicherstellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet.

---

**Ich empfehle in meinem Zuständigkeitsbereich für den Einsatz von Windows 10 die Trennung des Betriebssystems vom Internet, so wie sie in der Bundesverwaltung mit dem Bundesclient als Standardarbeitsplatz bis 2025 vorgesehen ist.**

---

### Intensiver Dialog zu Windows 10 und MS 365 erforderlich, auch perspektivisch

Die skizzierten Entscheidungen basieren auf einem intensiven Dialog mit Microsoft und einer gemeinsamen Bewertung innerhalb der DSK. Dieser Austausch ist auch in Zukunft wichtig, um allgemeingültige und tragfähige datenschutzrechtliche Handlungsempfehlungen ableiten zu können.

Exemplarisch gilt dies auch für die aktuelle Diskussion um die rechtlichen Verbesserungspotenziale der Auftragsverarbeitungsunterlagen von Microsoft im Kontext MS 365. Im Ergebnis hat die DSK hier einige Defizite festgestellt, beispielsweise bei der Festlegung, welche Daten zu welchen Zwecken verarbeitet werden sollen, bei der Möglichkeit für Verantwortliche, technisch-organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu prüfen oder bei den Informationen zu Unterauftragnehmern. Eine Arbeitsgruppe der DSK wird nun mit Microsoft in Kontakt treten, um zeitnah datenschutzgerechte Nachbesserungen zu erzielen. Die Gespräche sollen auch dazu dienen, Anpassungen an die durch die

Schrems II-Entscheidung des EuGH (vgl. Nr.4.3) aufgezeigten Maßstäbe an die Übermittlung personenbezogener Daten in die USA oder andere Staaten außerhalb der Europäischen Union zu erreichen.

### **Digitale Souveränität in weiter Ferne**

Die „digitale Souveränität“ hat sich als politische Zielvorstellung mittlerweile etabliert, auch wenn hierbei keine einheitliche, konturenscharfe Definition Verwendung findet. Im Kern geht es stets darum, die Abhängigkeiten zu einzelnen Hard- und Software-Anbietern zu verringern und einer wachsenden Technologieabhängigkeit entgegenzuwirken. Souverän sein zielt darauf ab, seine Rolle in der digitalen Welt selbständig, selbstbestimmt und sicher ausüben zu können. Ein souveräner datenschutzrechtlich Verantwortlicher kann damit also frei entscheiden, welche Handlungsoptionen er wählt, um die Datenschutzanforderungen sicher umzusetzen.

Die Beratungsgesellschaft PWC hat Ende 2019 für die Bundesverwaltung eine strategische Marktanalyse zur Reduzierung von Abhängigkeiten zu einzelnen Software-Anbietern vorgelegt. Gezeigt wurde, dass die Bundesverwaltung in einem kritischen Maße von einzelnen Anbietern abhängig ist. Das gilt besonders für Microsoft, dessen Produkte vielfach eingesetzt werden und die eng mit Fachanwendungen verknüpft sind. Es steht also nicht wirklich gut um die digitale Souveränität der deutschen Verwaltung.<sup>17</sup>

Um zukunftsfähige Modelle für die IT der öffentlichen Verwaltung zu entwickeln, sind wir aus meiner Sicht gut beraten, hier den Blick zu weiten und auf Diversität sowie Open Source zu setzen. Gerade der perspektivische Einsatz von neuen Cloud-Infrastrukturen kann hierbei ein wichtiger Wendepunkt werden und die Herstellerabhängigkeit reduzieren.

## **7.9 Künstliche Intelligenz – Fortschritte**

Anwendungen der Künstlichen Intelligenz (KI) und algorithmisch gesteuerte Entscheidungsprozesse beherrschen aktuelle Entwicklungen in Wissenschaft, Forschung, Wirtschaft und Politik. Viele Lebensbereiche werden zunehmend und fundamental durch die enormen Möglichkeiten geprägt, die uns KI eröffnet. Unterdessen werden Schwächen und Risiken dieser Systeme deutlich, die genauso thematisiert werden müssen wie ihre Potenziale.

Für viele gesellschaftliche Bereiche ist Künstliche Intelligenz (KI) heute bedeutend. Die potentiell großen Auswirkungen von KI-Systemen auf alle Lebensbereiche erfordern deshalb klare Vorgaben und Regelungen. Ich bin der festen Überzeugung, dass KI-Anwendungen einen hohen Mehrwert für eine moderne, digitale Gesellschaft erbringen. Darüber hinaus bin ich mir sicher, dass sich der Fortschritt in diesem Bereich so gestalten lässt, dass KI gleichzeitig datenschutzkonform und am Gemeinwohl orientiert sein kann. Ich engagiere mich aktiv in nationalen und internationalen Gremien, die sich mit der KI-Entwicklung befassen, um an diesem Gestaltungsprozess mitzuwirken.

### **Transparenz und Nachvollziehbarkeit**

Algorithmische Entscheidungsfindung kann als Grundlage einer KI z. B. einen enormen Mehrwert bei der Objektivierung von Entscheidungen schaffen. Je größer das Schädigungspotenzial von KI und Algorithmen ist, umso mehr Anforderungen sind an ihren Einsatz zu stellen und umso mehr Kontrollmöglichkeiten sind vorzusehen. Für den Bereich der KI spielt die Transparenz von Entscheidungen eine ganz wesentliche Rolle.

KI-Anwendungen müssen deshalb immer wieder von den zuständigen Aufsichtsbehörden auf ihre Rechtmäßigkeit geprüft werden, so dass Verstöße geahndet werden können. Dafür müssen die Aufsichtsbehörden personell gestärkt werden. Sie benötigen außerdem eine verbesserte technische Ausstattung und eine dauerhafte Fortbildung des Personals, um die teils hochkomplexen KI-Systeme und die dahinterstehenden Algorithmen bewerten zu können. Nur starke Datenschutzbehörden können eine starke unabhängige Kontrolle gewährleisten.

### **KI in nationalen und internationalen Gremien**

Im Sinne einer positiven Technikgestaltung möchte ich die Entwicklungen zur KI aktiv begleiten. Deshalb habe ich mich daran beteiligt, eine Resolution zum Umgang mit der Nutzung von KI auf internationaler Ebene zu erarbeiten, die von der Global Privacy Assembly im Oktober 2020 erfolgreich verabschiedet wurde. Das Papier stellt die grundsätzlichen Anforderungen für die Entwicklung und Nutzung von KI dar, die es benötigt, um den Rechenschaftspflichten nachzukommen. Ganz maßgeblich sind hier die Aspekte Risikoabwägung, Transparenz, Überprüfbarkeit und Intervenierbarkeit. Das Papier ist abrufbar unter: <https://globalprivacyassembly.org/wp-content/uploads/2020/11/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf>

<sup>17</sup> Dies hat auch die DSK in ihrer Erschließung vom 22. September 2020 festgestellt ([www.bfdi.bund.de/entschließungen](http://www.bfdi.bund.de/entschließungen)).

Auch die Datenethikkommission (DEK) betont in ihrem Abschlussgutachten die herausragende Rolle des Datenschutzes auf dem Feld der KI. Die DEK gibt konkrete Handlungsempfehlungen zur Gestaltung der digitalen Zukunft in diesem Bereich. Als Mitglied der Kommission freue mich sehr darüber, dass dem Datenschutz dort eine zentrale Bedeutung zugemessen wurde.

Neben der DEK haben sich zahlreiche andere Gremien mit dem Thema beschäftigt. So hat sich die Enquete Kommission des Bundestags mit Fragen zur KI, der gesellschaftlichen Verantwortung und der wirtschaftlichen, sozialen und ökologischen Potenziale befasst. Ich begrüße es sehr, dass die Entwicklungen rund um KI intensiv diskutiert und im Rahmen politischer und gesellschaftlicher Prozesse behandelt werden. Jetzt ist es an der Zeit, dass hieraus die richtigen Schlüsse gezogen und geeignete Maßnahmen umgesetzt werden. Es darf nicht bei Empfehlungen bleiben.

### **Der Mensch im Mittelpunkt**

Die Bundesregierung verfolgt die Strategie, dass Deutschland seinen Marktanteil im Bereich der KI zukünftig ausbaut. Bei der Umsetzung dieser Strategie und der begleitenden Projekte müssen KI-Anwendungen den Menschen in den Mittelpunkt stellen und dabei die datenschutzrechtlichen Vorgaben beachten. Beispielsweise hat jede betroffene Person das datenschutzrechtlich verbürgte Recht, nicht ausschließlich Entscheidungen unterworfen zu sein, die auf automatisierten Verarbeitungen beruhen. Dieses Betroffenenrecht muss auch tatsächlich umgesetzt werden können.

Gerade weil die technologischen Entwicklungen in diesem Bereich dynamisch und rasant verlaufen, ist eine fortwährende gesellschaftliche Debatte zur Anwendung bestimmter KI-Technologien erforderlich. Das Leitbild der Debatte muss dabei eine menschenzentrierte KI sein.

Datenschutz ist ein essentieller Erfolgsfaktor für KI-Anwendungen. Ich setze mich dafür ein, dass Datenschutz in diesem Kontext nicht nur als notwendige, sondern auch als wertvolle Eigenschaft wahrgenommen wird.

## **7.10 Zertifizierung und Akkreditierung – erste Verfahren starten**

Mit der Datenschutz-Grundgrundverordnung (DSGVO) wird in den Artikeln 42 und 43 die datenschutzspezifische Zertifizierung auf europäischer Ebene eingeführt.

**Damit soll die Einhaltung der Verordnung gefördert und der Nachweis der Konformität erleichtert werden. Erste Akkreditierungsanträge liegen bereits vor. Zertifizierungen sind im Laufe des Jahres 2021 zu erwarten.**

Die Artikel 42 und 43 der DSGVO enthalten Grundlagen und Rahmenbedingungen für die Schaffung eines Zertifizierungsverfahrens im Bereich des Datenschutzes. Die Mitgliedsstaaten gestalten konkrete Vorgaben, so dass nationale Besonderheiten berücksichtigt werden. Auf diese Weise werden verbindliche und unmittelbar in den EU-Mitgliedstaaten geltende Regelungen für Datenschutz-Zertifizierungen getroffen.

### **Keine Zertifizierung ohne Akkreditierung**

Datenschutz-Zertifizierungen gemäß der Artikel 42 und 43 DSGVO darf nur erteilen, wer zuvor als Zertifizierungsstelle akkreditiert wurde. Dieses mehrstufige System dient der Qualitätssicherung und soll einen „Wildwuchs“ an Siegeln und Prüfzeichen verhindern. Für die Aufsichtsbehörden ergeben sich dadurch eine ganze Reihe an neuen Aufgaben.

Nach § 39 Bundesdatenschutzgesetz (BDSG) entscheiden die zuständigen Datenschutzaufsichtsbehörden, ob eine Stelle als Zertifizierungsstelle tätig werden darf. Das tun sie auf Grundlage einer Akkreditierung durch die deutsche Akkreditierungsstelle (DAKKS) und im Einvernehmen mit dieser (vgl. § 4 Abs. 3 AkkStelleG).

Die Akkreditierung ist ein sehr komplexer Prozess<sup>18</sup>. Er erfordert die Einhaltung festgelegter Kriterien. Diese wurden von den unabhängigen Aufsichtsbehörden von Bund und Ländern im Arbeitskreis Zertifizierung, einer Untergruppe der Datenschutzkonferenz (DSK), erarbeitet. Die Kriterien wurden nach ISO/IEC 17065/2012 mit einer speziellen Ausrichtung auf den Bereich des Datenschutzes entwickelt. Gemäß Art. 64 DSGVO wurden die Vorgaben anschließend dem Europäischen Datenschutzausschuss (EDSA) zur Stellungnahme vorgelegt. Dadurch soll europaweit möglichst viel Einheitlichkeit bei den Vorgaben erreicht werden, ohne dabei nationale Gegebenheiten zu vernachlässigen.

Wesentlich für die Akkreditierung einer Zertifizierungsstelle ist außerdem das Vorliegen eines Zertifizierungsprogramms, das entsprechende Zertifizierungskriterien enthält. Gemäß Art. 42 DSGVO müssen diese Kriterien genehmigt werden. Auf europäischer Ebene wurde diesbezüglich eine Leitlinie erarbeitet.<sup>19</sup> Der Arbeitskreis Zertifizierung hat sich bei der Ausgestaltung von Orientierungsvorgaben für die nationalen Prozesse eng daran orientiert.

<sup>18</sup> Eine Übersicht der einzelnen Prozessschritte des Akkreditierungsprozesses finden Sie unter: <https://www.dakks.de/content/projekt-datenschutz>

<sup>19</sup> Die Guideline 1/2018 in der Version vom 4. Juni 2019 finden Sie unter: <https://www.bfdi.bund.de/edsa-guidelines>



## Das Zertifizierungsverfahren

Ist im Rahmen einer erfolgreichen Akkreditierung die sogenannte „Befugniserteilung“ durch die zuständige Aufsichtsbehörde erfolgt, kann die Zertifizierungsstelle auf der Grundlage ihres Zertifizierungsprogramms tätig werden. Hierbei ist wichtig, dass die Qualitätssicherung fortlaufend gewährleistet ist. Notfalls kann eine Zertifizierungsstelle gemäß Art. 58 DSGVO von der zuständigen Aufsichtsbehörde jederzeit angewiesen werden, keine Zertifizierungen mehr zu erteilen, wenn die Voraussetzungen dafür nicht oder nicht mehr vorliegen.

Den Aufsichtsbehörden ist es grundsätzlich freigestellt, selbst Zertifizierungen zu erteilen. Eine Akkreditierung benötigen sie in diesem Fall nicht. Meine Behörde wird keine eigenen Zertifizierungen anbieten, wie – nach aktuellem Stand – auch die Mehrheit der Aufsichtsbehörden der Länder. Ich bin sicher, dass eine lebendige Landschaft an zertifizierten Akkreditierungsstellen entstehen wird.

Über die Zertifizierungen auf nationaler Ebene hinaus besteht auch die Möglichkeit, ein Europäisches Datenschutzsiegel zu erlangen. Die diesbezüglichen Kriterien müssen vom EDSA gebilligt werden. Die europaweit zugelassenen Zertifizierungsverfahren sollen anschließend in einer zentralen Liste geführt werden. Die wesentlichen Prozessschritte wurden zwischenzeitlich vom EDSA verabschiedet, weitere Details werden nach und nach konkretisiert.<sup>20</sup>

## Zertifizierung als Qualitätsmerkmal

Verlässliche und transparente Verfahren für die Akkreditierung und die Zertifizierung sind eine zwingende Voraussetzung für einen glaubwürdigen Nachweis, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Gerade deshalb wurde sowohl auf nationaler als auch auf europäischer Ebene besonderer Wert auf eine fundierte Ausgestaltung der Prozesse gelegt. Mein Ziel ist es, auf dieser Grundlage künftig vertrauenswürdige Siegel zu schaffen. Zertifizierter Datenschutz wird so zu einem objektiven Qualitätsmerkmal.

## 7.11 Videoidentverfahren: Aktuelle Grundsatzentscheidung des BfDI mit Ausstrahlwirkung für viele Bereiche

Videoidentifizierungsverfahren sind risikobehaftet. Wo ein sehr hohes Vertrauensniveau erreicht werden muss, sind sie datenschutzrechtlich sogar unzulässig.

In der Vergangenheit habe ich mehrfach, zuletzt in meinem 27. TB, auf die Risiken hinsichtlich der Durchführung von Identifizierungen per Video-Chat hingewiesen. Bedingt auch durch die Corona-Pandemie bin ich nach der datenschutzrechtlichen Zulässigkeit von Videoidentifizierungsverfahren gefragt worden, da diese eine Identifizierung ohne persönlichen Kontakt ermöglichen.

Videoidentifizierungen werden in vielen unterschiedlichen Lebensbereichen durchgeführt, insbesondere bei der Eröffnung von Online-Bankkonten oder beim Abschluss von Mobilfunkverträgen. Zunehmend wird überlegt, Videoidentifizierung auch in Bereichen einzuführen, in denen die Identifizierung ein sehr hohes Vertrauensniveau erfüllen muss. Beispielsweise zum Schutz besonders schutzbedürftiger Kategorien von personenbezogenen Daten nach Artikel 9 DSGVO, wie etwa im Gesundheitswesen.

Diesen sehr hohen Schutzbedarf können Videoidentifizierungen nicht gewährleisten. Zunehmend sind täuschend echt wirkende Audio- und auch Videomanipulationen, sogenannte Deepfakes, zu beobachten. In einer Antwort der Bundesregierung auf eine Kleine Anfrage (BT-Drs. 19/15657) heißt es zu diesem Thema: „Die Arbeitseinheiten in den Abteilungen „Digitale Gesellschaft; Verwaltungsmodernisierung und Informationstechnik“ und „Öffentliche Sicherheit“ beschäftigen sich mit dem Thema im Kontext der Fernidentifizierung. Durch den Einsatz von Deepfakes ist es möglich, videobasierte Verfahren zu manipulieren. Beispielsweise kann eine zu identifizierende Person eine andere Person auf einem gestohlenen Ausweisdokument imitieren.“

Grundsätzlich sind bei der Beurteilung der datenschutzrechtlichen Zulässigkeit von Videoidentifizierungsverfahren mehrere Fragen zu berücksichtigen: Für welchen Zweck sollen sie vorgenommen werden, welche Gefährdungslagen gibt es und welcher Schutzbedarf besteht? Zudem sind die möglichen Folgen für die Betroffenen bei der Bewertung der Zulässigkeit heranzuziehen und die Frage zu klären, wie die Betroffenen gegen die entstehenden Risiken (z.B. einem Identitätsdiebstahl)

<sup>20</sup> Das Dokument des EDSA vom 28. Januar 2020 finden Sie unter: [www.bfdi.bund.de/edsa-dokumente](http://www.bfdi.bund.de/edsa-dokumente)



abgesichert sind. Orientierung bietet das Standarddatenschutzmodell (zu finden unter: [www.bfdi.bund.de/sdm](http://www.bfdi.bund.de/sdm)) mit den Schutzbedarfsstufen „normal“, „hoch“ und „sehr hoch“. Hinsichtlich von Identifizierungen, für die die Schutzbedarfsstufe „sehr hoch“ erreicht werden muss, lehne ich Videoidentifizierungsverfahren ausnahmslos ab.

In den übrigen Fällen ist anhand von Datenschutzfolgenabschätzungen die datenschutzrechtliche Zulässigkeit einer Videoidentifizierung zu prüfen, insbesondere im Hinblick auf die potentiellen Risiken für die Betroffenen. Sofern es möglich ist, durch flankierende technische und organisatorische Maßnahmen die Risiken der Verarbeitungstätigkeit auf ein angemessenes und somit verantwortbares Niveau zu verringern, könnten Videoidentifizierungsverfahren datenschutzrechtlich zulässig sein.

## 7.12 Folgen des Brexit

Der vorgesehene Übergangszeitraum im Austrittsabkommen zwischen der Europäischen Union und dem Vereinigten Königreich endete am 31. Dezember 2020. Das nunmehr seit dem 1. Januar 2021 geltende -Handels- und Kooperationsabkommen sieht eine weitere, maximal sechsmonatige, Übergangsregelung für Datenübermittlungen vor.

Am 31. Dezember 2020 endete der Übergangszeitraum, in dem das Vereinigte Königreich zwar nicht mehr Mitglied der Europäischen Union (EU) war, aber das Recht der EU und die Datenschutz-Grundverordnung (DSGVO) noch angewendet wurden. Das kurz vor Ablauf des Übergangszeitraums ausverhandelte Handels- und Kooperationsabkommen<sup>21</sup> sieht nunmehr eine Übergangsregelung für Datenübermittlungen an Verantwortliche und Auftragsverarbeiter im Vereinigten Königreich vor.

Danach sollen Übermittlungen personenbezogener Daten von der EU in das Vereinigte Königreich für eine Übergangsperiode nicht als Übermittlungen in ein Drittland (Art. 44 DSGVO) angesehen werden. Diese Periode endet, wenn die EU-Kommission das Vereinigte Königreich betreffende Angemessenheitsbeschlüsse getroffen hat, spätestens jedoch nach vier Monaten. Dieses Enddatum kann um zwei Monate verlängert werden, falls keine der beteiligten Parteien widerspricht.



Mit einem Angemessenheitsbeschluss wird in einem festgelegten Verfahren von der Europäischen Kommission festgestellt, dass ein Drittland ein dem Unionsrecht angemessenes Datenschutzniveau bietet. Bei Vorliegen des Beschlusses bedürfen Datenübermittlungen in Drittländer keinen besonderen Genehmigungen.

## 7.13 Neue Entwicklungen in der Forschung mit Gesundheitsdaten

Forschung mit Gesundheitsdaten ist von erheblicher gesellschaftlicher Bedeutung. Der „neue Trend“ zur verpflichtenden Datensammlung auf gesetzlicher Basis führt zu nachvollziehbaren Vorbehalten. Ich plädiere – auch auf EU-Ebene – für Forschung mit einer Einwilligung der Betroffenen.

Auf EU-Ebene wurden die Leitlinien 3/2020 für die Verarbeitung von personenbezogenen Gesundheitsdaten zu wissenschaftlichen Forschungszwecken im Zusammenhang mit dem COVID-19-Ausbruch verabschiedet. Parallel dazu werden derzeit vom EDSA Leitlinien zur Verarbeitung von personenbezogenen Daten für Forschungszwecke erarbeitet, die Aussagen zur Forschung mit Gesundheitsdaten enthalten und sich mit der Frage der Rechtsgrundlage und der Betroffenenrechte auseinandersetzen sollen. In der EU gibt es mehrere Mitgliedsstaaten, die die Zulässigkeit von Forschung mit Gesundheitsdaten unmittelbar durch Gesetze regeln. Nicht abschließend geklärt ist bisher die Reichweite der Regelung in Artikel 5 Abs. 1 lit. b), 2. Halbsatz DSGVO: Unter welchen Voraussetzungen kann der Zweck Forschung vereinbar sein mit dem Zweck, zu dem die Daten ursprünglich erhoben wurden?

Wenn beispielsweise der deutsche Gesetzgeber gesetzliche Grundlagen für die Nutzung von Gesundheitsdaten zu Forschungszwecken vorsehen möchte, so bin ich der Auffassung, dass es dem Schutz der sensiblen und besonders zu schützenden Gesundheitsdaten am ehesten gerecht wird, wenn dieses Gesetz eine Einwilligung der Betroffenen als Zulässigkeitsvoraussetzung enthält. Wenn, wie bislang in Deutschland üblich, die Einwilligung der Betroffenen die Rechtsgrundlage für die Datenverarbeitung zu Forschungszwecken darstellt, ist - soweit das Forschungsvorhaben und damit der Verarbeitungszweck (noch) nicht abschließend beschrieben werden können - , eine sog. breite Einwilligung (broad

21 [https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22020A1231\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN) (zuletzt abgerufen am 6.1.2021)

consent) grundsätzlich möglich. Hierbei sind bestimmte Schutzmaßnahmen der verantwortlichen forschenden Stellen erforderlich, welche die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder in einem Beschluss aus dem Jahr 2019 konkretisiert hat. Diese zusätzlichen Maßnahmen werden auch auf europäischer Ebene derzeit diskutiert.

National wurde das Forschungsdatenzentrum zur Datentransparenz auf gesetzlicher Grundlage wesentlich erweitert, bedauerlicherweise ohne eine Einwilligung oder zumindest eine allgemeine, voraussetzungslose Widerspruchsmöglichkeit der Betroffenen vorzusehen.

In Deutschland entstehen immer mehr Register, die medizinische personenbezogene Daten für die Forschung zur Verfügung stellen. Selbst wenn die Datenverarbeitung auf gesetzlicher Grundlage erfolgt, halte ich es für geboten, dass die Betroffenen zusätzlich – als Teil der Rechtsgrundlage – in die Nutzung ihrer Gesundheitsdaten für Forschungszwecke einwilligen müssen. Dann können sie selbst entscheiden, ob ihre personenbezogenen Gesundheitsdaten für die Forschung zur Verfügung gestellt werden. Denn die standardmäßige Pseudonymisierung und Verschlüsselung der Daten kann meist keinen absoluten Schutz vor einer Reidentifikation bieten. Je mehr Daten zu einem „Fall“ im Register vorliegen, desto größer ist diese Gefahr. Umso wichtiger sind zusätzliche Verfahren wie die Aggregation, die Forschung auf verschlüsselten Daten oder die „differential privacy“. Zudem ist die Möglichkeit der Forschung an anonymisierten Daten vorrangig zu prüfen. Soweit beispielsweise Künstliche Intelligenz einbezogen ist, sollte auch die Möglichkeit der Forschung an synthetischen Datensätzen, die keinen Bezug zu Personen aufweisen, berücksichtigt werden.

Eine einwilligungsbasierte Konzeption liegt der zukünftig möglichen Freigabe der Daten aus der elektronischen Patientenakte für das Forschungsdatenzentrum nach § 363 Abs. 1 bis 7 SGB V zugrunde. In vielen Fällen stellt die Einwilligung der Betroffenen die Rechtsgrundlage für auch umfassende Forschungsvorhaben, wie z. B. die Nationale Kohorte oder die Medizininformatikinitiative dar. Es hat nicht nur in Deutschland Tradition, dass Forschung am Menschen freiwillig sein muss. Letztlich gehört dieses Recht auch zu den anerkannten ethischen Standards im Forschungsbereich, auf die auch die DSGVO verweist. Diese grundsätzliche Freiwilligkeit der Forschung kann dadurch konterkariert werden, dass mit sensiblen personenbezogenen Gesundheitsdaten geforscht wird, ohne dass die Betroffenen sich dagegen wehren können.

Daher ist auch bei den zukünftig zu schaffenden Registern auf gesetzlicher Grundlage darauf zu achten, dass

die freiwillige und informierte Einwilligung der Betroffenen zumindest als Tatbestandsmerkmal festgeschrieben wird. Wenigstens ist ein umfassendes Widerspruchsrecht vor Verarbeitung der eigenen personenbezogenen Gesundheitsdaten zu Forschungszwecken unabdingbar, das über die Möglichkeiten von Art. 21 DSGVO weit hinausgeht.

#### **Querverweise:**

4.2 Patientendaten-Schutz-Gesetz, 5.7 Datentransparenzverordnung, 7.3 Register im Gesundheitsbereich

## **7.14 Berichtigung von Diagnosedaten**

**Bei unrichtigen Diagnosedaten hilft den Versicherten eine Ergänzung des nationalen Rechts, ihr durch die DSGVO garantiertes Recht auf Berichtigung unrichtiger Daten gegenüber den Krankenkassen durchzusetzen.**

Im Berichtszeitraum erreichten mich zahlreiche Beschwerden von Versicherten, die Anhaltspunkte dafür hatten, dass ihre Krankenkasse falsche Diagnosedaten über sie gespeichert hatte. Einer Abhilfe dieses datenschutzwidrigen Zustands stand § 303 Absatz 4 SGB V entgegen. Danach ist für den Fall, dass Datenübermittlungen zu Diagnosen nach den §§ 295 und 295a SGB V fehlerhaft oder unvollständig sind, eine erneute Übermittlung in korrigierter oder ergänzter Form nur im Falle technischer Übermittlungs- oder formaler Datenfehler zulässig.

Der mit dem Heil- und Hilfsmittelversorgungsgesetz vom 4. April 2017 geschaffene § 303 Absatz 4 SGB V verfolgt das Ziel, die unzulässige Praxis diverser Krankenkassen zu unterbinden. Diese könnten ansonsten nachträglich Einfluss auf Diagnosen nehmen, um dadurch die finanziellen Zuweisungen aus dem Risikostrukturausgleich zu erhöhen (sog. Upcoding, vgl. 22. TB, Nr. 10.2.3). Diese begrüßenswerte Zielsetzung führte dazu, dass nicht mehr nur unzulässige Diagnosekorrekturen durch die Krankenkassen verhindert werden, sondern die Versicherten keine Möglichkeit mehr hatten, eine Korrektur ihrer unrichtig gespeicherten Diagnosedaten durchzusetzen. Diese Beschneidung von Versichertenrechten steht im Widerspruch zu Art. 16 Datenschutz-Grundverordnung (DSGVO). Die Norm verleiht der betroffenen Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

Ich habe den Gesetzgeber auf die Unvereinbarkeit der nationalen Rechtslage mit dem höherrangigen europäischen Recht und die Notwendigkeit einer Rechtsanpassung hingewiesen. Mit einer Ergänzung des § 305 SGB V,

eingefügt durch das PDSG (s. 4.2), hat der nationale Gesetzgeber diesen dringenden Hinweis aufgegriffen. Nach Absatz 1 Satz 6 dieser Norm haben die Krankenkassen auf Antrag der Versicherten abweichend von § 303 Absatz 4 SGB V Diagnosedaten, die ihnen nach den §§ 295 und 295a SGB V übermittelt wurden und deren Unrichtigkeit durch einen ärztlichen Attest belegt wird, in berichteter Form bei der Unterrichtung nach Satz 1 („Versichertenankunft“) und bei der Übermittlung nach den Sätzen 2 und 3 (einwilligungsbasierte Übermittlung der Versichertenankunft an Dritte) zu verwenden. Diesen Antrag haben die Krankenkassen innerhalb von vier Wochen nach Erhalt des Antrags zu bescheiden.

Ich gehe davon aus, dass die Regelung den Versicherten die Durchsetzung ihres Rechts auf Berichtigung nach § 16 DSGVO ermöglicht. Ich werde die praktische Umsetzung des § 305 Absatz 1 SGB V im folgenden Berichtszeitraum daher aufmerksam beobachten.

#### Querverweis:

4.2 Patientendaten-Schutz-Gesetz

## 7.15 Das Krankengeldfallmanagement – Kein Konsens über den Umfang der Datenerhebungsbefugnisse der Krankenkassen

Die Gespräche mit dem Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) und dem Bundesministerium für Gesundheit (BMG) über eine datenschutzkonforme Gestaltung der „Begutachtungsanleitung Arbeitsunfähigkeit“ konnten (noch) nicht abgeschlossen werden.

Die Richtlinie „Begutachtungsanleitung Arbeitsunfähigkeit“ ermöglicht den Krankenkassen und den Medizinischen Diensten der Krankenkassen (MD), Arbeitsunfähigkeitsfälle ihrer Versicherten strukturiert zu begutachten. Dadurch wird der Erhalt der Arbeits- bzw. Erwerbsfähigkeit gefördert. Zahlreiche Beschwerden von Versicherten, aber auch meine Kontrollen bei Krankenkassen, zeigen wiederholt, dass das Verständnis einzelner Krankenkassen von ihren aus den Richtlinien abgeleiteten Befugnissen über die gesetzlichen Regelungen weit hinausgeht.

So sind die Krankenkassen beim Vorliegen von Zweifeln an der Arbeitsunfähigkeit (AU) nach § 275 Abs. 1 Nr. 3 b) SGB V verpflichtet, eine Stellungnahme des MD einzuholen. Dies ermächtigt sie jedoch nicht, zusätzliche Daten zur Erhärtung oder Beseitigung der Zweifel zu erheben. Soweit dies im Einzelfall erforderlich ist, können auf Grundlage des § 284 Abs. 1 Nr. 4 SGB V im besten Fall

Nachfragen bei Versicherten zulässig sein. Diese müssen mit der Prüfung der formalen Leistungsvoraussetzungen in unmittelbarem Zusammenhang stehen. In Betracht kommen nur Fragen nach einer voraussichtlichen Anschluss-AU oder nach geplanten diagnostischen/therapeutischen Maßnahmen, die einer Arbeitsaufnahme entgegenstehen.

Für generell unzulässig erachte ich (fern-)mündliche Versichertenanfragen. An mich gerichtete Versichertenbeschwerden zeigen, dass insbesondere die telefonischen Versichertenanfragen von einigen Krankenkassen wiederholt zu unkontrollierten, teilweise druckerhöhen Datenerhebungen genutzt werden. Mir wurde von unzulässigen Fragen zur gesundheitlichen und familiären Situation, sozialen Problemen oder Details aus Reha- oder Krankenhausentlassungsberichten sowie den Überredungsversuchen zu einem Krankenkassenwechsel berichtet.

Gespräche mit dem GKV-Spitzenverband und dem BMG erbrachten kein gemeinsames Verständnis zum Umfang der Datenerhebungsbefugnisse der Krankenkassen vor einer Beauftragung des MD. Deshalb werde ich die zurückgestellten Beschwerdeverfahren nach Art. 77 Datenschutz-Grundverordnung wieder aufnehmen und die Einhaltung der gesetzlichen Vorgaben mit aufsichtsrechtlichen Mitteln durchsetzen.

## 7.16 Zuständigkeitsaufteilung im Bereich Telekommunikation

Datenschutzaufsicht und -kontrolle gehören auch im Bereich der Telekommunikationsdienstleistungen in eine Hand. Die bisherige Zuständigkeitsverteilung zwischen der Bundesnetzagentur und mir hat sich in der Praxis als wenig zielführend erwiesen. Dem BfDI sollten beide Kompetenzen übertragen werden.

Die aktuelle Zuständigkeitsverteilung zwischen der Bundesnetzagentur (BNetzA) und mir ist nach wie vor reformbedürftig. Nach aktueller Rechtslage verfüge ich über keine Befugnisse zur Durchsetzung der Datenschutzvorschriften des Telekommunikationsgesetzes (TKG). Vielmehr soll ich meine Beanstandungen an die BNetzA übermitteln. Diese Regelung steht nicht im Einklang mit dem europäischen Primärrecht. Die Einhaltung der Vorschriften über den Datenschutz muss gemäß Art. 8 Abs. 3 Grundrechte-Charta endlich auch in Deutschland von unabhängigen Behörden überwacht werden (vgl. auch 28. TB Nr. 5.2). Daher empfehle ich dem Gesetzgeber im Rahmen des neuen Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des TKG, des Telemediengesetzes und

weiterer Gesetze (TTDSG) dringend, eine eindeutige und einheitliche Regelung der Zuständigkeit für die Überwachung der Einhaltung des Schutzes personenbezogener Daten zu schaffen (vgl. auch Nr. 5.10). Die Zuständigkeit muss einheitlich sein, unabhängig davon, ob dieser Schutz aus der Datenschutz-Grundverordnung, dem Bundesdatenschutzgesetz oder dem Fernmeldegeheimnis (bisher in § 88 ff. TKG geregelt) stammt. Die bisherige Verwaltungspraxis hat oft erst nach unverhältnismäßig langer Zeit und manchmal gar nicht zum Erfolg geführt. Und es liegt hauptsächlich daran, dass ich Verstöße der Unternehmen gegen das TKG nicht selbst verfolgen, sondern lediglich gegenüber der BNetzA beanstanden kann.

Dies ist für alle Betroffenen mehr als unbefriedigend. Nur durch eine klare und ausschließliche Zuweisung der Datenschutzaufsicht an meine Behörde können Betroffene von einheitlichen Prüfungen der Unternehmen und, wenn notwendig, auch Ahndungen im Sinne der Datenschutzvorschriften ausgehen.

#### Querverweis:

5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich

## 7.17 Cyber-Angriff auf die Bundesanstalt für Immobilienaufgaben

**Die Veröffentlichung einer Information über einen Angriff der Schadsoftware Emotet auf der Internetseite einer betroffenen Behörde ersetzt nicht die Benachrichtigung der betroffenen Personen, wenn personenbezogene Daten abgeflossen sind.**



Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung (Art. 34 Abs. 1 DSGVO).

Im Dezember 2019 wurde die Bundesanstalt für Immobilienaufgaben (BImA) durch die Schadsoftware Emotet angegriffen. Der Software gelang es, mehrere Computer von BImA-Beschäftigten zu befallen. Die BImA hat am 19. Dezember 2019 auf ihrer Internetseite eine Pressemitteilung mit dem Hinweis veröffentlicht, es könne nicht ausgeschlossen werden, dass auch personenbezogene Daten abgeflossen seien.

Dieser allgemeine Hinweis ersetzt nicht die gemäß Art. 34 Abs. 1 Datenschutz-Grundverordnung (DSGVO) erforderliche Benachrichtigung der betroffenen Personen.

Bei diesem Cyber-Angriff sind in neun Fällen die Vor- und Zunamen sowie teilweise die privaten E-Mail-Adressen und Bankverbindungen offengelegt worden. In einem weiteren Fall sind zudem der Vor- und Zuname einer Person in einem Kontext offenbart worden, der auf eine Langzeiterkrankung dieser Person schließen lassen könnte. Hierbei handelt es sich um Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO.

Ich habe darauf hingewirkt, dass die BImA die betroffenen Personen gemäß Art. 34 Abs. 1 DSGVO benachrichtigt.



## 8.1 Einzelthemen

Obgleich es sich hier um eine Auswahl handelt, zeigen die für diesen Bericht ausgewählten Einzelthemen aus meiner Beratungs- und Vermittlungstätigkeit zum Informationsfreiheitsgesetz (IFG), wie breit das inhaltliche Spektrum der Anfragen und damit das der Interessen der antragstellenden Personen ist.

### 8.1.1 Informationsfreiheit in der Pandemie

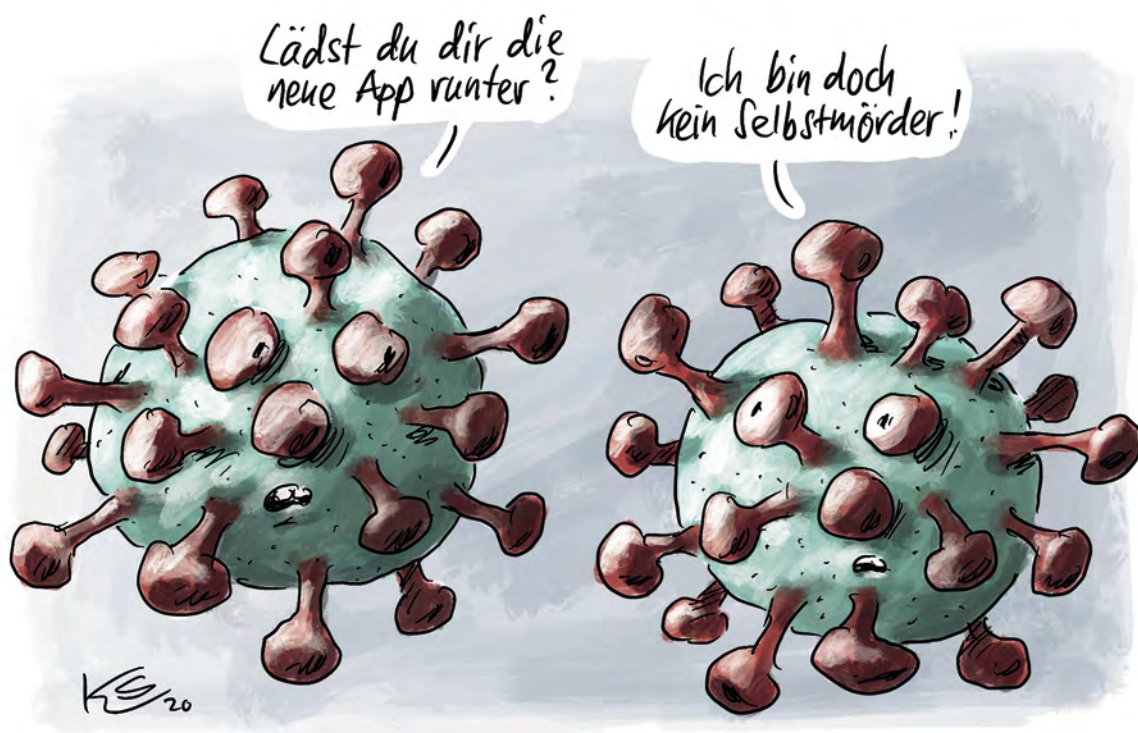
Die Corona-Pandemie war Gegenstand von Vermittlungsverfahren und von an mich gerichteten Anträgen nach dem Informationsfreiheitsgesetz (IFG).

Die Entwicklung der Pandemie ließ sich auch im Aufkommen und an den Inhalten der Anrufungen nachvollziehen, die mich erreichten. Ein Großteil dieser Beschwerden bezog sich auf IFG-Anträge an das Bun-

desministerium für Gesundheit (BMG) und das Robert Koch-Institut (RKI).

Zu Beginn der Pandemie waren auch die Modalitäten der Rückholaktion des Auswärtigen Amtes Gegenstand von Anträgen und Anrufungen. Mit Fortschreiten der pandemischen Lage ging es zunehmend um Informationen zu Fallzahlen, zur Ausgestaltung der Testmöglichkeiten, zur Amtshilfe durch andere Behörden oder auch um Lageberichte der Bundesregierung und des Bundesministeriums des Inneren, für Bau und Heimat (BMI). Die IFG-Eingaben zur Corona-Warn-App erreichten mich zur Jahresmitte.

Der mit über 1000 gleichartigen IFG-Anträgen einer Antragstellerin wohl aufkommensstärkste Informationswunsch betraf die „Einsparungen im Geschäftsbetrieb





der Bundesbehörden durch die pandemische Lage“ und lautete:

„Wie hoch waren die Einsparungen im laufenden Geschäftsbetrieb durch die COVID-19-Krise vom März bis Mai 2020 für

- den laufenden Geschäftsbetrieb, z.B. für Strom, Wasser, Papier etc. durch
- die Anordnung/ Wahrnehmung von Homeoffice-Regelungen
- die Absage von Veranstaltungen und Dienstreisen
- die Einsparungen durch Verringerungen von Wach- und Schutzleistungen
- sonstige Einsparungen?

Dabei reichen mir ungefähre Zahlen, um hier einen Eindruck zu gewinnen.“

Da die begehrten Informationen bei den angeschriebenen Stellen oftmals nicht vorlagen, war das Ergebnis für die Antragstellerin hier unerheblich.

Oftmals wandten sich Antragsteller an mich, weil die Monatsfrist des § 7 Abs. 5 Satz 2 IFG zur Entscheidung über den Informationszugang überschritten wurde. Sofern dies, wie insbesondere von dem durch die Bewältigung der Pandemie extrem stark belasteten RKI, aber auch vom BMG mit dem außergewöhnlich hohen Arbeitsaufkommen schlüssig begründet werden konnte, habe ich die Antragsteller um Verständnis für diese extreme Ausnahmesituation gebeten. Ich hoffe aber, dass eine zeitnahe Bearbeitung in zunehmenden Maße möglich sein wird.

IFG-Anträge zum Thema „Corona“ wurden auch an mein Haus gestellt. Das Interesse der Petenten richtete sich hier insbesondere auf meine Begleitung von Gesetzgebungsverfahren und auf meine Einschätzungen zu Maßnahmen wie etwa der Corona-Warn-App, zu digitalen Angeboten des BMG oder der sogenannten Aussteigekarte.

### 8.1.2 Was ist eigentlich ein Geschäftsgeheimnis?

#### Auswirkungen des neuen Geschäftsgeheimnisgesetzes auf die Informationsfreiheit

Ein Petent hatte beim Bundesministerium für Wirtschaft und Energie (BMWi) beantragt, ihm alle Dokumente zum geplanten Digital Services Act der EU zu übersenden. Dabei bezog er insbesondere die Korrespondenz mit Interessenvertretern ein. Ein Unternehmen, das zu dem Rechtsetzungsprojekt eine Stellungnahme abgegeben hatte, widersprach im Rahmen der Drittbeteiligung einer Offenlegung, da das Schreiben „Betriebs- oder Geschäftsgeheimnisse“ im Sinne von § 6 S. 2 Informations-

freiheitsgesetz (IFG) enthalte. Das BMWi gab daraufhin dem Antrag des Petenten nur teilweise statt.

Nachdem er erfolglos Widerspruch eingelegt hatte, wandte sich der Petent im IFG-Ombudsverfahren an mich. Er vertrat die Ansicht, dass bei der Auslegung der Richtlinie (EU) 2016/943 vom 8. Juni 2016 zum Schutz von Geschäftsgeheimnissen heranzuziehen sei, die in Deutschland durch das Geschäftsgeheimnisgesetz (GeschGehG) vom 18. April 2020 umgesetzt wurde. Ein Geschäftsgeheimnis muss nach Artikel 2 Nr. 1 c der Richtlinie bzw. nach § 2 Nr. 1 lit. b GeschGehG „Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber“ sein. Der Petent argumentierte, das Unternehmen habe auf angemessene Geheimhaltungsmaßnahmen verzichtet. Denn es habe die Stellungnahme selbst, freiwillig und aus eigener Initiative an das BMWi geschickt und dieses auch nicht zum Schweigen verpflichtet. „Betriebs- oder Geschäftsgeheimnisse“ i.S.v. § 6 IFG lägen somit nicht vor.

Angemessene Geheimhaltungsmaßnahmen sind nach bisherigem Verständnis kein Merkmal von Betriebs- und Geschäftsgeheimnissen. Da im IFG eine Definition fehlt, wurde der Begriff mit Blick auf den verfassungsrechtlichen Schutz unternehmerischer Tätigkeit entwickelt. Als Betriebs- und Geschäftsgeheimnisse werden danach „alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat“ (vgl. BVerfG 14.03.2006 – 1 BvR 2087/03, 1 BvR 2111/03, Rn. 87).

Der Petent hatte nun die Rechtsfrage aufgeworfen, ob das neue GeschGehG die Auslegung von „Betriebs- oder Geschäftsgeheimnissen“ in § 6 IFG verändert hatte. Die Bestimmungen zum Anwendungsbereich (vgl. § 1 Abs. 2, Abs. 3 Nr. 2 GeschGehG und Art. 1 Abs. 2 lit. a, b Richtlinie (EU) 2016/943) sprechen dagegen. Auch nach der Gesetzesbegründung soll das Gesetz nicht anwendbar sein „auf Informationsansprüche gegen staatliche Stellen, öffentlich-rechtliche Vorschriften zur Geheimhaltung von Geschäftsgeheimnissen oder Verschwiegenheitspflichten für Angehörige des öffentlichen Dienstes“ (BT-Drucks. 19/4724, zu § 1 Absatz 2 - S. 23). Gleichwohl ist die Frage in der juristischen Diskussion umstritten.

Die Frage konnte im betreffenden Vermittlungsverfahren letztlich offen bleiben. Das Ministerium machte plausibel, dass die Information Rückschlüsse auf die Marktstrategie des Unternehmens zulasse und daher wettbewerbsrelevant sei. Es wies auf die Verschwiegenheitspflichten seiner Beschäftigten hin, die auch ohne spezielle Vertraulichkeitsvereinbarungen gelten (z.B.

§ 67 Abs. 1 Bundesbeamtenengesetz). Durch die Übermittlung an das BMWi sei die Information daher nicht offenkundig geworden. Diese Sicht wird durch Erwägungsgrund 18 der Richtlinie (EU) 2016/943 gestützt. Danach soll eine Übermittlung von Geschäftsgeheimnissen an Behörden, diese „nicht von ihrer Pflicht zur Geheimhaltung (...) entbinden, und zwar unabhängig davon, ob diese Pflichten in Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegt sind“. Dies spricht dafür, dass sensible betriebliche Informationen – auch – nach der Richtlinie die Eigenschaft als Geschäftsgeheimnis nicht allein dadurch verlieren, dass sie ohne weitere Vertraulichkeitsabreden an Behörden übermittelt werden. Es liegt auch nicht nahe, dass das Unternehmen durch die Übermittlung an eine bekanntermaßen zur Verschwiegenheit verpflichtete Stelle auf angemessene Geheimhaltungsmaßnahmen verzichtet hätte.

Kurz nach Abschluss der Vermittlungen befasste sich das Bundesverwaltungsgericht (BVerwG) mit dem Verhältnis von IFG und GeschGehG (vgl. BVerwG 17.06.2020 - 10 C 22.19, Rn. 16), was jedoch nur teilweise zur Klärung beigetragen hat: Geschäftsgeheimnisse nach § 2 Nr. 1 GeschGehG (Art. 2 Nr. 1 RL (EU) 2016/943) sieht das BVerwG quasi als Minimum dessen an, was durch § 6 Satz 2 IFG geschützt wird. Das Gericht geht davon aus, dass der Begriff des Betriebs- oder Geschäftsgeheimnisses in § 6 Satz 2 IFG zwar selbstständig auszulegen ist, sich aber am gewachsenen Begriffsverständnis des Wettbewerbsrechts zu orientieren hat. Dieses sei offen für Fortentwicklungen und werde auch durch das neue GeschGehG geprägt. Als Leitlinie sieht es das BVerwG an, dass der Schutz nach § 6 Satz 2 IFG mindestens das umfassen muss, was als Geschäftsgeheimnis dem Geschäftsgeheimnisgesetz oder der Know-how-Schutz-Richtlinie unterfällt, um den Schutz nicht durch eine Informationspflicht der Behörde zu unterlaufen. Das Gericht ließ jedoch offen, ob § 6 S. 2 IFG einen weiterreichenden Schutz gewährt, hielt dies aber für möglich.

Die Grenzen des Schutzbereiches sind derzeit also noch nicht abschließend konturiert. Die weitere Entwicklung der Rechtsprechung bleibt abzuwarten, insbesondere ob sich hier eine „Konvergenz“ entwickelt oder die Begrifflichkeiten in ihrer Interpretation durch die Gerichte „auseinanderdriften“.

### **8.1.3 Zugang zum Verzeichnis von Verarbeitungstätigkeiten**

Das Verarbeitungsverzeichnis von Bundesbehörden kann grundsätzlich auch Gegenstand eines Antrags auf Informationszugang nach dem Informationsfreiheitsgesetz sein.

Eine Antragstellerin beantragte beim Bundesamt für Migration und Flüchtlinge (BAMF) gestützt auf das Informationsfreiheitsgesetz (IFG) die Übersendung eines Auszugs aus dem nach Art. 30 Datenschutz-Grundverordnung (DSGVO) zu erstellenden Verzeichnis von Verarbeitungstätigkeiten. Das BAMF lehnte diesen Antrag unter Verweis auf die Regelung des Art. 30 Abs. 4 DSGVO ab, der eine dem IFG vorgehende Spezialregelung im Sinne des § 1 Abs. 3 IFG darstelle. Demnach werde das Verzeichnis auf Anfrage nur der Aufsichtsbehörde zur Verfügung gestellt. Ein allgemeines Einsichtsrecht, wie es das frühere Bundesdatenschutzgesetz (BDSG) vorgesehen habe, bestehe hingegen nicht mehr. Die Antragstellerin wandte sich daraufhin mit einer Eingabe an mich. Auch mir gegenüber hielt das BAMF an seiner Rechtsauffassung fest.

Der Rechtsauffassung des BAMF kann ich mich nicht anschließen. Art. 30 Abs. 4 DSGVO stellt keine dem IFG vorgehende Spezialregelung dar. Nach der Rechtsprechung des Bundesverwaltungsgerichts wird das IFG nur durch solche Regelungen verdrängt, die einen mit § 1 Abs. 1 IFG identischen sachlichen Regelungsgehalt aufweisen und sich als abschließende Regelung verstehen (vgl. BVerwG, Urteil vom 22. März 2018 – 7 C 30/15). Dies trifft auf Art. 30 Abs. 4 DSGVO jedoch nicht zu. Durch die Regelung des Art. 30 DSGVO soll den Aufsichtsbehörden die datenschutzrechtliche Ex-post-Kontrolle ermöglicht werden. Der Wahrnehmung dieser Kontrollaufgabe dient auch die Regelung von Absatz 4, der die Pflicht zur Übermittlung des Verzeichnisses auf Anfrage an die Aufsichtsbehörde normiert. Während Art. 30 Abs. 4 DSGVO somit die effektive Aufgabenwahrnehmung durch die Aufsichtsbehörden sicherstellen will, gewährt § 1 Abs. 1 IFG einen Anspruch für Jedermann auf Informationszugang zu amtlichen Dokumenten. Art. 30 Abs. 4 DSGVO ist somit bereits mangels identischen Regelungsgehalts nicht als eine das IFG verdrängende Spezialnorm i.S.d. § 1 Abs. 3 IFG zu sehen.

Darüber hinaus ist aber auch nicht von einer abschließenden Regelung auszugehen. Zwar ist die Regelung des § 4g Abs. 2 BDSG alt – die ihrerseits auf die Vorgaben der Richtlinie 95/46/EG (Datenschutz-Richtlinie) zurückzuführen ist – nicht in die DSGVO und die aktuelle Fassung des BDSG übernommen worden, jedoch finden sich keine Anhaltspunkte dafür, die Regelung des Art. 30 Abs. 4 DSGVO als abschließend zu verstehen. Vielmehr wurden mit den Regelungen in Art. 12ff. DSGVO spezielle Pflichten geschaffen, die vorrangig der Information der betroffenen Personen dienen sollen und somit die ursprünglich zu diesem Zweck geschaffene Regelung zur Übersendung des Verarbeitungsverzeichnisses in der Datenschutz-Richtlinie abgelöst haben. Dem Transparenzgedanken der DSGVO folgend, scheint die Intention

des Ausschlusses einer überobligatorischen Information interessierter Personen durch Bereitstellung des Verzeichnisses über Verarbeitungstätigkeiten auch fernliegend.

Somit ist im Ergebnis davon auszugehen, dass unter Zugrundelegung der durch das Bundesverwaltungsgericht entwickelten Kriterien die Regelung des Art. 30 Abs. 4 DSGVO keine das IFG verdrängende Spezialregelung ist.

#### **8.1.4 Informationsfreiheitsgesetz des Bundes gilt nicht für der Deutschen Städtetag**

Der Deutsche Städtetag ist keine Bundesbehörde. Deshalb gilt hier nicht das Informationsfreiheitsgesetz (IFG) des Bundes. Auskunftspflichtig sind die Mitglieder des Städtetages nach dem jeweiligen Landesrecht.

Ein Petent bat mich um Vermittlung, weil er sein Recht auf Informationszugang durch den Deutschen Städtetag als verletzt ansah.

Der Deutsche Städtetag hatte ihm mitgeteilt, dass er „als Verein nicht Adressat der einschlägigen Gesetze sei, die einen Auskunftsanspruch des Bürgers gegen staatliche Institutionen vorsehen“ und ihm die begehrte interne Information nicht übersandt.

Zu Recht: In der Tat gewährt das IFG des Bundes keinen Anspruch auf Informationszugang gegenüber dem Deutschen Städtetag.

Denn: Auskunftspflichtig nach § 1 Abs. 1 Satz 1 IFG sind nur Behörden des Bundes. Das IFG gewährt keinen Anspruch auf Informationszugang gegenüber privaten oder juristischen Personen des Privatrechts. Eine solche ist der Städtetag als zivilrechtliche Vereinigung von Kommunen. Private sind ausnahmsweise und nur dann zur Gewährung des Informationszuganges verpflichtet, wenn sie als sog. Beliehene hoheitliche Aufgaben für den Bund wahrnehmen und damit funktional als Behörde tätig werden. Der Deutsche Städtetag ist ein freiwilliger Zusammenschluss von kreisfreien und kreisangehörigen Städten in Deutschland. Er nimmt als kommunaler Spitzenverband die Interessen der Städte wahr. Bundesaufgaben sind dem Städtetag nicht übertragen worden. Der Städtetag ist deshalb auch kein sonstiges Bundesorgan und auch keine sonstige Bundeseinrichtung, die nach dem Wortlaut des § 1 Abs. 1 Satz 2 IFG grundsätzlich zur Gewährung des Informationszuganges verpflichtet wäre.

Dem Petenten habe ich letztlich empfohlen, den Antrag auf Informationszugang an eine Stadt zu richten, die Mitglied im Deutschen Städtetag ist und einem Landesgesetz zur Informationsfreiheit unterliegt.

## **8.2 Rechtsprechung**

Auch im Berichtsjahr 2020 haben die Gerichte einen wesentlichen Beitrag zur Konkretisierung und Fortentwicklung des Informationsfreiheitsrechtes geleistet. Nicht nur die mehr als 45.000 IFG-Antragstellenden hatten ein großes Interesse an der Entscheidung des LG Köln zur Glyphosat-Stellungnahme des Bundesamtes für Risikobewertung.

Das VG Berlin stellte klar, dass Direktnachrichten aus dem Twitter-Account des Bundesministeriums des Innern und für Heimat amtliche Informationen im Sinne des IFG sind.

#### **8.2.1 Streit um die Veröffentlichung einer Stellungnahme zu Glyphosat: Berechtigter Schutz geistigen Eigentums oder Zensur?**

Inwieweit kann sich eine Behörde auf das Urheberrecht berufen, um die Weiterverbreitung amtlicher Informationen zu untersagen?

Reichweite und Bedeutung des Urheberrechtsschutzes für die Informationsfreiheit sind noch nicht umfassend geklärt. Umstritten ist insbesondere, inwieweit Behörden sich darauf berufen können. Im teilweise öffentlich geführten Streit fielen sogar Schlagworte wie „Zensur“ und „Zensur(ur)heberrecht“.

Gegenstand des Streites ist eine Ausarbeitung zum Herbizid Glyphosat. Das Bundesinstitut für Risikobewertung (BfR) hatte mit eigenen Mitarbeitern eine „Stellungnahme“ zu einer 95-seitigen englischsprachigen Monographie der Internationalen Agentur für Krebsforschung (International Agency for Research on Cancer – IARC) zu Glyphosat verfasst. Die sechsseitige Stellungnahme stellt eine Zusammenfassung dar und enthält Übersetzungen von durch das BfR ausgewählten Passagen der Monographie.

Das BfR erhielt seit März 2019 mehr als 45.000 IFG-Anträge auf Zugang zu der Stellungnahme. Daraufhin entschied das BfR durch Allgemeinverfügung, jeder antragstellenden Person das Dokument über eine Internetseite des BfR bereitzustellen. Der Zugang erfolgte dabei über einen auf sieben Tage befristeten individuellen Lesezugang; Speichern, Weiterleiten und Ausdrucken des Dokuments waren nicht möglich. Einer Veröffentlichung widersprach das BfR ausdrücklich. Das BfR wählte diese Art des Informationszugangs, um einerseits dem IFG zu genügen und andererseits das von ihm als wissenschaftliches Institut in Anspruch genommene Urheberrecht zu wahren.

Einige Petenten wandten sich an mich, da sie sich durch die Art und Weise der Bereitstellung des Dokuments unter zeitlicher Limitierung und Ausschluss der Ver-

öffentlichung in ihrem Recht auf Informationszugang nach dem IFG als verletzt ansahen. Damit stand nicht der Informationszugang als solcher im Streit, sondern die auf das Urheberrecht gestützten Beschränkungen der Verwendung, insbesondere der Veröffentlichung.

Ein Verein – die Open Knowledge Foundation (OKF) – hatte die Stellungnahme über einen IFG-Antrag vom BfR erhalten, wobei dieses jedoch die weitere Veröffentlichung unter Zustimmungsvorbehalt gestellt hatte. Der Verein stellte das Dokument – ohne Zustimmung des BfR – in einem redaktionellen Artikel auf seiner Internetseite „Frag den Staat“ öffentlich zugänglich ein. Das BfR mahnte den Verein ab und forderte gerichtlich Unterlassung. Vor dem Landgericht Köln (LG Köln) hatte die Klage keinen Erfolg.

Das LG Köln urteilte am 12. November 2020 (Az. 14 O 163/19), die Veröffentlichung der Stellungnahme stelle keine Urheberrechtsverletzung. Das Gericht begründet seine Entscheidung damit, dass das BfR seine Stellungnahme selbst veröffentlicht habe, indem es dem IFG-Antrag stattgab. Die Information sei damit nicht nur einer beschränkten und bestimmten Anzahl an Personen, sondern der Allgemeinheit zugänglich gemacht worden. Daraus folge die Zustimmung zur weiteren Veröffentlichung. Das Publizieren durch den Verein in einem Artikel sei ein nach § 51 Urheberrechtsgesetz (UrhG) zulässiges „Zitat“. Zudem sei spätestens mit Veröffentlichung der Allgemeinverfügung im Bundesanzeiger das Gutachten als amtliches Werk im Sinne des § 5 Abs. 2 UrhG zu qualifizieren. Die Allgemeinverfügung belege, dass es dem BfR nicht auf eine Beschränkung des Empfängerkreises angekommen sei.

Das LG Köln führt die Diskussion zum Verhältnis von Urheberrechtsschutz und IFG in interessanter Weise fort. Die Entscheidung ist auch deswegen von besonderem Interesse, da über den Fragenkreis bislang noch nicht höchststrichterlich entschieden ist. Nach der Argumentation des LG kann bereits eine einfache Zugangsgewährung nach dem IFG eine Veröffentlichung im Sinne des Urheberrechtes darstellen. Wenn dies für jede Informationszugangsgewährung gilt, wäre dies eine erhebliche Stärkung des Rechtes auf Informationsfreiheit gegenüber Behörden, welche die weitere Nutzung von Informationen unter Berufung auf ihre Urheberrechte beschränken wollen. Zum Redaktionsschluss meines Tätigkeitsberichtes war das Urteil noch nicht rechtskräftig.

### **8.2.2 Was gilt? Das Parteiengesetz oder das Informationsfreiheitsgesetz?**

Ist das Parteiengesetz eine spezialgesetzliche Regelung im Sinne des Informationsfreiheitsgesetzes (IFG)? Das Bundesverwaltungsgericht hat nun entschieden.

Ein Petent hatte mich um Vermittlung gebeten, weil der Deutsche Bundestag seinen Antrag auf Übersendung von Korrespondenzen, Vermerken, Notizen und Dienstabweisungen im Zusammenhang mit Rechenschaftsberichten und Parteispenden für die Jahre 2013 und 2014 abgelehnt hatte.

Seine Ablehnung des Informationszugangs stützte der Deutsche Bundestag auf das Parteiengesetz (PartG), das als spezialgesetzliche Regelung des Informationszugangs nach § 1 Absatz 3 IFG die Anwendung des IFG und damit den Informationszugang nach dem IFG ausschließt.

Hierzu habe ich bereits im 4. Tätigkeitsbericht zur Informationsfreiheit eine andere Rechtsauffassung vertreten:

Zwar haben nach § 1 Absatz 3 IFG spezialgesetzliche Zugangsregelungen Vorrang, und das unabhängig davon, ob sie ein engeres oder ein weiteres Zugangsrecht gewähren. Dies gilt jedoch nur, soweit der Anwendungsbereich der Spezialnorm reicht und sie als abschließende Regelung anzusehen ist. Im Übrigen bleibt das IFG anwendbar.

Die vom Deutschen Bundestag in Bezug genommen Regelungen der §§ 23 ff. PartG sehe ich als objektive Transparenzregelungen und deshalb nicht als bereichsspezifische, spezielle Zugangsregelungen, die den Informationszugang nach dem IFG ausschließen (vgl. 4.TB IFG, Nr. 5.1.3).

Der Petent hatte gegen die ablehnende Entscheidung des Deutschen Bundestages geklagt und war damit auch in den ersten beiden Instanzen erfolgreich. Sowohl das VG Berlin als auch das OVG Berlin-Brandenburg entschieden, dass „die Vorschriften über die Rechenschaftslegung der politischen Parteien im PartG keine vorrangigen Spezialregelungen im Sinne des § 1 Abs. 3 IFG sind, die dem Informationsfreiheitsgesetz vorgehen und Sperrwirkung entfalten“ (vgl. VG Berlin, 2 K 69.16 vom 26.01.2017, OVG Berlin-Brandenburg, 12 B 6.17 vom 26.04.2018).

Anders als die Vorinstanzen bewertet das BVerwG die Transparenzregelungen des PartG als „ein in sich geschlossenes Regelungskonzept zur Veröffentlichung von Informationen, die im Zusammenhang mit der Rechenschaftslegung der Parteien und der Entwicklung der Parteifinancen stehen“ und sieht deshalb den Informationszugang nach dem IFG als ausgeschlossen an (BVerwG, Urt. v. 17.06.2020, Az 10 C 16.19).

### **8.2.3 Social-Media und die Informationsfreiheit**

Auch die über Social-Media ausgetauschten Nachrichten von Bundesbehörden können Gegenstand eines Antrags auf Informationszugang nach dem Informationsfreiheitsgesetz sein.



Ein Antragsteller beehrte vom Bundesministerium des Innern, für Bau und Heimat (BMI) Zugang zu den über dessen Twitter-Account ausgetauschten Direktnachrichten. Nachdem das BMI den Zugang verweigerte, erhob der Antragsteller Klage vor dem Verwaltungsgericht Berlin und bekam dort Recht (VG Berlin, Urteil vom 26. August 2020, VG 2 K 163.18). Nach Auffassung des Gerichts handelt es sich auch bei Twitter-Direktnachrichten um amtliche Informationen, da diese nicht ausschließlich und eindeutig privaten (persönlichen) Zwecken dienen. Dabei spiele es auch keine Rolle, dass diese nicht Bestandteil eines Verwaltungsvorgangs geworden seien. Auch die Frage, ob die Informationen beim BMI überhaupt vorhanden sind, bejahte das Gericht, da das BMI diese noch über seinen Twitter-Account abrufen könne. Unerheblich sei in diesem Zusammenhang, dass die Nachrichten nicht auf eigenen Servern des BMI abgelegt seien. Im Übrigen wies das Gericht auch die seitens des BMI geltend gemachten Ausschlussgründe zurück.

Sofern diese Rechtsprechung Bestand hat, könnten auch andere Bereiche der Kommunikation von Bundesbehörden hiervon erfasst werden. Besondere Bedeutung kommt dabei der Tatsache zu, dass es für einen Informationszugang keiner Veraktung in einem Verwaltungsvorgang bedarf, sondern auch anderweitig gespeicherte Informationen Gegenstand eines Informationszugangsbegehrens sein können. Dies betrifft insbesondere auch die Nutzung von Kommunikationskanälen jenseits der klassischen E-Mail, wie etwa Messenger-Dienste oder SMS. Sofern entsprechende Nachrichten noch abrufbar und somit vorhanden sind, käme ein Anspruch auf Herausgabe grundsätzlich in Betracht.

Das BMI hat gegen die Entscheidung Revision beim Bundesverwaltungsgericht eingelegt. Die weitere Entwicklung bleibt somit abzuwarten.

## 8.3 Statistik zur Informationsfreiheit

In 2020 setzte sich die kontinuierliche Steigerung meiner Vermittlungstätigkeit gegenüber den Vorjahren fort.

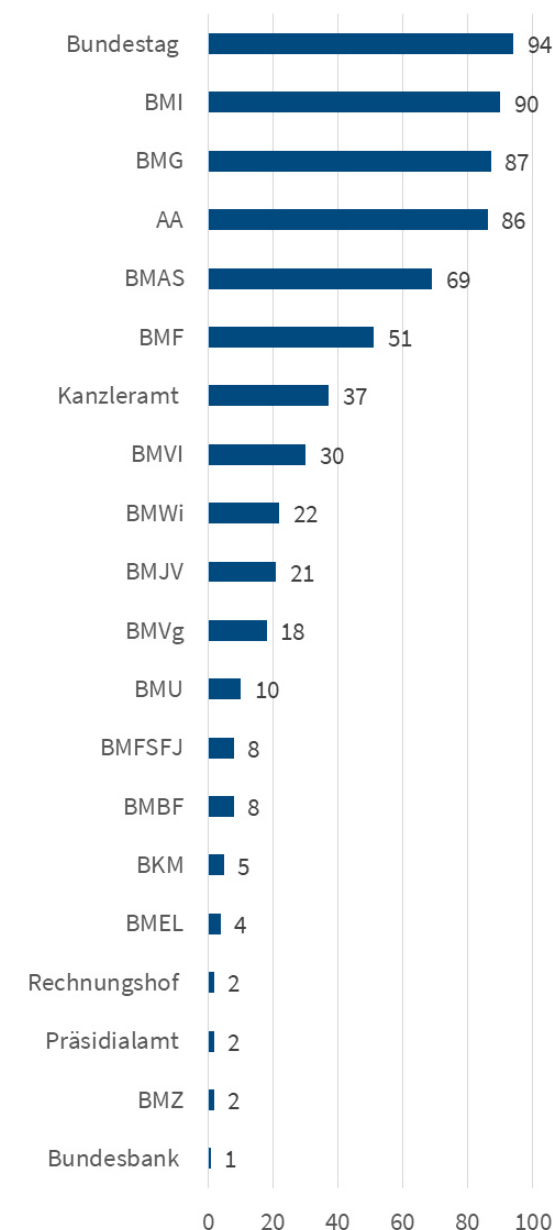
Mich erreichten im Berichtszeitraum insgesamt 900 Eingaben. Dies entspricht einem Anstieg von rund 12 Prozent.

In 647 Fällen riefen mich Petenten als Ombudsperson nach § 12 Abs. 1 IFG an. Sie sahen ihr Recht auf Informationszugang nach dem IFG verletzt, weil Informationen nicht, nicht rechtzeitig und/oder unter Berechnung überhöhter Gebühren zugänglich gemacht worden waren. Damit wurde ich im Berichtsjahr deutlich häufiger um Vermittlung gebeten als im Jahr 2019. Damals gingen

461 Anrufungen ein. Dies entspricht einem Anstieg um 47 Prozent.

Bezogen auf die Ressorts verteilten sich die Eingaben auch anders als in vergangenen Perioden (siehe nachfolgende Grafik). Schwerpunkte lagen diesmal bei der IFG-Bearbeitung durch die Bundestagsverwaltung, durch das Bundesministerium des Innern und das Auswärtige Amt. Ein weiterer Schwerpunkt waren IFG-Anträge an das Bundesministerium für Gesundheit, was am starken Interesse der Antragsteller nach Informationen im Zusammenhang mit der Corona-Pandemie liegt. Antragsinhalte waren hier unter anderem das Risikomanagement bei Coronaerkrankungen, Quarantänebestimmungen und Kontaktpersonen-Nachverfolgung.

Anrufungen nach § 12 Abs. 1 IFG





Neben den Anrufen wegen Verletzung des Rechtes auf Informationszugang waren im Berichtszeitraum auch zahlreiche allgemeine Anfragen zu bearbeiten, mit denen ich meist um Rechtsauskünfte zum IFG oder anderen Regelungen des Informationsfreiheitsrechtes oder um Vermittlung auch außerhalb meiner Zuständigkeit gebeten wurde.

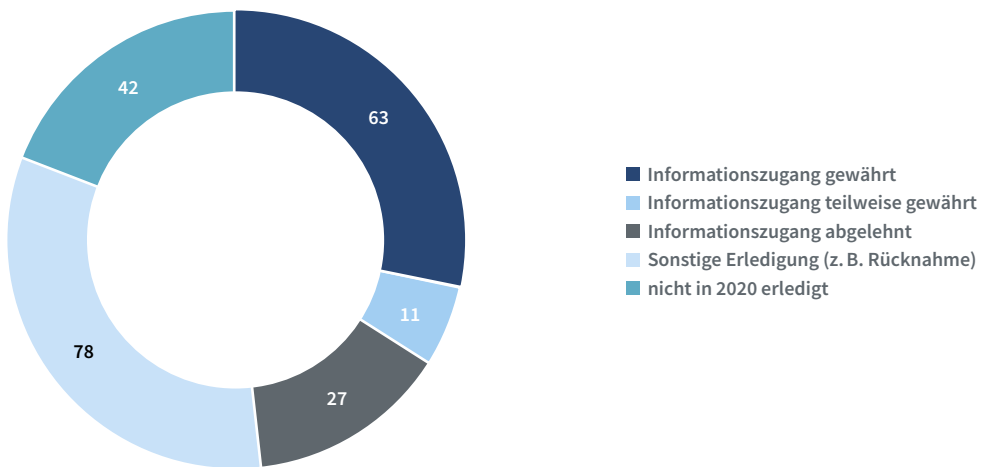
#### IFG-Anträge an meine Behörde

Im Berichtszeitraum gingen insgesamt 221 Anträge auf Zugang zu amtlichen Informationen in meiner Behörde

ein. Im Vergleich zu den Vorjahren bleibt das Aufkommen auf hohem Niveau stabil. Die Anträge richteten sich u.a. auf die Bereitstellung von Berichten zu Beratungs- und Kontrollbesuchen und meine Stellungnahmen zu oftmals datenschutzrechtlich sensiblen Gesetzesvorhaben, aber auch zu meinen Akten zu einzelnen Vermittlungsverfahren. Aus der Abbildung ergibt sich die Verteilung der Zugangsgewährung, der Zugangsablehnung und der sonstigen Erledigung im Berichtszeitraum.

---

#### IFG-Anträge an meine Behörde



# 9 Kontrollen und Auswirkungen

Bedingt durch die Regeln zur Bekämpfung des Corona-Virus konnten im Jahr 2020 nur wenige der eigentlich geplanten Vor-Ort-Kontrollen durchgeführt werden. Aus diesem Grund wurden vermehrt neue Arten von Kontrollen, wie z.B. die Fragebogenkontrolle eingesetzt.

## 9.1 Fragebogenkontrolle zur Authentifizierung bei Call-Centern

Bei einer telefonischen Hotline kann man keinen Ausweis vorzeigen. Wie kann und muss ein Telekommunikationsunternehmen feststellen, ob tatsächlich der Kunde anruft?

Ein Stalking-Fall, bei dem eine Ex-Lebenspartnerin die neue Handynummer ihres früheren Lebensgefährten an der Telefon-Hotline eines Telekommunikationsanbieters erhalten hatte, indem sie sich – ohne dabei vorzugeben, der Vertragspartner selbst zu sein – mit dessen Geburtsdatum authentifiziert hatte, zeigt auf, dass die Authentifizierung beim telefonischen Service nicht immer ausreichend durchgeführt wird. Gegen das betroffene Unternehmen habe ich ein Bußgeld verhängt, wogegen das Unternehmen gerichtlich vorging. In diesem Verfahren wurden verschiedene grundsätzliche Rechtsfragen geklärt (s. Nr. 10.2). Unter anderem hat das Gericht meine Auffassung bestätigt, dass ein Verstoß gegen die Anforderungen zur Sicherheit der Verarbeitung gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO) vorlag.

Das Geburtsdatum ist vielen Personen aus dem privaten und beruflichen Umfeld bekannt und somit ungeeignet, um die Datenherausgabe oder eine Veränderung von personenbezogenen Daten bei einem Anruf zu legitimieren. Die Anforderungen der DSGVO, technische und organisatorische Maßnahmen zur Datensicherheit zu treffen, werden damit nicht erfüllt. In dem konkreten Fall hatte das Unternehmen vorgebracht, dass es eine

„Zwei-Faktor-Authentifizierung“ mit den „Faktoren“ Name und Geburtsdatum durchführen würde. Im Bereich der Informationssicherheit wird der Begriff „Faktor“ jedoch anders verwendet. Neben den Daten, die zur Identifizierung einer Person erforderlich sind, z. B. Name mit Adresse, Kundennummer oder Benutzername, sind die Faktoren

- Wissen (ein Geheimnis, z.B. Passwort oder PIN),
- Besitz (z.B. eine Chipkarte oder ein TAN-Generator) und
- Biometrie (z.B. ein Fingerabdruck)

notwendig.

Am einfachsten zu realisieren ist meist ein Geheimnis, z. B. durch ein Passwort. Dabei muss dem Nutzer bewusst sein, dass es sich um ein Geheimnis handelt. Dies kann derzeit in vielen Bereichen als noch ausreichende Maßnahme betrachtet werden. Allerdings wird z.B. durch betrügerische E-Mails und gefälschte Websites versucht, Zugangsdaten auszuspionieren. Insofern ist eine Zwei-Faktor-Authentifizierung anzustreben, insbesondere, wenn eine höhere Sicherheit erreicht werden muss (vgl. dazu auch den Katalog von Sicherheitsanforderungen der Bundesnetzagentur, der im Berichtszeitraum überarbeitet wurde<sup>22</sup>). Kundennummern und ähnliches können bei einer Authentifizierung nicht als ein Geheimwissen angesehen werden, höchstens als sogenannte Spezialwissen.

Ausgehend von diesem Vorfall habe ich bei den großen Telekommunikationsunternehmen eine schriftliche Fragebogenkontrolle zu den dortigen Verfahren der Authentifizierung von Anrufern durchgeführt. Auch wenn diese Kontrollen noch nicht alle vollständig abgeschlossen sind, so lässt sich doch schon jetzt folgendes festhalten: Die Mehrheit der kontrollierten Unternehmen nutzt Passwörter oder vergleichbar sichere Verfah-

22 Siehe Abschnitt 3.1 in Anlage 1 des Katalogs von Sicherheitsanforderungen. Siehe: Amtsblatt der BNetzA 24/2020, Mitteilung Nr. 427/2020

ren wie eine PIN. Allerdings wurde oft eine Alternative für ein vergessenes Passwort angeboten, bei dem nur die Kundennummer oder ähnliche Daten, die nicht als Geheimwissen zu werten sind, für eine Authentifizierung herangezogen werden. Solche Verfahren sind zwar eindeutig besser als allein Name und Geburtsdatum abzufragen, dennoch kann ich auch sie nicht als ausreichend bewerten. Die entsprechenden Unternehmen – aber selbstverständlich auch alle nicht zu dieser Fragestellung kontrollierten Telekommunikationsunternehmen – sind aufgefordert, zeitnah sichere und dem Stand der Technik entsprechende Verfahren umzusetzen.

Bei zwei Unternehmen musste ich feststellen, dass ähnlich unsichere Verfahren zur Authentifizierung wie im Ausgangsverfahren im Einsatz sind, so dass ich entsprechende Abhilfemaßnahmen prüfe.

Alle Unternehmen sind dazu verpflichtet, ausreichend sichere Verfahren anzubieten. Dabei sind Verfahren regelmäßig zu überprüfen und anzupassen, wenn die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nicht (mehr) ausreichen.

#### Querverweis:

10.2 Urteil des Landgerichts Bonn bestätigt Rechtsauffassung des BfDI

## 9.2 Fragebogenkontrolle Handscanner

In der zweiten Jahreshälfte habe ich eine Fragebogenkontrolle bei 30 Paketdienstleistern durchgeführt, um den datenschutzkonformen Einsatz von Handscannern zu prüfen.

Die Zustellkräfte der Paketdienstleister nutzen mobile Datenerfassungsgeräte, um die Übergabe von Sendungen an den Empfänger zu dokumentieren und direkt an das Warenwirtschaftssystem zu übermitteln. Mich erreichten immer wieder Eingaben von Bürgerinnen und Bürgern, die befürchteten, dass mit diesen Geräten Fingerabdrücke erfasst, unerlaubt Bild- und Tonaufnahmen gefertigt oder Ausweisdaten unerlaubt erfasst werden. Oftmals konnten begründete Fragen der Sendungsempfänger von den sich stets in Eile befindlichen Zustellkräften nicht beantwortet werden.

Das Postgesetz erlaubt den Dienstleistern, gewisse personenbezogene Daten zu erheben, um eine ordnungsgemäße Zustellung oder eine erfolgte Altersverifikation zu dokumentieren. Dazu zählen unter anderem die Ausweisnummer, das Ablaufdatum des Ausweisdokumentes, die Unterschrift des Empfängers und gegebenenfalls

auch der Name eines Ersatzempfängers. Die Postdienstleister verwenden hierzu jeweils unterschiedliche Geräte und Verfahren. Zudem werden die Zustellungen während der Corona-Pandemie anders dokumentiert, um eine kontaktarme Zustellung zu ermöglichen. Dies hat zu einer weiteren Verunsicherung der Sendungsempfänger beigetragen.

Ich habe den Unternehmen einen umfassenden, strukturierten Fragebogen zu den jeweils eingesetzten Geräten, deren Anbindung an das Sendungsverfolgungssystem und zur Prüfung der datenschutzkonformen Verarbeitung personenbezogener Daten übermittelt.

Das Ergebnis der Fragebogenkontrolle ist positiv. Die Geräte, die Software und die dahinterliegenden Prozesse arbeiten datenschutzkonform – so werden beispielsweise niemals biometrische Daten wie Fingerabdrücke erfasst. In den meisten Fällen ist dies durch die eingesetzten Geräte – mangels Fingerabdruckscanner – technisch überhaupt nicht möglich. Einzelne, mir im Voraus bekanntgewordene Verstöße gegen den Datenschutz, sind in der Regel auf Fehlbedienungen zurückzuführen, wodurch z.B. einem Empfänger fehlerhafte Daten in der Sendungsverfolgung angezeigt werden. Strukturelle datenschutzrechtliche Mängel, etwa Möglichkeiten der ungewollten Datenweitergabe an Dritte oder eine Erfassung von zu vielen personenbezogenen Daten, konnten nicht festgestellt werden. Die von den Zustellkräften der Paketdienstleister genutzten Handscanner werden datenschutzkonform eingesetzt.

## 9.3 Änderung der Organisation des behördlichen Datenschutzes im Bundesministerium der Verteidigung

Defizite im Hinblick auf die Unabhängigkeit des behördlichen Datenschutzbeauftragten im Bundesministerium der Verteidigung wurden durch meine Intervention beseitigt.

Im Rahmen eines Beratungs- und Kontrollbesuchs wurde die Organisation des behördlichen Datenschutzes (BfDBw) im Bundesministerium der Verteidigung (BMVg) bewertet. Meine Mitarbeiterinnen und Mitarbeiter haben festgestellt, dass die bisherige organisatorische Stellung und Einbindung der BfDBw innerhalb des BMVg deren Unabhängigkeit und Weisungsfreiheit unangemessen einschränkt. Insbesondere das fehlende unmittelbare Vortragsrecht bei der Hausleitung und die Einbindung in die ministerielle Linienorganisation stießen auf datenschutzrechtliche Bedenken. Auch die Abläufe bei der Genehmigung von Dienstreisen

und Fortbildungen der BfDBw und ihrer Mitarbeiterinnen und Mitarbeiter, ihrer jeweiligen dienstlichen Beurteilung sowie der organisatorischen Einbindung der Außenstellen waren mit der gesetzlich normierten Unabhängigkeit der BfDBw unvereinbar. In der Folge der datenschutzrechtlichen Kontrolle wurde das unmittelbare Vortragsrecht der BfDBw gegenüber der Hausleitung in der Geschäftsordnung des BMVg festgeschrieben. Die BfDBw wurde aus der Linienorganisation des BMVg herausgelöst und direkt dem Büro des Staatssekretärs unterstellt. Für die unabhängige Wahrnehmung ihrer Aufgaben wurden der BfDBw eine Dauerdienstreisegenehmigung für das Inland erteilt sowie weitreichendere Möglichkeiten in Bezug auf Auslandsdienstreisen und Fortbildungsmaßnahmen eingeräumt. Zur Sicherstellung der Unabhängigkeit ihrer Mitarbeiterinnen und Mitarbeiter wurde der BfDBw deren dienstliche Beurteilung übertragen. Die dienstliche Beurteilung der BfDBw selbst erfolgt künftig durch den Staatssekretär. Zwecks Wahrung der unabhängigen Aufgabenerfüllung in den Außenstellen der BfDBw wurden die dort angesiedelten Dienstposten der BfDBw unterstellt. Durch diese Maßnahmen wurden die Unabhängigkeit der BfDBw und damit der Datenschutz innerhalb der Bundeswehr nachhaltig gestärkt.

## 9.4 Beratungs- und Kontrollbesuche zur Anwendung des Informationsfreiheitsgesetzes

**Meine Kontroll- und Beratungsbesuche bei der Bundeszentrale für politische Bildung und beim Technischen Hilfswerk führten zu erfreulichen Ergebnissen.**

### **Bundeszentrale für politische Bildung**

Mein Kontrollbesuch bei der Bundeszentrale für politische Bildung (bpb) zeigte, dass die Anwendung des Informationsfreiheitsgesetzes (IFG) bürger- und serviceorientiert erfolgt und die Verfahrensvorschriften sowie die materiell-rechtlichen Vorgaben des IFG beachtet werden. Die Kontrolle erfolgte auf Grundlage der Auswertung eines Großteiles der IFG-Verfahrensakten aus den Jahren 2016 bis 2020. Die Bearbeitung von IFG-Anträgen und die Beteiligung der Fachreferate erfolgt konzentriert bei der Stabstelle Kommunikation, die auch als Pressestelle fungiert und zudem für Bürgeranfragen zuständig ist. Damit werden eine schnelle und zuverlässige Zuordnung sowie eine sachkundige und serviceorientierte Bearbeitung der unterschiedlichen Informationsbegehren gewährleistet. Die Antragsbearbeitung erfolgt durchgehend rasch und die Entscheidung und der Informationszugang erfolgen regelmäßig problemlos innerhalb der Monatsfrist.

### **Technisches Hilfswerk**

Auch das technische Hilfswerk (THW) zeigt einen bürger- und serviceorientierten Umgang mit IFG-Anträgen und beachtet die materiellen sowie die formellen Anforderungen des IFG. Ich konnte alle IFG-Verfahrensakten von 2016 bis August 2020 einsehen. IFG-Anträge werden zentral in der THW-Leitung in Bonn bearbeitet. Sofern IFG-Anträge bei den nicht selbständigen acht Landes- bzw. 668 Ortsverbände des THW eingehen, sind diese an das zuständige zentrale Referat weiterzuleiten. Die Bearbeitung nach Weiterleitung erfolgt durchweg zügig. Die Prüfung der Aktenführung ergab keine Auffälligkeiten. Zu Einzelpunkten der Praxis, wie z.B. Gebühren, gab ich beratende Hinweise und Anregungen. Am Beispiel von IFG-Anträgen aus dem Kreise der Helfer ließ ich mir vom THW die Umsetzung des Datenschutzes in IFG-Verfahren erläutern; Hinweise auf Unregelmäßigkeiten, wie z.B. standardisierte Abgleiche mit zweckfremden Daten, ergaben sich für mich nicht. Basisinformationen zum Informationszugang stellt das THW online bereit.

## 9.5 Kontrollen im Sicherheitsbereich

Neben gesetzlich vorgeschriebenen Pflichtkontrollen – diesmal beim Bundesamt für den Militärischen Abschirmdienst – habe ich trotz der pandemiebedingten Einschränkungen einige wichtige Beratungs- und Kontrollbesuche im Sicherheitsbereich durchführen können. Unter anderem wurde dabei die Datenübermittlung an Sicherheitsbehörden in Drittstaaten sowie die Umsetzung der Vorgaben des Sicherheitsüberprüfungsgesetzes in den Fokus genommen.

### **9.5.1 Kontrollen und Beanstandungen im Bereich des Bundesamtes für Verfassungsschutz**

Beim Bundesamt für Verfassungsschutz (BfV) habe ich im Berichtszeitraum Datenverarbeitungen im Zusammenhang mit Ausschreibungen im Schengener Informationssystem der 2. Generation (SIS II), mit Recherchen im Visa-Informationssystem (VIS) und mit Datenübermittlungen des Bundesamtes für Migration und Flüchtlinge (BAMF) kontrolliert.

#### **Kontrolle verdeckter Ausschreibungen im SIS II**

Im ersten Quartal habe ich beim BfV verdeckte Ausschreibungen im SIS II kontrolliert. Das BfV kann Ausschreibungen im SIS II veranlassen, wenn die darüber zu gewinnenden Informationen zur Abwehr einer von der betroffenen Person ausgehenden erheblichen Gefährdung oder anderer erheblicher Gefahren für die Sicherheit des Staates erforderlich sind. Neben Dokumenta-

tionsdefiziten fiel in den kontrollierten Vorgängen vor allem auf, dass der zwischen den beteiligten Behörden ausgetauschte Datenumfang nicht von den europäischen Vorschriften zum SIS II gedeckt ist. Auch die Speicher- und Löschprozesse bedürfen nach Maßgabe der gesetzlichen Anforderungen einer Überarbeitung.

Bis zum Zeitpunkt des Redaktionsschlusses ist eine Stellungnahme zu meinem Kontrollbericht seitens des zuständigen Bundesministeriums des Innern, für Bau und Heimat (BMI) nicht eingegangen. Für das Jahr 2021 erwarte ich eine weitergehende konstruktive Diskussion zu meinen Feststellungen und den hieraus erforderlich werdenden Änderungen der Datenverarbeitungen im BfV.

### **Kontrolle von Recherchen im VIS**

Außerdem habe ich ebenfalls Anfang 2020 Recherchen des BfV im VIS kontrolliert. Derartige Recherchen kann das BfV vornehmen, wenn sie zur Verhütung oder Aufdeckung schwerwiegender Straftaten einen erheblichen Beitrag leisten und erforderlich sind. Bei der Kontrolle ist u. a. auffällig gewesen, dass die Dokumentation und Überprüfung des Vorliegens der Recherchevoraussetzungen nicht den gesetzlichen Vorgaben entspricht und die Speicherdauer der recherchierten Daten differenzierter ausgestaltet werden muss.

Die Stellungnahme des BfV bzw. des BMI erreichte mich kurz vor Ende des Redaktionsschlusses. Ich werde diese nun auswerten und gehe davon aus, dass sich auch hieran ein weiterer Austausch über ggf. noch notwendige Anpassungen der Datenverarbeitungen anschließt.

### **Kontrolle von Datenübermittlungen zwischen BAMF und BfV**

Im dritten und vierten Quartal habe ich des Weiteren Aspekte der Datenübermittlungen des BAMF an das BfV gemäß § 18 Abs. 1a S. 1 BVerfSchG geprüft. Das BAMF darf dem BfV Informationen über Personen übermitteln, die es bei Wahrnehmung seiner Aufgaben erhebt, wenn es tatsächliche Anhaltspunkte dafür feststellt, dass sie zur Sammlung und Auswertung von verfassungsfeindlichen Bestrebungen oder Tätigkeiten im Sinne des § 3 Absatz 1 BVerfSchG erforderlich sind. Die Kontrolle hat u. a. ergeben, dass die in der Praxis seitens des BfV aufgestellten Kriterien, bei deren Vorliegen das BAMF eine Übermittlung vornimmt, überarbeitet werden müssen. Die Kriterien gewährleisten nicht für jeden Fall, dass tatsächliche Anhaltspunkte für eine Aufgabenrelevanz des BfV bestehen. Auch hierüber werden im weiteren Verlauf mit dem BfV und dem BMI als Fachaufsicht noch Gespräche geführt werden.

### **9.5.2 Kontrolle der Anti-Terror Datei**

Beim Bundesamt für den Militärischen Abschirmdienst habe ich eine Pflichtkontrolle zur Nutzung der Anti-Terror-Datei durchgeführt. Auf Grundlage der Erkenntnisse der Kontrolle im Jahr 2018 habe ich zusätzlich die Möglichkeit und Auswirkung eines additiven Grundrechtseingriffs nachverfolgt. Dabei entstand ein erheblicher Kontrollaufwand.

Bei der diesjährigen Kontrolle der Anti-Terror-Datei (ATD) beim Bundesamt für den Militärischen Abschirmdienst (BAMAD) wurden keine Datenschutzverstöße festgestellt. Dasselbe gilt für die im Jahr 2018 durchgeführte Kontrolle. Im Nachgang zu dieser Kontrolle habe ich allerdings im Jahr 2019 und jetzt abschließend im Jahr 2020 eine Prüfung auf sog. additive Grundrechtseingriffe durchgeführt.

Im Zuge der Beteiligung mehrerer Behörden an der ATD können Datensätze zu einer Person von mehreren Stellen genutzt und gespeichert werden. Beteiligte Behörden sind nach § 1 Abs. 1 ATDG neben Bundesbehörden auch die Landeskriminalämter und Verfassungsschutzbehörden der Länder. Dadurch kann ein sogenannter additiver Grundrechtseingriff entstehen, insbesondere wenn neben der Speicherung in der ATD ein und dieselbe Person von verschiedenen Behörden gleichzeitig mit nachrichtendienstlichen oder polizeilichen Mitteln beobachtet wird. Maßnahmen, die isoliert betrachtet verhältnismäßig sind, können so ggf. unverhältnismäßig werden.

Um dies beurteilen zu können, ist eine Gesamtschau und ein Zusammenwirken verschiedener Aufsichtsbehörden notwendig. Ich habe deshalb im Berichtszeitraum im Zusammenhang mit der Kontrolle im Jahr 2018 das Bundeskriminalamt um Übermittlung der Protokolldaten gebeten, die darüber Aufschluss geben, welche Behörden Suchanfragen mit Treffern zu den vom BAMAD gespeicherten Datensätzen gestellt bzw. erzielt haben. Im Ergebnis konnten mehrere Bundes- und Landesbehörden festgestellt werden. Daraufhin habe ich die für diese Behörden zuständigen Landesdatenschutzbeauftragten (LfD) angeschrieben und um Prüfung gebeten, weil die Kontrolle der Suchanfragen von Landesbehörden zu Datenbeständen von Bundesbehörden in der Zuständigkeit der jeweiligen LfD liegt. Meine Kolleginnen und Kollegen in den zuständigen Landesbehörden haben mich bei dieser Prüfung auch entsprechend unterstützt.

Inhaltlich konnten im Ergebnis weder datenschutzrechtlichen Verstöße noch additive rechtswidrige Grundrechtseingriffe festgestellt werden. Die Prüfung, ob additive Grundrechtseingriffe vorlagen, führte allerdings zu unterschiedlichen Ergebnissen. Teilweise resultierten aus den Suchanfragen mit Treffern keine weiteren Maßnahmen seitens der anfragenden Behörde. Zum



Teil waren die zugrundeliegenden Daten mittlerweile – rechtmäßig – gelöscht, da der Abfragezeitpunkt schon länger zurücklag. Auch stellten sich technisch-organisatorische Herausforderungen, die eine Prüfung durch die LfD erschwerte. Andere Abfragen blieben ohne positives Ergebnis, d.h. offenbar stimmte die gesuchte Person nicht mit der seitens BAMAD gespeicherten Person überein.

Insgesamt zeigte sich, dass diese Art der Prüfung einen erheblichen zusätzlichen Aufwand bedeutet. Ich habe für den gesamten Vorgang einen Zeitraum von ca. acht Monaten benötigt. Bei einer alle zwei Jahre durchzuführenden datenschutzrechtlichen Kontrolle der ATD bei den beteiligten Bundesbehörden stellt dieser zeitliche Aspekt eine große Hürde zur Bewertung eines möglichen additiven Grundrechtseingriffs dar.

Im Tätigkeitsbericht 2017-2018 hatte ich bereits festgestellt, dass der Aufwand, den die Behörden bei der Speicherung, Pflege und Löschung der Daten aus ATD und RED betreiben, sehr hoch ist und für diese offenbar in keinem Verhältnis zum Nutzen steht (vgl. 27. TB Nr. 9.3.5 und 9.3.11). Trotz der sich einstellenden Routine bei der Kontrolle dieser Dateien auf Seiten des BfDI bleibt der Aufwand auch in meiner Behörde ebenfalls hoch. Da die Kosten-Nutzen-Analyse für die einspeichernden Behörden so negativ ausfällt, empfehle ich weiterhin, beide Dateien abzuschaffen.

### 9.5.3 Das Vorgangsbearbeitungssystem beim BKA

Das Vorgangsbearbeitungssystem (VBS) ist ein zentrales Werkzeug für die tägliche Arbeit des Bundeskriminalamtes (BKA) mit elektronischen Informationen. Seine aktuelle Ausgestaltung weist nach wie vor erhebliche datenschutzrechtliche Mängel auf.

Das VBS dient der Erstellung und Bearbeitung von Vorgängen. Es bietet darüber hinaus verschiedene, für die polizeiliche Sachbearbeitung relevante Funktionalitäten wie die Vorgangsverwaltung und Dokumentation sowie Recherchemöglichkeiten in den dort erfassten Daten etc.

Bei einem früheren Beratungs- und Kontrollbesuch habe ich erhebliche datenschutzrechtliche Mängel der Datenverarbeitung im VBS beim BKA festgestellt und beanstandet. Darüber habe ich in meinem letzten Tätigkeitsbericht ausführlich informiert (vgl. 28. TB, 6.7.3).

Beanstandet hatte ich insbesondere Folgendes:

- die mangelnde Abgrenzung der zu verschiedenen Zwecken im VBS gespeicherten Daten,
- die Vergabe der Zugriffsrechte im VBS,
- die Funktion „Dateienrundlauf“,

- die fehlende Konkretisierung der Aussonderungsprüffristen,
- die Speicherung von Dateien auf den Gruppenlaufwerken als „Aktenersatz“,
- die fehlende Möglichkeit, Daten zu kennzeichnen, die bei verdeckten Maßnahmen erhoben wurden.

Inzwischen informierte mich das Bundesministerium des Inneren, für Bau und Heimat (BMI) darüber, das VBS sei bereits Ende 2019 funktional so angepasst worden, dass Daten aus besonders eingriffsintensiven Maßnahmen gekennzeichnet werden könnten, so dass ihre Herkunft damit erkennbar sei. Abgesehen davon sei beabsichtigt, die Nutzung des VBS im Hinblick auf Aussonderungsprüffristen und die Vorgangsführung unter Beachtung des Aufgabenspektrums des BKA soweit wie möglich zu vereinheitlichen. Zur Gewährleistung einer lückenlosen, revisionssicheren und einheitlichen Aktenführung im BKA sei die Einführung einer bedarfsangepassten elektronischen Akte geplant.

Im Hinblick auf die von mir festgestellten Mängel der Dokumentation und Aktenführung teilt das BMI zwar meine Ansicht, dass diese einer umfassenden Neuausrichtung bedürfen. Die Konzeptionierungsphase solle bis Mitte 2021 abgeschlossen sein. Es ist allerdings gleichermaßen bedauerlich wie verwunderlich, dass die Konzeptionierung solch dringend notwendiger Änderungen erst knapp zwei Jahre nach der Übersendung meines Prüfberichts abgeschlossen sein und die eigentliche Umsetzung entsprechend noch später erfolgen soll.

Andere – gerade zentrale – Punkte der Beanstandungen wurden vom BMI bislang nicht aufgegriffen.

Ganz elementar ist für mich die Notwendigkeit einer Trennung zwischen den verschiedenen Zwecken, zu denen das BKA personenbezogene Daten im VBS verarbeitet. Insofern vertritt das BMI z. B. im Hinblick auf die Verarbeitung von personenbezogenen Daten zur Vorgangsverwaltung und zur Dokumentation polizeilichen Handelns die Rechtsansicht, § 22 Abs. 2 BKAG erlaube eine Speicherung insbesondere in den Fällen, in denen die Erforderlichkeit einer Weiterverarbeitung zur Aufgabenerfüllung noch nicht beurteilt werden kann und es nicht ausgeschlossen ist, dass das betreffende Datum zu einem späteren Zeitpunkt einen polizeilichen Nutzen haben könnte. „Das Datum kann“ – so das BMI – „aufbewahrt und ggf. mit weiteren Erkenntnissen angereichert werden, bis eine Entscheidung über die Erforderlichkeit der Speicherung zur Aufgabenerfüllung herbeigeführt werden kann oder das Datum ausgesondert wird oder aufgrund des Ablaufs von Höchstspeicherfristen zu löschen ist“.

Eine solche Sichtweise findet im Gesetz keine Grundlage und widerspricht dem verfassungsrechtlichen Grundverständnis, wonach Daten von vornherein nur zu bestimmten, präzise und normenklar festgelegten Zwecken gespeichert werden dürfen. Bereits bei der Speicherung muss hinreichend gewährleistet sein, dass die Daten nur für solche Zwecke verwendet werden, die das Gewicht der Datenspeicherung rechtfertigen. Das ist ständige Rechtsprechung des Bundesverfassungsgerichts. Eine Datenspeicherung auf Halde für den Fall, dass sie irgendwann einmal für die polizeiliche Aufgabenerfüllung „nützlich“ sein könnten, ist nicht zulässig.

Ich werde auf eine zeitnahe datenschutzkonforme Ausgestaltung des VBS beim BKA drängen und erforderlichenfalls geeignete Maßnahmen zur Beseitigung der festgestellten Mängel gemäß § 69 Abs. 2 BKAG treffen.

#### **9.5.4 Datenübermittlungen des BKA im internationalen Bereich**

In 2016 hat das Bundesverfassungsgericht erstmals Aussagen zu den Anforderungen an die Übermittlungen von Daten durch das Bundeskriminalamt (BKA) an öffentliche Stellen im Ausland getroffen (Urteil vom 20. April 2016, Az. BvR 966/09). Deshalb musste der Gesetzgeber regelmäßige Kontrollintervalle im zweijährigen Turnus festlegen. Einen verpflichtenden Beratungs- und Kontrolltermin habe ich dieses Jahr beim BKA wahrgenommen und ausgewählte Datenübermittlungen in die Länder Russland, Katar, Japan und Israel geprüft. Das BKA hat einigen Aufwand betrieben, die rechtlichen Fragen auszuarbeiten und die Abteilungen zu schulen. In Einzelfällen habe ich aber dennoch Datenschutzmängel festgestellt und diese beanstandet.

Die Datenübermittlungen in Drittstaaten (Staaten außerhalb der EU) stellen für das BKA ein tägliches „Massengeschäft“ dar. Positiv erwähnenswert bei meiner Kontrolle ist daher, dass das BKA bestrebt ist, alle zuständigen Abteilungen regelmäßig zu schulen und für die Thematik zu sensibilisieren.

Die gesetzlichen Regelungen sehen eine Prüfung des datenschutzrechtlichen Niveaus eines jeden Landes nach den Vorschriften des Bundesdatenschutzgesetzes vor. Hier ist zu unterscheiden, ob die EU für das jeweilige Land einen Angemessenheitsbeschluss erlassen hat oder ob geeignete Garantien in einem rechtsverbindlichen Instrument festgeschrieben sind. Für die Bewertung des jeweiligen Schutzniveaus bedient sich das BKA – auch in Zusammenarbeit mit dem Bundesamt für Justiz – unterschiedlichster Informationen, z. B. Menschenrechtsjahresberichte, Berichte des Auswärtigen Amtes sowie bilaterale und sonstige Abkommen. Welche Anforderungen an geeignete Garantien in einem rechtsverbindlichen

Instrument zu stellen sind, ist allerdings sowohl auf nationaler als auch auf europäischer Ebenen noch nicht abschließend geklärt.

Im Ergebnis ist diese Beurteilung für das BKA aber eher von dogmatischer Natur als von praktischer Relevanz. Der nationale Gesetzgeber hat für Datenübermittlung in Drittstaaten vorgesehen, in jedem Einzelfall zu prüfen, ob ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrer Umgang mit den Daten beim Empfänger der Übermittlung sichergestellt ist. In meiner Kontrolle konnte ich feststellen, dass das BKA diese Einzelfallprüfung auch überwiegend durchführt.

Nur in zwei Fällen habe ich eine Beanstandung ausgesprochen: Es handelte sich um Fälle, in denen Landespolizeibehörden von einem Drittstaat um eine Datenübermittlung ersucht worden waren. In derartigen Fällen kann es vorkommen, dass die jeweilige Landesbehörde das BKA bittet, den Datenaustausch mit dem ersuchenden Land zu übernehmen. Das BKA handelt dann in einer gesetzlich vorgesehenen „Korrespondenzfunktion“.

In solchen Konstellationen geht das BKA davon aus, dass eine materielle Rechtmäßigkeitsprüfung der Datenübermittlung durch die jeweilige Landesbehörde erfolgt.

Aus Anlass eines vor Ort geprüften Falles habe ich dem BKA dringend geraten, mindestens eine summarische Rechtmäßigkeitsprüfung vorzunehmen, da das BKA für die Datenübermittlung auch in dieser Korrespondenzfunktion die datenschutzrechtliche Verantwortung trägt. Das BKA handelt hier nicht als bloßer „Bote“, sondern führt die Korrespondenz eigenständig. Es handelt sich um eine gesetzliche Aufgabe des BKA, nicht um eine reine Auftragsverarbeitung.

In einem anderen Fall ermittelten die japanischen Behörden wegen (räuberischen) Diebstahls und traten an das BKA heran. Das BKA bat die zuständige Landespolizeibehörde um eine Auskunft der über den Betroffenen gespeicherten Daten. Das BKA hat an Japan fast alle seitens der Landespolizeibehörde zur Verfügung gestellten Daten übermittelt ohne jedoch vorher zu prüfen, auf welcher Verdachtslage der Betroffene überhaupt gespeichert war. Außerdem wurde der japanischen Behörde mitgeteilt, dass der Betroffene hier als „politisch-motiviert-links“ eingeordnet sei. Die Datenqualität und Datenvalidität halte ich für ungenügend. Außerdem ging die Übermittlung über den angeforderten Datenumfang der anfragenden Behörde hinaus. Die Vorgehensweise des BKA habe ich daher als Verstoß gegen den Erforderlichkeitsgrundsatz beanstandet.

#### **9.5.5 Allgemeiner Beitrag über die durchgeführten SÜG-Kontrollen**

Die datenschutzrechtlichen Kontrollen der Vorgaben des Sicherheitsüberprüfungsgesetzes (SÜG) bei zwei öffentlichen Stellen und einem Wirtschaftsunternehmen ergaben Verbesserungspotential bei der Führung von Sicherheitsakten und Dateien sowie bei der Kommunikation zwischen den beteiligten Stellen.

Im Berichtszeitraum habe ich bei zwei Bundesbehörden und einem Wirtschaftsunternehmen kontrolliert, ob sie die datenschutzrechtlichen Vorgaben aus dem SÜG einhalten.

Die erste Stelle war das Assessmentcenter für Führungskräfte der Bundeswehr. Gegenstand der Prüfung waren die Einstellungsüberprüfungen von Soldatinnen und Soldaten als Führungskräfte bei der Bundeswehr. Seit 2017 sind alle Soldatinnen und Soldaten gemäß § 37 Abs. 3 Soldatengesetz bei ihrer erstmaligen Berufung in ein Dienstverhältnis mindestens einer einfachen Sicherheitsüberprüfung zu unterziehen.

Überprüft habe ich auch das Bundesamt für Verfassungsschutz (BfV). Hier betraf die Kontrolle die Sicherheitsüberprüfungen eigener Mitarbeiterinnen und Mitarbeiter des BfV.

Bei dem geprüften Wirtschaftsunternehmen handelte es sich um eine Firma aus Bonn. Kontrollgegenstand waren in diesem Fall die Sicherheitsüberprüfungen für den Geheimschutz.

In allen drei Fällen habe ich vereinzelte Verstöße gegen die Vorgaben, wie Sicherheitsakten zu führen sind, festgestellt. Diese reichen von unvollständigen Akten über unzulässige Unterlagen in den Sicherheitsakten bis hin zu Akten, deren Vernichtung überfällig war.

Auch in den geprüften Dateien, die zur Erleichterung der Verfahren geführt werden dürfen, gab es in Einzelfällen Fehler. Diese betrafen die unzulässige Speicherung von Daten bzw. deren nicht durchgeführte Löschung.

Insbesondere bei dem kontrollierten Unternehmen war außerdem die Kommunikation zwischen der Personalverwaltung und der für die Sicherheitsüberprüfung zuständigen Stelle stark zu bemängeln. So erhielt die für die Sicherheitsüberprüfung zuständige Stelle von der Personalverwaltung aktiv gar keine oder nur sehr verspätet Mitteilung über das Ausscheiden sicherheitsüberprüfter Personen.

Die Kontrolle beim Assessmentcenter für Führungskräfte der Bundeswehr war zum Redaktionsschluss bereits abgeschlossen. In den übrigen beiden Fällen haben die kontrollierten Stellen noch Gelegenheit zur Stellungnahme. Die kontrollierten Stellen haben sich aber kooperationsbereit gezeigt und einige festgestellte Mängel bereits behoben. Auch in der Nachbereitung der Kontrollen kann ich bislang über eine konstruktive Zusammenarbeit mit den kontrollierten Stellen berichten.

## 10 BfDI intern

### 10.1 Handlungsmöglichkeiten des BfDI bei europarechtswidriger Gesetzgebung

Nationale Regelungen müssen im Einklang mit der Datenschutz-Grundverordnung (DSGVO) stehen. Ist dies nicht der Fall, kann durch die Umsetzung dieser Regelungen gegen die DSGVO verstoßen werden. Diesen Fällen versuche ich bereits im Gesetzgebungsverfahren entgegenzuwirken, indem ich entsprechende Stellungnahmen abgebe und notfalls den unter meiner Aufsicht stehenden Stellen die Ergreifung aufsichtsrechtlicher Maßnahmen für den Fall ankündige, dass sie die nationalen Regelungen trotz Verstoßes gegen die DSGVO anwenden.

Zeigt sich anhand eines Gesetzesentwurfs, dass Regelungen den Anforderungen der DSGVO nicht ausreichend gerecht werden, bringe ich dies im Rahmen meiner Stellungnahmen im Gesetzgebungsverfahren frühzeitig ein. Beispiele hierfür sind einige Regelungen im Patientendaten-Schutz-Gesetz (vgl. 4.2). So sieht § 342 Absatz 2 Nr. 2 lit. b) SGB V nur für Nutzende von geeigneten Endgeräten wie Mobiltelefonen oder Tablets einen datenschutzrechtlich ausreichenden Zugriff auf ihre eigene elektronische Patientenakte vor und dies zudem erst ab dem Jahr 2022. Unabhängig mit der damit verbundenen Ungleichbehandlung bei der Ausübung des Rechts auf informationelle Selbstbestimmung ab 2022, wird durch die Regelung in der ersten Umsetzungsphase gegen das Prinzip der Erforderlichkeit verstoßen. Denn in dieser Phase erhalten alle Leistungserbringer, denen die Versicherten Einsicht in ihre Daten gewähren, Einblick in alle dort enthaltenen Informationen. Und dies unabhängig davon, ob sie für die konkrete Behandlung erforderlich sind. Ein weiteres Beispiel ist § 87a Absatz 1 Satz 3 2. Halbsatz Abgabenordnung, nach dem der unverschlüsselte E-Mail-Verkehr des Finanzamts im Falle einer Einwilligung aller Beteiligten zulässig ist (vgl. 7.6). Dem steht entgegen, dass die Regelungen der DSGVO, die den Verantwortlichen zur Einhaltung der technischen

und organisatorischen Maßnahmen verpflichten, nicht abdingbar sind.

Ich habe den gesetzlichen Auftrag, die unter meiner Aufsicht stehenden Stellen über die ihnen aus der DSGVO, dem Bundesdatenschutzgesetz und den sonstigen Vorschriften über den Datenschutz entstehenden Pflichten zu sensibilisieren und zu beraten. Daher teile ich den von der jeweiligen Neuregelung betroffenen Stellen meine Position hierzu ebenfalls mit. Diesen gegenüber behalte ich mir neben der formellen Warnung, dass beabsichtigte Verarbeitungsvorgänge wegen des Anwendungsvorrangs der DSGVO voraussichtlich gegen diese verstoßen, für den Fall der nicht DSGVO-konformen Umsetzung der Neuregelungen die Ausübung der weiteren mir zur Verfügung stehenden Abhelfebefugnisse vor. Diese sind in Art. 58 Absatz 2 DSGVO geregelt. In Betracht kommt u.a. die Anweisung, die europarechtswidrigen Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen. Zudem ist auch eine Untersagung der betreffenden Verarbeitungsvorgänge möglich.

#### Querverweise:

4.2 Patientendaten-Schutz-Gesetz, 7.6 Unverschlüsselte Steuerdaten

### 10.2 Urteil des Landgerichts Bonn bestätigt Rechtsauffassung des BfDI

In seinem Urteil vom 11. November 2020 hat das Landgericht Bonn wesentliche Grundsatzfragen mit bundes- und europaweiter Bedeutung zur bußgeldrechtlichen Haftung von Unternehmen nach der Datenschutz-Grundverordnung (DSGVO) geklärt und ist dabei weitestgehend meinen Rechtsauffassungen gefolgt. Die Haftung ist nicht auf Verstöße durch Organe oder Leitungspersonen beschränkt. Zudem ist bei der Geldbuße auf den Umsatz der so genannten wirtschaftlichen Einheit abzustellen. Im konkreten Fall sah das

## **Landgericht nur einen leichten Verstoß und reduzierte daher die Höhe der Geldbuße.**

In meinem letzten Tätigkeitsbericht habe ich über eine Geldbuße gegen die 1&1 Telecom GmbH berichtet (s. 28. TB, Anlage 2). In meiner Bußgeldentscheidung hatte ich den Vorwurf erhoben, dass das Unternehmen seine Kundendaten bei der telefonischen Kundenbetreuung zeitweise nicht ausreichend geschützt hatte. So bestand das Risiko, dass unberechtigte Dritte durch bloße Kenntnis von Name und Geburtsdatum des Kunden weitere Kundendaten erfragen konnten. Um das zu verhindern, bedurfte es aus meiner Sicht einer angemessenen Prüfung der Berechtigung der Anrufer (Authentifizierung). Die Kenntnis von Name und Geburtsdatum des Kunden reichten bei den betroffenen Daten aus meiner Sicht nicht. Die 1&1 Telecom GmbH hatte während meines Ordnungswidrigkeitenverfahrens die internen Maßnahmen zeitnah angepasst, um ein höheres Schutzniveau zu gewährleisten. Im Rahmen der telefonischen Kundenbetreuung setzt das Unternehmen nunmehr auf eine PIN-Lösung zur Authentifizierung seiner Kundinnen und Kunden. Aus Anlass des vorliegenden Falls habe ich auch andere Telekommunikationsanbieter im Rahmen einer Kontrolle auf die telefonischen Authentifizierungsmaßnahmen hin überprüft, auf etwaige notwendige Änderungen hingewirkt und prüfe, ob Aufsichtsmaßnahmen notwendig sind (s. 9.1).

Nachdem das Unternehmen Einspruch gegen meinen Bußgeldbeschluss eingelegt hatte, wurde die Bußgeldsache über die Staatsanwaltschaft an das Landgericht Bonn abgegeben. In seinem Urteil vom 11. November 2020 bestätigte das Landgericht meine Bußgeldentscheidung dem Grunde nach, setzte aber eine geminderte Geldbuße fest. Das Urteil ist über den konkreten Bußgeldfall hinaus wegweisend für die gesamte bundes- und europaweite Ahndungspraxis unter der DSGVO und bringt mehr Rechtsklarheit und -sicherheit für Unternehmen und Aufsichtsbehörden. Insbesondere bestätigte das Landgericht zahlreiche meiner Rechtsauffassungen, die von Wirtschaftsverbänden zuvor in Frage gestellt worden waren. Zugleich gab das Gericht den Datenschutzaufsichtsbehörden wichtige Hinweise und Orientierungen zur Bestimmung wirksamer, verhältnismäßiger und abschreckender Geldbußen mit auf den Weg.

So bestätigte das Landgericht etwa, dass nach der DSGVO die Haftung von juristischen Personen nicht auf Verstöße durch Organe oder Leitungspersonen beschränkt ist. Die unmittelbare Verbandshaftung der DSGVO ist insoweit vorrangig und lässt keinen Spielraum für abweichende Regelungen des deutschen Gesetzgebers. Denn solche würden den fairen Wettbewerb innerhalb der EU verzerren und dem Ziel der DSGVO zu einer einheitlichen Sanktionierung widersprechen. Die Vorschrift

des § 30 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) ist damit unvereinbar und aufgrund des sog. Anwendungsvorrangs des Unionsrechts unanwendbar.

Zudem sind Strukturen in Unternehmen häufig komplex. Sie können aus Mutter- und mehreren Tochtergesellschaften bestehen, die teilweise aber vollständig von der Muttergesellschaft kontrolliert und zwischen denen wirtschaftliche Werte verschoben werden. Aus wirtschaftlicher Sicht können sie dann in einer Gesamtschau gemeinsam eine Einheit bilden. Das Landgericht Bonn hat in seiner Entscheidung bestätigt, dass für die Frage der Obergrenze einer Geldbuße auf den Gesamtumsatz der wirtschaftlichen Einheit abzustellen ist und nicht nur auf den Umsatz der Tochtergesellschaft. Es folgt damit dem erklärten Willen des europäischen Gesetzgebers.

## **Neuberechnung Bußgeld durch Gericht**

Bei der Zumessung der konkreten Geldbuße sind sowohl die tatbezogenen Gesichtspunkte des Art. 83 Abs. 2 DSGVO als auch die übergreifenden Ahndungsprinzipien des Art. 83 Abs. 1 DSGVO heranzuziehen. Die Prinzipien der Wirksamkeit, Verhältnismäßigkeit und Abschreckung erlauben dabei auch die Berücksichtigung der individuellen Ahndungsempfindlichkeit, wie das Gericht klarstellte. Diese kann je nach Unternehmensgröße unterschiedlich sein. Es geht bei DSGVO-Geldbußen also auch um elementare Fragen der Belastungsgleichheit. Denn die identische Bußgeldhöhe kann einen Kleinstunternehmer wirtschaftlich ungleich stärker belasten als ein Großunternehmen. Das Gericht bestätigte, dass der Umsatz und andere wirtschaftliche Faktoren eine erste Orientierung für die Bestimmung der Bußgeldhöhe geben können. Damit wird den Forderungen der Wirtschaftsverbände, der Umsatz dürfe bei der Zumessung keine Rolle spielen, eine klare Absage erteilt. Diese erste Orientierung ist dann durch gebührende Berücksichtigung der Schwere der Tat nach oben oder unten anzupassen.

Dass sowohl die Schwere der Tat als auch die Unternehmensgröße zu berücksichtigen sind, entsprach dabei bereits der gängigen Praxis der Datenschutzbehörden. Neue Erkenntnisse ergeben sich aber aus den darauf folgenden Ausführungen des Gerichts: Je leichter oder schwerer der Verstoß, desto höheres Gewicht hat die Schwere der Tat dann gegenüber der Unternehmensgröße. Dabei wird in der Praxis nach meiner Auffassung auch bei sehr leichten und sehr schweren Verstößen ein besonderes Augenmerk darauf liegen müssen, dass die Unternehmensgröße nicht derart bedeutungslos wird, dass die Geldbußen gegenüber großen Unternehmen wirkungslos oder gegenüber Kleinstunternehmen unverhältnismäßig werden könnten. Dies stünde im Wider-



spruch zu den übergreifenden Ahndungsprinzipien des Art. 83 Abs. 1 DSGVO.

Im konkreten Fall der 1&1 Telecom GmbH sah das Landgericht bei Anwendung der oben skizzierten Zumessungsgesichtspunkte nur einen leichten Verstoß und reduzierte den Betrag daher auf knapp ein Zehntel meiner ursprünglich verhängten Geldbuße. Bei Anwendung der aufgezeigten Zumessungsmethode ist die gerichtliche Geldbuße nachvollziehbar und dürfte jedenfalls aus spezialpräventiver Sicht aufgrund der generellen Datenschutzsensibilität der 1&1 Telecom GmbH noch hinreichend wirksam sein.

### **Das Urteil ist inzwischen rechtskräftig**

Die Erwägungen des Landgerichts zur Bemessung der Höhe einer Geldbuße unter der DSGVO sind sowohl für die Weiterentwicklung des deutschen Bußgeldkonzeptes als auch für die Ausarbeitung von europäischen Bußgeldleitlinien von besonderem Interesse. Ich habe sie daher sowohl auf deutscher wie auch auf europäischer Ebene in die Beratungen mit meinen Schwesterbehörden eingebracht und erörtert. Dabei ist mir wichtig, dass wir am Ende der Beratungen zu einer deutschland- und europaweit möglichst einheitlichen Vorgehensweise gelangen werden. Dies erfordert aber nicht nur die Veröffentlichung gemeinsamer Papiere, sondern vor allem auch eine entsprechend gelebte Rechtsdurchsetzungs- und Ahndungspraxis.

## **10.3 Personalentwicklung im Jahr 2020**

Im Zeitraum 2016 bis 2020 hat der Deutsche Bundestag die dem BfDI zur Verfügung stehenden Planstellen auf 324,9 Stellen fast verdreifacht. Trotz der allgegenwärtigen Corona-Pandemie ist es im Jahr 2020 gelungen, ca. 80 Prozent dieser Stellen zu besetzen. Durch das frühe Anwerben von Nachwuchskräften und ein neues geplantes Personalentwicklungs- und Aufstiegskonzept sehe ich mich für die Zukunft gut gewappnet.

Seit dem 1. Januar 2016 ist der BfDI die jüngste, eigenständige oberste Bundesbehörde. Zuvor war er Teil des Bundesministeriums des Inneren, für Bau und Heimat und benötigte weder einen eigenen organisatorischen noch personellen Unterbau. Damit meine Arbeitsfähigkeit sichergestellt ist, bedarf es einer ausreichenden organisatorischen und personellen Ausstattung. Hatte meine Dienststelle im Jahr 2016, dem Jahr der Verselbständigung, noch 110,5 Planstellen, konnte ich seitdem einen weiteren Stellenaufwuchs auf insgesamt 324,9 Planstellen verzeichnen. Allein für das Jahr 2020 wurden mir vom Haushaltsgesetzgeber für die Aufsicht

über die Sicherheitsbehörden und für die Wahrnehmung neuer Aufgaben insgesamt 67 Stellen bewilligt.

Zur Besetzung vakanter Positionen habe ich 2020 trotz der Corona-Pandemie insgesamt 14 Auswahlverfahren, darunter Sammelausschreibungen für mehrere Positionen, durchgeführt. Dabei habe ich auch auf den Einsatz moderner hausinterner Videokonferenztechnik zurückgegriffen, um qualifiziertes Personal zu finden. Im Jahr 2020 haben sich aus 361 eingegangenen Bewerbungen insgesamt 185 Personen in meinem Hause vorgestellt, aus denen ich über 50 neue Kolleginnen und Kollegen gewinnen konnte. Hierdurch war es mir möglich, von den 324,9 Stellen insgesamt über 250 Stellen zu besetzen. Ich bin zuversichtlich, dass ich im kommenden Jahr, gerade mit Blick auf die weiteren 23,5 Stellen, die mir der Haushaltsgesetzgeber zugesprochen hat, die meisten noch offenen Positionen in meinem Hause besetzen können werde. Hierfür habe ich im Jahr 2020 bereits die Weichen gestellt und nach dem Umzug in die Graurheindorfer Straße wieder vermehrt Studierende und Referendare eingeladen, ihre praktischen Ausbildungszeiten bei mir zu absolvieren, um Nachwuchskräfte zu interessieren und an mich zu binden. Außerdem erarbeite ich derzeit ein aktualisiertes und an die moderne Arbeitswelt angepasstes Personalentwicklungs- und Aufstiegskonzept.

Zur Gewährleistung einer regelmäßigen und effizienten Datenschutzaufsicht wurde meine Dienststelle als Kontrollorgan der Sicherheitsbehörden und Nachrichtendienste personell so ausgestattet, dass die verfassungsgerichtlich geforderte Kompensationsfunktion effizient erfüllt werden kann. Mit dem personellen Aufwuchs wurde nicht nur eine Neustrukturierung des Bereichs Polizei und Nachrichtendienste erforderlich, indem aus den ursprünglich vier Referaten sechs wurden. Sondern es erfolgte auch eine Umbenennung der Gruppen in Abteilungen, um eine Angleichung an die bei Bundesministerien und anderen Behörden übliche Begrifflichkeit herbeizuführen. Ich bin dem Gesetzgeber dankbar, dass er mich dabei unterstützt, auch weiterhin meine Datenschutzaufsicht zu stärken. Sollten weitere Aufgaben zu meinen bisherigen Tätigkeiten hinzukommen oder aufgrund der rechtlichen sowie technischen Entwicklung verstärkte Maßnahmen notwendig sein, wäre eine weitere personelle Stärkung erforderlich.

## 10.4 Die neue Liegenschaft

**Moderne Arbeitsplätze, verbesserte Barrierefreiheit und Sicherheit – der BfDI hat im Mai 2020 eine neue Liegenschaft am Standort Bonn bezogen.**

Am 25. Mai 2020 nahm die Hausleitung des BfDI symbolisch den Schlüssel für ein neues Dienstgebäude in der Graurheindorfer Straße in Bonn entgegen. Nach einer mehrmonatigen intensiven Umbau- und Umzugsphase wurde ein wichtiges Ziel planmäßig erreicht: Die Zusammenführung aller Arbeitsplätze am Standort Bonn in einer modern ausgestatteten Liegenschaft. Die beiden bisherigen Liegenschaften reichten für den Raumbedarf der wachsenden Behörde nicht mehr aus. Bei der Ausstattung des Gebäudes stand zum einen die Einhaltung der Sicherheitsstandards im Vordergrund: Der stark wachsende Bereich zur Kontrolle der Polizei und der Nachrichtendienste benötigt besonders gesicherte Netze, abhörsichere Räume und strenge Zugangskontrollen. Zum anderen wurde bei den Umbauarbeiten ein besonderes Augenmerk auf die Barrierefreiheit gelegt. Hierdurch erhalten Beschäftigte ebenso wie Besuchende bestmögliche Voraussetzungen für das Arbeiten und den Aufenthalt in der Dienststelle. Ein weiterer Schwerpunkt bei der Ausstattung des Gebäudes lag auf moderner Informations- und Kommunikationstechnik. Besprechungsräume mit aktueller Videokonferenztech-

nik entsprechen dem Bedarf an modernen Kommunikationsmitteln. Durch den Umzug wurden nun sehr gute und zukunftsfähige Arbeitsbedingungen für die Beschäftigten des BfDI geschaffen.

## 10.5 Presse- und Öffentlichkeitsarbeit

Der Informationsbedarf der Öffentlichkeit zu Fragen des Datenschutzes und der Informationsfreiheit war im Jahr 2020 ungebrochen stark. Um dem gesetzlichen Auftrag zur Sensibilisierung und Aufklärung der Gesellschaft für meine Themen nachzukommen, habe ich deshalb die Presse- und Öffentlichkeitsarbeit weiter ausgebaut. Unter anderem bin ich seit diesem Jahr auch beim dezentralen und besonders datenschutzfreundlichen Mikrobloggingdienst Mastodon aktiv.

### Pressearbeit

Das mediale Interesse an meiner Arbeit ist im Berichtszeitraum weiter gestiegen. Dies zeigt auch die thematische Vielfalt der Anfragen:

Das größte Interesse galt Datenschutzfragen im Zusammenhang mit der Corona-Pandemie. Schon während der Entwicklungsphase der Corona-Warn-App (vgl. Nr. 4.1.1) im Frühjahr wurde ich sehr oft nach meiner Ein-



schätzung gefragt. Die zweite Welle der Pandemie war auch bei den Presseanfragen ab November spürbar, als öffentlichkeitswirksam eine Weiterentwicklung der App gefordert wurde.

Der Themenbereich Datenschutz im Gesundheitswesen stieß grundsätzlich auf hohes journalistisches Interesse. Dies lag nicht zuletzt an der Vielzahl der Gesetzesvorhaben in diesem Bereich. Gerade die Einführung der elektronischen Patientenakte (vgl. Nr. 4.2) und das Verhalten der verschiedenen Akteure in diesem Zusammenhang warfen neue Fragen auf. Die medizinische Fachpresse fragte hier nach teilweise sehr detaillierten Informationen.

Auch Gesetzesvorhaben außerhalb des Themenbereichs Gesundheit waren Gegenstand von Presseanfragen, beispielsweise die geplante Registermodernisierung (vgl. Nr. 5.1).

Daneben waren es oft Einzelereignisse, die zu Anfragen führten. Hier sind vor allem die Berichterstattung zur US-amerikanischen Plattform Clearview, das Urteil des Europäischen Gerichtshofs zu Schrems II (s.a. 4.3) und das Urteil des Bundesverfassungsgerichts zum Bundesnachrichtendienst (s.a. 6.3) zu nennen.

Bei etlichen Anfragen habe ich auf meine zuständigen Kolleginnen und Kollegen in den Ländern verwiesen, da mich immer wieder Anfragen z. B. zur Deutschen Bahn (zuständige Aufsichtsbehörden Berlin und Hessen), zu Facebook und Google (zuständige Aufsichtsbehörde Hamburg bzw. Irland) und zur SCHUFA (zuständige Aufsichtsbehörde Hessen) erreichen, für die ich keine rechtliche Zuständigkeit habe. Gleiches gilt für Anfragen zu Unternehmen ohne Zentrale oder Hauptsitz in Deutschland, wie beispielsweise PimEyes (zuständige Aufsichtsbehörde Polen) oder ByteDance bzw. TikTok.

Ich habe darüber hinaus im Berichtszeitraum 30 Pressemitteilungen herausgegeben und war zwei Mal zu Gast in der Bundespressekonferenz. Außerdem habe ich zwölf Gastbeiträge bzw. Aufsätze für verschiedene Medien verfasst.

### **Social Media**

Im Oktober 2020 habe ich eine eigene Instanz des dezentralen Mikrobloggingdienstes Mastodon eingerichtet. Dort betreibe ich einen offiziellen Behörden-Account (<https://social.bund.de/@bfdi>). Hiermit möchte ich interessierten Bürgerinnen und Bürger die Möglichkeit zum Gedankenaustausch auf einer datenschutzfreundlichen Alternative zu anderen etablierten Social-Media-Angeboten geben. Diese können auf Mastodon kommunizieren und müssen dabei keine oder nur sehr wenige personenbezogene Daten preisgeben. Das reine Lesen

meiner Beiträge ist sogar ohne eigene Registrierung bei Mastodon möglich.

### **Veranstaltungen**

Im Berichtszeitraum konnten aufgrund der Einschränkungen durch die Corona-Pandemie keine Präsenzveranstaltungen mit größerem Teilnehmerkreis durchgeführt werden. So musste unter anderen das für September geplante IFG-Symposium in Berlin bedauerlicherweise genauso abgesagt werden wie eine Fortsetzung der gemeinsamen Veranstaltungsreihe mit dem Europäischen Datenschutzbeauftragten in Brüssel.

### **Besuchergruppen**

Auch die Besuchergruppen-Betreuung war durch die Corona-Pandemie sehr eingeschränkt. Meine Mitarbeiterinnen und Mitarbeiter betreuten insgesamt vier Gruppen mit bis zu 50 Teilnehmern.

### **Informationsmaterial**

Ein Schwerpunkt meiner Öffentlichkeitsarbeit ist nach wie vor die Veröffentlichung von Informationen zu grundsätzlichen sowie aktuellen Themen in den Bereichen Datenschutz und Informationsfreiheit.

Die aktuell sechs angebotenen Broschüren richten sich hauptsächlich an das Fachpublikum. Die 14 verfügbaren Flyer richten sich mit ihren vielfältigen und praktischen Themen insbesondere an Bürgerinnen und Bürger. Neben den regelmäßigen Aktualisierungen dieser bestehenden Materialien entwickeln meine Kolleginnen und Kollegen und ich auch regelmäßig neue Konzepte für entsprechende Informationsangebote.

In diesem Zusammenhang habe ich in diesem Jahr die Übersetzung ausgewählter Flyer in unterschiedlichen Sprachen in Auftrag gegeben. Zudem wurden die Arbeiten an einem neuen Flyer zur Thematik „Datenschutz für Geflüchtete und Asylsuchende“ begonnen.

Weiterhin möchte ich meine Beratungs- und Aufklärungsarbeit insbesondere für Kinder und Eltern ausweiten. Dafür entwickle ich gegenwärtig mit dem CARLSEN Verlag ein Pixi-Buch und ein Pixi Wissen, die für Kinder und ihre Eltern einen Einstieg in das Thema Datenschutz und Informationsfreiheit bieten sollen. Die ersten Hefte werden im nächsten Jahr erscheinen und sollen der Auftakt zu einer neuen Pixi-Reihe werden.

Obwohl alle aktuellen Publikationen, unter [www.bfdi.bund.de/informationsmaterial](http://www.bfdi.bund.de/informationsmaterial), als barrierefreie PDF-Dokumente heruntergeladen werden können, stelle ich fest, dass nach wie vor ein ungebrochenes Interesse an Print-Veröffentlichungen besteht. Daher biete ich im Rahmen der jeweiligen Verfügbarkeit neben dem Download auch immer noch die Bestellung von Papierexemp-



laren an. Beim Versand dieser arbeite ich übrigens seit mehreren Jahren mit einer Einrichtung zusammen, die die Eingliederung von psychisch beeinträchtigten Menschen in das Arbeitsleben unterstützt.

## 10.6 BfDI in Zahlen

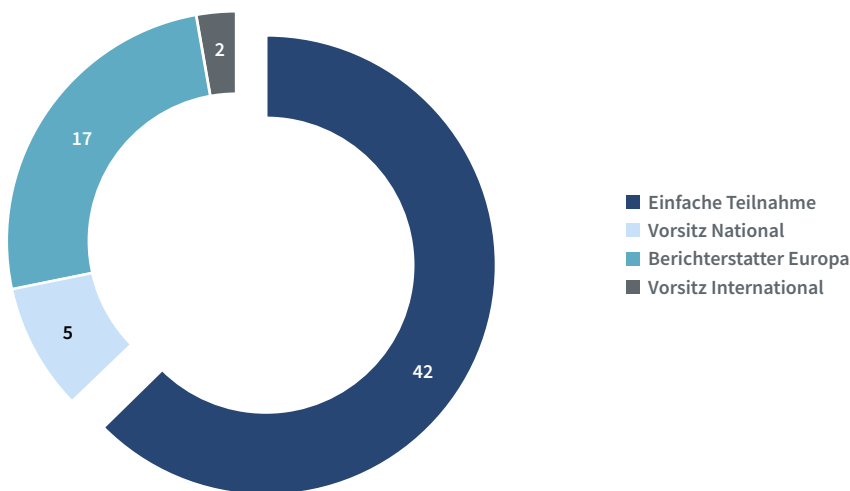
In den vorangegangenen Kapiteln habe ich meine wichtigsten Tätigkeiten aus dem Jahr 2020 nachgezeichnet. Daneben ist meine Tätigkeit aber auch ganz allgemein von den zahlreichen Anfragen und Beschwerden von Bürgerinnen und Bürgern, der Aufsicht über datenverarbeitende Stellen und der Beratung verschiedenster Institutionen geprägt. An dieser Stelle möchte ich anhand der wichtigsten Zahlen auch hierzu einen kurzen Überblick geben.

### Gremienarbeit

Der Datenschutz erfasst immer mehr Lebensbereiche und entfaltet dadurch Wechselwirkungen, die oft über den Zuständigkeitsbereich einer einzelnen Aufsichtsbehörde hinausgehen. Zudem erfordert die Datenschutzgrundverordnung (DSGVO) ein europaweit koordiniertes Vorgehen, das mitunter zu einer komplexen Angelegenheit werden kann. Dies belegt auch das Bestehen von insgesamt 66 nationalen und internationalen Arbeitsgremien, in denen der BfDI vertreten ist. Bei gut einem Drittel dieser Gremien habe ich (teils auch zeitweise) besondere Verantwortung in den Funktionen als Vorsitzender bzw. Berichterstatter übernommen.

In diesem Zusammenhang hat meine Behörde an knapp 350 Sitzungen teilgenommen und dabei sieben Entschlüsse eingebracht, davon fünf auf nationaler und je eine auf europäischer und internationaler Ebene.

#### Mitarbeit in nationalen und internationalen Gremien

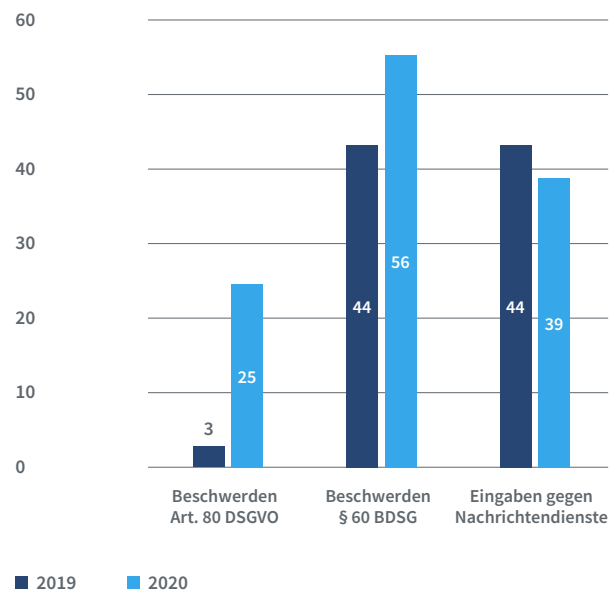
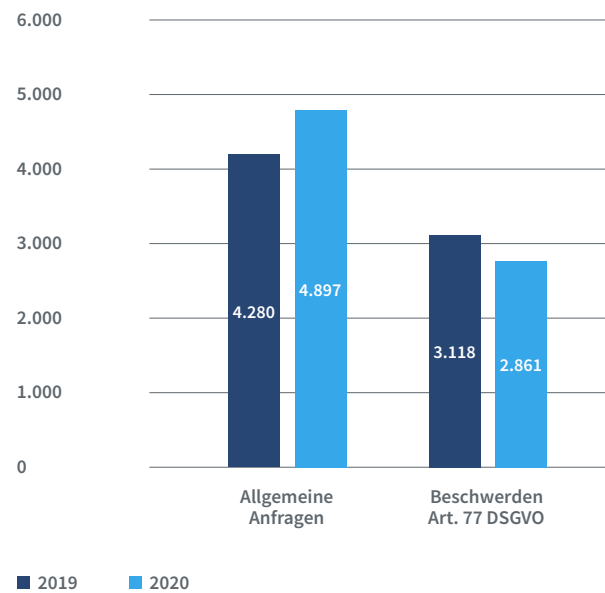


## Beschwerden und allgemeine Anfragen

Im Jahr 2020 richteten Bürgerinnen und Bürger insgesamt 7.878 Beschwerden und Anfragen an mich. Im Vergleich zum Vorjahr, als ich 7.489 Eingänge verzeichnen konnte, war also ein etwas stärkeres Interesse am Datenschutz zu verzeichnen.

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.

### Beschwerden und Anfragen



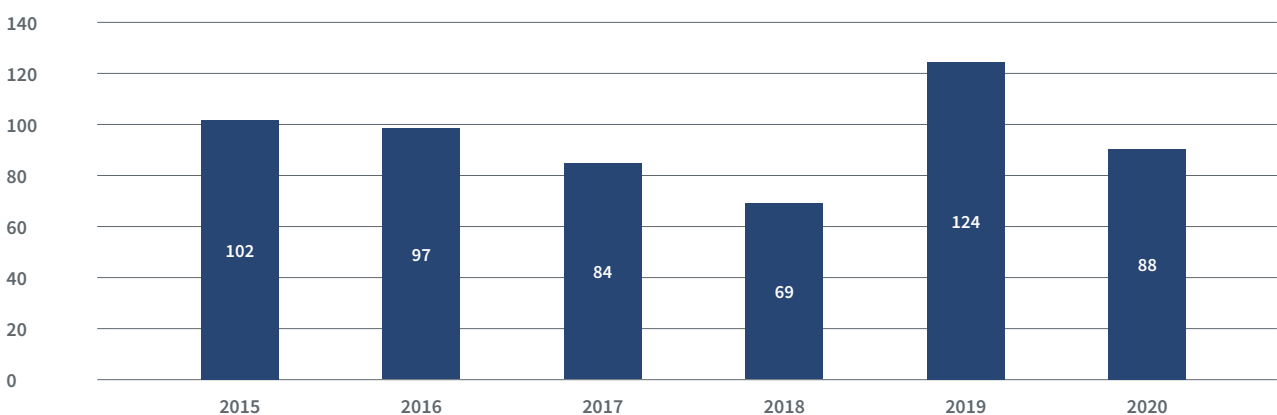
## Beratung und Kontrolle

Ein wichtiger Teil meiner Arbeit ist die Beratung von verantwortlichen Stellen und betroffenen Personen. Neben 4.897 allgemeinen Anfragen konnte ich in 7.212 Fällen telefonisch beraten.

Die Möglichkeit für Vor-Ort-Termine war im Berichtsjahr durch die Auswirkungen der Corona-Pandemie stark

eingeschränkt. Dies hat sich auch auf meine Kontrollpraxis ausgewirkt. Trotzdem konnten im Berichtszeitraum noch 88 Beratungen und Kontrollen durchgeführt werden. Um hier meiner gesetzlichen Aufgabe unter den besonderen Bedingungen einer Pandemie gerecht zu werden, habe ich vermehrt auch auf alternative Methoden wie schriftliche Kontrollen zurückgegriffen.

### Beratungen und Kontrollen von beaufsichtigten Stellen





## Meldungen von Datenschutzverstößen

Sämtliche öffentlichen und nicht-öffentlichen Stellen müssen gegenüber der zuständigen Aufsichtsbehörde Datenschutzverstöße melden. Ich habe im Berichtszeitraum 10.024 entsprechende Meldungen erhalten.

Besonders viele Meldungen gingen im Jahr 2020 von Finanzämtern, Jobcentern und Telekommunikationsunternehmen ein.

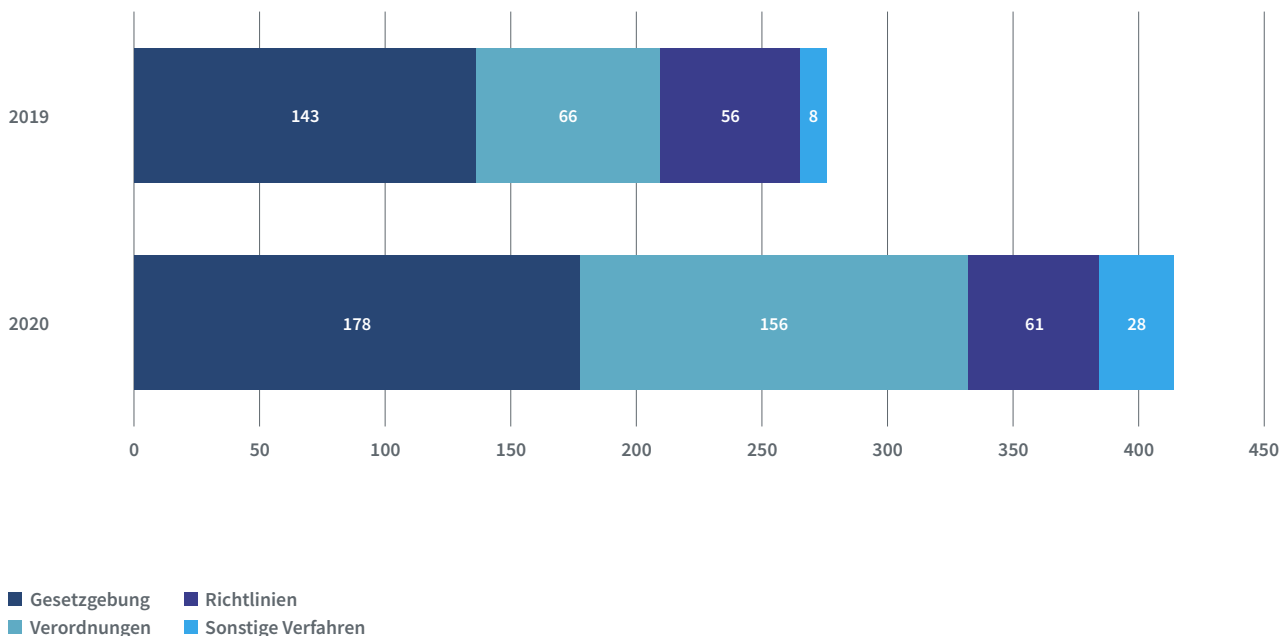
Meldungen von Datenschutzverstößen	2019	2020
Art. 33 DSGVO	14.649	9.985
§ 65 BDSG	0	2
§ 109 a Absatz 1 TKG	40	37

## 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 wurde ich in 423 Fällen nach § 21 GGO eingebunden. Die deutliche Steigerung gegenüber dem vorangegangenen Berichtszeitraum (273 Beteiligungen im Jahr 2019) hängt auch mit der gesteigerten gesetzgeberischen Tätigkeit durch die Corona-Pandemie zusammen.

Darüber hinaus habe ich zu 31 Dateianordnungen, vier Verfahren des Bundesverfassungsgerichts und sieben EU-Rechtsakten Stellung genommen. Außerdem habe ich bei fünf öffentlichen Anhörungen im Deutschen Bundestag und bei drei Anhörungen der Bundesregierung meine Expertise einbringen können.

## Beteiligungen nach § 21 GGO



# 11 BfDI als zentrale Anlaufstelle (ZAST)

## 11.1 Stärkung der Zentralen Anlaufstelle

Die Aufsichtsbehörden des Bundes und der Länder bestätigen den eingeschlagenen Weg zur Zusammenarbeit mit der beim BfDI eingerichteten Zentralen Anlaufstelle (ZAST) in EU-Angelegenheiten und vertrauen ihr weitere wichtige Koordinierungsaufgaben an.

Der BfDI und die Aufsichtsbehörden der Länder arbeiten in EU Angelegenheiten mit dem Ziel einer einheitlichen Anwendung der Datenschutz-Grundverordnung (DSGVO) und der Richtlinie für den Datenschutz im Polizei- und Justizbereich (JI-Richtlinie) zusammen. Die ZAST fungiert hier als Schnittstelle und stellt die wirksame Beteiligung der nationalen Aufsichtsbehörden sowie die rasche und reibungslose Zusammenarbeit auf europäischer Ebene sicher. Diese Zusammenarbeit zwischen den Aufsichtsbehörden des Bundes und der Länder und der ZAST richtet sich nach Erwägungsgrund 119 zu Art. 51 DSGVO sowie den §§ 17 f. Bundesdatenschutzgesetz (BDSG) und wurde im so genannten ZAST-Konzept näher ausgestaltet. Dieses von der Datenschutzkonferenz (DSK) am 23. April 2018 verabschiedete Regelwerk wurde nach gut zwei Jahren einer ersten Evaluierung unterzogen.

Der Evaluierungsbericht gelangte zu dem Schluss, dass sich das ZAST-Konzept mit seinen Regeln zur Zusammenarbeit zwischen der ZAST und den Aufsichtsbehörden von Bund und Ländern grundsätzlich gut bewährt hat. Punktueller Anpassungsbedarf beruht größtenteils darauf, dass es zwischenzeitlich Entwicklungen auf EU-Ebene gab, die Auswirkungen auf die nationale Zusammenarbeit haben. Zudem wurden verschiedene Verfahrens- und Zuständigkeitsfragen zwischenzeitlich von der DSK und ihren Arbeitskreisen entschieden. Um der Rolle als zentrales Regelwerk zur Zusammenarbeit weiterhin gerecht zu werden, wurde das ZAST-Konzept um die betreffenden Beschlüsse und Abreden ergänzt sowie auf die nunmehr weitgehend eingeübten Prozesse angepasst.

Die wichtigsten Anpassungsbedarfe betreffen die Rolle der ZAST bei den freiwilligen Amtshilfeverfahren (vgl. u. Nr. 11.2), den schriftlichen Verfahren des Europäischen Datenschutzausschusses (EDSA) (vgl. u. Nr. 11.2) sowie bei der Zusammenarbeit mit meiner vom Bundesrat zu wählenden Vertretung im EDSA.

Die Vertretung Deutschlands im EDSA obliegt mir als gemeinsamen Vertreter sowie einer vom Bundesrat aus dem Kreise der Leitungen der Aufsichtsbehörden der Länder zu wählenden Stellvertretung (§ 17 Abs. 1 BDSG). In dieser wichtigen und verantwortungsvollen Rolle ist es Aufgabe der Stellvertretung, zusammen mit mir möglichst im Einvernehmen gemeinsame Standpunkte für die Verhandlungsführung im EDSA vorzuschlagen. Zudem wird der Stellvertretung in bestimmten Länderangelegenheiten das Stimmrecht im EDSA übertragen. Leider hat der Bundesrat bis heute noch keine Person für das Amt der Stellvertretung gewählt. Obwohl deshalb praktische Erfahrungen zur Zusammenarbeit bislang fehlen, wurde der ZAST durch die DSK eine wichtige Rolle bei der Koordinierung zwischen gemeinsamen Vertreter und künftiger Stellvertretung zugewiesen, insbesondere soweit dies für die Herstellung gemeinsamer Standpunkte erforderlich ist.

Im Hinblick auf die weiterhin dynamische Entwicklung der europäischen Prozesse der Zusammenarbeit und darauf, dass hinreichende Erfahrungswerte bei einigen Verfahrensarten der DSGVO bislang noch nicht gesammelt werden konnten, wurde eine erneute Evaluierung spätestens nach drei weiteren Jahren vereinbart.

Auf Grundlage des Evaluierungsberichts hat die DSK im November 2020 einstimmig das neue ZAST-Konzept beschlossen und damit den Weg für eine weiterhin erfolgreiche und vertrauensvolle Zusammenarbeit geebnet.

### Querverweis:

11.2 Statistischer Überblick über die Verfahren der Zusammenarbeit und Kohärenz auf europäischer Ebene aus Sicht der ZAST

## 11.2 Statistischer Einblick in die Arbeit der ZAST im Rahmen der Verfahren der Zusammenarbeit und Kohärenz auf europäischer Ebene

Die grenzüberschreitende Fallbearbeitung nimmt Fahrt auf. Erste Erfolge, aber auch Herausforderungen bei der Zusammenarbeit im EDSA zeichnen sich ab.

### Verantwortungsübernahme im One-Stop-Shop-Verfahren der DSGVO

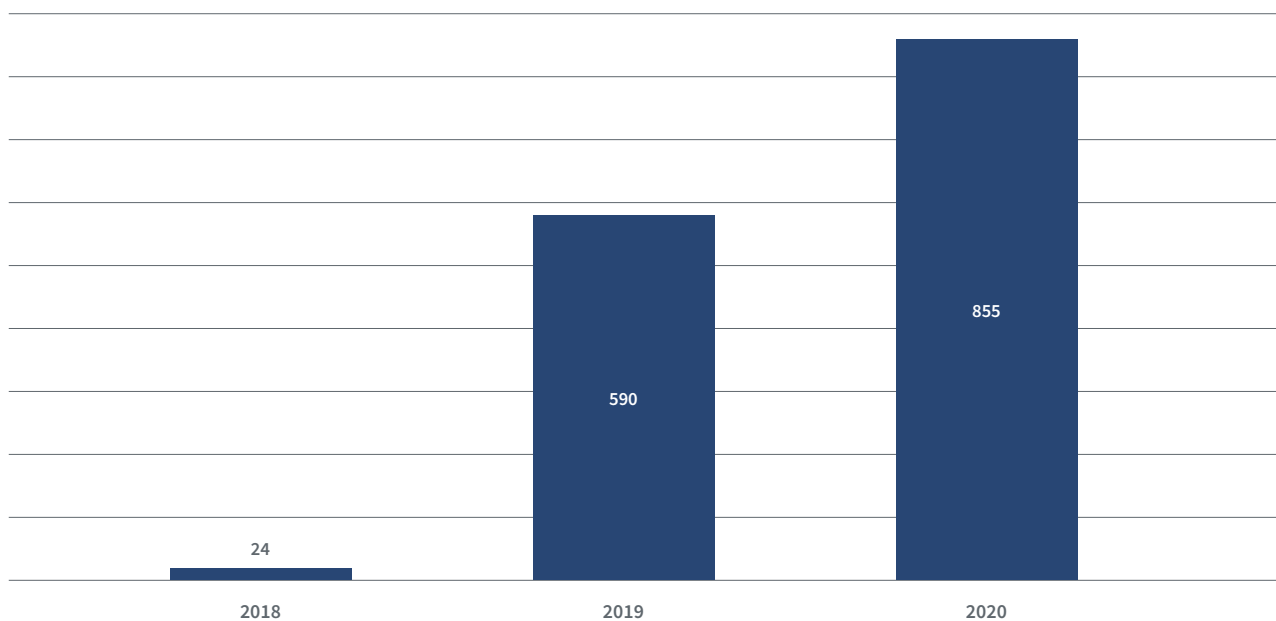
Die Bearbeitung von grenzüberschreitenden Fällen durchläuft bei der Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden verschiedene Pha-

sen. Seit Anwendungsbeginn der DSGVO im Mai 2018 verschieben sich die Schwerpunkte der Bearbeitung zunehmend von formellen Fragen hin zur inhaltlichen Befassung.

Der erste formelle Schritt der grenzüberschreitenden Fallbearbeitung ist das Verfahren zur Identifikation der federführenden Aufsichtsbehörde sowie der betroffenen Aufsichtsbehörden nach Art. 56 DSGVO (56ID). Nachdem 543 dieser Verfahren im Jahr 2018 (25. Mai bis 31. Dezember) und 798 Verfahren im Jahr 2019 eingeleitet wurden, waren dies im Jahr 2020 nur noch 742 Verfahren.

Insgesamt existieren derzeit 2083 Verfahren nach Art. 56 DSGVO zur Bestimmung der federführenden und der betroffenen Aufsichtsbehörden. Dabei trägt die federführende Aufsichtsbehörde die Hauptverantwortung

### Entwicklung der freiwilligen Amtshilfeverfahren mit deutscher Beteiligung



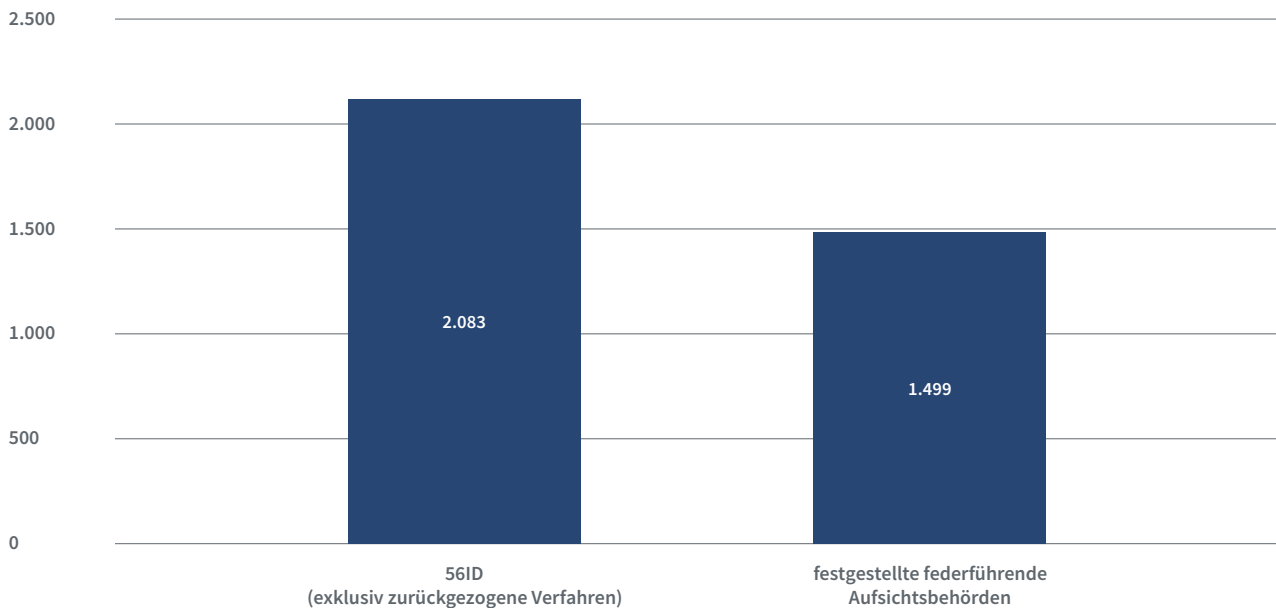
und wird von den jeweils betroffenen Aufsichtsbehörden konstruktiv-kritisch begleitet sowie unterstützt mit dem Ziel einer EU-weit harmonischen Rechtsanwendung.

In mittlerweile 1499 dieser Fälle wurde die federführende Aufsichtsbehörde bereits identifiziert, indem sie sich im Binnenmarktinformationssystem (englisch: Internal Market Information System – kurz IMI), dem IT-Tool zur europäischen Verwaltungszusammenarbeit, offiziell für

zuständig erklärt hat. Gemessen an der Gesamtzahl der angelegten Fälle konnte die federführende Aufsichtsbehörde bereits in einem Großteil bestimmt werden, sodass die inhaltliche Bearbeitung erfolgen kann.

Der Übergang zur inhaltlichen Bearbeitung wird auch durch die stark gestiegene Anzahl der Verfahren der freiwilligen Amtshilfe nach Art. 61 DSGVO belegt. Diese Verfahren werden hauptsächlich für zwei Anwendungs-

## Anzahl 56ID und festgestellte federführende Aufsichtsbehörden seit DSGVO



fälle genutzt: In ca. 10 Prozent der Fälle geht es um allgemeine Rechtsfragen, zu denen die Anwendungspraxis oder rechtliche Expertise der Aufsichtsbehörden abgefragt wird. Die überwiegende Anzahl der Verfahren werden jedoch für fallbezogene Anfragen genutzt. Dies kann beispielsweise eine Anfrage einer betroffenen Aufsichtsbehörde an die federführende Aufsichtsbehörde bezüglich des Bearbeitungsstands sein oder die Bitte einer federführenden Aufsichtsbehörde an die betroffene Aufsichtsbehörde um Übermittlung der im Rahmen der Beschwerde eingereichten Dokumente.

### Das Jahr 2020 war für die ZAST mit neuen Herausforderungen und Aufgaben verbunden

Im Zusammenhang mit den zuvor betrachteten freiwilligen Amtshilfverfahren hat die ZAST von der DSK zudem eine neue Rolle zugewiesen bekommen.

Anfang Dezember 2019 gab es eine technische Umstellung im IMI, die es ermöglichen sollte, freiwillige Amtshilfverfahren parallel an mehrere Empfänger aus unterschiedlichen Mitgliedstaaten des europäischen Wirtschaftsraums versenden zu können. Damit einher ging allerdings die Nebenwirkung, dass freiwillige Amtshilfeersuchen nur noch an Mitgliedstaaten insgesamt adressiert werden konnten und nicht mehr an einzelne Aufsichtsbehörden des Bundes und der Länder. Folge war, dass die an Deutschland gerichteten Ersuchen zunächst von allen 18 deutschen Aufsichtsbehörden empfangen wurden, obwohl diese häufig nur an eine dieser Stellen gerichtet waren. Dies führte einerseits zu

einem Mehraufwand, da jede einzelne Aufsichtsbehörde jeweils für sich klären musste, ob sie zuständig ist. Andererseits hatten alle deutschen Aufsichtsbehörden unabhängig von ihrer Zuständigkeit gleichermaßen Zugriff auf die Inhalte der Verfahren und die darin enthaltene Kommunikation, was bereits auf europäischer Ebene aus Datenschutzgründen bemängelt wurde.

Aufgrund Abstimmung in der DSK nimmt seit dem 24. April 2020 zunächst alleine die ZAST die Verfahren zur freiwilligen Amtshilfe entgegen und verteilt diese zielgerichtet an die Empfängerbehörden in Deutschland. Dabei erfolgt durch die ZAST keine verbindliche Zuständigkeitsprüfung, sondern nur eine vorläufige Zuordnung, die dann von der jeweiligen Aufsichtsbehörde geprüft und erforderlichenfalls in Absprache mit der ZAST angepasst wird. Dies führt neben einer erheblichen administrativen Entlastung der einzelnen Aufsichtsbehörden auch zu einem erhöhten Datenschutzniveau, da nur noch die wirklich beteiligten Aufsichtsbehörden die erforderlichen Zugriffe auf mit dem Fall verbundene personenbezogene Daten erhalten.

Seit der Umstellung hat die ZAST diese neue Aufgabe bereits in 329 Fällen ausgeführt. Die eingehenden allgemeinen Rechtsfragen werden von der ZAST in der Regel für eine abgestimmte und koordinierte deutsche Beantwortung einem der Arbeitskreise der DSK übermittelt.

Wie in allen anderen Bereichen des Lebens stellte zudem die COVID-19-Pandemie auch die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden

vor neue Herausforderungen. Aufgrund der nicht mehr möglichen Präsenztageungen des EDSA ab März 2020 wurde von der in dessen Geschäftsordnung vorgesehenen Möglichkeit zur Entscheidungsfindung im schriftlichen Verfahren merklich häufiger Gebrauch gemacht.

Zur Vorbereitung des Abstimmungsverhaltens im EDSA ist es bei schriftlichen Verfahren Aufgabe der ZAST, die Herstellung eines gemeinsamen Standpunktes zwischen den Aufsichtsbehörden des Bundes und der Länder nach § 18 Bundesdatenschutzgesetz (BDSG) zu koordinieren. Während diese Aufgabe im Jahr 2018 sechs Mal und im Jahr 2019 lediglich vier Mal zu verrichten war, führten die Auswirkungen der COVID-19-Pandemie im Jahr 2020 zu einem erheblichen Anstieg auf 47 schriftliche Verfahren des EDSA.

Zur Optimierung dieses in Europa einzigartigen internen Abstimmungsprozesses wurde auf Anregung der ZAST im Jahr 2020 begonnen, ein neues, auf die Bedürfnisse der deutschen Aufsichtsbehörden zugeschnittenes Modul im IMI zu konzipieren. Hierbei arbeitet die ZAST eng mit den deutschen Aufsichtsbehörden, dem EDSA-Sekretariat und der für das IMI-System insgesamt verantwortlichen Europäischen Kommission zusammen. Durch das neue Modul wird das deutschlandinterne Abstimmungsverfahren künftig in einer medienbruchfreien Umge-

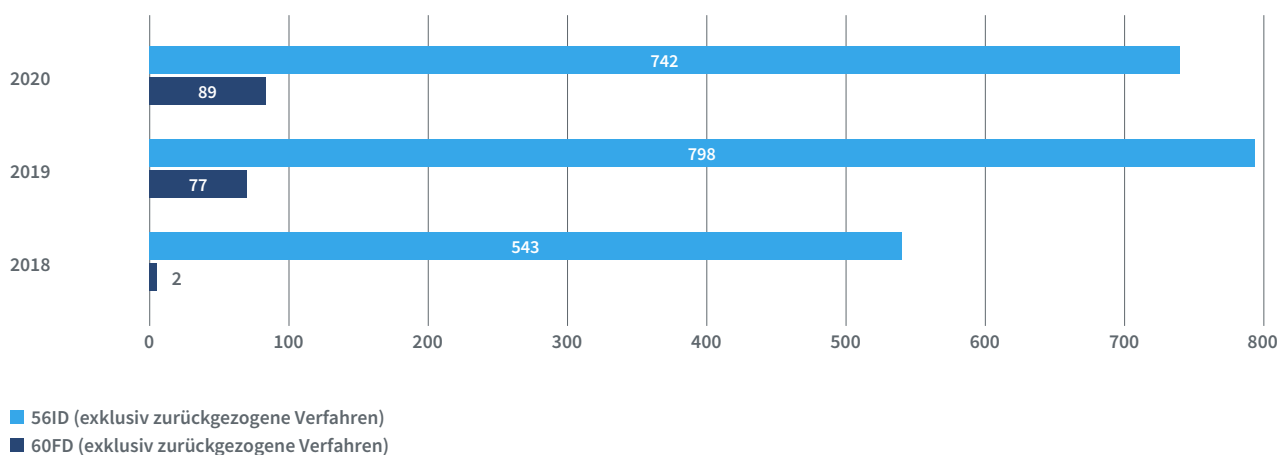
bung noch arbeitseffizienter und sicherer durchgeführt werden können.

### Vermehrter Abschluss von Verfahren im One-Stop-Shop-Verfahren

Das Jahr 2020 markiert insofern eine Zäsur, als dass die Anzahl der Beendigung von Datenschutzverfahren durch abschließende Entscheidung der federführenden Aufsichtsbehörde unter Beteiligung der betroffenen Aufsichtsbehörden nach Art. 60 DSGVO (60FD) kontinuierlich steigt, die Anzahl der 56er-Verfahren im Jahre 2020 jedoch erstmalig (leicht) rückläufig ist (siehe Abbildung „Entwicklung der Verfahren 56ID und 60FD“). Neben dem formellen Abschluss im Verfahren nach Art. 60 DSGVO wurden zudem eine Reihe grenzüberschreitender Fälle durch sogenannte gütliche Einigungen („amicable settlement“) zwischen den verantwortlichen Stellen und den Beschwerdeführenden beendet. Nicht unproblematisch an dieser Art der Verfahrensbeendigung ist, dass die federführende Aufsichtsbehörde die betroffenen Aufsichtsbehörden hierbei häufig nicht beteiligt.

Die deutschen Aufsichtsbehörden sind im europäischen Abstimmungsprozess stark gefordert: Wie die letzte Abbildung dieses Kapitels zeigt, übernimmt Deutschland am dritthäufigsten die Rolle als federführende Aufsichtsbehörde und hat bereits zu 52 von diesen 176 Fällen

Entwicklung der Verfahren 56ID und 60FD

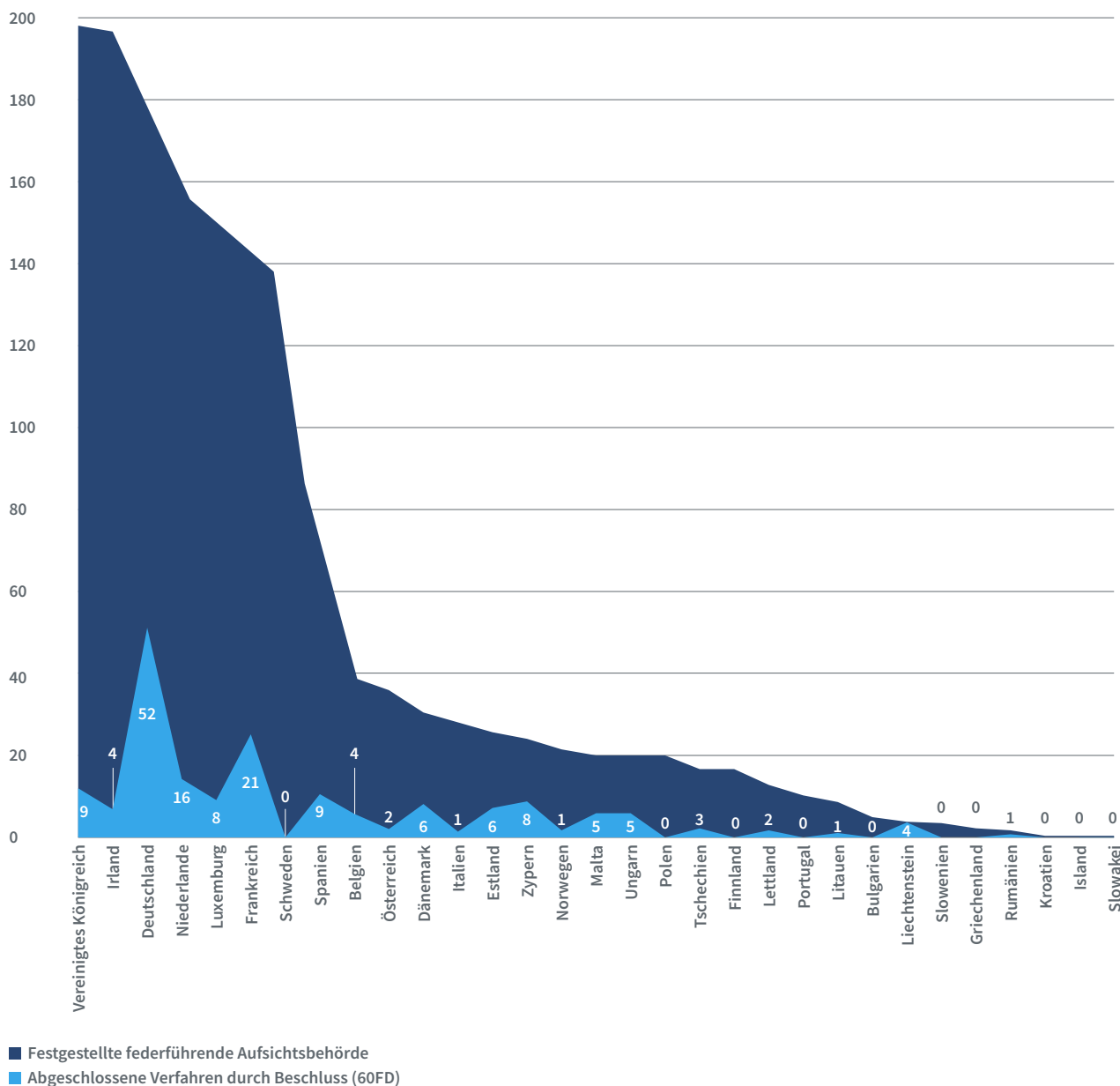


einen verfahrensbeendenden Beschluss vorgelegt. Nach dem endgültigen Ausscheiden Großbritanniens aus der grenzüberschreitenden Fallbearbeitung nach DSGVO zum Ende des Jahres 2020 bearbeitet einzig Irland noch mehr Fälle in federführender Rolle als Deutschland. Allerdings wurden bei 196 Fällen mit festgestellter irischer Federführung bislang nur vier Fälle durch verfahrensbeendenden Beschluss im förmlichen Verfahren nach Art. 60 DSGVO

zum Abschluss gebracht. Dazu kommt eine Reihe von Verfahrensbeendigungen, die die irische Aufsichtsbehörde im Wege gütlicher Einigung herbeigeführt hat.



## Festgestellte federführende Aufsichtsbehörde und Anzahl deren 60FD seit DSGVO-Einführung



Es ist davon auszugehen, dass die Anzahl der 56er-Verfahren auch im Jahr 2021 zurückgehen und die Anzahl der abschließenden Entscheidungen nach Art. 60 DSGVO weiter steigen werden. Mit Spannung darf erwartet werden, wie die Fallbearbeitungen zu den Datenverarbeitungen großer, global agierender Internetkonzerne fortschreiten, die häufig in Irland und Luxemburg ihren europäischen Hauptsitz haben.

# 12 Und dann war da noch...

## 12.1 Die Sache mit den Memes

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) berät unter anderem die Bundesregierung bei datenschutzrechtlich relevanten Gesetzgebungsverfahren. Wie er dabei einzubinden ist und welche Einwirkungsmöglichkeiten er hat, scheint leider nicht allen Beteiligten immer ganz klar zu sein ...

Seit der BfDI im Jahre 2016 aus dem Bundesministerium des Inneren herausgelöst und als eigenständige oberste Bundesbehörde institutionalisiert wurde, ist er auch formell kein Verfassungsorgan mehr. Eine meiner wesentlichsten Aufgaben, die Beratung der Verfassungsorgane bei Gesetzgebungsverfahren mit datenschutzrechtlichen Auswirkungen, nehme ich – wie auch schon in all den Jahren vor seiner Unabhängigkeit - nach wie vor unverändert wahr.

Damit ich meine Beratungsfunktion beispielsweise gegenüber der Bundesregierung effektiv wahrnehmen kann, ist in der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) in § 21 festgelegt, dass der BfDI frühzeitig in alle für ihn relevante Vorhaben der Regierung einzubinden ist. Das war schon immer so, auch vor 2016. Leider war es auch schon immer so, dass die in der GGO festgeschriebene Einbindung immer mal wieder „vergessen“ wurde oder jedenfalls alles andere als frühzeitig erfolgte.

### BfDI vs. Weihnachtsmann

	 BfDI	
1x pro Jahr Tätigkeitsbericht	✓	✓
Liste mit Verstößen	✓	✓
unabhängig	✓	✓
konnte dem BMG <b>keine</b> verpflichtenden Vorgaben beim PDSG machen	✓	✓
Rauschebart	✗	✓

Und leider ist es der Bundesregierung bis heute nicht gelungen, dieses Problem konsequent in den Griff zu kriegen. Auch in diesem Berichtszeitraum gab es zahlreiche Beispiele, in denen ich Gesetzesentwürfe erst mit oder nach der öffentlichen Beteiligung von Verbänden erhalten habe. Oder Fälle, wo ich im Verlauf einer Ressortbeteiligung, in der ich bereits Stellung genommen habe, aus unerklärlichen Gründen auf einmal nicht mehr auf dem E-Mailverteiler stand und dann von einem Kabinettsentwurf überrascht wurde, der 40 Seiten länger als der mir bekannte erste Referentenentwurf war.

### BfDI vs. Batman

	 BfDI	
hilft den Menschen	✓	✓
schützt Identitäten	✓	✓
cooles Logo	✓	✓
kann den Gesetzgeber <b>nicht</b> zwingen seine Vorschläge anzunehmen	✓	✓
hält sich an Recht und Gesetz	✓	✗

### BfDI vs. Harry Potter

	 BfDI	
immer die gleichen Bösewichte	✓	✓
Konflikte mit Ministerien	✓	✓
reist viel mit dem Zug	✓	✓
setzt europäisches Recht um und hält sich an Gerichtsentscheidungen	✓	✗
Ballsportfan	✓	✓

## BfDI vs. Indiana Jones

	 BfDI	
wohnt in einer Universitätsstadt	✓	✓
erzählt historische Anekdoten	✓	✓
Professor	✓	✓
hat <b>mehrfach</b> vor Problemen beim PDSG gewarnt	✓	✗
hasst Schlangen	✗	✓

Natürlich sind das meist unglückliche Zufälle, die grundsätzlich nichts damit zu tun haben, dass Gesetzentwürfe datenschutzrechtlich etwas problematischer sind. Honi soit qui mal y pense!

Vor diesem Hintergrund sollte man bedenken, dass es einen freuen müsste, wenn sich ein Ministerium auf einmal ganz genau daran erinnert, dass und wie der BfDI in Gesetzgebungsverfahren zu beteiligen ist. Daher habe ich das Bundesministerium für Gesundheit (BMG) im Gesetzgebungsverfahren auch über einen langen Zeitraum und ausführlich zum Patientendaten-Schutz-Gesetz (PDSG) beraten (vgl. Nr. 4.2).

Nun ist es so, dass ich – anders als die Ministerien – im Rahmen von Ressortabstimmungen kein Vetorecht habe. Hierfür gab es noch nie eine gesetzliche Grundlage. Sowohl die Bundesregierung als auch erst recht der Gesetzgeber haben die Freiheit, meine Empfehlungen zu ignorieren. Dieser Umstand ist logischerweise auch dem BMG bekannt, das sich im o.g. Verfahren dazu entschieden hatte, einigen meiner Empfehlungen, insbesondere im Zusammenhang mit der elektronischen Patientenakte, nicht zu folgen. Das ist zwar schade, allerdings auch sein gutes Recht.

## BfDI vs. Breaking Bad

	 BfDI	
trägt wenn nötig Maske	✓	✓
vertraut der Wissenschaft	✓	✓
klopft an	✓	✓
warnt die Krankenkassen, weil <b>das BMG seine Beratung ignoriert hat</b>	✓	✗
arbeitet transparent	✓	✗

Umso überraschender war es daher, dass dem Ministerium meine Rolle und Funktion auf einmal urplötzlich entfallen ist, als es darum ging, meine Kritik an Teilen des PDSG gegenüber der Presse zu kommentieren. Dort fanden sich mehrfach Aussagen wie: „Außerdem war der BfDI selbst in die fachlichen Diskussionen eingebunden und hat an der Erarbeitung der Regelungen mitgewirkt.“

Da Gesetzestexte und ähnliche Regelungen oft komplex formuliert sein können und ich meine Beratungsfunktion gegenüber der Bundesregierung als umfassend verstehe, habe ich versucht, die Einwirkungsmöglichkeiten des BfDI u.a. bei Gesetzgebungsverfahren noch einmal mit verständlichen Vergleichen graphisch in Memes aufzubereiten und über Twitter sowie Mastodon zu teilen.

Eine Auswahl dieser Memes möchte ich an dieser Stelle mit Ihnen teilen.

### Querverweis:

#### 4.2 Das Patientendaten-Schutz-Gesetz



# Themenzuordnung nach Bundestagsausschüssen

## **Ausschuss für Arbeit und Soziales**

- 5.8 Die Grundrente kommt – aber auch datenschutzgerecht?
- 7.2 Interdisziplinärer Beirat Beschäftigendatenschutz

## **Auswärtiger Ausschuss**

- 3.3 Global Privacy Assembly
- 7.12 Folgen des Brexit

## **Ausschuss für Bau, Wohnen, Stadtentwicklung und Kommunen**

- 8.1.4 Informationsfreiheitsgesetz des Bundes gilt nicht für der Deutschen Städtetag

## **Ausschuss für Bildung, Forschung und Technikfolgenabschätzung**

- 7.5 Anonymisierung - Eine Standortbestimmung zwischen der DSGVO und dem TKG

## **Ausschuss Digitale Agenda**

- 3.1.3 Datensouveränität
- 3.2.2 Abschluss Evaluierung DSGVO: Die erste Runde ist abgeschlossen
- 3.3 Global Privacy Assembly
- 4.1.1 Die Corona-Warn-App der Bundesregierung
- 4.1.2 Die Datenspende-App
- 4.1.6 Messenger und Videokonferenzsysteme – Fluch und Segen in Corona-Zeiten
- 4.2 Das Patientendaten-Schutz-Gesetz
- 5.2 Die Digitalisierung der Verwaltung schreitet voran
- 5.6 Die Verordnung zu den „Apps auf Rezept“

- 5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich

- 7.8 Microsoft, der Datenschutz und die digitale Souveränität

- 7.9 Künstliche Intelligenz - Fortschritt

- 7.10 Zertifizierung und Akkreditierung – erste Verfahren starten

## **Ausschuss für Ernährung und Landwirtschaft**

- 8.2.1 Streit um die Veröffentlichung einer Stellungnahme zu Glyphosat: Berechtigter Schutz geistigen Eigentums oder Zensur?

## **Ausschuss für Angelegenheiten der Europäischen Union**

- 7.12 Folgen des Brexit

## **Ausschuss für Familie, Senioren, Frauen und Jugend**

- 5.9 Das Digitale Familienleistungen-Gesetz

## **Finanzausschuss**

- 6.8 Neugestaltung des Informationsverbund FIU 2.0
- 6.9 Datenschutzverstoß im Bereich der Zollfahndung
- 6.10 Beschäftigendatenschutz in der Zollverwaltung

## **Ausschuss für Gesundheit**

- 3.1.1 Entschließung zum Patientendaten-Schutz-Gesetz
- 4.1.1 Die Corona-Warn-App der Bundesregierung
- 4.1.2 Die Datenspende-App
- 4.1.3 Corona-Maßnahmen und -Projekte
- 4.1.4 Änderungen des Infektionsschutzgesetzes



- 4.1.5 Schutzmaske nur gegen Daten?
- 4.2 Das Patientendaten-Schutz-Gesetz
- 5.6 Die Verordnung zu den „Apps auf Rezept“
- 5.7 Datentransparenzverordnung
- 7.13 Neue Entwicklungen in der Forschung mit Gesundheitsdaten
- 7.14 Berichtigung von Diagnosedaten
- 7.15 Das Krankengeldfallmanagement – Kein Konsens über den Umfang der Datenerhebungsbefugnisse der Krankenkassen
- 8.1.1 Informationsfreiheit in der Pandemie

#### **Haushaltsausschuss**

- 7.7 IT-Konsolidierung Bund
- 10.3 Personalentwicklung im Jahr 2020
- 10.4 Die neue Liegenschaft

#### **Ausschuss für Inneres und Heimat**

- 3.2.2 Abschluss Evaluierung DSGVO: Die erste Runde ist abgeschlossen
- 5.1 Registermodernisierung
- 5.2 Die Digitalisierung der Verwaltung schreitet voran
- 5.3 IT-Sicherheitsgesetz 2.0
- 5.4 Novellierung des Gesetzes über den Bundesnachrichtendienst
- 5.5 Gesetzgebungsverfahren zur Änderung des Verfassungsschutzrechts
- 5.9 Das Digitale Familienleistungen-Gesetz
- 6.1 Polizei 2020
- 6.2 Einheitliches Fallbearbeitungssystem
- 6.4 Haber-Verfahren
- 6.5 Sicherheitsüberprüfung von Bewerberinnen und Bewerbern der Nachrichtendienste
- 6.11 Beschäftigtendatenschutz in der Zollverwaltung
- 6.12 Geschützter Grenzfeldzugsbestand
- 7.4 Nachbessern, aber bitte richtig – der zweite Beschluss des Bundesverfassungsgerichts zur Bestandsdatenauskunft
- 8.1.1 Informationsfreiheit in der Pandemie

- 8.1.3 Zugang zum Verzeichnis von Verarbeitungstätigkeiten
- 8.1.4 Informationsfreiheitsgesetz des Bundes gilt nicht für der Deutschen Städtetag
- 8.2.2 Was gilt? Das Parteiengesetz oder das Informationsfreiheitsgesetz?
- 8.2.3 Social-Media und die Informationsfreiheit
- 9.4 Beratungs- und Kontrollbesuche zur Anwendung des Informationsfreiheitsgesetzes
- 9.5.1 Kontrollen und Beanstandungen im Bereich des Bundesamtes für Verfassungsschutz
- 9.5.2 Kontrolle der Anti-Terror-Datei
- 9.5.3 Das Vorgangsbearbeitungssystem beim BKA
- 10.2 Urteil des Landgerichts Bonn bestätigt Rechtsauffassung des BfDI

#### **Ausschuss für Menschenrechte und humanitäre Hilfe**

- 3.3 Global Privacy Assembly

#### **Ausschuss für Recht und Verbraucherschutz**

- 4.1.6 Messenger und Videokonferenzsysteme – Fluch und Segen in Corona-Zeiten
- 4.1.7 Zustellung von Paketen unter Pandemiebedingungen
- 5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich
- 6.1 Polizei 2020
- 6.4 Haber-Verfahren
- 7.4 Nachbessern, aber bitte richtig – der zweite Beschluss des Bundesverfassungsgerichts zur Bestandsdatenauskunft
- 7.5 Anonymisierung - Eine Standortbestimmung zwischen der DSGVO und dem TKG
- 8.1.2 Was ist eigentlich ein Geschäftsgeheimnis?
- 8.2.1 Streit um die Veröffentlichung einer Stellungnahme zu Glyphosat: Berechtigter Schutz geistigen Eigentums oder Zensur?
- 8.2.2 Was gilt? Das Parteiengesetz oder das Informationsfreiheitsgesetz?
- 9.5.3 Das Vorgangsbearbeitungssystem beim BKA
- 10.2 Urteil des Landgerichts Bonn bestätigt Rechtsauffassung des BfDI

## **Verteidigungsausschuss**

- 9.3 Änderung der Organisation des behördlichen Datenschutzes im Bundesministerium der Verteidigung
- 9.5.2 Kontrolle der Anti-Terror-Datei

## **Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung**

- 7.1 Datenschutzaufsicht im parlamentarischen Bereich
- 8.2.2 Was gilt? Das Parteiengesetz oder das Informationsfreiheitsgesetz?

## **Ausschuss für Wirtschaft und Energie**

- 4.1.2 Die Datenspende-App
- 4.1.6 Messenger und Videokonferenzsysteme – Fluch und Segen in Corona-Zeiten
- 4.1.7 Zustellung von Paketen unter Pandemiebedingungen
- 4.1.8 Programme für Sofort- bzw. Überbrückungshilfen des Bundes im Zusammenhang mit der Corona-Pandemie
- 5.10 Aktuelle Gesetzgebung und sonstige Regelungen im Telekommunikationsbereich
- 7.5 Anonymisierung - Eine Standortbestimmung zwischen der DSGVO und dem TKG
- 7.12 Folgen des Brexit
- 8.1.2 Was ist eigentlich ein Geschäftsgeheimnis?
- 9.1 Fragenbogenkontrolle zur Authentifizierung bei Call-Centern
- 9.2 Fragebogenkontrolle Handscanner
- 10.2 Urteil des Landgerichts Bonn bestätigt Rechtsauffassung des BfDI

# Anlagen

## Anlage 1

### Kontrollen, Beratungs- und Informationsbesuche

1&1 Drillisch AG incl. aller Konzernmarken  
Amazon Deutschland E1 Transport GmbH  
Amazon Deutschland E2 Transport GmbH  
Amazon Deutschland E3 Transport GmbH  
Amazon Deutschland E4 Transport GmbH  
Amazon Deutschland E5 Transport GmbH  
Amazon Deutschland N1 Transport GmbH  
Amazon Deutschland N2 Transport GmbH  
Amazon Deutschland N3 Transport GmbH  
Amazon Deutschland N6 Transport GmbH  
Amazon Deutschland N7 Transport GmbH  
Amazon Deutschland S3 Transport GmbH  
Amazon Deutschland S4 Transport GmbH  
Amazon Deutschland Transport GmbH  
Amazon Deutschland W1 Transport GmbH  
Amazon Deutschland W2 Transport GmbH  
Amazon Deutschland W4 Transport GmbH  
Amazon Deutschland W5 Transport GmbH  
Amazon Deutschland W7 Transport GmbH  
Amazon Logistik Westfalenhütte GmbH  
Bundesamt für den Militärischen Abschirmdienst  
Bundesamt für die Sicherheit der nuklearen Entsorgung  
Bundesamt für Verfassungsschutz

Bundesanstalt für Finanzdienstleistungen  
Bundesinstitut für Arzneimittel und Medizinprodukte  
Bundeskriminalamt  
Bundesnachrichtendienst  
Bundespolizei  
Bundeswehr, Assessmentcenter für Führungskräfte  
Bundeszentrale für politische Bildung  
Deutsche Rentenversicherung Bund  
Deutsche Telekom AG incl. aller Konzernmarken  
Deutsche Welle  
DHL Paket GmbH  
DPD Deutschland GmbH  
Drillisch Online GmbH  
Ein Unternehmen im Rahmen des Sicherheitsüberprüfungsgesetzes\*  
EWE-TEL GmbH  
Freenet AG incl. aller Konzernmarken  
General Logistics Systems Germany GmbH & Co. OHG  
Generalzolldirektion  
Hanse-Jobcenter-Rostock  
Hermes Germany GmbH  
Jobcenter Berlin Friedrichshain-Kreuzberg  
Jobcenter Bremen  
Jobcenter Dresden  
Jobcenter Erfurt  
Jobcenter Kaiserslautern Stadt  
Jobcenter Kiel  
Jobcenter Köln

Jobcenter Landeshauptstadt Potsdam

Jobcenter Landkreis Diepholz

Jobcenter Landkreis Kaiserslautern

Jobcenter Landkreis Karlsruhe

Jobcenter Magdeburg

Jobcenter Mainz

Jobcenter Mannheim

Jobcenter München

Jobcenter Region Hannover

Jobcenter Regionalverband Saarbrücken

Jobcenter Stadt Kassel

Jobcenter team.arbeit.hamburg

Jobcenter Vorpommern-Greifswald Nord

Jobcenter Zollernalbkreis

KEVAG Telekom GmbH

Lycamobile Germany GmbH

M-net Telekommunikations GmbH

NetCologne Gesellschaft für Telekommunikation mbH

SSY Transport und Personalleasing GmbH

Statistisches Bundesamt

Technisches Hilfswerk

Tele Columbus AG

Telefónica Germany GmbH & Co. OHG incl. aller Konzernmarken

United Parcel Service Deutschland S.à.r.l. & Co. OHG

Unitymedia GmbH incl. aller Konzernmarken

Vodafone GmbH incl. aller Konzernmarken

Zentralstelle für Finanztransaktionsuntersuchungen

Zollfahndungsamt Frankfurt

Zollkriminalamt

Einige Stellen wurden mehr als einmal besucht/kontrolliert

\*Der Name darf aus sicherheitspolitischen Gründen nicht genannt werden

## Anlage 2

### Übersicht über Anweisungen, Beanstandungen, Verwarnungen, Geldbußen

#### 2. Kompanie Feldjägerregiment 3

Unzulässiger Betrieb einer Videoüberwachungsanlage

#### Ausbildungszentrum Technik Landsysteme der Bundeswehr

Freigabe dienstlicher Laptops zum Verkauf ohne vorherige Löschung personenbezogener Daten

#### Bayerisches Landesamt für Steuern

Warnung wegen Einwilligungsmo-  
dell bei unverschlüsselter E-Mail-Versand

#### Bundesagentur für Arbeit

Beteiligung des Personalrats im Gleichstellungsverfahren trotz fehlender Zustimmung des betroffenen Mitarbeiters

#### Bundesamt für Justiz

Verwarnung wegen der gem. DSGVO nicht erforderlichen, unverschlüsselten Übermittlung von personenbezogenen Daten in versendeten Eingangsbestätigungen an Nutzerinnen und Nutzer von durch das Bundesamt für Justiz bereitgestellten Kontaktformularen und dadurch erfolgter Verstoß gegen den Datenverarbeitungsgrundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO)

#### Bundesamt für Verfassungsschutz

Beanstandung, weil Datenverarbeitungen im Rahmen des sog. Haber-Verfahrens ohne gesetzliche Rechtsgrundlage erfolgen

#### Bundesamt für Wirtschaft und Ausfuhrkontrolle

Verwarnung wegen fehlender Auftragsverarbeitungsverträge

#### Bundeskriminalamt

Beanstandung wegen Datenübermittlungen in Drittstaaten

Beanstandung wegen unzulässiger Übermittlung von Daten

Beanstandung wegen 30 Jahre andauernder Speicherung als Kontakt- und Begleitperson ohne nachweisbaren Kontakt/Verweigerung der Beauskunftung

Beanstandung wegen Auskunftsverlangens des BKA vom 5. November 2019, Rechtmäßigkeit von Bestandsdatenauskünften, Auskunftersuchen wurde auf § 113 Abs. 1 TKG i. V. m. § 100j Abs. 1, 2 StPO gestützt

#### Bundeswehrkrankenhaus Koblenz

Zugriff auf das Zeiterfassungssystem durch einen unberechtigten Personenkreis

#### Deutsche Post AG

Verwarnung wegen kontinuierlichen Falschzustellungen

#### Deutsche Telekom AG

Verwarnung wegen fehlerhafter Zusammenlegung von Kundendaten

#### Finanzamt Halle (Saale)

Verwarnung wegen Verstoßes gegen Art. 5 Abs. 1 lit. f DSGVO sowie gegen Art. 6 Abs. 1 lit. e, Abs. 3 DSGVO i.V.m. § 29b Abgabenordnung (AO) i.V.m. § 5 Abs. 1 S. 1 Verwaltungszustellungsgesetz (VwZG), indem Mitarbeiter Firmenunterlagen in einem unverschlossenem Behältnis an den Sohn des Liquidators dieser Firma übergeben haben

#### Finanzamt Stade

Verwarnung wegen zu geringer Sorgfalt im Vorfeld einer Kontopfändung

#### Finanzamt Starnberg

Verwarnung wegen Interessenkollision Datenschutzbeauftragter

#### Finanzministerium des Landes Schleswig-Holstein

Warnung wegen Verstoßes gegen die in den Artikeln 5 Absatz 1 lit. f), 24 und 32 DSGVO geregelten Anforderungen zur angemessenen Sicherheit der personenbezogenen Daten im Falle von unverschlüsselter Versand von E-Mails durch die der Aufsicht des Finanzministeriums unterliegenden Finanzbehörden an Steuerpflichtige und Dritte je nach Art und Sensibilität der übermittelten Informationen auch trotz einer vermeintlichen Einwilligung aller Beteiligten gegen die in den Artikeln 5 Absatz 1 lit. f), 24 und 32 DSGVO geregelten Anforderungen zur angemessenen Sicherheit der personenbezogenen Daten.

#### Hauptzollamt Gießen

Untersagung der Löschung einer Beurteilungsnotiz

#### Hermes Germany GmbH

Verwarnung wegen Verlust von Orientierungslisten

Verwarnung wegen Fertigung von Fotografien von Sendungsempfängern



**Institut für Präventivmedizin**

Überschreiten der Aufbewahrungsfrist bei der Speicherung von Gesundheitsdaten auf Mikrofilmen

**Jobcenter Bad Kreuznach**

Erhebung und Speicherung personenbezogener Daten ohne Rechtsgrundlage, Verstoß gegen die Voraussetzungen einer Einwilligung nach Art. 4 Nr. 11 und Art. 7 DSGVO

**Jobcenter Berlin Neukölln**

Verfristete Auskunft nach Art. 15 DSGVO

**Jobcenter Berlin Pankow**

Filmen der Kunden mit dem Diensthandy ohne Rechtsgrundlage

**Jobcenter Düsseldorf**

Fehlende Unterrichtung des Leistungsempfängers über das Ergebnis des erfolgten Kontenabrufes nach § 93 AO

**Jobcenter Erfurt**

Verarbeitung von Sozialdaten für die Arbeitsvermittlung, obwohl kein Leistungsbezug mehr vorlag

**Jobcenter Hildesheim**

Verstoß gegen das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO

**Jobcenter Jerichower Land**

Verfristete und unvollständige Auskunft nach Art. 15 DSGVO

**Jobcenter Köln**

Verfristete Auskunft nach Art. 15 DSGVO

**Jobcenter Landkreis Germersheim**

Verstoß gegen den „Ersterhebungsgrundsatz“ (§ 67a Abs. 2 Satz 1 SGB X)

**Jobcenter Landkreis Harburg**

Erhebung und Speicherung personenbezogener Daten ohne Rechtsgrundlage

**Jobcenter Landkreis Konstanz**

Verfristete Auskunft nach Art. 15 DSGVO

**Jobcenter Nürnberg Stadt**

Unzulässige Erhebung personenbezogener Daten bei Dritten

**Jobcenter Osnabrück**

Unzulässige Anforderung von Einkommensbescheinigungen beim Arbeitgeber im Rahmen des Datenabgleiches

**Jobcenter Rhein-Kreis Neuss**

Verstoß gegen den „Ersterhebungsgrundsatz“ (§ 67a Abs. 2 Satz 1 SGB X)

**Jobcenter Städteregion Aachen**

Unzulässige Aushändigung von Briefpost an einen Dritten

**Jobcenter team.arbeit.hamburg**

Versendung besonderer Kategorien von Sozialdaten per unverschlüsselter E-Mail

**Jobcenter Vorpommern Greifswald Nord**

Erhebung und Speicherung personenbezogener Daten ohne Rechtsgrundlage

**Systemzentrum 25 (Bundeswehr)**

Veröffentlichung von Profilbildern der Beschäftigten der Dienststelle auf Befehl im Blog „Confluence“

**Tele Columbus AG**

Anweisung, da keine Stellungnahme zu einer Petentenbeschwerde abgegeben wurde

**Telefónica Germany GmbH & Co. OHG**

Beanstandung gemäß § 115 Abs. 4 TKG i. V. m. § 104 TKG wegen Eintragungen in gedruckte und in Online-Teilnehmerverzeichnisse, ohne die hierfür erforderlichen Zustimmungen einzuholen

**Telekom Deutschland GmbH**

Verwarnung wegen fehlender Einwilligung bei Magenta1 Tarifen

**Unitymedia BW GmbH**

Verwarnung wegen verspäteter Meldung einer Datenschutzverletzung nach Art. 33 DSGVO

**Vodafone BW GmbH**

Verwarnung, da die Löschung eines Eintrags in Telefonbüchern- und -verzeichnissen nicht veranlasst worden ist

**Vodafone Kabel Deutschland GmbH**

Anweisung wegen mangelnder Löschung von Bestandsdaten nach Vertragsende

**Vodafone NRW GmbH**

Verwarnung DSGVO wegen unrechtmäßiger Verarbeitung der IBAN eines Dritten

**Zollfahndungsamt Berlin-Brandenburg**

Nicht datenschutzkonformer Betrieb einer elektronischen Zutrittskontroll- und Alarmanlage, Verstoß gegen die Informationspflichten

## Abkürzungsverzeichnis

<b>Abs.</b>	Absatz	<b>BND-Gesetz</b>	Gesetz über den Bundesnachrichtendienst
<b>AG</b>	Aktiengesellschaft	<b>BNetzA</b>	Bundesnetzagentur
<b>AK</b>	Arbeitskreis	<b>bpb</b>	Bundeszentrale für politische Bildung
<b>AkkStelleG</b>	Gesetz über die Akkreditierungsstelle	<b>BPol</b>	Bundespolizei
<b>AO</b>	Abgabenordnung	<b>BPolG</b>	Gesetz über die Bundespolizei
<b>API-Daten</b>	Advanced Passenger Information (Vorab-Passagier-Information)	<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>API-RL</b>	RICHTLINIE 2004/82/EG DES RATES vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln	<b>BT</b>	Bundestag
<b>App(s)</b>	Applikation(en)	<b>BVerfG</b>	Bundesverfassungsgericht
<b>Art.</b>	Artikel	<b>BVerfSchG</b>	Bundesverfassungsschutzgesetz
<b>ATD</b>	Anti-Terror-Datei	<b>BVerwG</b>	Bundesverwaltungsgericht
<b>ATDG</b>	Antiterrordateigesetz	<b>BvR</b>	Aktenzeichen einer Verfassungsbeschwerde beim Bundesverfassungsgericht
<b>Az.</b>	Aktenzeichen	<b>bzw.</b>	beziehungsweise
<b>BAMAD</b>	Bundesamt für den Militärischen Abschirmdienst	<b>CCC</b>	Chaos Computer Club
<b>BAMF</b>	Bundesamt für Migration und Flüchtlinge	<b>CWA</b>	Corona Warn App
<b>BCR</b>	Binding Corporate Rules	<b>d.h.</b>	das heißt
<b>BDSG</b>	Bundesdatenschutzgesetz	<b>DAkkS</b>	Deutsche Akkreditierungsstelle
<b>BEEG</b>	Bundeselterngeld- und Elternzeitgesetzes	<b>DEK</b>	Datenethikkommission
<b>BfArM</b>	Bundesinstitut für Arzneimittel und Medizinprodukte	<b>DEMIS</b>	Deutsches Elektronischen Melde- und Informationssystems für den Infektionsschutz
<b>BfDBw</b>	behördliche Datenschutzbeauftragte des Bundesministeriums der Verteidigung	<b>DiGA</b>	Digitale Gesundheitsanwendungen
<b>BfDI</b>	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	<b>DiGAV</b>	Digitale Gesundheitsanwendungen Verordnung
<b>BfR</b>	Bundesinstitut für Risikobewertung	<b>DigFamG</b>	Gesetz zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen
<b>BfV</b>	Bundesamt für Verfassungsschutz	<b>DIMDI</b>	Deutsches Institut für Medizinische Dokumentation und Information
<b>BImA</b>	Bundesanstalt für Immobilienaufgaben	<b>DSGVO</b>	Datenschutz-Grundverordnung
<b>BKA</b>	Bundeskriminalamt	<b>DSK</b>	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
<b>BKAG</b>	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten	<b>DSRV</b>	Datenstelle der Rentenversicherung
<b>BMG</b>	Bundesministerium für Gesundheit	<b>DVG</b>	Digitale-Versorgungs-Gesetz
<b>BMI</b>	Bundesministerium des Innern, für Bau und Heimat	<b>EDSA</b>	Europäischer Datenausschuss
<b>BMVg</b>	Bundesministeriums der Verteidigung	<b>eFBS</b>	einheitliches Fallbearbeitungssystem
<b>BMWl</b>	Bundesministeriums für Wirtschaft und Energie	<b>EG</b>	Europäische Gemeinschaft
<b>BND</b>	Bundesnachrichtendienst	<b>eGK</b>	elektronische Gesundheitskarte
<b>BNDG</b>	Gesetz über den Bundesnachrichtendienst	<b>EGovG</b>	E-Government-Gesetzes
		<b>eIDAS</b>	Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen
		<b>ePA</b>	Elektronische Patientenakte
		<b>EU</b>	Europäische Union
		<b>EuGH</b>	Europäischer Gerichtshof
		<b>EWR</b>	Europäischer Wirtschaftsraum

<b>FDZ</b>	Forschungsdatenzentrum	<b>MAD-Gesetz</b>	Gesetz über den Militärischen Abschirmdienst
<b>ff.</b>	fortfolgende		
<b>FIU</b>	Zentralstelle für Finanztransaktionsuntersuchungen, Abk. für Financial Intelligence Unit	<b>MHH</b>	Medizinische Hochschule Hannover
		<b>Mio.</b>	Millionen
<b>FlugDaG</b>	Gesetz über die Verarbeitung von Fluggastdaten	<b>NFC</b>	Near Field Communication
		<b>Nr.</b>	Nummer
<b>gem.</b>	gemäß	<b>OHG</b>	offene Handelsgesellschaft
<b>GeschGehG</b>	Geschäftsgeheimnisgesetz	<b>OKF</b>	Open Knowledge Foundation
<b>GG</b>	Grundgesetz	<b>OVG</b>	Oberverwaltungsgericht
<b>ggf.</b>	gegebenenfalls	<b>OWiG</b>	Ordnungswidrigkeitengesetz
<b>GGFB</b>	Geschützter Grenzfahndungsbestand	<b>OZG</b>	Onlinezugangsgesetz
<b>GGO</b>	Gemeinsame Geschäftsordnung der Bundesministerien	<b>PartG</b>	Parteiengesetz
<b>GKV</b>	Gesetzliche Krankenversicherung	<b>PDSG</b>	Patientendaten-Schutz-Gesetz
<b>GKV-SP</b>	Spitzenverband Bund der Krankenkassen	<b>PEPP-PT</b>	Pan-European Privacy-Preserving Proximity Tracing
<b>GmbH</b>	Gesellschaft mit beschränkter Haftung	<b>PIAV</b>	polizeilicher Informations- und Analyseverbund
<b>GPA</b>	Global Privacy Assembly	<b>PIMS</b>	Personal Information Management Systems
<b>HS</b>	Halbsatz	<b>PIN</b>	Persönliche Identifikationsnummer
<b>HZI</b>	Helmholtz-Zentrum für Infektionsforschung	<b>PNR-Daten</b>	Fluggastdatensätze
		<b>PNR-RL</b>	Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen
<b>i.S.d.</b>	im Sinne des	<b>PoC</b>	Proof of Concept
<b>i.v.m.</b>	in Verbindung mit		
<b>IARC</b>	International Agency for Research on Cancer	<b>RED</b>	Rechtsextremismus-Datei
<b>IFG</b>	Informationsfreiheitsgesetz	<b>RegMoG</b>	Registermodernisierungsgesetz
<b>IfSG</b>	Infektionsschutzgesetz	<b>RKI</b>	Robert Koch-Institut
<b>IMI</b>	Binnenmarkt-Informationssystem	<b>RL</b>	Richtlinie
<b>IP</b>	Internet Protocol		
<b>IT</b>	Informationstechnik	<b>s.</b>	siehe
<b>ITZ Bund</b>	Informationstechnikzentrum Bund	<b>S.</b>	Seite
		<b>S.</b>	Satz
<b>JI-Richtlinie</b>	Richtlinie zum Datenschutz bei Polizei und Justiz	<b>SGB</b>	Sozialgesetzbuch
		<b>SMS</b>	Short Message Service
		<b>sog.</b>	so genannte
<b>KaDoIn</b>	Kartenbasierte Dokumentation von Indexpatienten	<b>SORMAS</b>	Surveillance Outbreak Response Management und Analysis System
<b>KEYP</b>	Key Provisions Expert Subgroup	<b>SSO</b>	Single Sign-On
<b>KI</b>	Künstliche Intelligenz	<b>Steuer-ID</b>	Steuer-Identifikationsnummer
<b>KMU</b>	kleine und mittlere Unternehmen	<b>StPO</b>	Strafprozessordnung
		<b>SÜG</b>	Sicherheitsüberprüfungsgesetz
<b>LfD</b>	Landesbeauftragter für den Datenschutz	<b>TB</b>	Tätigkeitsbericht
<b>LfDI/LDI</b>	Landesbeauftragte/r für den Datenschutz und die Informationsfreiheit	<b>THW</b>	Technisches Hilfswerk
<b>LG</b>	Landgericht	<b>TI</b>	Telematikinfrastruktur
<b>LIBE</b>	Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des EU-Parlaments	<b>TK</b>	Telekommunikation
<b>lit.</b>	Litera	<b>TKG</b>	Telekommunikationsgesetz
		<b>TKMoG</b>	Telekommunikationsmodernisierungsgesetz

<b>TTDSG</b>	Telekommunikations-Telemedien-Datenschutz-Gesetz	<b>z.B.</b>	zum Beispiel
<b>u.a.</b>	unter anderem	<b>ZAST</b>	Zentrale Anlaufstelle
<b>UIG</b>	Umweltinformationsgesetz	<b>ZenDis</b>	Zentrum Digitale Souveränität
<b>USA</b>	United States of America	<b>ZFdG</b>	Gesetz über das Zollkriminalamt und die Zollfahndungsämter
<b>UrhG</b>	Urheberrechtsgesetz	<b>ZfKD</b>	Zentrum für Krebsregisterdaten
<b>VBS</b>	Vorgangsbearbeitungssystem	<b>56ID</b>	Identifikation der federführenden Aufsichtsbehörde
<b>VG</b>	Verwaltungsgericht	<b>60FD</b>	endgültiger Beschluss der federführenden Aufsichtsbehörde (Final Decision)
<b>vgl.</b>	vergleiche		
<b>VIS</b>	Visa-Informationssystem		
<b>vs.</b>	versus		

# Schlagwortverzeichnis

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

Abhilfemaßnahmen	4.1.2, 9.1
Akkreditierung	3.2, 3.2.4, 7.10
Angemessenheitsbeschluss	7.12, 9.5.4
Anonymisierung	4.1.3, 6.1, 7.5
Anti-Terror-Datei	9.5.2
Apps	3.3, 4.1.1, 4.1.2, 4.1.6, 4.2, 5.4, 5.6, 8.1.1, 10.5
Auftragsverarbeitung	6.10, 7.8, 9.5.4
Befugnisse	4.1.4, 5.2, 5.3, 5.4, 5.5, 6.4, 6.7, 6.10, 7.4, 7.16, 10.1
Beschäftigtendatenschutz	4.1.6, 6.10, 7.2,
Beschwerden	4.1.5, 6.11, 7.14, 7.15, 8.1.1, 10.6
Biometrie	3.2, 9.1
Brexit	7.12
Bundesagentur für Arbeit	4.1.9
Bundesamt für Verfassungsschutz	9.5.1
Bundesclient	7.7, 7.8
Bundescloud	7.7
Bundesdatenschutzgesetz	5.10, 7.10, 7.16, 8.1.3, 10.1, 11.1, 11.2
Bundeskriminalamt	6.1, 7.4, 9.5.2, 9.5.3, 9.5.4
Bundesnachrichtendienst	5.4, 6.3
Bundesnetzagentur	7.16, 9.1
Bundespolizei	4.1.4, 6.2, 6.7, 6.11, 6.12, 7.4
Bußgeld	4.1.4, 4.1.5, 9.1, 10.2
Cookies	3.2.1, 5.10
Datenbank	5.1, 5.7, 6.6, 6.8
Datenethikkommission	7.9
Datenminimierung	4.1.2
Datenschutzbeauftragte, betrieblich/behördlich	9.3
Datenschutz-Grundverordnung	3.1.3, 3.2.2, 4.2, 4.3, 5.10, 7.1, 7.5, 7.6, 7.12, 7.14, 7.15, 8.1.3, 10.1, 10.2, 11.1
Datenschutzkonferenz,national	3.1 ff, 5.1, 7.8, 7.10, 11.1
Datenschutzkonferenz, international	3.3
Datenschutzverletzung	6.9
Datensouveränität	3.1.3, 4.3
Datentransparenz	4.2, 5.7, 7.3, 7.13
Datenübermittlung	3.2.2, 4.2, 4.3, 5.1, 5.4, 5.9, 6.1, 6.3, 6.7, 7.6, 7.8, 7.12, 7.14, 9.5.1, 9.5.4
Deutscher Bundestag	5.1, 5.5, 7.1, 7.9, 8.2.2, 10.3

Einwilligung	3.2, 3.2.1, 4.1.4, 5.2, 5.6, 5.10, 7.5, 7.6, 7.13, 7.14, 10.1
Entschließung	3.1.1, 3.1.2, 3.3, 4.2, 5.1, 6.1, 7.4
E-Privacy-Verordnung	5.10
Europäischer Datenschutzausschuss	3.2
Europäischer Gerichtshof	3.2, 4.3, 6.6, 7.1
Europäische Kommission	3.2.2, 5.10
EU-US Privacy Shield	4.3
Evaluierung	3.2.2, 4.1.2, 6.1, 11.1
Facebook	4.1.6, 4.3
Fallbearbeitungssystem, Einheitliches	6.2
Fluggastdaten	4.1.4, 6.6
Gesichtserkennung	3.2.3, 3.3
Global Privacy Assembly (Internationale Datenschutzkonferenz )	3.3
Informationsfreiheit	8 ff, 9.4
Interoperabilität	5.2, 5.10
IT-Dienstleister, Bund	6.2
IT-Konsolidierung, Bund	7.7
IT-Sicherheitsgesetz	5.3
JI-Richtlinie	6.7, 11.1
Jobcenter	4.1.9
Kohärenzverfahren	3.2, 3.2.4
Künstliche Intelligenz	6.1, 7.2, 7.9, 7.13
Meldepflicht	4.1.3, 4.1.4, 4.3
Messenger-Dienste	4.1.6, 5.10, 8.2.3
Onlinezugangsgesetz	5.2, 5.9
Passenger Name Records (PNR)	6.6
Patientenakte	4.2, 7.3, 7.13, 10.1
Patientendaten	3.1.1, 4.2, 10.1
Pflichtkontrollen	9.5
Polizei 2020	6.1,
Polizeigesetze	6.1, 6.7, 7.4
Post	4.1.7, 9.2
Privacy by Design	3.1.3
Registermodernisierung	3.1.2, 5.1, 5.2, 5.8
Schengener Informationssystem	6.12, 9.5.1
Schrems II	4.3
Sicherheit der Verarbeitung	4.1.4, 9.1
Sicherheitsüberprüfung	6.5, 9.5.5



Telekommunikationsgesetz	5.10, 7.4, 7.16
Telematik	4.2, 5.6
Tracing	4.1.1, 4.1.2
Tracking	3.2.1, 4.1.3, 5.6, 7.2
Verschlüsselung	3.1.5, 6.9, 7.13
Videoidentverfahren	7.11
Videokonferenz	3.1, 3.2, 4.1.6, 5.10, 10.3
Windows	7.8
Wirtschaftsunternehmen	9.5.5
Zensus	
Zentrale Anlaufstelle	11.1, 11.2
Zentralstelle	6.6, 6.8
ZfDG	6.7
Zollfahndung	6.7, 6.9

**Der Bundesbeauftragte für den Datenschutz  
und die Informationsfreiheit**

Graurheindorfer Str. 153  
53117 Bonn

Tel. +49 (0) 228 997799-0

E-Mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Internet: [www.datenschutz.bund.de](http://www.datenschutz.bund.de); [www.bfdi.bund.de](http://www.bfdi.bund.de)

Bonn 2021

Dieser Bericht ist als Bundestagsdrucksache erschienen.

Bildnachweis: BfDI, TOMZ, Pfohlmann, T. Plaßmann, Schwarwel, Klaus Stuttmann, Kittihawk

Druck:

Silber Druck oHG

Otto-Hahn-Straße 25

34253 Lohfelden









