Tätigkeitsbericht 2022

31. Tätigkeitsbericht
für den Datenschutz und
die Informationsfreiheit

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Dieser Bericht wurde der Präsidentin des Deutschen Bundestags, Frau Bärbel Bas, 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 2022
– 31. Tätigkeitsbericht –

Inhaltsverzeichnis

Einleitung ... 8

2 Empfehlungen ... 10
2.1 Zusammenfassung der Empfehlungen des 31. Tätigkeitsberichts ... 10
2.2 Empfehlungen des 30. Tätigkeitsberichts ... 11

3 Gremien ... 12
3.1 Übersicht Gremienarbeit ... 12
3.2 Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ... 12
3.2.1 DSK-Vorsitz und DSK 2.0 ... 13
3.2.2 DSK Taskforce Souveräne Cloud ... 14
3.2.3 DSK Arbeitskreis Microsoft ... 15
3.2.4 Neue Entschließung der DSK zum Beschäftigtendatenschutzgesetz ... 16
3.2.5 Aktenvernichtungs- und Datenlöschmoratorium ... 17
3.2.6 Orientierungshilfe Werbung 2.0 ... 18
3.3 Europäischer Datenschutzausschuss ... 18
3.3.1 Allgemeiner Bericht ... 18
3.3.2 Umsetzung der EDSA-Strategie 2021-2023 ... 22
3.3.3 Coordinated Enforcement Action 2021/2022 ... 22
3.3.4 EU-Systeme: Zentrale Koordinierung der Aufsicht im CSC ... 23
3.3.5 EDSA veröffentlicht Leitlinien zum Auskunftsrecht ... 24
3.3.6 EDSA legt Bußgeld-Leitlinien vor ... 25
3.3.7 Leitlinien zu Art. 60 DSGVO ... 25
3.3.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Corporate Rules ... 26
3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield Nachfolge) ... 26
3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers ... 28
3.4 G7 Roundtable ... 29
3.5 Weitere internationale Gremien ... 30
3.5.1 Jahreskonferenz der Global Privacy Assembly 2022 ... 30
3.5.2 Berlin Group ... 31
3.5.3 Neues ETIAS-Beratungsgremium für Grundrechte ... 31
3.5.4 Bericht aus den SCGs ... 32

4 Schwerpunktthemen ... 34
4.1 Forschungsdaten ... 34
4.1.1 Symposium Forschung mit Gesundheitsdaten ... 34
4.1.2 Forschungsdatenzentrum Gesundheit ... 35

4.1.3 Taskforce Forschungsdaten ... 36
4.1.4 Petersberger Erklärung ... 37
4.2 Europäische Digitalrechtsakte ... 38
4.2.1 KI-Verordnung ... 38
4.2.2 Digital Services Act ... 39
4.2.3 Digital Markets Act ... 40
4.2.4 Data Governance Act ... 40
4.2.5 Data Act ... 41
4.2.6 Verordnung Politische Werbung ... 41
4.3 Digitale Medien ... 42
4.3.1 Verfahren Facebook Fanpages ... 42
4.3.2 Entscheidungen europäischen Aufsichtsbehörden zu Google Analytics ... 43
4.3.3 Einsatz eines Content-Distribution-Network (CDN) für die Website des Zensus 2022 ... 44
4.4 Einsatz von KI im Sicherheitsbereich ... 45
4.4.1 CSAM-Verordnung ... 45
4.4.2 Ergebnisse Konsultationsverfahren zur Künstlichen Intelligenz ... 46
4.4.3 EDSA-Richtlinien zum Einsatz von Gesichtserkennungstechnologie ... 47
4.5 Evaluierung der JI-Richtlinie und unzureichende Abhilfebefugnisse des BfDI in den Bereichen der Gefahrenabwehr und der Strafverfolgung ... 47

5 Gesetzgebung ... 49
5.1 European Health Data Space ... 49
5.2 Regelungen zur Bewältigung der COVID-19-Pandemie ... 50
5.3 Änderungen bei der Geldwäschebekämpfung und der Durchsetzung von Sanktionen ... 51
5.4 Hinweisgeberschutzgesetz ... 52
5.5 Dienste zur Einwilligungsverwaltung ... 53
5.6 Neues EES- und ETIAS-Durchführungsgesetz ... 54

6 Informationsfreiheit ... 55
6.1 Konferenz der Informationsfreiheitsbeauftragten ... 55
6.2 Erfahrungsaustausch der obersten Bundesbehörden ... 55
6.3 Transparenzgesetz ... 56
6.4 Beratungs- und Kontrollbesuch beim BSI ... 57
6.5 IFG-Vermittlungsverfahren ... 57
6.5.1 Kampagne zum Lobbyregister ... 57
6.5.2 Die Bestimmtheit eines IFG-Antrages ... 57
6.5.3 Recht aus Auskunft nach dem Umweltinformationsrecht ... 58
6.5.4 Bahnunfälle auf Schweizer Gebiet – erfolgreiche Vermittlung für eine Petentin ... 58
6.5.5 Die Bereichsausnahme für Nachrichtendienste gilt auch für den BfDI ... 58
6.6 Statistische Auswertungen IFG für 2022 ... 59

7 Sicherheitsbereich ... 61
7. 1 Passenger Name Records (PNR) – Grundsatzurteil des EuGH bestätigt Handlungsbedarf ... 61
7.2 Polizei 20/20 – P 20 ... 62
7.3 Einschaltung Dritter bei Quellen-TKÜ und Onlinedurchsuchung ... 64
7.4 Kennzeichenerfassung Bundespolizei ... 64
7.5 Verstärkte Tätigkeiten im Bereich der Strafjustizbehörden ... 65
7.6 Der Verfassungsschutz und das Bundesverfassungsgericht ... 65
7.7 Beanstandungen des BAMAD und des BfV aufgrund der Verletzung der Unterstützungspflicht ... 68
7.8 Personenbezogene Daten in Informationsschreiben des BfV ... 69
7.9 Endlich: eine gesetzliche Grundlage für die ZITiS ... 69
7.10 Wildwuchs bei Überprüfungsverfahren ... 70

8 Weitere Einzelthemen ... 72
8.1 Aktuelles aus der Telematikinfrastruktur und von ihren Anwendungen ... 72
8.2 Digitale Gesundheitsanwendungen ... 74
8.3 Sormas (follow up) ... 75
8.4 Nutzung der Krankenversichertennummer (follow up) ... 75
8.5 Corona-Warn-App: Änderungen 2022 ... 75
8.6 Registermodernisierung/OZG-Umsetzung ... 76
8.7. Betriebliches Eingliederungsmanagement (BEM) ... 78
8.8 Zensus 2022 ... 79
8.9 Datenschutz bei Onlinevirenscannern ... 80
8.10 Digitale Datenräume und Mobilitätsdaten im Verkehrssektor ... 81
8.11 TrustPid – neue Wege der personalisierten Werbung ... 82
8.12 Videokonferenzdienste ... 83
8.13 Neues von der E-Mail – Zuständigkeitswechsel zum BfDI ... 84
8.14 Datenschutz bei digitalen Identitäten ... 84
8.15 Datenschutz im Smart Home ... 85
8.16 Zertifizierung und Akkreditierung ... 87

9 Kontrollen und Beratungsbesuche ... 89
9.1. Corona-angepasste Kontrollen ... 89
9.2 Kontrolle Aufbewahrungsvorschriften in der Finanzverwaltung ... 90
9.3 Kontrollen in Auslandvertretungen in Kasachstan ... 91
9.4 Kontrollen im Sicherheitsbereich ... 91
9.4.1 Pflichtkontrolle: Verdeckte Maßnahmen beim BKA ... 91
9.4.2 Pflichtkontrolle eingriffsintensiver Maßnahmen im Zollfahndungsamt München ... 92
9.4.3 Datenübermittlung des BKA im internationalen Bereich ... 92
9.4.4 Pflichtkontrollen ATD/RED ... 93
9.4.5 PIAV-Kontrolle ... 94
9.4.6 Kontrolle der Abrufe von Daten im automatisierten Auskunftsverfahren ... 95
9.4.7 Funkzellendatei des Bundeskriminalamts ... 95
9.4.8 Koordinierte Kontrollen zu Ausschreibungen zur verdeckten/gezielten Kontrolle im Schengener Informationssystem ... 96
9.4.9 Datenschutzaufsicht und Beratung beim BfV ... 96
9.4.10 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst ... 98
9.4.11 Datenverarbeitung beim BND ... 99
9.4.12 Datenschutzkontrollen im Sicherheitsüberprüfungsrecht – von vorbildlich bis mangelhaft ... 100

10 BfDI Intern ... 102
10.1 Neue Strategie für den BfDI ... 102
10.2 Aufbau Labor ... 103
10.3 Nach der Organisationsuntersuchung – Anschlussprojekte ... 104
10.4 Personalentwicklung und Haushaltslage im Jahr 2022 ... 104
10.5 Im Wachstum – das Verbindungsbüro des BfDI in Berlin ... 105
10.6 Bericht zu Presse- und Öffentlichkeitsarbeit ... 106
10.7 Gut vernetzt: Das Hauptstadtteam des BfDI ... 109
10.8 Sichere Kommunikation Behördenpostfach ... 109
10.9 Statistik 2022 ... 110

11 Zentrale Anlaufstelle ... 113
11.1 ZASt Rückblick ... 113

12 Wo bleibt das Positive? ... 116
12.1 Datenschutzorganisation bei der DRV Bund ... 116
12.2 Datenschutzrechtliche Aspekte von Telemedienangeboten ... 116

12.3 Alternative Bereitstellung von Bundes-Apps 117
12.4 Beratung und fachlicher Austausch zum SÜG – Eine fruchtbare Ergänzung 117
12.5 Protokollauswertetool für Inzoll 119
12.6 Verbesserungen im Vorgangsbearbeitungssystem BKA 119
12.7 Einlenken beim Ausländervereinsregister 120
12.8 Postdienstleister stellt sich datenschutzrechtlich neu auf 120
12.9 Beratung und Aufsicht – gemeinsam mehr für den Datenschutz erreichen 121

Themenzuordnung nach Bundestagsausschüssen 122

Anlagen

Anlage 1 Kontrollierte Stellen 125
Anlage 2 Übersicht über Maßnahmen/Beanstandungen gegenüber öffentlichen Stellen 126
Übersicht über Maßnahmen/Beanstandungen gegenüber nicht-öffentlichen Stellen 129
Abkürzungsverzeichnis 132

Impressum

1 Einleitung

2022 war für meine Behörde ein überaus ereignisreiches Jahr, in dem deutlich wurde, dass die nationale und internationale Zusammenarbeit der Datenschutzbehörden unweigerlich einen immer größeren Stellenwert einnimmt.

Im Januar übernahm ich den Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Im Zuge des deutschen G7-Vorsitzes habe ich die G7-Datenschutzaufsichtsbehörden zu einem Treffen nach Bonn eingeladen. Als Mitglied des Exekutiv-Komitees der Global Privacy Assembly (GPA), des internationalen Zusammenschlusses der nationalen Datenschutzaufsichtsbehörden, nahm ich an der GPA-Konferenz in Istanbul teil. Als Vorsitzender der International Working Group on Data Protection in Technolgy konnte ich zwei Sitzungen in Tel Aviv und London leiten. Daneben fanden zahlreiche Sitzungen des Europäischen Datenschutzausschusses (EDSA) statt. Aber der Reihe nach.

Als Vorsitzender des DSK hatte ich mir neben der organisatorischen Weiterentwicklung des Gremiums (s. 3.2.1) zwei Schwerpunktthemen vorgenommen: der Beschäftigtendatenschutz und der Umgang mit Patientendaten, insbesondere in der Forschung. Bei drei Zwischen- und zwei Hauptkonferenzen wurden für beide Themen Entschließungen der DSK erarbeitet und verabschiedet (s. 3.2.4 und 4.1.4), die dem Gesetzgeber und den Stakeholdern Hinweise auf Möglichkeiten und Grenzen in diesem Bereich geben. Daneben haben wir uns u. a. mit der nationalen Umsetzung der Beschlüsse des EDSA befasst.

Der EDSA hat im Berichtsjahr eine Reihe von wichtigen Beschlüssen zur einheitlichen Umsetzung und Anwendung der DSGVO in der EU gefasst. (s. 3.3 ff.) Schwerpunkte waren hier der Transfer von Daten in Drittstaaten sowie der Umgang mit Bußgeldern und dem Auskunftsrecht. Zudem geht es endlich auch mit den schon viel zu lange vorliegenden Klagen gegen Meta (Facebook, Instagram, WhatsApp) voran, die alle in die federführende Zuständigkeit der irischen Datenschutzbehörde (DPC) fallen. Die 2022 endlich vorgelegten Beschussvorschläge der DPC wurden durch den EDSA gerade auch auf deutschen Vorschlag hin zum Teil erheblich verschärft.

Seit 2021 treffen sich im Rahmen der G7-Konsultationen auch die G7-Datenschutzbehörden, um über wichtige internationale Probleme zu beratschlagen. Mussten wir 2021 noch virtuell zusammenkommen, konnte ich meine G7-Kolleginnen und Kollegen in diesem Jahr zu uns nach Bonn einladen. Thema war u. a. die Weiterentwicklung der internationalen Data Free Flow with Trust (DFFT)-Initiative, zu dem die G7-Digitalminister kurz zuvor einen Aktionsplan vorgelegt hatten. Es war gut zu sehen, dass die Datenschutzbehörden über Europa hinaus gemeinsame Vorstellungen für die Voraussetzungen von DFFT haben.

Auch die GPA hat sich auf ihrer Konferenz in Istanbul intensiv mit den Folgen der Globalisierung und Digitalisierung befasst. In einer Entschließung über die zukünftige strategische Ausrichtung der GPA wurden die internationale Zusammenarbeit, der Wissenstransfer und das möglichst gleichwertige, hohe Schutzniveau der Privatsphäre und des Datenschutzes als Ziele formuliert.

Daneben fanden noch viele weitere Gremiensitzungen auf nationaler und internationaler Ebene statt, die viel Zeit und Arbeit nicht nur für mich, sondern vor allem auch für meine Mitarbeiterinnen und Mitarbeiter bedeuten, die in diesen Gremien gefragte Expertinnen und Experten sind und oft federführende Berichterstattungen innerhaben. Diese Arbeit ist notwendig, um die Digitalisierung positiv und vertrauensvoll weiter zu entwickeln sowie die Datenschutzschutzanforderungen zu harmonisieren.

Neben der Gremienarbeit bildete auch im Jahr 2022 die Beratung und Kontrolle weiter einen Schwerpunkt der Arbeit meines Hauses.

Die Gesetzgebungspläne der EU zu den europäischen Digitalrechtsakten, die Umsetzung von EU-Vorgaben in deutsches Recht sowie die Pläne der Bundesregierung zur weiteren Digitalisierung im Gesundheits-, Verwaltungs- und Kommunikationsbereich beschäftigen mich und mein Haus intensiv. Dass der Datenschutz bei vielen Projekten erst sehr spät mitbedacht und eingebunden wird, habe ich immer wieder beklagt und kritisiert, leider muss ich es auch an dieser Stelle wieder tun. Es ist eigentlich eine schlichte Erkenntnis: wer den Datenschutz von Anfang an mitdenkt und entwickelt, hat deutlich geringere Probleme, Kosten und Einwände, als derjenige, der später aufwendig nachbessern muss. Wir reden hier durchaus auch über unnötige Verzögerungen und Verteuerungen im Größenbereich von Jahren und Millionen Euro.

Insbesondere die Kontrollen und Beratungen der Behörden und Firmen im Sicherheitsbereich sind ein bedeutsamer Teil meines gesetzlichen Auftrags. Hier konnten im Jahr 2022 wieder zahlreiche Kontroll- und Beratungsbesuche in Präsenz stattfinden, was die Arbeit doch für beide Seiten deutlich verbessert. Und auch wenn es in diesem Bereich nach wie vor einzelne Beanstandungen und Kritik gab und gibt, so möchte ich doch auch an dieser Stelle festhalten, dass die Hartnäckigkeit meiner Mitarbeiterinnen und Mitarbeiter, aber auch das Verständnis der kontrollierten Behörden, zu einigen deutlichen Verbesserungen geführt hat (s. Kap. 12).

Das Recht der Bürgerinnen und Bürger auf Information über Verwaltungshandeln hat auch im Jahr 2022 zu zahlreichen Anfragen und Bitten um Unterstützung an mein Haus geführt. Das Recht auf Informationsfreiheit ist in vielen Behörden immer noch ein lästiger Störfaktor. Deswegen arbeiten wir intensiv daran, mehr Verständnis für das Bürgerrecht und seine Umsetzung zu wecken. Das von der Regierungskoalition geplante Transparenzgesetz könnte hier einen Fortschritt bringen, weswegen ich mich an der Gesetzesberatung eindringlich beteiligen werde und auch schon mehrfach Vorschläge für den Inhalt gemacht habe.

Im Jahr 2023 habe ich zudem den Vorsitz über die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) inne. Mein Ziel ist, auch aus dieser Position heraus für mehr Transparenz im Verwaltungshandeln und für das Recht der Menschen auf Information zu werben.

Dieser kurze Abriss über einige wichtige Themen im Jahr 2022 stellt nur einen Ausschnitt der vielfältigen Arbeit meines Hauses dar. Mit der weiter fortschreitenden Digitalisierung aller Lebens- und Arbeitsbereiche und der damit einhergehenden Verarbeitung teils sensibelster Daten kommt zukünftig immer mehr Arbeit auf meine Behörde zu. Ich kann diese Arbeit nur dank meiner überaus motivierten und engagierten Mitarbeiterinnen und Mitarbeiter leisten. Für ihren Einsatz, ihr profundes Wissen und ihre Hilfsbereitschaft möchte ich mich an dieser Stelle ganz herzlich bedanken! Der gleiche Dank geht an die engagierten behördlichen und betrieblichen Datenschutzbeauftragten, mit denen wir zusammenarbeiten dürfen, eine engagierte Zivilgesellschaft, die mit uns kooperiert, sowie an die Bürgerinnen und Bürger, die ihre Rechte wahrnehmen und uns auf Missstände aufmerksam machen. Und nicht zuletzt danke ich dem Deutschen Bundestag und hier insbesondere den Haushaltsberichterstattern für den BfDI-Haushaltsplan, für das stets offene Ohr und für die Unterstützung unserer Arbeit.

Prof. Ulrich Kelber

2 Empfehlungen

2.1 Zusammenfassung der Empfehlungen des 31. Tätigkeitsberichts

Ich empfehle der Bundesregierung ein Beschäftigtendatenschutzgesetz zu erlassen, in dem etwa der Einsatz von KI im Beschäftigungskontext, die Grenzen der Verhaltens- und Leistungskontrolle sowie typische Datenverarbeitungen im Bewerbungs- und Auswahlverfahren klar geregelt werden. (s. 3.2.4)

Eine datenschutzkonforme Nutzung von Facebook Fanpages ist h. E. weiterhin nicht möglich. Ich empfehle daher, die Fanpages abzuschalten. (s. 4.3.1)

Um den Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr rechtlich abzusichern, empfehle ich dem Gesetzgeber, eine umfassende, empirische und interdisziplinäre Bestandsaufnahme durch eine Expertenkommission durchzuführen. (s. 4.4.2)

Ich empfehle der Bundesregierung, auf eine erhebliche, grundrechtskonforme Überarbeitung des VO-Entwurfs zur Chat-Kontrolle zu drängen und ansonsten den Verordnungsentwurf insgesamt abzulehnen. (s. 4.4.1)

Ich empfehle die Einführung von Datentreuhändern auf Basis des TTDSG grundsätzlich zu überarbeiten und DSGVO-konform umzusetzen. (s. 5.5)

Ich empfehle die Zusammenlegung von Informationsfreiheitsgesetz und Umweltinformationsgesetz (und möglichst auch des Verbraucherinformationsgesetzes) sowie die Weiterentwicklung zu einem Bundestransparenzgesetz mit proaktiven Veröffentlichungspflichten. Der Informationsfreiheitsbeauftragte benötigt in einem Bundestransparenzgesetz Anordnungs- und Durchsetzungsbefugnisse, um im Konfliktfall handlungsfähig zu sein. (s. 6.3)

Ich empfehle dem Gesetzgeber, die anstehende Evaluierung des Sicherheitsüberprüfungsgesetzes (SÜG) zu nutzen, um ein schlüssiges Gesamtkonzept für Personenüberprüfungen auf Bundesebene zu entwickeln. Anstelle einer ausufernden Anwendung der Öffnungsklausel auf ganze Behörden, verschiedene Überprüfungsformate außerhalb des SÜG sowie Mehrfachüberprüfungen aufgrund verschiedener Tätigkeiten sollte der Anwendungsbereich des Gesetzes neu definiert werden. (s. 7.10)

Ich empfehle dem Gesetzgeber weiterhin, angesichts des festgestellten geringen Nutzwertes von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen. (s. 9.2.4)

Ich empfehle dem Gesetzgeber, eine gesetzliche Klarstellung hinsichtlich der Zuständigkeit für Reservistinnen und Reservisten zwischen BAMAD und BfV vorzunehmen. (s. 9.2.10)

Ich empfehle, die Einbindung von Videos auf den Webseiten des Bundes zu überprüfen und datenschutzkonforme Alternativen zur weit verbreiteten Praxis der Einbindung mittels YouTube umzusetzen. (s. 12.2)

2.2 Empfehlungen des 30. Tätigkeitsberichts

	Empfehlungen des 30. Tätigkeitsberichts	Stand der Umsetzung
🟡	Ich empfehle der Bundesregierung, die im Koalitionsvertrag angekündigte Institutionalisierung der DSK und die verbesserte verbindliche Kooperation der deutschen Datenschutzaufsichtsbehörden durch die entsprechenden gesetzgeberischen Maßnahmen alsbald in Angriff zu nehmen. (30. TB Nr. 3.1.1, 5.7)	In dem noch laufenden Gesetzgebungsverfahren wurden meine Anmerkungen zur Institutionalisierung der DSK und der verbesserten Kooperation der deutschen Datenschutzaufsichtsbehörden bisher zwar teilweise umgesetzt. Innerhalb der laufenden Legislaturperiode werde ich mich jedoch weiterhin insbesondere dafür einsetzen, sowohl Regelungen für die Verbindlichkeit der innerdeutschen Kooperation auf DSK-Ebene als auch die gesetzlichen Rahmenbedingungen für die Einrichtung einer dauerhaften DSK-Geschäftsstelle im BDSG zu schaffen.
🔴	Ich empfehle, die Wege und den Datenkranz bei der Meldung von Impfungen – Impfquotenmonitoring – zu überprüfen. (30. TB Nr. 4.1.9)	Kein Hinweis auf Prüfung und Anpassung.
🔴	Ich empfehle dem BMG, für den Betrieb des Implantateregisters eine geeignete Behörde vorzusehen – und gegebenenfalls zu schaffen -, die den Registerbetrieb dauerhaft rechtssicher und datenschutzkonform ohne Interessenkonflikte übernehmen kann. (30. TB Nr. 5.10)	Bisher keine geeignete Behörde, keine Pläne bekannt.
🔴	Ich empfehle, beim Modellvorhaben Genomsequenzierung den Aufbau der „gemeinsamen Dateninfrastruktur“ dezentral zu strukturieren und statt einer doppelten Datenhaltung jeweils anlassbezogene Datenzugänge vorzusehen. (30. TB Nr. 6.6)	Bisher keine Pläne zur Struktur bekannt.
🔴	Ich empfehle, das Einsichtsrecht der betrieblichen Datenschutzbeauftragten in die im Unternehmen geführten Sicherheitsakten, den Adressaten einer Beanstandung im nichtöffentlichen Bereich, den Umfang der Maßnahmen bei Sicherheitsüberprüfungen gem. § 33 SÜG sowie die Datenübermittlung im sogenannten Besuchskontrollverfahren im SÜG zu regeln. (30. TB Nr. 6.21)	Es gibt bisher keine entsprechenden Änderungen des SÜG. Eine Novellierung ist aber in Planung.
🔴	Ich empfehle dem Gesetzgeber weiterhin angesichts des festgestellten geringen Nutzwerts von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen. (30. TB Nr. 8.1.1)	Es gibt bisher keine Anzeichen für eine Abschaffung der beiden Dateien.

Empfehlungen aus älteren Tätigkeitsberichten und deren Umsetzungsstand finden Sie unter www.bfdi.bund.de/tb-empfehlungen.

3 Gremien

3.1 Übersicht Gremienarbeit

Egal, ob national, europäisch oder global: wichtige Entscheidungen werden mittlerweile nicht mehr von einzelnen Aufsichtsbehörden individuell, sondern verstärkt in Gremien getroffen. Dementsprechend nimmt auch die Arbeit in diesen sowie den diversen dazugehörigen (Unter-)Arbeitsgruppen einen großen und wichtigen Teil meiner Arbeit ein. Dabei versuche ich – wo immer es möglich und sinnvoll ist – mich als Vorsitz oder Berichterstatter aktiv in die Gremienarbeit einzubringen.

Auf nationaler Ebene nimmt die Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) den wohl wichtigsten und größten Teil meiner Gremienarbeit ein. Dabei findet die Arbeit nicht nur in den jährlich stattfindenden zwei Haupt- und drei Zwischenkonferenzen auf Plenumsebene, sondern vor allem in den vielen Arbeitskreisen, Unterarbeitskreisen und Taskforces statt. Im Berichtszeitraum waren dies über 50 Gruppen, in denen meine Kolleginnen und Kollegen vertreten waren; in zwölf Gruppen sogar als Vorsitz.

Der europäische Datenschutzausschuss und seine vielen Unterarbeitsgruppen sind ein weiterer wesentlicher Bereich meiner Gremienarbeit. Neben den mittlerweile rund 15 Plenarterminen im Jahr ist mein Haus auch in zwölf Unterarbeitsgruppen und zwei Taskforces vertreten. Dabei übernimmt der BfDI in einer Arbeitsgruppe die Rolle des Vorsitzes/Koordinators. Zudem haben meine Kolleginnen und Kollegen in zwei Fällen Haupt- und in drei Fällen Co-Berichterstatteraufgaben übernommen, sowie in weiteren zwei Fällen in Drafting-Teams mitgearbeitet. So konnten wir erheblich Einfluss auf die Ergebnisse dieser Gremien nehmen.

Auch auf internationaler Ebene wird der Mehrwert von Vernetzung und gemeinsamer Arbeit immer relevanter. Hier ist vor allem natürlich die als Global Privacy Assembly bekannte internationale Datenschutzkonferenz zu nennen. Hier engagiere ich mich als Mitglied des Executive Committees maßgeblich bei der Steuerung und Ausrichtung der Konferenz und ihrer Ziele.

Ebenfalls immer wichtiger ist das im Jahr 2021 neu eingeführte Gremium der G7-Data-Protection-Roundtable. Hier wechselt der Vorsitz – analog zu den sonstigen G7-Veranstaltungen – jährlich, so dass ich meine Kolleginnen und Kollegen zur Konferenz in diesem Jahr in Bonn begrüßen konnte. Neben diesem Hauptevent stehen aber noch viele weitere vorbereitende Treffen auf Arbeitsebene.

Den Vorsitz der International Working Group on Data Protection in Technology, die nach dem Ort ihrer Gründung auch als „Berlin Group“ bezeichnet wird und zweimal jährlich tagt, habe ich bereits im Jahr 2021 übernommen.

Zusammen mit Teilnahmen bei der Datenschutzgruppe T-PD des Europarats und einigen weiteren nationalen und internationalen Runden Tischen, Beiräten und ähnlichem kommt mein Haus damit auf eine dreistellige Zahl an Gremienbeteiligungen pro Jahr.

3.2 Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Die DSK ist der Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie verfolgt das Ziel, die Datenschutzgrundrechte zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten.

2022 übernahm ich den jährlich wechselnden Vorsitz. Die 103. DSK fand im Weltsaal des Auswärtigen Amts in Bonn und die 104. DSK im früheren Gästehaus der Bundesregierung auf dem Petersberg statt. Die erste Zwischenkonferenz wurde aufgrund der pandemischen

Gruppenbild der 104. DSK auf dem Petersberg

Situation als Videokonferenz durchgeführt. Die beiden weiteren Zwischenkonferenzen fanden in den Räumlichkeiten der Bundespressekonferenz in Berlin statt.

Es wurden vier Entschließungen zu den Themen Löschmoratorien bei Parlamentarischen Untersuchungssauschüssen, Datenschutz und wissenschaftliche Forschungen, Beschäftigtendatenschutz sowie die Petersberger Erklärung zu Forschungsdaten und fünf Beschlüsse zu verschiedenen Einzelfragen wie z. B. datenschutzkonformen Online-Handel, den Auftragsverarbeitungsvertrag zu Microsoft 365, Verarbeitung von personenbezogenen Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht und zu Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht verabschiedet.

Darüber hinaus überarbeitete die DSK ihre Orientierungshilfe zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der DSGVO und für Anbieterinnen und Anbietern von Telemedien und verabschiedete FAQ zu Facebook-Fanpages.

Querverweise:

3.2.4 Neue Entschließung der DSK zum Beschäftigtendatenschutzgesetz, 3.2.5 Aktenvernichtungs- und Datenlöschmoratorium, 3.2.6 Orientierungshilfe Werbung 2.0, 4.1.4 Petersberger Erklärung

3.2.1 DSK-Vorsitz und DSK 2.0

Die Datenschutzkonferenz (DSK) übt eine unverzichtbare Schnittstellenfunktion in der Koordination der Aufsicht der Datenschutzaufsichtsbehörden des Bundes und der Länder aus. Diese Rolle bringt aber auch besondere Herausforderungen – gerade bei der Binnenorganisation – mit sich, wenn eine effektive Arbeit sichergestellt werden soll. Erste Schritte für notwendige Anpassungen wurden in 2022 unter meinem Vorsitz eingeleitet.

Mit Beginn des Jahres habe ich turnusmäßig den Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) für ein Jahr übernommen. Neben dem inhaltlichen Schwerpunkt meines Vorsitzes, der das Thema Forschungsdaten betraf (vgl. 4.1.1. – 4.1.4), war ich über die allgemeine Organisation der Arbeit der DSK und der Ausrichtung ihrer Konferenzen auch mit der Fortentwicklung des Gremiums befasst.

Wie ich im letzten Tätigkeitsbericht ausgeführt hatte, besteht innerhalb der DSK Einvernehmen, das Gremium zu reformieren und ausgehend von den Ergebnissen des Arbeitskreises DSK 2.0 eigene Vorschläge hierfür zu unterbreiten (vgl. 30. TB 3.1.1). Diesen Prozess habe ich als Vorsitzender aktiv weiter voranzubringen versucht. Hierbei ist es mein über die Amtszeit des DSK-Vorsitzes

hinaus andauerndes Bestreben, durch pragmatische, zielorientierte Angebote etwaige Vorbehalte gegen die föderale Struktur zu zerstreuen und tragfähige gemeinsame Lösungen zu entwickeln.

Ein immer wieder – mitunter leider auch zurecht – gehörter Vorwurf ist es, dass die föderale Struktur der Datenschutzaufsicht in Deutschland zu uneinheitlichen Auslegungen und Anwendungen des geltenden Rechts führt. Für die Akzeptanz der Arbeit der Datenschutzaufsicht und ihr Gewicht in der Öffentlichkeit ist es aber unerlässlich, möglichst einheitlich aufzutreten, und dadurch ein hohes Maß an Rechtssicherheit zu vermitteln. Daher halte ich es für ein wichtiges Signal, dass die DSK in diesem Jahr mit einer Änderung ihrer Geschäftsordnung bindende Mehrheitsentscheidungen eingeführt hat. So haben mit einer Zweidrittelmehrheit gefasste Beschlüsse künftig grundsätzlich für alle Mitglieder der DSK bindende Wirkung.

Zu den weiteren Ergebnissen des AK DSK 2.0 gehören, dass die DSK weniger reaktiv und mehr aktiv handeln muss. Schnelle und verlässliche Antworten und Entscheidungen zu aktuellen und künftigen Fragen des Datenschutzes und die Teilhabe am datenschutzpolitischen Diskurs in Echtzeit verlangen effiziente Strukturen und Prozesse.

Ich bin deshalb froh, dass sich die DSK auf die Bildung eines Präsidiums für ihr strategisch-planerisches und inhaltlich-operatives Management nach Innen und Außen geeinigt hat. Ab dem Jahr 2023 steht der DSK als Kollegialorgan zunächst probehalber ein Präsidium aus letztjährigem, aktuellem und nächstjährigem Vorsitz vor. Ergänzt wird dieses um die beiden Vertreter im Europäischen Datenschutzausschuss (EDSA), zu denen auch der BfDI gehört. So ist sichergestellt, dass von der Bundesebene, den Bundesländern und direkt aus dem EDSA als dem zentralen Gremium des europäischen Datenschutzes, alle Informationen zügig fließen.

Der Erfolg der Arbeit von Präsidium und Plenum der DSK hängt meiner Auffassung nach auch an der Schaffung einer gemeinsamen Geschäftsstelle, die den Vorsitz und das künftige Präsidium unterstützen und zu einer weiteren Professionalisierung sowie Beschleunigung der Arbeit der DSK beitragen soll. Ich habe angeboten, die Geschäftsstelle bei der in meinem Haus angegliederten Zentralen Anlaufstelle (ZASt) einzurichten. Schon heute erbringt die ZASt für die Aufsichtsbehörden des Bundes und der Länder koordinierende und unterstützende Tätigkeiten in Angelegenheiten der grenzüberschreitenden Zusammenarbeit mit den europäischen Aufsichtsbehörden und dem EDSA. Aufgrund dieses Erfahrungsschatzes und der teils überlappenden bzw. sich ergänzenden Aufgabenfelder zu einer künftigen Geschäftsstelle sehe ich erhebliche Synergieeffekte und Effizienzgewinne für die Arbeit der DSK. Durch die gesetzlich untermauerte organisatorische Trennung von den Aufgaben meines Hauses als Aufsichtsbehörde kann die ZASt auch in einer neuen Rolle als Geschäftsstelle der DSK weiterhin als unabhängiger Sachwalter im Interessen aller deutschen Datenschutzaufsichtsbehörden agieren.

Leider konnte bis Redaktionsschluss noch keine Einigung über die Einführung einer Geschäftsstelle gefunden werden. Ich gehe allerdings davon aus, dass das Thema auch im nächsten Jahr unter dem Vorsitz meiner Kollegin aus Schleswig Holstein weiter vorangetrieben werden wird. Als BfDI werde ich weiter alle Initiativen unterstützen, die zu einer zielführenden Reform der DSK beitragen.

Querverweise:

4.1 Forschungsdaten

3.2.2 DSK Taskforce Souveräne Cloud

Souveräne Clouds sollen die digitale Souveränität von Cloud-Anwendenden stärken und ihre Abhängigkeit von einzelnen Cloud-Anbietenden reduzieren. Letztlich handelt es sich dabei bisher aber primär um einen Marketingbegriff, der – durch die Anbietenden selbst definiert – keine verbindlichen Rückschlüsse auf das eigentliche Angebot zulässt. Die DSK hat daher auf meine Initiative hin die Taskforce Souveräne Cloud gegründet, die diesen Begriff aus einer neutralen Position heraus mit Leben füllen soll. Zur 104. DSK im November 2022 hat sie ein Positionspapier mit Anforderungen an souveräne Clouds vorgelegt, das Anwendende zukünftig bei der Wahl der genutzten Cloud-Dienste und Anbietende bei der Auslegung ihrer Angebote unterstützen kann.

Cloud-Computing ist aus der heutigen IT-Landschaft nicht mehr wegzudenken. In dem ausgelagerten Betrieb sehen viele Anwendende das Potential für Einsparungen und Aufwandsreduzierungen. Er birgt aber auch das Risiko wachsender Abhängigkeiten, da sich Datenhaltung und –verarbeitung nicht mehr in der unmittelbaren Verfügungsgewalt der Anwendenden befinden. Vor dem Hintergrund eines wachsenden Bedürfnisses nach digitaler Souveränität stellen sich Anwendende zunehmend die Frage, inwieweit ein solches Abhängigkeitsverhältnis tragbar ist, insbesondere wenn es um die Verarbeitung personenbezogener Daten geht, für die die Anwendenden datenschutzrechtlich verantwortlich sind. Cloudanbietende reagieren auf diesen Bedarf mit dem Angebot sog. souveräner Clouds, wobei dieser Begriff nicht allgemeingültig definiert ist; die Deutungshoheit darüber, was eine souveräne Cloud ausmacht, haben bislang die jeweiligen Anbietenden.

Taskforce Souveräne Cloud

Auf meine Initiative hin wurde auf der 103. DSK im März 2022 die Taskforce Souveräne Cloud eingerichtet. Sie hatte zunächst das Ziel, den Begriff der souveränen Cloud aus einer neutralen Position heraus zu definieren, eine Abgrenzung von anderen Cloudangeboten vorzunehmen und Anforderungen festzulegen, die eine Cloud erfüllen muss, um als souverän zu gelten. Noch im November des gleichen Jahres hat die von mir geleitete Taskforce ein dann von der 104. DSK angenommenes Positionspapier vorgelegt, das Anforderungen und Erwartungen an souveräne Clouds aus der Sicht des Datenschutzes formuliert. Zentrale Prämissen sind dabei, dass die Rechte und Freiheiten der betroffenen Personen im Kontext der Verarbeitung ihrer personenbezogenen Daten im Mittelpunkt stehen und dass digitale Souveränität die Befolgung des anwendbaren Datenschutzrechts voraussetzt, wobei die Anforderungen selbst über eine reine Datenschutzkonformität hinausgehen. Aus meiner Sicht besonders wichtig ist dabei die Feststellung, dass in einer souveränen Cloud Verarbeitungen ausgeschlossen sind, die einzig im Interesse der Anbietenden erfolgen. Dies schließt Finanzierungsmodelle aus, in denen letztlich mit personenbezogenen Daten gezahlt wird. Eine entsprechende Zusicherung muss dabei mindestens so weit in die Zukunft wirken, dass Anwendende die Möglichkeit haben, auf ein ihre Souveränität wahrendes Cloudangebot zu wechseln. Um diese Wechselmöglichkeit überhaupt zu schaffen, sehe ich weiterhin die Nutzung offener Standards, zumindest aber die Verfügbarkeit dokumentierter Schnittstellen als unabdingbar an. Diese Schnittstellen ermöglichen idealerweise auch den Austausch einzelner Komponenten des angebotenen Clouddienstes, sodass Anwendende die für sie am besten geeignete Implementierung wählen können. Möglicherweise ist dies sogar eine, bei der sie dank verfügbarer Quelltexte die Möglichkeit zum eigenen Audit haben.

Ein ganz wesentliches Thema, mit dem ich mich auch in diesem Berichtsjahr wieder intensiv auseinandergesetzt habe, ist der Drittstaateneinfluss (Staaten außerhalb der EU) auf die Cloudanbietenden. Hier stellt die Taskforce in ihrem Positionspapier fest: Clouds können nur dann als souverän gelten, wenn ein Drittstaateneinfluss gänzlich ausgeschlossen werden kann und eine effektive Durchsetzung vertraglich vereinbarter Pflichten gewährleistet ist. Hieraus ergeben sich aus Sicht der EU u. a. die Anforderungen, dass sowohl Sitz als auch Serverstandort von Anbietenden souveräner Clouds und ihren Auftragsverarbeitern in der EU liegen müssen. Damit Anwendende nicht am Ende doch wieder auf Zusicherungen angewiesen sind, müssen Anbietende ihnen die Möglichkeit zur Überprüfung der Erfüllung dieser Anforderungen bieten und aktiv an solchen mitwirken. Darüber hinaus sehe ich den Nachweis durch Zertifizierung als wirkungsvolle vertrauensbildende Maßnahme an. Mit einer solchen Cloud kann datenschutzkonformer und souveränitätswahrender IT-Betrieb gelingen.

3.2.3 DSK Arbeitskreis Microsoft

Kaum ein Softwareprodukt wird so flächendeckend verwendet wie Microsoft Office, zunehmend auch in seiner cloudbasierten Variante MS 365. Verantwortliche stehen dabei vor dem Problem, dass die MS 365 immer wieder wegen datenschutzrechtlicher Bedenken in der Kritik steht. Um für mehr Klarheit zu sorgen und Verantwortlichen konkrete Empfehlungen an die Hand geben zu können, hat die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einen intensiven Dialog mit Microsoft geführt – mit ernüchterndem Ergebnis.

Die DSK hat Ende 2020 eine Dialogreihe mit Microsoft unter der Leitung der Aufsichtsbehörden aus Bayern (Landesamt für Datenschutzaufsicht LDA) und Brandenburg (bis Ende Januar 2022) begonnen. Zusätzlich haben sich die Aufsichtsbehörden aus Berlin, Schleswig-Holstein, Sachsen, Mecklenburg-Vorpommern, Baden-Württemberg, Hessen, Nordrhein-Westfalen und mein Haus eingebracht. Im Fokus der Gespräche standen die Vertragsgrundlagen zu Onlinediensten, zu denen u. a. auch das bekannte Microsoft 365 gehört, sowie praktische Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II“).

Bereits im Vorfeld hatte die DSK Kritikpunkte an den vertraglichen Grundlagen festgestellt. Im Rahmen des Dialoges mit Microsoft konnten aus Sicht der DSK einige Punkte behoben werden. Die gravierendsten Probleme bleiben aber weiterhin bestehen.

Besonders kritisch ist die Nutzung personenbezogener Daten aus der Auftragsverarbeitung für eigene Zwecke von Microsoft. Für diese Nutzung ist eine tragfähige Rechtsgrundlage notwendig. Die Prüfung einer solchen Rechtsgrundlage setzt Kenntnis über die Art der verarbeiteten Daten sowie den korrespondierenden konkreten Zweck der Verarbeitung voraus. Auf Grundlage des aktuellen, von Microsoft bereitgestellten „Datenschutznachtrages vom 15. September 2022“, lässt sich diese Prüfung allerdings nicht abschließend durchführen.

Verantwortliche, die Microsoft 365 einsetzen wollen, stehen in der Pflicht, die datenschutzkonforme Nutzung nachzuweisen. Solange Microsoft die hierfür notwendige Transparenz nicht herstellt, bleiben Nutzende im Unklaren darüber, was mit ihren Daten geschieht. Die DSK ist daher zu dem Schluss gekommen, dass auf Basis des

aktuellen Datenschutznachtrags der datenschutzkonforme Einsatz von Microsoft 365 nicht möglich ist. Weitergehende Informationen können der Zusammenfassung des Berichts der Arbeitsgruppe der DSK „Microsoft-Onlinedienste“ entnommen werden.[1]

Federführend zuständige Datenschutzaufsichtsbehörde für Microsoft und den mit MS 365 verbundenen Datenverarbeitungen ist nach europäischem Recht die irische Datenschutzaufsichtsbehörde DPC, da Irland der Hauptstandort von Microsoft in Europa ist. Der BfDI und die deutschen Landesdatenschutzbehörden sind allerdings datenschutzrechtlich zuständig für den Einsatz von MS 365 (und anderer Software) durch die von ihnen kontrollierten Stellen, daher der Schwerpunkt des Arbeitskreises.

3.2.4 Neue Entschließung der DSK zum Beschäftigtendatenschutzgesetz

Die immer schnellere Digitalisierung der Arbeitswelt ist Realität. Der aktuelle Rechtsrahmen im Beschäftigtendatenschutz wird dem leider nicht gerecht. Die Generalklausel des § 26 Bundesdatenschutzgesetz (BDSG) reicht nicht aus, um den Beschäftigten einen hinreichenden Schutz ihres Persönlichkeitsrechts zu bieten. Die bei allen Beteiligten darüber hinaus bestehende Unsicherheit hinsichtlich der Frage, welche Datenverarbeitungen im Beschäftigungsverhältnis rechtlich zulässig sind und welche nicht, bedarf einer klaren und differenzierenden Lösung. In ihrer Entschließung aus dem April 2022 fordert die DSK den Gesetzgeber auf, zeitnah ein Beschäftigtendatenschutzgesetz vorzulegen.

Die DSK hatte bereits 2014 die Schaffung eines Beschäftigtendatenschutzgesetzes gefordert (vgl. 25. TB Nr. 9.3.1 und Anlage 9). Mittlerweile sind neue Regelungen zum Beschäftigtendatenschutz dringender denn je, denn die aktuelle Bestimmung des § 26 BDSG reicht vor dem Hintergrund aktueller technischer Entwicklungen nicht aus. Sie ist zu unbestimmt, lässt zu viel Interpretationsspielraum, ist nicht hinreichend praktikabel, normenklar und sachgerecht. Dadurch führt sie zu Unklarheiten über die Zulässigkeit von Verarbeitungen personenbezogener Daten im Beschäftigungskontext für Arbeitgeberinnen und Arbeitgeber, Beschäftigte, Bewerberinnen und Bewerber, Personalvertretungen oder Gerichte. Außerdem bleiben Praktiken möglich, die das Schutzbedürfnis von Beschäftigten verletzen. Weitergehende Regelungen sind notwendig und überfällig. Das hat auch die Bundesregierung erkannt und sich im Koalitionsvertrag zur Schaffung von Regelungen zum Beschäftigtendatenschutz bekannt, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen. Ein Referentenentwurf soll nach Auskunft der Bundesregierung in gemeinsamer Federführung des Bundesministeriums für Arbeit und Soziales (BMAS) und des Bundesministeriums des Innern (BMI) erarbeitet werden, wobei das BMAS die technische Federführung hat. Im Vorfeld werden dazu Eckpunkte erarbeitet. Der vom BMAS eingesetzte unabhängige Beirat zum Beschäftigtendatenschutz, dessen Mitglied ich war, kommt ebenfalls zu dem Ergebnis, dass die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes geboten ist.

In ihrer Entschließung „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt‘!“ vom 29. April 2022[2] fordert die DSK, beschäftigtendatenschutzrechtliche Regelungen im Rahmen eines eigenständigen Gesetzes mindestens in den folgenden Bereichen zu schaffen:

Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI)

Die Grenzen und Rahmenbedingungen des Einsatzes algorithmischer Systeme im Beschäftigungs- und Bewerbungskontext sollten gesetzlich geregelt werden. Aufgrund des bestehenden Abhängigkeitsverhältnisses sind Beschäftigte bzw. Bewerberinnen und Bewerber diesbezüglich besonders schutzbedürftig. Zu berücksichtigen sind neben der Hambacher Erklärung der DSK und der von der Datenethikkommission entwickelten „Kritikalitätspyramide“ (vgl. 28. TB, Nr. 4.4. und 4.6) etwa auch die aktuellen Entwicklungen zur Schaffung eines EU-Rechtsrahmens für KI. Antidiskriminierungs- oder Transparenzvorgaben sowie verbesserte Möglichkeiten der Rechtsdurchsetzung bedürfen ebenfalls gesetzlicher Normierung.

Grenzen der Verhaltens- und Leistungskontrolle

Die Grenzen der Verhaltens- und Leistungskontrolle sollten gesetzlich geregelt werden, beispielsweise für den des Zugriffs auf und für die Auswertung von E-Mails und weiteren IT-Daten der Beschäftigten durch Arbeitgeberinnen und Arbeitgeber, für den Einsatz von Geoinformationssystemen (GPS-Tracking) und biometrischen Verfahren im Beschäftigungsverhältnis oder Regelungen zum Einsatz von Videoüberwachung. Heimliche Kontrollen im Beschäftigungsverhältnis oder Dauerüberwachungen des Verhaltens der Beschäftigten sollten verboten sein.

1 Zu den Beschlüssen zu Microsoft, abrufbar unter: https://www.bfdi.bund.de/beschlüsse-positionspapiere
2 Entschließung vom 29. April 2022, abrufbar unter: https://www.bfdi.bund.de/entschliessungen

Ergänzungen zu den Rahmenbedingungen der Einwilligung

Wichtig sind etwa Regelbeispiele für die Unzulässigkeit der Nutzung von Einwilligungen zur Verarbeitung von Beschäftigtendaten.

Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen

Der Gesetzgeber sollte klarstellen, ob Kollektivvereinbarungen zusätzliche Rechtsgrundlagen für Datenverarbeitungen im Beschäftigungsverhältnis bilden können.

Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Art. 6 und 9 DSGVO

Die DSK empfiehlt, eindeutige konkretisierende Regelungen für die Verarbeitung von besonderen Kategorien personenbezogener Daten wie Gesundheitsdaten im Beschäftigungsverhältnis zu schaffen.

Beweisverwertungsverbote

Die DSK spricht sich für eine gesetzliche Normierung eines Beweisverwertungsverbots für rechtswidrig verarbeitete Beschäftigtendaten aus.

Datenverarbeitung bei Bewerbungs- und Auswahlverfahren

Geregelt werden sollten zudem die typischen Datenverarbeitungssituationen in Bewerbungs- und Auswahlverfahren.

Vor dem Hintergrund dieser Entschließung, des Beiratsberichts und der aktuellen Pläne der Bundesregierung bin ich optimistisch, dass das Beschäftigtendatenschutzgesetz gerade jetzt auf einem guten Weg ist. Im Rahmen des anstehenden Gesetzgebungsverfahrens werde ich mich weiter für einen fairen Ausgleich zwischen den grundrechtlich geschützten Interessen der Arbeitgeberinnen und Arbeitgeber und dem ebenso geschütztem Recht auf informationelle Selbstbestimmung der Beschäftigten einsetzen.

Ich empfehle der Bundesregierung ein Beschäftigtendatenschutzgesetz zu erlassen, in dem etwa der Einsatz von KI im Beschäftigungskontext, die Grenzen der Verhaltens- und Leistungskontrolle sowie typische Datenverarbeitungen im Bewerbungs- und Auswahlverfahren klar geregelt werden.

3.2.5 Aktenvernichtungs- und Datenlöschmoratorium

Ende 2012 war bekannt geworden, dass das Bundesamt für Verfassungsschutz Akten zum sog. NSU vernichtet hatte. In der Folgezeit bat der Vorsitzende des NSU-Untersuchungsausschusses des Bundstages deshalb darum, keinerlei Akten mit Bezug zum Rechtsextremismus zu vernichten. Es wurde ein umfassendes Aktenvernichtungs- und Löschmoratorium auf Bundesebene ausgesprochen. Entgegen der ursprünglichen Absicht, das Moratorium aufzuheben, soll dieses nun erneut verlängert werden.

Parlamentarische Untersuchungsausschüsse möchten für ihre Aufklärungsarbeit eine ausreichende Datengrundlage sicherstellen. Dafür sprechen sie u. a. sog. Löschmoratorien aus. Diese verbieten es den Polizeibehörden und Nachrichtendiensten, solche Daten zu löschen, die den Untersuchungsgegenstand betreffen. Gerade für die Untersuchungsausschüsse zum rechtsextremistischen Terrorismus durch Gruppen wie den sog. NSU ist das Interesse der Parlamentarischen Untersuchungsausschüsse an dem Erhalt personenbezogener Daten besonders nachvollziehbar und gewichtig.

Dennoch besteht Kritik an den Löschmoratorien. Denn diese benennen nicht einzelne spezifische Akten oder Datensätze, sondern beschreiben allgemein ein Themengebiet. Daher sind der Umfang und der Kreis der weiter gespeicherten Daten schwer abgrenzbar. Die Behörden speichern in der Folge in großem Umfang personenbezogene Daten weiter, die eigentlich zu löschen wären. Löschmoratorien greifen damit in die Grundrechte der betroffenen Personen ein. Besonders intensiv sind diese Eingriffe, wenn die Personen tatsächlich in keinerlei Bezug zum Untersuchungsgegenstand stehen bzw. die Daten sogar zu löschen wären. Zu löschen sind im Normalfall gerade die Daten, die die Behörden für ihre Aufgaben nicht mehr benötigen, z. B. weil sich ein Tatverdacht gegen die betroffene Person nicht erhärtet hat. Deshalb ist ein Löschmoratorium, das gerade auf den Erhalt solcher eigentlich zu löschender Daten gerichtet ist, ein besonders sensibler Eingriff. Trotz dieser besonderen Sensibilität existieren bislang keine gesetzlichen Grundlagen, welche die Verarbeitung personenbezogener Daten bei den Behörden zum Zwecke der Durchführung eines parlamentarischen Untersuchungsausschusses regeln.

Zusammen mit den Datenschutzaufsichtsbehörden der Länder habe ich im März 2022 daher eine Entschließung verabschiedet und Datenschutz durch klare Vorgaben

und Verarbeitungsbeschränkungen für Behörden gefordert.[3]

Darin appelliert die DSK an die Gesetzgeber des Bundes und der Länder, den Sicherheitsbehörden klare gesetzlichen Vorgaben an die Hand zu geben, wie sie im Falle eines Löschmoratoriums mit zu löschenden Daten umzugehen haben. Diese müssen den Untersuchungsausschüssen den Zugriff auf die Daten sichern. Gleichzeitig ist sicherzustellen, dass die Daten dem Verwaltungsvollzug der Behörde vollständig entzogen sind.

Einige Landesgesetzgeber sind schon entsprechend tätig geworden. Das Bundesministerium des Innern und für Heimat (BMI) teilte mir kürzlich mit, gesetzliche Grundlagen für eine Verarbeitungsbeschränkung zur parlamentarischen Beweissicherung zu begrüßen. Die Initiative müsse aber aus dem Bundestag selbst kommen. Darauf sei in einem Schreiben an den Ausschuss für Inneres und Heimat hingewiesen worden. Das BMI hält ein Löschmoratorium aber auch ohne klare gesetzliche Grundlagen für rechtskonform und erforderlich. Ob der Bundesgesetzgeber tätig werden wird, bleibt daher abzuwarten.

3.2.6 Orientierungshilfe Werbung 2.0

Was ist Werbung? Was ist Direktwerbung? Was regelt die DSGVO? Die DSK hat eine Orientierungshilfe zu den wichtigsten Grundsätzen der DSGVO für die Direktwerbung veröffentlicht.

Zu den wichtigsten datenschutzrechtlichen Grundsätzen für die Direktwerbung hat die Datenschutzkonferenz im Februar 2022 eine neue Orientierungshilfe (OH) veröffentlicht. Die OH baut auf den Anwendungshinweisen der DSK aus dem Jahr 2018 zur Verarbeitung personenbezogener Daten für werbliche Zwecke unter Berücksichtigung der DSGVO-Regelungen und den Regelungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) auf. Die DSGVO selbst enthält keine einschlägigen Regelungen für Direktwerbung. Die DSK hat in der OH nunmehr beispielsweise die Begriffe „Werbung“ und „Direktwerbung“ definiert. Im Wesentlichen umfasst sie fünf Themenbereiche:

- Interessenabwägung bei Direktwerbung,
- Informationspflichten,
- Einwilligung in die Datenverarbeitung für Direktwerbung,
- praktische Fallgestaltungen,
- Werbewiderspruch.

Die „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DSGVO)“ ist auf der Website der DSK abrufbar.[4]

3.3 Europäischer Datenschutzausschuss

Der europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union beiträgt und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördert. Diese Aufgaben habe ich bereits in meinen vorangegangenen Tätigkeitsberichten näher erläutert. Als gemeinsamer Vertreter aller deutschen Datenschutzbehörden ist der BfDI Mitglied des Ausschusses. Nähere Ausführungen können über meinen Internetauftritt abgerufen werden.[5]

Zu den Informationen zum EDSA geht’s hier:

(QR-Code scannen oder klicken)

3.3.1 Allgemeiner Bericht

Der Europäische Datenschutzausschuss (EDSA) hat im Berichtsjahr seine Arbeit an einer europaweit einheitlichen Anwendung der Datenschutz-Grundverordnung (DSGVO) weiter verstärkt. Leitlinien wurden angenommen und Stellungnahmen abgegeben. Auch die grenzüberschreitende Zusammenarbeit wurde weiter intensiviert, vor allem im Wege einer koordinierten Durchsetzungsmaßnahme mehrerer Aufsichtsbehörden. Zudem wurden fünf Verfahren der Streitbeilegung entschieden, weitere stehen an.

2022 hat der EDSA seine hohe Dichte an Plenarsitzungen weiter verfestigt und insgesamt 15 Mal konferiert, im Wechsel in Form von Videokonferenzen und Präsenzveranstaltungen in Brüssel. Hinzu kommen zahlreiche

3 Entschließung „Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden“ Entschließung vom 23. März 2022, abrufbar unter www.bfdi.bund.de/entschliessungen
4 Orientierungshilfe der DSK, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf
5 Informationen zum EDSA unter: https://www.bfdi.bund.de/edsa

Sitzungen der Arbeitsgruppen (Expert Subgroups) des EDSA. Ergänzend hat im April ein hochrangiges Treffen der Mitglieder des EDSA mit dem Ziel der Verbesserung der Zusammenarbeit in der Durchsetzung des Datenschutzes auf europäischer Ebene stattgefunden.

Ein Schwerpunkt der Arbeiten lag auch in diesem Berichtsjahr auf der Erarbeitung von Leitlinien bzw. Empfehlungen nach Art. 70 DSGVO zur einheitlichen Umsetzung der DSGVO in Europa. Daneben hat der Ausschuss zahlreiche Stellungnahmen im Kohärenzverfahren nach Art. 64 DSGVO angenommen und gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) Stellungnahmen in Rechtsetzungsverfahren abgegeben. In meinen letzten beiden Tätigkeitsberichten (30. TB Nr. 3.2.1, 29. TB Nr. 3.2) habe ich auf erste Entscheidungen gegenüber weltweit führenden Tech-Unternehmen hingewiesen. Auch hier hat es weitere Entwicklungen gegeben.

Der EDSA hat zudem seine Strategie für die Jahre 2021 bis 2023 weiter umgesetzt (Nr. 3.3.2). Einen Schwerpunkt bildeten dabei koordinierte Mechanismen der Durchsetzung des Datenschutzes auf europäischer Ebene bei grenzüberschreitenden Sachverhalten.

Leitlinien, Empfehlungen und Stellungnahmen/ Kohärenzverfahren

Der EDSA hat im Berichtsjahr zahlreiche Leitlinien und Stellungnahmen verabschiedet[6], an denen ich regelmäßig als Berichterstatter oder Mitberichterstatter mitgearbeitet habe. Diese wurden im Regelfall zur Wahrung der Transparenz einer öffentlichen Konsultation unterzogen.

- Die **Leitlinien 01/2022 zu den Rechten betroffener Personen** (Guidelines 01/2022 on data subject rights - Right of access) zielen darauf ab, die verschiedenen Aspekte des Auskunftsrechts nach Art. 15 DSGVO zu analysieren und näher zu präzisieren, wie das Auskunftsrecht in der Praxis umzusetzen ist. Die Leitlinien enthalten unter anderem Klarstellungen zum Umfang des Auskunftsrechts, zu den Informationen, welche die für die Verarbeitung Verantwortlichen der betroffenen Person zur Verfügung stellen müssen und zu den wichtigsten Modalitäten für die Gewährung der Auskunft. Zudem wird der Begriff des offensichtlich unbegründeten oder übermäßigen Antrags erläutert.
- Die **Leitlinien 02/2022 zu Art. 60 DSGVO** (Guidelines 02/2022 on the application of Article 60 GDPR) sollen dazu dienen, die Anwendung der rechtlichen Bestimmungen über das Verfahren der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden („One-Stop-Shop-Mechanismus“) weiter zu vereinheitlichen. Die Leitlinien sollen den Aufsichtsbehörden dabei helfen, ihre eigenen nationalen Verfahren so auszulegen und anzuwenden, dass sie mit diesem Verfahren der Zusammenarbeit übereinstimmen und ineinandergreifen (Nr. 3.3.7).
- Die **Leitlinien 03/2022 zu Dark Patterns auf der Benutzeroberfläche von Social-Media-Plattformen** (Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them) bieten für das Entwickeln und Nutzen solcher Plattformen praktische Empfehlungen zur Bewertung und Vermeidung von gegen die DSGVO verstoßenden „dunklen Designmustern“ auf Benutzeroberflächen. Dark Patterns (künftig: „deceptive design patterns“) beeinflussen das Verhalten der Nutzer und deren Fähigkeit, ihre personenbezogenen Daten wirksam zu schützen.
- Die **Leitlinien 04/2022 für die Berechnung von Geldbußen** (Guidelines 04/2022 on the calculation of administrative fines under the GDPR) harmonisieren die bestehenden Verfahrensweisen der Datenschutzbehörden und enthalten zudem einheitliche „Ausgangspunkte“ für die Berechnung einer Geldbuße. Dabei werden drei Aspekte berücksichtigt: die Art (Kategorie) des Verstoßes, dessen Schwere und der Umsatz des betreffenden Unternehmens.
- Die **Leitlinien 05/2022 für den Einsatz von Gesichtserkennungstechnologien im Strafverfolgungsbereich** (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement) bieten den Gesetzgebern auf EU- und nationaler Ebene sowie den Strafverfolgungsbehörden eine Orientierungshilfe bei der Einführung und Nutzung solcher Technologien. Der EDSA bekräftigt darin u. a. seine Forderung nach einem Verbot des Einsatzes von Gesichtserkennungstechnologien in bestimmten Fällen, z. B. die biometrische Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen.
- Die **Leitlinien 06/2022 für die praktische Umsetzung der gütlichen Einigung** (Guidelines 06/2022 on the practical implementation of amicable settlements) sollen dazu beitragen, die Unterschiede in der Behandlung betroffener Personen und der Durchsetzungsmaßnahmen auf nationaler Ebene im Falle der

6 Leitlinien und Stellungnahmen des EDSA, abrufbar unter: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

Beendigung des Verfahrens durch gütliche Einigung zu beseitigen. Diese Unterscheide ergeben sich bisher daraus, dass gütliche Einigungen in den Mitgliedstaaten zum Teil gar nicht existieren oder aber sehr unterschiedlich geregelt sind und gehandhabt werden.

- Die **Leitlinien 07/2022 über Zertifizierung als Instrument für Übermittlungen** (Guidelines 07/2022 on certification as tool for transfers) erläutern die praktische Anwendung der Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen auf der Grundlage von Zertifizierungen. In Ergänzung zu den allgemeinen Leitlinien für die Zertifizierung und Akkreditierung nach der DSGVO konzentrieren sich die vorliegenden Leitlinien auf die spezifischen Aspekte der Zertifizierung als Instrument für Drittstaatenübermittlungen (Nr. 3.3.10).
- Die **Leitlinien 08/2022 zur Ermittlung der federführenden Aufsichtsbehörde eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters** (Guidelines 08/2022 on identifying a controller or processor's lead supervisory authority) wurden im Hinblick auf die Bestimmung einer „Hauptniederlassung" für die Situation der gemeinsamen Verantwortlichkeit im Sinne des Artikels 26 DSGVO angepasst.
- Die **Leitlinien 09/2022 zur Meldung von Datenschutzverletzungen nach der DSGVO** (Guidelines 9/2022 on personal data breach notification under GDPR) wurden für die Konstellation angepasst, in der Verantwortliche über keine eigene Niederlassung in einem Mitgliedstaat verfügt. Die Existenz eines Vertreters in einem Mitgliedstaat reicht nicht aus, um in den Genuss des One-Stop-Shop-Mechanismus zu kommen. Daher muss ein solcher Verantwortlicher mit der Aufsichtsbehörde jedes Mitgliedsstaates in Kontakt treten, in dem er operiert.
- Die **Empfehlungen 1/2022 zum Zulassungsantrag und zu den notwendigen Elementen und Grundsätzen in verbindlichen internen Datenschutzvorschriften von Verantwortlichen nach Art. 47 DSGVO** (Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)) enthalten eine Aktualisierung des bestehenden „BCR-C-Referentials", welches Kriterien für die Zulassung von verbindlichen internen Datenschutzvorschriften für Verantwortliche enthält, und verschmelzen sie mit dem dazugehörigen Standardantragsformular. Die neuen Empfehlungen bauen auf den Vereinbarungen auf, die Datenschutzbehörden im Zuge von Genehmigungsverfahren zu konkreten BCR-Anwendungen seit Inkrafttreten der DSGVO getroffen haben und nehmen die Anforderungen des Schrems II-Urteils des EuGH auf.

Im **Kohärenzverfahren** hat der EDSA zahlreiche Stellungnahmen verfasst. Diese betreffen zum großen Teil:

- durch Mitgliedstaaten vorgelegte verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO),
- die Akkreditierung von Zertifizierungsstellen (Art. 43 Abs. 3 DSGVO) und
- Stellen zur Überwachung der Einhaltung von Verhaltensregeln (Art. 41 DSGVO).

Erstmals hat der EDSA auch eine Stellungnahme zu genehmigten Kriterien eines deutschen Unternehmens für die europaweite Zertifizierung von Auftragsverarbeitern abgegeben (Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors).[7]

Im Rahmen der **Konsultation im Rechtsetzungsverfahren** sind zwei gemeinsame Stellungnahmen des EDSA und des EDSB besonders hervorzuheben:

- In der **gemeinsamen Stellungnahme 04/2022 zum Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern** (Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse) haben EDSA und EDSB deutlich gemacht, dass der Vorschlag möglicherweise mehr Risiken für Eingriffe in Grundrechte der Einzelnen und damit für die Gesellschaft insgesamt birgt, als dass er eine erfolgreiche Bekämpfung des sexuellen Missbrauchs von Kindern gewährleistet. Zwar unterstützen der EDSA und der EDSB uneingeschränkt die Ziele und die Absichten des Vorschlags, befürchten aber, dass er als Grundlage für ein allgemeines und undifferenziertes Durchleuchten des Inhalts praktisch aller Arten elektronischer Kommunikation herangezogen werden könnte (Nr. 4.4.1).
- In der **gemeinsamen Stellungnahme 03/2022 zum Vorschlag für einen Rechtsakt zum Europäischen Gesundheitsdatenraum** (Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space) haben EDSA und EDSB die im Vorschlag verankerte Idee befürwortet, die Kontrolle des Einzelnen über seine personenbezogenen Gesundheitsdaten zu stärken. Zugleich sehen der EDSA und der

7 Stellungnahme des EDSA, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-252022-regarding-european-privacy-seal_en

EDSB aber die Gefahr, dass der Schutz der Rechte auf Privatsphäre und Datenschutz geschwächt werden könnte. Diese Gefahr bestehe vor allem mit Blick auf die Kategorien personenbezogener Daten und der Zwecke, die mit der sog. Sekundärnutzung von Daten verbunden sind (Nr. 5.1).

Entscheidungen in Streitbeilegungsverfahren

Im Juli hat der EDSA eine Entscheidung im Streitbeilegungsverfahren zum Verfahren der irischen Aufsichtsbehörde (DPC) gegen Meta Irland gefällt (Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR)[8]. Der EDSA verpflichtet darin die DPC, einen zusätzlichen Verstoß gegen Art. 6 Abs. 1 DSGVO festzustellen, weil sich Instagram als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten im Zusammenhang mit Benutzerkonten von Kindern weder auf die Notwendigkeit der Vertragserfüllung (Art. 6 Abs. 1 lit. b) DSGVO) noch auf berechtigte Interessen (Art. 6 Abs. 1 lit. f) DSGVO) berufen kann. Folgerichtig wird die DPC angewiesen, ihre geplanten Abhilfemaßnahmen im Einklang mit den Schlussfolgerungen des EDSA erneut zu bewerten, um dem zusätzlichen Verstoß Rechnung zu tragen und um sicherzustellen, dass Instagram die Verpflichtungen in vollem Umfang umsetzt. Hinsichtlich der Berechnung der Bußgeldhöhe weist der EDSA die DPC an sicherzustellen, dass die endgültig verhängten Beträge der Geldbußen wirksam, verhältnismäßig und abschreckend sind. Demnach musste die Geldbuße signifikant erhöht werden. Infolge dieser Entscheidung des EDSA hat die DPC eine Geldbuße in Höhe von 405 Mio. Euro gegen Instagram verhängt. Die Entscheidung des EDSA beruht auf sog. „maßgeblichen und begründeten" Einsprüchen, die auch durch mehrere deutsche Aufsichtsbehörden, u. a. auch durch meine Behörde, unter Federführung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit eingelegt wurden.

Bereits im Juni 2022 hat der EDSA eine Entscheidung im Streitbeilegungsverfahren zum Verfahren der französischen Aufsichtsbehörde (CNIL) gegen Accor SA getroffen (Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR).[9] Diese verpflichtet die CNIL, die gegen die Accor SA zu verhängende Geldbuße neu zu berechnen. Die Geldbuße wurde verhängt, da Accor Cookies in unzulässiger Weise auf seiner Webseite eingebunden hatte.

Der EDSA erließ im Dezember 2022 drei weitere Entscheidungen zur Streitbeilegung betreffend Meta Platforms Ireland Limited (Meta IE). Die verbindlichen Entscheidungen befassen sich mit wichtigen rechtlichen Fragen, die sich aus den Entscheidungsentwürfen der irischen DPC als federführende Aufsichtsbehörde in Bezug auf Meta IE-Plattformen Facebook, Instagram und WhatsApp ergeben. Ich halte diese Entscheidungen für nicht vereinbar mit den Vorgaben der DSGVO und hatte dementsprechend als betroffene Aufsichtsbehörde gegen die Entscheidung zu WhatsApp Einspruch eingelegt. In den beiden Entscheidungen gegen Meta IE widersprach der EDSA der von der DPC vorgeschlagenen Schlussfolgerung, dass Meta IE rechtlich nicht verpflichtet ist, sich auf die Zustimmung zur Durchführung der Verarbeitungstätigkeiten im Zusammenhang mit der Bereitstellung seiner Facebook- und Instagram-Dienste zu stützen. Dieses könne ohne weitere Untersuchungen nicht kategorisch ausgeschlossen werden konnte.

Daher entschied der EDSA, dass die DPC eine neue Untersuchung durchführen muss. Darüber hinaus wies der EDSA die DPC an, in beiden endgültigen Entscheidungen eine Verletzung des Grundsatzes der Fairness festzustellen und geeignete Korrekturmaßnahmen zu ergreifen. Der EDSA stellte auch schwerwiegende Verstöße gegen die Transparenzverpflichtungen fest und dass Meta IE seine Dienste den Nutzern auf irreführende Weise präsentiert habe. In Bezug auf die Geldbußen wies der EDSA die DPC an, wegen der zusätzlichen Verstöße gegen Art. 6 Abs. 1 DSGVO (mangelnde Rechtsgrundlage für die Verarbeitung personenbezogener Daten) für die festgestellten Transparenzverstöße eine erhebliche höhere Geldbuße zu verhängen. Denn die vorgeschlagenen Geldbußen erfüllten das Erfordernis einer wirksamen, verhältnismäßigen und abschreckenden Wirkung nicht. Die weitere Umsetzung der Entscheidungen erfolgt im kommenden Berichtsjahr.

Querverweise:

3.3.2 Umsetzung EDSA-Strategie, 3.3.7 Leitlinien zu Art. 60 DSGVO, 3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers, 4.4.1 CSAM-Verordnung, 5.1 European Health Data Space,

8 Entscheidung im Streitbeilegungsverfahren, abrufbar unter: https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf

9 Entscheidung des EDSA im Streitbeilegungsverfahren, abrufbar unter: https://edpb.europa.eu/system/files/2022-08/edpb_binding_decision_01_2022_accor_en_redacted_en.pdf

3.3.2 Umsetzung der EDSA-Strategie 2021-2023

Neben seinen jährlichen Arbeitsprogrammen hat der EDSA eine übergreifende Strategie für den Zeitraum von 2021 bis 2023 aufgestellt. Einen Schwerpunkt im zweiten Jahr der gemeinsamen Umsetzung bilden dabei koordinierte Mechanismen der Durchsetzung des Datenschutzes auf europäischer Ebene.

Die vier Säulen der EDSA-Strategie[10] für den Zeitraum 2021-2023

1. Förderung der Harmonisierung und die Erleichterung der Rechtskonformität (Compliance),
2. Unterstützung einer effektiven Durchsetzung und einer effizienten Zusammenarbeit zwischen nationalen Aufsichtsbehörden,
3. ein grundrechtlicher Ansatz für neue Technologien und
4. die globale Dimension

sowie deren Umsetzung im ersten Jahr habe ich in meinen letzten Tätigkeitsberichten beschrieben (30. TB Nr. 3.2.1, 29. TB Nr. 3.2). Auch in diesem Berichtsjahr habe ich an der Umsetzung der Strategie auf nationaler wie auf europäischer Ebene mitgewirkt.

Zur Umsetzung der ersten Säule hat der EDSA die Benennung und Stellung der Datenschutzbeauftragten (u. a. in Betrieben und Behörden) im Sinne der Artikel 37 – 39 DSGVO als Thema für seine zweite koordinierte Durchsetzungsmaßnahme in 2023 beschlossen. Für das vergangene Jahr hatte der EDSA die Nutzung von Cloud-basierten Diensten durch den öffentlichen Sektor als erste koordinierte Aktion ausgewählt, die ich im Bereich der Bundesverwaltung umsetze. Die beiden koordinierten Maßnahmen folgen auf den Beschluss des EDSA im Oktober 2020, einen koordinierten Durchsetzungsrahmen *(Coordinated Enforcement Framework – CEF)*[11] einzurichten (Nr. 3.3.3). Der CEF ist zusammen mit dem unterstützenden Expertenpool *(Support Pool of Experts)*[12] eine Schlüsselmaßnahme des EDSA im Rahmen seiner Strategie. Die beiden Initiativen zielen darauf ab, die Durchsetzung und die Zusammenarbeit zwischen den Datenschutzbehörden zu stärken. Letzteres Ziel ist Teil der im April 2022 in Wien gefundenen Absprache zu einer Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes auf europäischer Ebene, vor allem bei grenzüberschreitenden Fällen („cross-border cases").[13]

In der zweiten Säule hat der EDSA gemäß dieser Absprache, neben dem koordinierten Durchsetzungsrahmen (CEF), Kriterien für grenzüberschreitende Fälle von strategischer Bedeutung definiert[14] und drei erste strategische Fälle für eine vertiefte und beschleunigte Kooperation ausgewählt. Als weiteres Ergebnis des Treffens in Wien hat der EDSA eine Liste von zum Teil hinderlichen Aspekten der nationalen Verfahrensrechte angenommen, die zur Verbesserung der Durchsetzung der DSGVO auf europäischer Ebene harmonisiert werden sollten. Die Liste befasst sich unter anderem mit dem Status und den Rechten der Parteien in den nationalen Verwaltungsverfahren, den Verfahrensfristen im Kooperationsverfahren, den Anforderungen für die Zulässigkeit oder Ablehnung von Beschwerden, den Ermittlungsbefugnissen der Datenschutzbehörden und der praktischen Umsetzung des Kooperationsverfahrens. Diese sogenannte *„Wishlist"*[15] wurde der Europäischen Kommission zur Prüfung möglicher Verbesserungen übermittelt.

3.3.3 Coordinated Enforcement Action 2021/2022

Die europäischen Datenschutz-Aufsichtsbehörden koordinieren ihr Vorgehen im Rahmen der ersten „Coordinated Enforcement Action" (CEF) und untersuchen die Nutzung cloudbasierter Dienste durch den öffentlichen Sektor.

Bei der „Coordinated Enforcement Action" handelt es sich um eine geplante jährliche koordinierte Maßnahme der europäischen Aufsichtsbehörden im Rahmen des CEF. Sie ist eine Initiative des EDSA, mit welcher die Kooperation und die Rechtsdurchsetzung unter den Aufsichtsbehörden gefördert werden soll und stellt eine wesentliche Maßnahme der EDSA-Strategie 2021-2023 dar (Nr. 3.3.2). Hierbei wird ein vorher festgelegtes Thema gemeinsam nach einer vorab vereinbarten Methodik bearbeitet. Das Thema der aktuellen und ersten „Coordinated Enforcement Action" ist die Nutzung cloudbasierter Dienste durch den öffentlichen Sektor. Meine Behörde nimmt hieran im Rahmen meiner Zuständigkeit für die

10 EDSA-Strategie für den Zeitraum 2021-2023: https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2021-2023_en
11 Informationen des EDSA zum CEF: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en
12 Informationen des EDSA zum Expertenpool: https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-terms-reference-edpb-support-pool-experts_en
13 https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf
14 https://edpb.europa.eu/system/files/2022-07/edpb_document_20220712_selectionofstrategiccases_en.pdf
15 Zur Wishlist: https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf

Datenschutzaufsicht über die Bundesverwaltung neben 21 weiteren Aufsichtsbehörden teil und hat Untersuchungen zur Nutzung von Cloud-Diensten im Bereich der Arbeits- und Gesundheitsverwaltung sowie dem ITZBund als zentralem Dienstleister für Cloud-Dienste der Bundesbehörden durchgeführt.

Die von der Arbeitsgruppe begonnene Untersuchung betrifft etwa 75 Aufsichtsobjekte aus unterschiedlichen Fachbereichen. Schwerpunkte bilden hier unter anderem Datenübermittlungen an Drittländer und Regelungen im Zusammenhang mit Auftragsverarbeitungen. Im Anschluss an die Auswertung wird ein gemeinsamer Bericht erstellt und vom EDSA angenommen. Danach werden die Aufsichtsbehörden über koordinierte nationale Aufsichts- und Durchsetzungsmaßnahmen entscheiden.

Querverweise:

3.3.8 Umsetzung der Controller Binding Corporate Rules

3.3.4 EU-Systeme: Zentrale Koordinierung der Aufsicht im CSC

Die Zuständigkeit für die Koordinierung der Aufsicht über die EU-Systeme und -Institutionen wird schon jetzt und zukünftig noch stärker im Coordinated Supervision Committee des EDSA konzentriert. Dieses Jahr kam Europol hinzu, in den kommenden Jahren werden weitere EU-Systeme folgen.

Im beim EDSA angesiedelten Coordinated Supervision Committee (CSC) koordinieren die nationalen Aufsichtsbehörden und der Europäische Datenschutzbeauftragte (EDSB) ihre Aufsichtstätigkeit und unterstützen sich gegenseitig, soweit bestimmte EU-Informationssysteme und EU-Institutionen betroffen sind. Die Zuständigkeit des CSC umfasst aktuell vier große Bereiche. Dies sind zunächst das *Internal Market Information System* (IMI), *Eurojust* und die *Europäische Staatsanwaltschaft*. Mit der Änderung der Europol-Verordnung (VO) durch die VO (EU) 2022/991 im Juni 2022 wurde zudem der Beirat für die Zusammenarbeit (vgl. 27. TB Nr. 9.2.3) aufgelöst und *Europol* in den Zuständigkeitsbereich des CSC überführt.

In den kommenden Jahren wird die Zuständigkeit des CSC um zahlreiche EU-Systeme erweitert. Die bereits bestehenden *Systeme Schengener Informationssystem* (SIS), *Zollinformationssystem* (CIS), *Eurodac* und *Visa*-Informationssystem (VIS) sollen beim CSC angesiedelt werden. Für diese sind derzeit noch jeweils eigene

„Supervision Coordination Groups“ eingerichtet. Das CSC soll künftig auch für die geplanten EU-Systeme *Europäisches Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose* (ECRIS-TCN), *Einreise-/Ausreisesystem* (EES) und *Europäisches Reiseinformations- und -genehmigungssystem* (ETIAS) sowie den *EU-Interoperabilitätsrahmen* zuständig sein.

Gemeinsam mit der jeweiligen Ländervertretung beteilige ich mich aktiv an den regelmäßigen Sitzungen des CSC und der Ausarbeitung gemeinsamer Dokumente wie etwa der Erstellung eines einheitlichen Informationsschreibens für betroffene Personen zur EU-weiten Nutzung von IMI. Zudem habe ich im Dezember 2021 den stellvertretenden Vorsitz übernommen.

Das Arbeitsprogramm des CSC für den Zeitraum 2022-2024 ist über den CSC-Bereich der EDSA-Website abrufbar.[16] Schwerpunkte der Arbeit im Gremium sind die Ausübung von Betroffenenrechten und die Förderung des Informationsaustausches zwischen den Mitgliedern sowie der Durchführung gemeinsamer Kontrollen. Hinzu kommt die Vorbereitung der anstehenden Erweiterung des Zuständigkeitsbereichs des CSC.

Querverweise:

3.5.3 Neues ETIAS-Beratungsgremium für Grundrechte, 3.5.4 Bericht aus den SCGs, 9.2.8 Koordinierte Kontrollen zu Ausschreibungen zur verdeckten/gezielten Kontrolle im Schengener Informationssystem

3.3.5 EDSA veröffentlicht Leitlinien zum Auskunftsrecht

Mit dem Auskunftsrecht können Betroffene in Erfahrung bringen, welche Daten Unternehmen und Behörden über sie verarbeiten und gespeichert haben. Mit neuen Leitlinien sorgt der EDSA für mehr Klarheit und Einheitlichkeit.

Das Recht auf Auskunft ist in der Praxis sehr bedeutsam. Der entsprechende Art. 15 der DSGVO lässt aber einen großen Interpretationsspielraum, der zu unterschiedlichen Auffassungen in der juristischen Literatur, unter den Aufsichtsbehörden und zu divergierenden Gerichtsentscheidungen geführt hat. Nach über zweijährigen Arbeiten hat der EDSA im Januar 2022 Leitlinien zum Auskunftsrecht[17] verabschiedet, an denen ich als Co-Berichterstatter mitgearbeitet habe.

Besonders wichtige Punkte, die in den Leitlinien festgelegt wurden:

- Der Umfang des Auskunftsanspruchs richtet sich im Wesentlichen nach der Definition der personenbezogenen Daten (Art. 4 Nr. 1 DSGVO). Eine einschränkende Auslegung findet nicht statt. Auch interne Dokumente und etwa E-Mail-Verkehr können umfasst sein.
- Das Recht auf Kopie (Art. 15 Abs. 3 DSGVO) ist kein eigenständiges Recht, sondern eine Modalität zur Erfüllung des Auskunftsanspruchs. Im Regelfall ist der betroffenen Person allerdings eine Kopie zu übergeben.
- Den Verantwortlichen trifft die Verpflichtung, angemessene Maßnahmen zur Identifikation der betroffenen Person zu treffen, um zu verhindern, dass durch das Auskunftsrecht personenbezogene Daten an unberechtigte Dritte gelangen. Auf der anderen Seite dürfen aber auch keine höheren Hürden aufgebaut werden als für die Bereitstellung der Daten selbst.
- Werden große Datenmengen verarbeitet, kann der Verantwortliche insbesondere im Online-Kontext die Informationen in mehreren voneinander getrennten Ebenen übermitteln (sog. layered approach).
- Ein Auskunftsersuchen kann von dem Verantwortlichen nicht allein unter Verweis auf den Aufwand der Beantwortung oder andere Verhältnismäßigkeitserwägungen abgelehnt werden. Die Motivation hinter einem Auskunftsersuchen ist grundsätzlich irrelevant.
- Die Leitlinien geben zusätzlich Hinweise und konkrete Beispiele, in welchen zeitlichen Abständen Betroffene das Auskunftsrecht geltend machen können. Wann liegt eine häufige Wiederholung vor? Ab wann wird das Auskunftsrecht missbraucht? Bei Auskunfteien beispielsweise ist ein Intervall von einmal jährlich nicht exzessiv. Bei rechtsmissbräuchlichen Anträgen kann ein Auskunftsersuchen im Einzelfall ausnahmsweise als exzessiv abgelehnt werden.

Ich begrüße die gemeinsamen Leitlinien. Bei den Verhandlungen habe ich zusammen mit meiner Kollegin aus Nordrhein-Westfalen die deutsche Auslegung des Auskunftsrechts gemäß Art. 15 DSGVO in den Prozess eingebracht. Die Leitlinien stellen eine gelungene gemeinsame Position der europäischen Aufsichtsbehörden da und leisten einen wichtigen Beitrag zur Stärkung des Auskunftsrechts in der EU. Der EDSA hat eine öffentliche Konsultation zu den Leitlinien durchgeführt, derzeit

16 Arbeitsprogramm des CSC, abrufbar unter: https://edpb.europa.eu/csc/about-csc/work-programme-coordinated-supervision-committee_en
17 Guidelines 01/2022 on data subject rights - Right of access, abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

läuft die Auswertung der eingegangenen Stellungnahmen. Mit einer Annahme des endgültigen Textes der Leitlinien durch den EDSA ist Anfang 2023 zu rechnen.

3.3.6 EDSA legt Bußgeld-Leitlinien vor

Der EDSA hat neue Leitlinien zur Berechnung von Geldbußen nach der DSGVO beschlossen. Sie dienen der europaweiten Harmonisierung der Bußgeldpraxis und geben Orientierungspunkte zur Berechnung von Geldbußen bei gleichzeitigem Spielraum für das Ermessen im Einzelfall.

Bei Verstößen gegen die DSGVO haben die nationalen Datenschutzaufsichtsbehörden bisher als Folge verschiedener Rechtstraditionen und –kulturen unterschiedliche Methoden zur Berechnung von Geldbußen verwendet. Durch die im Mai 2022 beschlossenen Leitlinien[18] erfolgt die Bußgeldpraxis nun mithilfe einer einheitlichen europäischen Methodik. Die Leitlinien fügen sich als wichtiger Baustein in eine Gesamtentwicklung der Datenschutzbehörden zu einer stärkeren Annäherung und strategischeren Ausrichtung ihrer Rechtsdurchsetzung ein.

Die nunmehr durch den EDSA erlassenen Leitlinien zur Berechnung von Geldbußen nach der DSGVO geben dabei weder zwingende Pauschalbeträge (sog. Preisschilder) vor noch sehen sie eine rein mathematische Berechnungsformel vor. Beides wäre rechtlich zweifelhaft und letzteres aus meiner Sicht sogar rechtswidrig. Stattdessen geben die Leitlinien Orientierungspunkte für Startbeträge und wie diese durch weitere Ermessenfaktoren erhöht oder gemindert werden können. Sie führen daher einerseits zu einer Annäherung der Bußgeldbeträge, lassen zugleich aber auch den notwendigen Ermessensspielraum für den Einzelfall zu.

Die Leitlinien gewährleisten mehr Transparenz für den genauen Anwendungsbereich der wirtschaftlichen Einheit und bestätigten auch das unionsrechtliche Prinzip der unmittelbaren Verbandshaftung (vgl. dazu auch 29. TB Nr. 10.2). Begrüßenswert ist auch, dass einerseits die vom europäischen Gesetzgeber beabsichtigten abschreckenden hohen Geldbußen gerade gegen große Konzerne weiterhin möglich sind, während andererseits den Besonderheiten von Kleinstunternehmen sowie kleinen und mittleren Unternehmen (KMU) bei der Ermessensausübung hinreichend Rechnung getragen und die Ahndungsempfindlichkeit nicht überreizt wird.

Es liegt nun an den nationalen Datenschutzbehörden, dem EDSA sowie den nationalen und Europäischen Gerichten, die neuen Leitlinien in ihrer jeweiligen Entscheidungspraxis mit Leben zu füllen und eine tatsächliche europaweite Harmonisierung zu erreichen. Es ist zudem ein Lackmustest, ob eine Harmonisierung der Datenschutzdurchsetzung bei nationaler Aufsichtsstruktur gelingen kann.

3.3.7 Leitlinien zu Art. 60 DSGVO

Der EDSA hat im März 2022 die endgültige Fassung der Leitlinien zu Art. 60 Datenschutz-Grundverordnung (DSGVO) angenommen. Die Leitlinien sind Bestandteil der Strategie und des Arbeitsprogramms des EDSA für die Jahre 2021-2023. Sie sollen eine effiziente Zusammenarbeit und schnelle Konsensfindung zwischen den nationalen Aufsichtsbehörden im Kooperationsverfahren unterstützen und damit zu einer wirksameren Durchsetzung der Anforderungen der DSGVO beitragen. Ich habe bei der Erarbeitung dieser Leitlinien als Hauptberichterstatter fungiert.

Als eine der wichtigsten Neuerungen wurde mit der DSGVO der sog. One-Stop-Shop-Mechanismus eingeführt. Dieser Mechanismus besagt, dass bei Fällen mit grenzüberschreitender Datenverarbeitung die Aufsichtsbehörde des Mitgliedstaats für die Durchsetzung der DSGVO federführend ist, in dem die Hauptniederlassung des Verantwortlichen oder Auftragsverarbeiters liegt. Die DSGVO sieht zugleich vor, dass betroffene Personen ihre Beschwerden immer auch bei einer Aufsichtsbehörde an ihrem gewöhnlichen Aufenthaltsort einreichen können. Diese Aufsichtsbehörde ist auch im weiteren Verlauf des Beschwerdeverfahrens Ansprechpartner für die Beschwerdeführer. Um diese parallelen Anforderungen zu erfüllen, wird mit Art. 60 DSGVO das Kooperationsverfahren zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden geregelt.

Die Leitlinien zu Art. 60 DSGVO beziehen sich u. a. auf die Interaktionen der Aufsichtsbehörden in diesem One-Stop-Shop-Mechanismus untereinander und auf die Kooperation mit dem EDSA selbst. Hierfür treffen die Leitlinien folgende Kernaussagen:

- Das Kooperationsverfahren gilt grundsätzlich für jeden Fall der grenzüberschreitenden Verarbeitung.
- Die federführende Aufsichtsbehörde ist in erster Linie für die Bearbeitung solcher Fälle zuständig, aber letztlich nicht befugt, alleine zu entscheiden.
- Das Kooperationsverfahren wirkt sich nicht auf die Unabhängigkeit der Aufsichtsbehörden aus. Viel-

18 Leitlinien zur Berechnung der Bußgelder, abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

mehr behalten diese im Rahmen der Zusammenarbeit ihren eigenen Ermessensspielraum.

→ Die beteiligten Aufsichtsbehörden tauschen frühzeitig alle relevanten Informationen untereinander aus, um einen Konsens zu erzielen (Nr. 3.3.2)[19].

Eine den Leitlinien als Anhang beigefügte Kurzanleitung soll den Mitarbeiterinnen und Mitarbeitern in den Aufsichtsbehörden einen schnellen Überblick über das Verfahren geben und das komplexe Verfahren veranschaulichen.

Querverweise:

3.3.2 Umsetzung der EDSA-Stratgie 2021-2023

3.3.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Corporate Rules

Die verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules, BCR) sind eine geeignete Garantie des Kapitels V der Datenschutz-Grundverordnung (Art. 47 DSGVO) für die Übermittlung personenbezogener Daten von der EU an Drittländer innerhalb einer Unternehmensgruppe (vgl. 30. TB Nr. 3.2.2.2). Im vergangenen Jahr hat der EDSA Stellungnahmen zu einer Vielzahl von BCR abgegeben, auf deren Basis diese BCR von den nationalen Aufsichtsbehörden genehmigt wurden. Darüber hinaus hat sich die EDSA-Expert Subgroup International Transfers (ITS ESG) mit der Weiterentwicklung des BCR-Annahmeverfahrens des EDSA im Hinblick auf dessen Effizienz (Qualitätssicherung, Beschleunigung, Vereinfachung) befasst.

In der ITS ESG, in der das BCR-Verfahren im Hinblick auf spezifische und allgemeine Fragestellungen behandelt wird, bin ich gemeinsam mit Vertretern der Aufsichtsbehörden der Länder vertreten. Im Berichtsjahr sind insbesondere die Arbeiten an den *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 DSGVO)*[20] – im Folgenden: BCR-C Referentials – zur Überarbeitung der Working Paper WP 256 rev.01[21] und des dazugehörigen Antragsformulars WP 264[22] des EDSA hervorzuheben.

Inhaltlich wurden die BCR-C Referentials auf Grundlage der neuen Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Drittländer[23] an die Anforderungen des Schrems II-Urteils des EuGH[24] angepasst. Außerdem wurden Ergebnisse bzw. Vereinbarungen berücksichtigt, die sich im Rahmen der Prüfung konkreter BCR-Anwendungen seit Inkrafttreten der DSGVO gezeigt haben. Die Beschreibung der erforderlichen BCR-Elemente wurde entsprechend präzisiert, um sowohl die Antragstellung als auch die Arbeit der prüfenden Aufsichtsbehörden zu erleichtern. Die Ergebnisse wurden vom 71. Plenum des EDSA im November 2022 angenommen. Die Überarbeitung der sogenannten „BCR-P Referentials" für Auftragsverarbeiter (WP 257 rev.01[25] und des dazugehörigen Antragsformulars WP 265[26]) werden folgen.

Darüber hinaus wurden die Vorlagen (Templates) für die Stellungnahme des EDSA und die nationale Genehmigungsentscheidung der Aufsichtsbehörden angepasst, um die Folgen des Schrems II Urteils zu berücksichtigen sowie den Umfang einer BCR-Genehmigung, auch im Hinblick auf die vorgenannten Änderungen in den „BCR-C Referentials" zu erläutern.

3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield Nachfolge)

Der EuGH hatte mit dem Schrems II Urteil (Rechtssache C-311/18[27]) den US- Angemessenheitsbeschluss, das sogenannte „Privacy Shield", für ungültig erklärt. Am Maßstab der sich aus dem EuGH Urteil ergebenden Anforderungen verhandelten daraufhin die Europäische Kommission und die US-Regierung zu einer

19 Die Verbesserung einer informellen Zusammenarbeit ist auch Teil der im April 2022 in Wien gefundenen Absprache zu einer Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes auf europäischer Ebene: https://edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf

20 BCR-C Recommendations, 1/2022, abrufbar unter: https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplicationform_en.pdf

21 WP 256 rev.01, abrufbar unter: https://ec.europa.eu/newsroom/article29/items/614109/en

22 Standard application form (WP 264), abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/recommendation-standard-application-form-approval-controller-binding_en

23 Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer, abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de

24 „Schrems II" Urteil des EuGH vom 16.07.2020, Rechtssache C-311/18, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

25 WP 257 rev.01, abrufbar unter: https://ec.europa.eu/newsroom/article29/items/614110/en

26 Standard application form (WP 265), abrufbar unter: https://ec.europa.eu/newsroom/article29/items/623848/en

27 Schrems II" Urteil des EuGH vom 16.07.2020, Rechtssache C-311/18, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

Nachfolgeregelung. Nach Bekanntgabe der grundsätzlichen Einigung beider Seiten im März 2022 folgte mit der am 7. Oktober 2022 veröffentlichten Executive Order 14086 on *'Enhancing Safeguards for United States Signals Intelligence Activities'*[28] ein weiterer Schritt in Richtung Privacy Shield Nachfolge, dem EU-U.S. Data Privacy Framework (EU-U.S. DPF). Und schließlich mit der Veröffentlichung des Entwurfs des Angemessenheitsbeschlusses zum EU-U.S. DPF, der Start des Annahmeverfahrens und die Aufforderung an den EDSA, eine Stellungnahme abzugeben. Daran werde ich mich intensiv beteiligen.

Hintergrund – Schrems II Urteil des EuGHs:

Mit dem Schrems II Urteil hatte der EuGH (a. a. O.) die Anforderungen an die Übermittlung von personenbezogenen Daten an die USA erneut klargestellt und präzisiert. Da durch das Urteil der Angemessenheitsbeschluss der EU für die USA für nichtig erklärt wurde, konnten auf dieser Grundlage keine personenbezogenen Daten mehr an die USA übermittelt werden. Außerdem enthält das Urteil die Feststellung, dass Standarddatenschutzklauseln gegebenenfalls um zusätzliche Maßnahmen *(supplementary measures)* zu ergänzen sind, damit die Daten im Drittland einen gleichwertigen Schutz genießen wie in der EU. Stehen keine geeigneten Maßnahmen zur Verfügung, ist eine Übermittlung personenbezogener Daten rechtswidrig. Begründet hat der EuGH das fehlende Schutzniveau in den USA insbesondere damit, dass die Rechtsvorschriften, auf deren Grundlage amerikanische Sicherheitsbehörden auf die an die USA übermittelten personenbezogenen Daten zugreifen könnten, unverhältnismäßig seien und damit gegen Art. 52 Abs. 1 Satz der EU- Grundrechtecharta (Schrems II Urteil, a. a. O., Rn. 184 f.) verstießen. Zum anderen bestehe kein wirksamer Rechtsschutz gegen die Zugriffe durch die amerikanischen Sicherheitsbehörden, der den Anforderungen des Art. 47 der EU-Grundrechtecharta genüge (Schrems II Urteil, a. a. O. Rn. 199).

Die erheblichen Auswirkungen des Urteils auf Datenübermittlungen – nicht nur an die USA, sondern an Drittländer grundsätzlich – sowie das Prüferfordernis einer Implementierung „zusätzlicher Maßnahmen", nicht nur im Hinblick auf die Standarddatenschutzklauseln, sondern auch bezüglich sonstiger Übermittlungsinstrumente (geeignete Garantien) im Sinne des Art. 46 DSGVO - stellen Verantwortliche, Auftragsverarbeiter und auch Aufsichtsbehörden seitdem vor große Herausforderungen. Der EDSA hatte zeitnah nach dem Urteil, das keine nähere Erläuterung zum Begriff „zusätzliche Maßnahmen" enthielt, diesbezüglich die Empfehlungen 01/2020[29] veröffentlicht, welche Beispiele für potentiell effektive technische, organisatorische oder vertragliche Maßnahmen zur Absicherung einer Datenübermittlung enthalten. Zu beachten ist aber, dass die Datenexporteure (explizit hervorgehoben durch den EuGH) die Verantwortung haben, für jede Datenübermittlung das Schutzniveau im Drittland zu prüfen (Schrems II Urteil, a. a. O., Rn. 134) und gegebenenfalls „zusätzliche Maßnahmen" für den Schutz der an ein Drittland übermittelten Daten vorzusehen (a. a. O., Rn. 131).

Vor diesem Hintergrund und um Rechtssicherheit zu erreichen, ist es wichtig, dass Datenübermittlungen an die USA auf eine neue, beständige rechtliche Grundlage gestellt werden. Dieses Ziel war allerdings nicht ohne Änderungen im US-Recht zu erreichen.

Entwicklungen zum EU-U.S. DPF:

In einer gemeinsamen Erklärung vom 25. März 2022 gaben EU-Kommissionspräsidentin von der Leyen und US-Präsident Biden bekannt, dass eine grundsätzliche Einigung über einen neuen EU-US-Datenschutzrahmen (EU-U.S. DPF) erzielt wurde[30]. Damit soll nun die Nachfolge für das vom EuGH in seinem Schrems II-Urteil für ungültig erklärte Privacy Shield geschaffen werden.

Eine erste wesentliche Regelung für eine Privacy Shield-Nachfolge erfolgte am 7. Oktober 2022 mit der von Präsident Biden unterzeichneten *Executive Order 14086 on 'Enhancing Safeguards for United States Signals Intelligence Activities'*[31]. Zusammen mit der vom *Attorney General (Justizminister)* erlassenen Verordnung zum sogenannten *Data Protection Review Court (DPRC)*[32] gestaltet die *Executive Order* nun die im März angekündigte Grundsatzvereinbarung aus. Zweck der Executive Order ist die Einführung von Schutzmaßnahmen, die die vom EuGH als rechtlich unzureichend bewerteten Punkte berücksichtigen und ausräumen sollen. Die Änderungen betreffen insbesondere die verhältnismäßige Beschränkung des Zugangs von US-Nachrichtendiensten auf Daten von Nicht-US-Bürgern, die stärkere interne Kontrolle des Datenschutzes innerhalb der Nachrichten-

28 Executive Order 14086, abrufbar unter: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/
29 EDSA Empfehlungen 1/2020, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
30 Gemeinsame Erklärung EU KOM/ USA, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087
31 Für den Link zur Executive Order, s. Fußnote 28
32 Verordnung zum DPRC, abrufbar unter: https://www.justice.gov/opcl/redress-data-protection-review-court

dienste sowie die Einrichtung eines Beschwerdemechanismus für Nicht-US-Bürger.

Die Executive Order und die Verordnungen des Justizministeriums für den DPRC werden ergänzt durch Regelungen des *Department of Commerce* im Hinblick auf die vom EU-U.S. DPF umfasste Datenschutz-Zertifizierung für Unternehmen, welche Voraussetzung dafür ist, Datentransfers von der EU in die USA auf Basis des angestrebtem EU-US-Angemessenheitsbeschlusses vornehmen zu können.

Weiteres Verfahren/Ausblick:

Die Europäische Kommission hat nun auf dieser Grundlage einen Entwurf für einen Angemessenheitsbeschluss erstellt und das Verfahren für dessen Annahme am 13. Dezember 2022 eingeleitet[33]. Hierzu gehört verpflichtend die Einholung einer – nicht bindenden – Stellungnahme des EDSA. Im Rahmen der Stellungnahme werden sich nun die europäischen Datenschutzaufsichtsbehörden ausführlich mit dem Entwurf für den neuen Angemessenheitsbeschluss auseinandersetzen. Ich werde mich intensiv in diese Arbeiten einbringen und gemeinsam mit den europäischen Kolleginnen und Kollegen insbesondere überprüfen, ob die Maßgaben des EuGHs aus dem Schrems II-Urteil durch die Änderungen im US-Recht effektiv umgesetzt wurden und auch die sonstigen datenschutzrechtlichen Anforderungen erfüllt sind.

Im Verfahren kann zudem das Europäische Parlament eine Entschließung zum Angemessenheitsbeschluss annehmen und schließlich muss der Ausschuss der ständigen Vertreter der EU-Mitgliedstaaten gem. Art. 5 der Verordnung (EU) Nr. 182/2011 (Komitologie-Verordnung) den Beschlussentwurf bestätigen. Sofern die vorgenannten Verfahrensschritte erfolgreich abgeschlossen werden können, wird die Europäische Kommission den Beschluss im Amtsblatt der Europäischen Union veröffentlichen. Anschließend können sich Unternehmen im Rahmen des EU-U.S. DPF zertifizieren.

Datenübermittlungen aus der EU in die USA könnten sodann auf Basis des Angemessenheitsbeschlusses ohne weitere Maßnahmen erfolgen.

3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers

Die Datenschutz-Grundverordnung (DSGVO) sieht vor, dass personenbezogene Daten in Drittländer ohne einen Angemessenheitsbeschluss nur dann übermittelt werden dürfen, wenn hierfür geeignete Garantien vorgesehen sind. Diese Garantien können beispielsweise in genehmigten Verhaltensregeln oder Zertifizierungsmechanismen als Transferinstrumente für Drittstaatentransfers bestehen. Hierzu hat der Europäische Datenschutzausschuss (EDSA auf Basis der Vorarbeiten der Expert Subgroup International Transfers (ITS ESG) im Berichtsjahr zwei entsprechende Leitlinien angenommen.

Zum einen handelt es sich um die Leitlinien für Zertifizierungen (Guidelines 07/2022 on certification as tool for transfers)[34] und zum anderen um die für genehmigte Verhaltensregeln (Guidelines 04/2021 on codes of conduct as tools for transfers)[35]. Bei der Ersteren war ich Hauptberichterstatter und bei der Letzteren Co-Berichterstatter. Die Leitlinien dienen zum einen als Orientierung für die Erarbeitung von Zertifizierungen oder Verhaltensregeln und legen zum anderen auch die Rahmenbedingungen für die Datenschutzaufsichtsbehörden fest, die die Instrumente genehmigen. Zudem ergänzen sie im Falle von Zertifizierungen bestehende Leitlinien zur nationalen Zertifizierung und Akkreditierung für Datentransfers in Drittstaaten.

Die Besonderheit der beiden Transferinstrumente liegt in ihrer Natur als Selbstregulierungsmechanismen. Unternehmen und Organisationen, die sich zertifizieren lassen oder den genehmigten Verhaltensregeln beitreten, müssen dauerhaft den vorgegebenen Anforderungen entsprechen. Im Gegenzug dürfen diese Verantwortlichen die Transferinstrumente heranziehen, um Ihrer Rechenschaftspflicht (Einhaltung der DSGVO) nachzukommen. Die Einhaltung der vorgegebenen Anforderungen werden in erster Linie von einer Zertifizierungsstelle (Certification body) oder einer Überwachungsstelle (Monitoring body) überwacht. Zudem verbleiben in zweiter Linie Möglichkeiten der Kontrolle und der Sanktion bei den Aufsichtsbehörden.

33 PM der EU KOM und Veröffentlichung des Entwurfs des Angemessenheitsbeschlusses zum EU-U.S. DPF, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_7631

34 Guidelines 07/2022 on certification as tool for transfers , abrufbar unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en

35 Guidelines 04/2021on codes of conduct as tools for transfers , abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en

Damit hat der EDSA jetzt zu allen Transferinstrumenten („geeignete Garantien“ im Sinne des Art. 46 DSGVO) veröffentlicht.[36]

Querverweise:

3.1 Übersicht Gremienarbeit, 3.3.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Corporate Rules, 3.4 G7 Roundtable

3.4 G7 Roundtable

Anlässlich der diesjährigen deutschen G7-Präsidentschaft fand unter meinem Vorsitz die zweite Ausgabe des Roundtable der Datenschutzaufsichtsbehörden der G7-Staaten statt. Hauptthema war „Data Free Flow with Trust“, also die Frage vertrauenswürdiger internationaler Datenübermittlungen. In dem verabschiedeten Communiqué betonen die G7-Datenschutzaufsichtsbehörden die Bedeutung der Einhaltung demokratischer Werte und Rechtsstaatlichkeitsstandards. Das G7 Roundtable-Treffen soll als ständiges Format auch in den kommenden Jahren fortgeführt werden.

In 2021 initiierte die britische G7-Präsidentschaft erstmalig ein Treffen der Datenschutzaufsichtsbehörden der G7-Staaten (G7 Data Protection Authorities, G7 DPA), das sich mit dem wichtigen Themenkomplex freier und vertrauenswürdiger globaler Datenflüsse (Data Free Flow with Trust, DFFT) befasste (vgl. 30. TB Nr. 3.4.1). Im 2022 hatte Deutschland die Präsidentschaft der G7 übernommen. Besonders begrüßt habe ich, dass DFFT auch unter deutschem Vorsitz ein Schwerpunktthema blieb. So haben die G7-Digitalministerinnen und Digitalminister in ihrer Erklärung[37] die Bedeutung demokratischer Werte für DFFT unterstrichen und einen G7-Aktionsplan zur Förderung von DFFT[38] beschlossen. Dieser Aktionsplan wird in der Erklärung der G7-Staats- und Regierungschefs[39] explizit unterstützt und sieht auch die Fortführung der Roundtable-Treffen (G7 DPA Roundtable) vor.

Mir war es eine große Ehre, den G7 DPA Roundtable 2022 ausrichten zu dürfen. Für das erste physische Treffen dieses Formates habe ich die Datenschutzbeauftragten der G7-Staaten, die Vorsitzende des Europäischen Datenschutzausschusses und den Europäischen Datenschutzbeauftragten im September 2022 nach Bonn eingeladen.

Zum G7 Leaders’ Communiqué 2022 geht’s hier:

(QR-Code scannen oder klicken)

Als Gäste teilgenommen haben zudem der Präsident des Bundeskartellamts sowie Vertreterinnen und Vertreter der OECD und der Zivilgesellschaft. Dieser Roundtable fokussierte sich beim Hauptthema DFFT auf einen Erfahrungs- und Wissensaustausch im Hinblick auf mögliche Perspektiven zu internationalen Datenräumen. Das hierzu verabschiedete Communiqué 2022[40] betont, dass zur Förderung von DFFT insbesondere die Einhaltung demokratischer Werte und Rechtsstaatlichkeitsstandards gehören. Damit einher geht die Beschränkung des staatlichen Zugriffs auf privat gespeicherte Daten auf das in demokratischen Gesellschaften notwendige und verhältnismäßige Maß. Im Mittelpunkt der Diskussionen zu DFFT stand, Elemente der Angleichung zwischen bestehenden Regulierungsansätzen und Transferinstrumenten (wie z. B. Standardvertragsklauseln, Zertifizierungen und Verhaltensregeln) zu ermitteln, um die Interoperabilität verschiedener Rechtssysteme und -Instrumente zu fördern. Besonders hervorzuheben sind ebenfalls die Arbeiten zur Datenminimierung und Zweckbindung, zwei Grundprinzipien der DSGVO, die auch für die Datenschutzaufsichtsbehörden aus dem Vereinigten Königreich, USA, Kanada und Japan eine wichtige Rolle spielen. Die konsequente Durchsetzung dieser Grundsätze ist entscheidend, um datenbasierte Geschäftsmodelle im Einklang mit den berechtigten Erwartungen der Verbraucherinnen und Verbrauchern zu bringen. Es sollen nur die personenbezogenen Daten erhoben werden, die für die Nutzung des jeweiligen Dienstes erforderlich sind. Weitere wichtige Themen des Austausches waren die Förderung von datenschutzfreundlichen Technologien (Privacy-Enhancing Technologies), rechtliche und technische Standards für De-Identifikationsinstrumente (de-identification tools) und die Rolle des Datenschutzes bei einem ethischen Umgang mit Künstlicher Intelligenz.

Obwohl die Treffen 2021 und 2022 jeweils Teil des offiziellen G7-Digital-Tracks waren, handelt es sich dabei um ein eigenständiges Format von unabhängigen Daten-

36 Leitlinien zum Datentransfer, abrufbar unter: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en
37 Die “Ministerial Declaration G7 Digital Ministers‘ meeting” ist abrufbar unter: https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration.pdf
38 Der “G7 Digital Ministers‘ Track - Annex 1 G7 Action Plan for Promoting Data Free Flow with Trust” ist abrufbar unter: https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf
39 Das „G7 Leaders’ Communiqué Elmau, 28 June 2022“ ist abrufbar unter: https://www.g7germany.de/resource/blob/974430/2062292/9c213e6b4b36ed1bd687e82480040399/2022-07-14-leaders-communique-data.pdf?download=1
40 Das Communiqué 2022 ist abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.html

schutzaufsichtsbehörden. Es ist wichtig, dass sie an den Diskussionen über den freien Datenverkehr beteiligt sind. Deswegen haben die Datenschutzaufsichtsbehörden der G7-Staaten ihre Regierungen in dem Communiqué 2022 ermutigt, dafür zu sorgen, dass der Dialog zwischen politischen Entscheidungsträgern und Regulierungsbehörden zu einem integralen Bestandteil der digitalen Agenda der G7 wird, wenn Datenschutzthemen betroffen sind. Unbeschadet dessen wurde vereinbart, die jährlichen hochrangigen Treffen auch unabhängig davon fortzuführen, ob diese offizieller Programmpunkt der jeweiligen G7-Präsidentschaft sind oder nicht. Darüber hinaus ist auch ein unterjähriger Austausch auf Expertinnen- und Expertenebene in drei neuen Arbeitsgruppen vorgesehen zu den Themen künftige Technologien (Emerging Technologies), Zusammenarbeit bei der Durchsetzung (Enforcement Cooperation) und freie und vertrauenswürdige Datenflüsse (DFFT). Die Arbeitsgruppen bereiten den kommenden Roundtable der G7-Datenschutzbehörden vor, der im Jahr 2023 unter japanischem Vorsitz stattfinden wird.

Querverweise:

3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield Nachfolge), 3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers, 3.5.1 44. Jahreskonferenz der Global Privacy Assembly 2022

3.5 Weitere internationale Gremien

3.5.1 Jahreskonferenz der Global Privacy Assembly 2022

Erstmals seit 2019 konnten sich Vertreterinnen und Vertreter der Datenschutzbehörden aus aller Welt wieder zu ihrer jährlichen Konferenz in Präsenz treffen. Die türkische Datenschutzbehörde hatte zur 44. Jahreskonferenz der Global Privacy Assembly (GPA) nach Istanbul eingeladen. Dabei wurden Grundsatzfragen zu internationalen Datentransfers und zu neuen Technologien besprochen. Für mich begann im Herbst 2022 meine zweite Amtszeit im Leitungsgremium „Executive Committee" der GPA.

Nach zwei virtuellen Treffen in den Jahren 2020 und 2021 wurde die 44. Jahreskonferenz der GPA von der türkischen Datenschutzbehörde „Kişisel Verileri Koruma Kurumu" (KVKK) vom 25. bis 28. Oktober 2022 in Istanbul ausgerichtet. Mehrere hundert Teilnehmende versammelten sich dabei unter dem Motto „A Matter of Balance. Privacy in The Era of Rapid Technological Advancement" (Datenschutz im Zeitalter des rasanten technologischen Fortschritts). Als neue Mitglieder wurden unter anderem die kenianische Datenschutzbehörde und die auf Ebene des Bundesstaates Kalifornien in den USA als erste dezidierte Datenschutzbehörde eingerichtete „California Privacy Protection Agency" (CPPA) aufgenommen. Begleitet von einer Fachdelegation habe ich an der Konferenz teilgenommen und mich in verschiedenen Formaten eingebracht.

Die Hauptvorträge und Diskussionsrunden in der für alle Teilnehmer offenen Sitzung konzentrierten sich auf die fortschreitenden technologischen Entwicklungen im Bereich der Gesichtserkennung, der Künstlichen Intelligenz und der Blockchain-Technologie sowie damit verbundene Herausforderungen für den Datenschutz. Weitere Schwerpunkte waren Fragen zu grenzüberschreitenden Datentransfers und Datenschutzrisiken im Bereich der humanitären Hilfe sowie bei schutzbedürftigen Gruppen wie z. B. Kinder und Minderjährige. Zusammen mit der Vorsitzenden der französischen Datenschutzbehörde „Commission National de L´Informatique et Libertes" (CNIL), Marie-Laure Denis, hielt ich eine Grundsatzrede zum Thema „Konvergenz der Datenschutzbestimmungen bei grenzüberschreitenden Datenübermittlungen". Mehrere meiner Kolleginnen und Kollegen aus dem Europäischen Datenschutzausschuss (EDSA) nahmen an verschiedenen Vorträgen und Diskussionsrunden teil und brachten die Positionen der Datenschutz-Grundverordnung (DSGVO) zum Ausdruck. In der geschlossenen Sitzung der Konferenz, zu der nur die akkreditierten Mitglieder und Beobachter der GPA zugelassen sind, berichteten die Arbeitsgruppen, der Unterausschuss für die strategische Ausrichtung und verschiedene GPA-Mitglieder und -Beobachter über bedeutende Ergebnisse und Tätigkeiten seit der letzten Jahreskonferenz im Herbst 2021. In diesem Zusammenhang konnte ich über die Arbeiten der „International Working Group on Data Protection in Technology" (IWGDPT) berichten, die auch unter der Bezeichnung „Berlin Group" bekannt ist (Nr. 3.5.2).

Darüber hinaus haben die Mitglieder der GPA folgende Entschließungen[41] angenommen:

- Entschließung zur Änderung des Fahrplans und des Zeitplans für die Einrichtung eines durch die Mitglieder finanzierten Sekretariats,
- Entschließung zum Aufbau von Kapazitäten für die internationale Zusammenarbeit zur Verbesserung der Regulierung der Cybersicherheit und zum

41 Entschließung vom 28. Oktober 2022, abrufbar unter: https://www.bfdi.bund.de/gpa

Verständnis der durch Cybervorfälle verursachten Schäden,

→ Entschließung zu den Grundsätzen und Erwartungen für die angemessene Verwendung personenbezogener Daten in der Gesichtserkennungstechnologie.

In organisatorischer Hinsicht ergab sich eine neue Zusammensetzung des Leitungsgremiums der GPA, dem „Executive Committee". Als neues Mitglied wurde der Jersey Information Commissioner, Paul Vane, gewählt. Ich selbst wurde für eine zweite Amtszeit bis Herbst 2024 als Mitglied des Executive Committee bestätigt. Die nächste Jahreskonferenz der GPA wird vom Bermuda Privacy Commissioner im Oktober 2023 ausgerichtet werden.

Querverweise:

3.5.2 Berlin Group, 4.4.3 EDSA-Richtlinien zum Einsatz von Gesichtserkennungstechnologie

3.5.2 Berlin Group

Nachdem ich im vergangenen Jahr den Vorsitz der internationalen Arbeitsgruppe zu Datenschutz in der Technik „International Working Group Data Protection in Technology" (IWGDPT) dauerhaft übernommen habe, konnte die sogenannte „Berlin Group" dieses Jahr wieder in Präsenz tagen und neue Mitglieder gewinnen.

Im März 2021 habe ich von der Berliner Beauftragten für den Datenschutz und die Informationsfreiheit den Vorsitz der internationalen Arbeitsgruppe zu Datenschutz in der Technik, „International Working Group Data Protection in Technology" (IWGDPT), übernommen (vgl. 30. TB, Nr. 3.4.2). Die IWGDPT, wegen ihrer Geschichte auch „Berlin Group" genannt, ist eine internationale Gruppe von Datenschutz-Aufsichtsbehörden, Nichtregierungsorganisationen, Expertinnen und Experten aus den Bereichen Wissenschaft und Forschung sowie Think Tanks.

Nachdem die Arbeit der Berlin Group im Jahr 2021 noch von den Einschränkungen der Corona-Pandemie gekennzeichnet war, konnte die Gruppe im Jahr 2022 unter meiner Leitung in Tel Aviv und London zu ihrem gewohnten Turnus von zwei Treffen pro Jahr zurückkehren. Nachdem 2021 die Themen intelligente Stadt („Smart Cities") sowie Gesichtserkennungstechnologie ins Blickfeld genommen wurden, hat die Gruppe dieses Jahr die entsprechenden Arbeitspapiere finalisiert. Des Weiteren wurden die Themen Telemetriedaten und digitales Zentralbankgeld neu aufgegriffen, zu denen im kommenden Jahr Arbeitspapiere verabschiedet werden sollen.

Um die Empfehlungen der Berlin Group an Unternehmen, Gesetzgeber, Datenschutzbehörden und andere Stakeholder noch frühzeitiger zu geben, wird sich die Gruppe verstärkt damit befassen, welche Technologien und Anwendungsfelder kurz vor Markteintritt stehen und dazu Papiere verfassen. Zur Vorbereitung wurden die entsprechenden Arbeiten der Mitglieder („future foresight", „tech radar") vorgestellt und diskutiert.

Neben der inhaltlichen Arbeit an den genannten Arbeitspapieren konnte ich im Jahr 2022 in Gesprächen mit internationalen Datenschutz-Aufsichtsbehörden und Interessengruppen neue teilnehmende Organisationen für die Mitarbeit in der Berlin Group gewinnen, z. B. die UN-Sonderberichterstatterin zum Recht auf den Schutz der Privatsphäre. Mein Ziel ist es, die Diversität der Gruppe und die Intensität des Dialogs weiter zu steigern sowie ihre Expertise und Arbeitsergebnisse sichtbarer zu machen.

3.5.3 Neues ETIAS-Beratungsgremium für Grundrechte

Zur Kontrolle der sog. ETIAS-Überwachungsregeln ist das unabhängige ETIAS-Beratungsgremium für Grundrechte neu eingesetzt worden. In diesem Gremium vertritt auch einer meiner Mitarbeitenden den EDSA.

Das neue Europäische Reiseinformations- und -genehmigungssystem (ETIAS) soll im Jahr 2023 in Betrieb gehen und betrifft Drittstaatsangehörige, die in die EU einreisen möchten und von der Visumspflicht befreit sind. Mit dem System soll überprüft werden, ob die Anwesenheit dieser Personen ein Risiko für die Sicherheit in der EU, ein Risiko der illegalen Einwanderung oder ein hohes Epidemierisiko bedeutet. Ein Mittel, mit dem diese Prüfung erfolgen soll, sind die sog. ETIAS-Überwachungsregeln, einem Profiling-Algorithmus, der auf spezifischen Risikoindikatoren beruht. Besonders mit Blick auf die Definition und Anwendung dieser Risikoindikatoren ist ein unabhängiges ETIAS-Beratungsgremium für Grundrechte geschaffen worden. Es besteht aus dem Grundrechtsbeauftragten und einem Vertreter des Konsultationsforums für Grundrechte der Europäischen Agentur für die Grenz- und Küstenwache Frontex sowie des Europäischen Datenschutzbeauftragten, der Agentur der Europäischen Union für Grundrechte und des EDSA. Ich freue mich, dass der EDSA einen meiner Beschäftigten als Vertreter bestimmt hat und dieser darüber hinaus zum Vorsitzenden des ETIAS-Beratungsgremiums für Grundrechte gewählt wurde. Auf diese Weise ist es mir möglich, aktiv auf die Achtung der Grundrechte, insbesondere den Schutz der Privatsphäre und personenbezogener Daten, sowie auf die Nichtdiskriminierung hinwirken zu können.

Querverweise:

3.3.4 EU-Systeme: Zentrale Koordinierung der Aufsicht im CSC

3.5.4 Bericht aus den SCGs

Im Rahmen der unterschiedlichen Supervision Coordination Groups (SCGs) arbeiten die europäischen Datenschutzbehörden und der Europäische Datenschutzbeauftragte (EDSB) zusammen, um die datenschutzrechtliche Aufsicht über die IT-Großsysteme der EU zu koordinieren. Schwerpunkte in diesem Jahr waren die Koordinierung der Kontrollen, die geplante Digitalisierung des Visa-Verfahrens, die Interoperabilität der verschiedenen EU-Systeme, die Implementierung der neuen Schengen-Rechtsakte und die Überarbeitung des Mechanismus der Schengen-Evaluierungen.

VIS/Eurodac SCG

Im Mittelpunkt der aktuellen Diskussionen standen die weitreichenden Änderungen der VIS-Verordnung und des Visa-Informationssystems. Durch rechtliche Änderungen wurden in erheblichem Maße Möglichkeiten geschaffen, VIS-Daten mit anderen Systemen automatisiert abzugleichen. Der Kreis der potentiell zugriffsberechtigten Behörden wurde damit erweitert. Die Vertreter der Datenschutzbehörden waren sich einig, dass man die gesamte Architektur der Informationssysteme unter Datenschutzaspekten analysieren muss, um Gefahren für die betroffenen Personen, die sich aus der Interoperabilität der verscheiden Systeme ergeben, zu begegnen. Daneben wurden mit Vertretern der EU-Kommission die datenschutzrechtlichen Implikationen der geplanten Digitalisierung des Visa-Verfahrens diskutiert. Die Beratungen hierzu dauern noch an.

Visa-Informationssystem

Das Visa-Informationssystem (VIS) ist ein System für den Austausch von Visa-Daten zwischen den Schengen-Staaten im Zusammenhang mit der Beantragung, Prüfung und Entscheidung im Hinblick auf Visa für den kurzfristigen Aufenthalt im Schengen-Raum.

Eurodac-Verordnung

Eurodac (European Dactyloscopy) ist eine Datenbank für Fingerabdrücke von Asylbewerbern und in der EU aufgegriffenen illegalen Einwanderern, die die effektive Anwendung des Dubliner Übereinkommens über die Bearbeitung von Asylanträgen gewährleiten soll.

Bezüglich der geplanten Änderung der Eurodac-Verordnung und der damit verbundenen Datenschutzrisiken (z. B. Absenkung des Alters zur verpflichtenden Abnahme von Fingerabdrücken von 14 auf 6 Jahre) verabschiedete die Gruppe einen Brief an das Europäische Parlament, um dieses entsprechend zu sensibilisieren. Darin wurde insbesondere kritisiert, dass die Notwendigkeit und Verhältnismäßigkeit der Herabsenkung des Alters nicht ausreichend begründet wurden. Außerdem begrüßte die Gruppe zwar die Bestimmungen zur „kindgerechten Anhörung“, sah jedoch einen Mangel an Kriterien für diese Formulierung.

SIS II SCG

In der SIS II SCG befasse ich mich mit der koordinierten Aufsicht über das Schengener Informationssystem der zweiten Generation (SIS II). Neben den Kontrollen zu Artikel 36-Ausschreibungen im SIS war ein Arbeitsschwerpunkt dieser SCG die Umsetzung der neuen SIS-Verordnungen (EU) 2018/1860, 2018/1861 und 2018/1862. Hierzu habe ich mich zudem auf nationaler Ebene im Rahmen der Ressortabstimmungen zum Gesetz zur Durchführung dieser Verordnungen (SIS-III-Gesetz) intensiv beteiligt. Mit diesen Verordnungen werden im SIS neue Ausschreibungskategorien geschaffen und die Datenerhebung bei bestehenden Ausschreibungskategorien teilweise erweitert, zudem erhalten mehr Behörden Zugriff auf Daten im SIS. Die rechtlichen und technischen Entwicklungen wurden dabei fortlaufend von der SIS II SCG in Augenschein genommen. Um auch die Öffentlichkeit ausreichend über wesentliche Änderungen der neuen Rechtsakte zu informieren, wurden beispielsweise Informationskampagnen sowie weitere Informationen zu Betroffenenrechten diskutiert, die sich derzeit in der Umsetzung befinden.

Ein weiterer Schwerpunkt der Arbeit der SCG war die Überarbeitung des Mechanismus der Schengen-Evaluierungen. Bei Schengen-Evaluierungen findet eine Überprüfung der Schengen-Staaten durch Teams statt, die sich aus Experten aus den Mitgliedsstaaten und der Kommission zusammensetzen. Dabei werden nationale Behörden auch im Hinblick auf die Umsetzung des Datenschutzes überprüft. Meine Mitarbeitenden nehmen regelmäßig selbst als Experten an Evaluierungen in anderen Staaten teil, dieses Jahr beispielsweise an den Evaluierungen in Norwegen und Island. Der diesen Evaluierungen zugrundeliegende Mechanismus wurde nun mit der Verordnung (EU) 2022/922 angepasst. Im Vorfeld habe ich mich sowohl auf nationaler als auch auf europäischer Ebene im Rechtsetzungsverfahren eingebracht. Im Rahmen der SIS II SCG wurde beispielsweise ein Schreiben an die am Gesetzgebungsverfahren beteiligten europäischen Stellen erarbeitet, um auf relevante datenschutzrechtliche Aspekte bei der Umsetzung aufmerksam zu machen. Aus meiner Sicht wichtige Punkte wurden dabei rechtlich verankert bzw. sind in Aussicht gestellt worden, wie z. B. spezielle Trainings für die Experten.

CIS SCG

In dieser Koordinierungsgruppe befasse ich mich mit der koordinierten Überwachung des Zollinformationssystems (CIS), im Berichtsjahr insbesondere die koordinierte, europaweite Überprüfung des datenschutzrechtlichen Trainings zum CIS durch die an das System angeschlossenen Behörden. Dazu wurde zunächst ein Fragebogen in der SCG entwickelt, welcher über die nationalen Datenschutzbehörden zur Beantwortung an die verantwortlichen Stellen verteilt wurde. Bei meiner diesbezüglichen Überprüfung des Zollkriminalamts habe ich keine Hinweise vorgefunden, dass Defizite beim datenschutzrechtlichen Training bestehen. Die gesammelten nationalen Antworten zu dem Fragebogen werden derzeit auf europäischer Ebene ausgewertet.

Querverweise:

9.2.8. Koordinierte Kontrollen zu Ausschreibungen zur verdeckten/gezielten Kontrolle im Schengener Informationssystem

4 Schwerpunktthemen

4.1 Forschungsdaten

Forschung ist die Grundlage gesellschaftlichen Fortschritts. Immer häufiger benötigt Forschung dafür große Mengen an Daten, auch personenbezogene Daten. Deshalb ist es richtig, dass die Datenschutz-Grundverordnung der Forschung eine privilegierte Stellung einräumt. Die Corona-Pandemie hat uns teilweise schmerzhaft gezeigt, dass es gerade bei der Forschung mit Gesundheitsdaten in Deutschland noch große Herausforderungen gibt, neben Datenschutzfragen stehen hier mangelnde Erfassung, inkompatible Datenformate und unzureichende digitale Meldewege im Mittelpunkt. Als BfDI war es mir wichtig, dieses Thema zum Schwerpunkt meiner Arbeit im Berichtszeitraum zu machen und mit verschiedenen Initiativen und Veranstaltungen für mehr Verständnis zwischen den beteiligten Akteuren zu werben und aufzuzeigen, wie mehr und grundrechtskonforme Forschung mit personenbezogenen Daten gelingen kann.

4.1.1 Symposium Forschung mit Gesundheitsdaten

Beim BfDI-Symposium 2022 wurde kontrovers und konstruktiv diskutiert. Alle Beteiligten waren sich einig, dass es insbesondere bei der Forschung mit Gesundheitsdaten zukünftig Veränderungen braucht. Die Veranstaltung war so erfolgreich, dass zukünftig weitere Symposien geplant sind.

Am 3. November 2022 trafen sich zahlreiche Akteure zum BfDI-Symposium mit dem Thema „Forschung mit Gesundheitsdaten – Herausforderungen im Zeichen der Datenschutz-Grundverordnung“ im Hörsaal der Kaiserin-Friedrich-Stiftung in Berlin.

Etwa 80 geladene Gäste aus Politik, Wissenschaft & Forschung, Behörden und Unternehmen tauschten sich mit Vertreterinnen und Vertretern des BfDI über den Stand und die Möglichkeiten einer datenschutzkonformen Forschung mit (Gesundheits-)Daten aus. Interessierte Bürgerinnen und Bürger hatten die Möglichkeit, die Veranstaltung parallel auch über einen Stream im Internet zu verfolgen.[42]

Zu der aufgezeichneten BfDI-Veranstaltung geht’s hier:

(QR-Code scannen oder klicken)

Besonders im Vordergrund standen dabei die aktuellen gesetzgeberischen Entwicklungen sowohl in Europa als auch in Deutschland. Die Diskussionen wurden lebhaft, kontrovers und zugleich konstruktiv geführt.

Zu den Entwicklungen in Europa wurde auf sehr anschauliche Weise herausgearbeitet, dass die Europäische Kommission in ihrem aktuell vorgelegten Verordnungsentwurf vom 3. Mai 2022 zu einem Europäischen Gesundheitsdatenraum (EHDS – European Health Data Space) wesentliche Rechtsgrundsätze (beispielsweise Art. 8, 52 Charta der Grundrechte der EU), jedenfalls aus Sicht der Datenschutzaufsichtsbehörden, nicht ausreichend berücksichtigt hat. So wurde beispielsweise darauf hingewiesen, dass der Kreis der zur Datenbereitstellung verpflichteten Stellen und der Kreis der antragsberechtigten Stellen im Verordnungsentwurf jeweils zu weit gefasst wurde. Auch die aktuell vorgesehene ausnahmslose Bereitstellungspflicht und die unzureichende Einräumung von Betroffenenrechten, speziell im Bereich der Sekundärdatennutzung, wurden kritisiert.

Im Verlauf des Symposiums wurde von den Rednern mehrfach betont, dass nicht nur in Europa, sondern auch in Deutschland noch ausreichend Raum für Verbesserungen besteht.

42 Die Aufzeichnung der Veranstaltung ist weiterhin abrufbar unter: https://www.bfdi.bund.de/DE/Service/Mediathek/Veranstaltungen/2022-Symposium-Forschungsdaten/Symposium-Forschungsdaten-2022_mit_iframe.html

Prof. Dr. Specht-Riemschneider während ihres Vortrags beim Symposium zu Forschungsdaten

So ist sicherlich zuzustimmen, wenn – wie im Verlauf des Symposiums gleich mehrfach – von den deutschen Aufsichtsbehörden noch mehr Anstrengungen zu vereinheitlichten Rechtsauffassungen eingefordert werden. Daran arbeiten die Aufsichtsbehörden bereits, beispielsweise in einer gemeinsam vom Hessischen Landesdatenschutzbeauftragten und mir geführten Taskforce.

Es wurde aber auch deutlich, dass bei der eingeforderten einheitlichen Rechtspraxis weniger die Aufsichtsbehörden als vielmehr unmittelbar der Gesetzgeber gefordert ist. Dazu habe ich im Verlauf der Gespräche mehrfach darauf hingewiesen, dass die in den einzelnen Bundesländern sich zum Teil widersprechenden Landeskrankenhausgesetze, ungenutzte Möglichkeiten der nationalen rechtlichen Klarstellung zu den Forschungs-Öffnungsklauseln der Datenschutz-Grundverordnung und letztlich auch eine missglückte Regelung der Datenschutzaufsicht für bundesweite Forschungsprojekte im „falschen“ Gesetzbuch (§ 287a SGB V), hier noch ausreichend Potential für den Gesetzgeber bereithalten.

Es ist geplant, das BfDI-Symposium künftig regelmäßig und zu wechselnden, aktuellen Themen durchzuführen.

Querverweise:

5.1 European Health Data Space

4.1.2 Forschungsdatenzentrum Gesundheit

Das Projekt eines Forschungsdatenzentrums für Gesundheitsdaten aus der elektronischen Patientenakte (ePA) und dem Datentransparenzverfahren schreitet voran und biegt auf die Zielgerade ein.

Über die Entwicklung des Forschungsdatenzentrums Gesundheit, einer Datenbank mit den pseudonymisierten Abrechnungsdaten aller gesetzlich Versicherten, die beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) als Registerstelle geführt wird, habe ich bereits in den letzten Jahren berichtet (30. TB Nr. 6.4). Das Forschungsdatenzentrum Gesundheit erhielt durch Gesetzesänderungen im Digitale-Versorgung-Gesetz aus dem Jahr 2019 und dem Patientendaten-Schutz-Gesetz im Jahr 2020 eine neue Konzeption (28. TB Nr. 5.6 und 29. TB Nr. 7.3).

In diesem Berichtsjahr habe ich das Robert Koch-Institut (RKI) beraten, bei dem die für die Pseudonymisierung der Datensätze zuständige Vertrauensstelle angesiedelt ist. Zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden Einzelheiten des Verfahrens, der kryptographischen Methoden, der Hostingarchitektur sowie den Lieferpseudonymen und des sog. periodenübergreifenden Pseudonyms behandelt, so dass ich schließlich mein Einvernehmen zum Verfahren erteilen konnte.

Das Forschungsdatenzentrum Gesundheit erhält jährlich die Abrechnungsdaten der gesetzlich Krankenversicherten und erschließt sie für Forschungszwecke. Dabei werden zum Schutz der Betroffenen vor Identifizierung verschiedene Pseudonyme verwendet: Das Lieferpseudonym wird von den Krankenkassen bei der Zulieferung der Datensätze an das Forschungsdatenzentrum verwendet und ersetzt identifizierende Angaben wie die Krankenversichertennummer. Das sog. periodenübergreifende Pseudonym wird vom RKI gebildet. Es dient der Zuordnung beim Forschungsdatenzentrum und ersetzt das Lieferpseudonym und damit auch die Krankenversichertennummer. Bei einer Datenfreigabe aus der elektronischen Patientenakte sorgt das periodenübergreifende Pseudonym für die Zuordnung im Forschungsdatenzentrum.

Bei einer Auswertung durch Dritte werden die Daten grundsätzlich anonymisiert, d. h. der Datensatz wird so aufbereitet, dass aus den Sachangaben nicht auf eine Person geschlossen werden kann.

Parallel dazu habe ich das BfArM und das Bundesministerium für Gesundheit regelmäßig bei den einzelnen Entwicklungsschritten der Registerstelle und der technischen Umsetzung begleitet und beraten. Denn wesentlich für die sichere Nutzung der Daten zu Forschungszwecken ist ein geeignetes, auf die Datenstruktur zugeschnittenes Anonymisierungsverfahren, das derzeit im Auftrag des BfArM entwickelt wird. Um eine optimale Anwendung auf den späteren Gesamtdatensatz zu gewährleisten, habe ich den Plan des BfArM, einen Teildatensatz zur Entwicklung zu verwenden, unter bestimmten Bedingungen mitgetragen. Der Teildatensatz besteht aus den Daten des Berichtsjahres 2016 und wurde vorab mit speziellen, mit mir abgestimmten Methoden aufbereitet, um die betroffenen Personen zu schützen, ohne jedoch die Charakteristiken des Realdatensatzes zu verlieren.

Neben den Daten aus dem Datentransparenzverfahren sind die freiwillig für Forschungszwecke freigegebenen Daten aus der elektronischen Patientenakte eine wichtige Datenquelle für das Forschungsdatenzentrum. Zur Freigabe können strukturiert vorliegende Daten, sog. Medizinische Informationsobjekte (MIO), wie zum Beispiel der Impfpass, ausgewählt werden. Vor der Übermittlung an das Forschungsdatenzentrum werden die identifizierenden Datenfelder, zum Beispiel der Name oder das Geburtsdatum, entfernt oder pseudonymisiert. In die Entwicklung dieses Pseudonymisierungsverfahrens bin ich ebenfalls eingebunden.

Insgesamt schreitet das Projekt Forschungsdatenzentrum Gesundheit weiter voran und ist auf einem guten Weg, endlich für die Nutzungsberechtigten zur Verfügung zu stehen. Dennoch gibt es weiterhin einige wichtige Baustellen und Fragestellungen, die zu bewältigen sind. Beispielsweise vermisse ich nach wie vor klare Regelungen zum Widerspruchsrecht.

4.1.3 Taskforce Forschungsdaten

Forschungsvorhaben mit Verbundpartnern in verschiedenen Bundesländern haben es mit unterschiedlichen Rechtsgrundlagen und Aufsichtsbehörden zu tun. Um die Abstimmung mit und unter den Aufsichtsbehörden zu erleichtern und damit letztlich die Forschung zu unterstützen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein eigenes Fachgremium gebildet.

Die Taskforce Forschungsdaten unter dem gemeinsamen Vorsitz des BfDI und des Hessischen Beauftragten für Datenschutz und Informationsfreiheit wurde durch Festlegung der 102. DSK im November 2021 als weiteres Fachgremium, ähnlich den Arbeitskreisen, gegründet. Ziel war die flexible und zeitnahe Möglichkeit zur Bearbeitung von aktuellen Fragen der Forschung im Gesundheitsbereich. Zudem sollte sie als Ansprechpartner für die vom Bundesministerium für Bildung und Forschung geförderte Medizininformatikinitiative (MII) sowie die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) dienen und deren Beratung strukturieren und erleichtern.

Eines der ersten Themen war die Befassung mit dem Forschungsprojekt RACOON, das im Zusammenhang mit der Corona-Pandemie innerhalb des Netzwerks Universitätsmedizin (NUM) gebildet wurde und die strukturierte Erfassung und übergreifende Auswertung von Röntgenbildern der Lunge zum Ziel hat. Hier zeigte sich die bekannte Problematik, dass in den jeweiligen Bundesländern verschiedene Regelungen in den Krankenhaus- und Datenschutzgesetzen die Nutzung von Patientendaten in unterschiedlichem Umfang und mit unterschiedlichen Voraussetzungen zulassen oder unterbinden. Die Sitzungen der Taskforce Forschungsdaten ermöglichten einen Austausch unter den Aufsichtsbehörden und eine koordinierte Kommunikation mit den Projektträgern.

In weiteren Sitzungen wurde die Arbeit der Taskforce Forschungsdaten in Bezug auf zu erwartende Gesetzgebungsvorhaben zur Forschung mit Gesundheitsdaten strukturiert. In vier Arbeitsgruppen wurden aktuelle Veröffentlichungen und Gutachten ausgewertet. Die

Arbeitsergebnisse mündeten schließlich in den Entwurf einer Entschließung für die DSK: Die Petersberger Erklärung.

Zudem wurden mögliche Anpassungen und ein Modul zum internationalen Austausch der Mustertexte zur Einwilligung der MII diskutiert und beraten.

4.1.4 Petersberger Erklärung

Zum Schwerpunkthema „Forschung" hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in diesem Jahr auf meine Initiative hin zwei Entschließungen verabschiedet. In der DSGVO wird die Forschung als Zweck privilegiert, mit zusätzliche Maßnahmen des Datenschutzes sind umfangreiche Forschungen mit personenbezogenen Daten bzw. aus ihnen abgeleiteten Daten möglich. Konkrete Hinweise gab die DSK vor allem in der Petersberger Erklärung vom November 2022.

Zum Schwerpunktthema „Forschung" hatte die 103. DSK im März 2022 eine Entschließung „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" gefasst und weitere Vorschläge zu diesem Thema angekündigt. Im Nachgang zu dieser Konferenz befasste sich die Taskforce Forschungsdaten mit den im Koalitionsvertrag angekündigten Gesetzgebungsvorhaben zur Forschungsdatennutzung und zu medizinischen Registern ausgehend von Rechtsgutachten, die zu diesen Themen im Auftrag der Bundesregierung verfasst worden waren. Ein wesentliches Ziel der Befassung der Taskforce war es, der Bundesregierung durch möglichst konkrete Hinweise in datenschutzrechtlicher Hinsicht Orientierung bei der Formulierung der Gesetzentwürfe zu bieten und dabei die Bedeutung einer datenschutzgerechten Gestaltung der geplanten Forschungsregelungen für das nötige Vertrauen der Betroffenen herauszustellen. Dabei kann als Leitformel gelten: Je höher der Schutz der Betroffenen durch geeignete Maßnahmen, desto umfangreicher und spezifischer können Daten genutzt werden.

Die Vorarbeiten der Taskforce waren Grundlage für den Entwurf einer „Entschließung zur Ermöglichung einer datenschutzkonformen Nutzung von Gesundheitsdaten in der wissenschaftlichen Forschung", die die 104. DSK am 23./24. November 2022 verabschiedet hat.[43]

Hierin kommen zentrale datenschutzrechtliche Anliegen der DSK zum Ausdruck:

- Die Menschen dürfen nicht zum bloßen Objekt der Datenverarbeitung gemacht werden. Sie stehen im Mittelpunkt der Forschung – ihnen kommen einerseits die Erkenntnisse zugute, andererseits sind sie den möglichen Risiken ausgesetzt. Die Verarbeitungsprozesse müssen daher rechtmäßig sowie für betroffene Personen stets transparent gestaltet sein. Auch wenn die Verarbeitung ihrer Daten im öffentlichen Interesse gesetzlich erlaubt sein und nicht auf ihre Einwilligung gestützt werden sollte, muss es für die betroffenen Personen immer die Möglichkeit der Mitwirkung und Gestaltung geben.
- Digitale Managementsysteme wie Datencockpit, Dashboard oder Portale sollen für die Betroffenen leicht zugängliche Wege bieten, Informations- Kontroll- und Mitwirkungsmöglichkeiten wahrzunehmen.
- Zu den wichtigsten Schutzmaßnahmen gehören die Verschlüsselung, die Pseudonymisierung durch unabhängige Vertrauensstellen sowie die frühestmögliche Anonymisierung.
- Die Voraussetzungen für den Datenzugang, möglichst auf dann anonymisierte Datensätze, für die Forschung müssen durch ein geeignetes Verfahren (Use-and-Acces-Verfahren) geprüft werden.
- Bei der Verknüpfung von Datensätzen aus verschiedenen Quellen sind besondere Schutzanforderungen zu erfüllen. Geeignete Verfahren müssen gewährleisten, dass rechtliche und technische Voraussetzungen für eine Datennutzung erfüllt sind.
- Die datenschutzrechtliche Verantwortung muss lückenlos festgelegt sein, um den Betroffenen die Ausübung ihrer Rechte zu erleichtern.
- Auch für geplante Regelungen zu medizinischen Registern hat die DSK Hinweise gegeben, beispielsweise zu Qualitätsanforderungen, Transparenz und Mitwirkungsmöglichkeiten. Ein zentrales Verzeichnis der bestehenden Register sollte eine strukturierte Übersicht über die vorhandenen Daten bieten und mehrfache Datensammlungen mit gleichen Inhalten vermeiden. Eine zentrale Stelle könnte hinsichtlich der Betroffenenrechte eine Beratungs- und Lotsenfunktion wahrnehmen.

Zur Petersberger Erklärung vom 24. November 2022 geht's hier:

(QR-Code scannen oder klicken)

43 Zur Petersberger Erklärung vom 24. November 2022: https://www.bfdi.bund.de/entschliessungen

Die DSK bekräftigt zudem ihre Forderung, gesetzliche Regelungen zu einem Forschungsgeheimnis (Stillschweigen über zur Kenntnis gelangte personenbezogene Informationen) zu erlassen, einschließlich eines Beschlagnahmeschutzes hinsichtlich der Forschungsdaten.

Um die Datenschutzbehörden in die Lage zu versetzen, die Einhaltung datenschutzrechtlicher Anforderungen effektiver durchsetzen zu können, sollte ihnen die Möglichkeit eingeräumt werden, gegenüber öffentlichen Stellen den sofortigen Vollzug von datenschutzrechtlichen Aufsichtsmaßnahmen anordnen zu können.

Querverweise:

4.1.3 Taskforce Forschungsdaten

4.2 Europäische Digitalrechtsakte

Die Europäische Union hat im Berichtszeitraum einige neue Rechtsakte in Form von Verordnungen im Bereich der Digitalisierung beschlossen. Weitere Rechtsakte sollen folgen und sind zum Teil schon in der Beratung. Das erklärte Ziel ist die Stärkung der europäischen Wirtschaft und die Regulierung im digitalen Raum. Weil es sich bei vielen dieser Rechtsakte um Verordnungen handelt, wird keine nationale Umsetzung benötigt. Sie gelten unmittelbar und ihre Regeln müssen von Behörden, Unternehmen und Privatpersonen befolgt werden. Das bedeutet natürlich auch für meine Behörde eine intensive Auseinandersetzung mit den Details dieser europäischen Digitalrechtsakte, auch beratend für EU-Kommission, Bundesregierung und Parlamente.

4.2.1 KI-Verordnung

Die Europäische Kommission hat im Frühjahr 2021 den weltweit ersten Entwurf für einen Rechtsrahmen für den Bereich der Künstlichen Intelligenz (KI) vorgelegt. Der umfassende Regulierungsentwurf soll die Entwicklung von KI fördern, ein hohes Schutzniveau für öffentliche Interessen gewährleisten und eine Vertrauensbasis für KI-Systeme schaffen. Dass die prinzipielle Beschäftigung mit einem Regulierungsrahmen auf diesem Weg angestoßen wurde, ist ein wichtiger Schritt. Ich werde mich dafür einsetzen, dass die Grundsätze der DSGVO durch das Gesetzesvorhaben nicht unterlaufen werden. Nur so kann im Ergebnis ein adäquater Rechtsrahmen entstehen, der die geltenden Regeln zum Datenschutz wirksam ergänzt und gleichzeitig Innovationen im Bereich der KI fördert.

Anwendungen im Bereich der Künstlichen Intelligenz (KI), algorithmenbasierte Entscheidungsprozesse und lernende Systeme haben das Potenzial, einen hohen Nutzen in nahezu allen Lebensbereichen zu schaffen. Sie bieten vielfach Lösungsansätze, die ohne KI kaum denkbar wären. Ihre immer stärkere Verbreitung gepaart mit der rasanten Weiterentwicklung von KI-Technologien birgt neben den zahlreichen möglichen Vorteilen aber auch die Gefahr tiefgreifender Verletzungen von Grundrechten. Ich habe mich wiederholt dafür eingesetzt, dass jegliche Form von KI datenschutzgerecht gestaltet werden muss.

Der Entwurf für eine EU-Verordnung zur Regulierung Künstlicher Intelligenz (KI-Verordnung) oder auch Artificial Intelligence Act (AI Act) soll diesen Entwicklungen einen rechtlichen Rahmen geben und damit zur ersten europäischen Verordnung werden, die KI in nahezu allen Lebensbereichen reguliert. Seit April 2021 liegen Vorschläge auf dem Tisch, die jetzt Teil des europäischen Gesetzgebungsprozesses sind und auch von Wirtschaft und Zivilgesellschaft kontrovers diskutiert werden. Die Erarbeitung eines solchen Rechtsrahmens wird weltweit genau beobachtet, da die Regelungen das Potenzial besitzen, auch weit über die EU hinaus grundlegende Wirkung zu zeigen.

Aus Sicht der EU-Kommission soll der vorgelegte Entwurf sicherstellen, dass der Einsatz KI-basierter Systeme keine negativen Auswirkungen auf die Sicherheit, Gesundheit und Grundrechte von Menschen hat. Nach dem Verordnungsentwurf werden KI-Anwendungen in vier Risikostufen eingeteilt: Ein minimales, ein begrenztes, ein hohes und ein inakzeptables Risiko. Je nach Einstufung werden unterschiedliche Zulassungsvoraussetzungen und Kontrollen mit jeweils verschiedener Regulierungsdichte erforderlich. Für Anwendungen, die mit einem hohen Risiko einhergehen, werden bestimmte Qualitätsanforderungen vorausgesetzt, z. B. Protokollierungs- und Dokumentationsvorgaben, eine weitreichende Information der Nutzenden, eine hohe Qualität der Datensätze oder auch eine menschliche Aufsicht zur Minimierung der Risiken. Um die Sicherheit und Einhaltung bestehender Rechtsvorschriften zum Schutz der Grundrechte über den gesamten Lebenszyklus von KI-Systemen hinweg zu gewährleisten, sollen Anbietenden und Nutzenden dieser Systeme also umfassende Pflichten auferlegt werden. Dies betrifft z. B. auch den Bereich der Konformitätsbewertung oder die Bereitstellung von Informationen für die Nutzenden.

Dieser im Entwurf für einen Rechtsrahmen zur KI vorgesehene risikobasierte Ansatz wurde bereits im vergangenen Jahr vom Europäischen Datenschutzausschuss (EDSA) in einer Stellungnahme grundsätzlich begrüßt. Gemeinsam mit meinen europäischen Kolleginnen und Kollegen und dem Europäischen Datenschutzbeauftragten (EDSB) im EDSA habe ich mich dafür ausgesprochen, dass der Einsatz von KI verboten wird, wenn Persönlichkeit und Würde des Menschen nicht ausreichend geach-

tet werden. Als Teil des Berichterstatter-Teams des EDSA habe ich mich dabei nachdrücklich für die herausragende Bedeutung des Datenschutzes bei der Gestaltung von KI eingesetzt (vgl. 30. TB Nr. 4.2.1). Trotz der grundsätzlich zu begrüßenden Vorschläge für einen Regulierungsrahmen im KI-Bereich hat der EDSA gemeinsam mit dem EDSB deutlich gemacht, dass dennoch an mehreren Stellen (teils wesentlicher) Veränderungsbedarf besteht.

Besonders kritisch sehe ich z. B. den etwaigen Einsatz von KI Systemen zur Bewertung sozialen Verhaltens. Das auch als „Social Scoring" bezeichnete Verfahren birgt ein hohes Diskriminierungsrisiko. Daher sollte die Regulierung von KI das Verbot jeder Art von Bewertung sozialen Verhaltens vorsehen. Darüber hinaus habe ich mich wiederholt für ein Verbot von KI eingesetzt, die natürliche Personen nach biometrischen Merkmalen in Cluster eingruppiert. Andernfalls bestünde die Gefahr, dass Menschen nach ethnischer Zugehörigkeit, Geschlecht, politischer oder sexueller Orientierung oder sonstigen Merkmalen gruppiert werden, die zu den gemäß Art. 21 der Charta der Grundrechte der Europäischen Union verbotenen Diskriminierungsgründen zählen.

Im Berichtsjahr wurden zwischenzeitlich mehrere aktualisierte Kompromissvorschläge vorgelegt. Aktuell verhandeln das EU-Parlament und der EU-Rat jeweils intern den von der EU-Kommission verfassten Gesetzentwurf, gefolgt von den Trilog-Verhandlungen. Die Debatten über die Details der Verordnung gestalten sich aufgrund der hohen Komplexität der Thematik erwartungsgemäß langwierig. Ich begleite diese Entwicklungen sowohl auf der europäischen als auch auf der nationalen Ebene. Über die finale Ausgestaltung des AI Acts wird voraussichtlich im Laufe des Jahres 2023 entschieden.

4.2.2 Digital Services Act

Der Digital Services Act (DSA), der als erster Teil des Legislativpakets Digitale Dienste der Europäischen Kommission illegale und schädliche Online-Inhalte bekämpfen soll, ist am 16. November 2022 in Kraft getreten und ab dem 17. Februar 2024 anzuwenden. Damit werden auch für den Datenschutz wichtige Impulse gesetzt, die ich im Gesetzgebungsverfahren unterstützt habe. Bei der Schaffung der nationalen Aufsichtsstruktur zum DSA sollte die Datenschutzaufsicht gewinnbringend eingebunden werden, indem ihre Unabhängigkeit beachtet und ihre Expertise genutzt wird.

Die Regelungen des DSA, der auch oft als das „Grundgesetz des Internets" bezeichnet wird, gelten insbesondere für große Online-Plattformen, beispielsweise große soziale Netzwerke. Sie verpflichten diese unter anderem zu deutlich mehr Transparenz und verbraucherfreundlicherer Gestaltung ihrer Dienste. Aus datenschutzrechtlicher Perspektive sind insbesondere die Regelungen zur Datennutzung für Tracking und Profiling im Rahmen der Online-Werbung von großer Bedeutung. Wie schon in meinem 30. TB (Nr. 5.9) erläutert, habe ich mich im Gesetzgebungsverfahren für ein umfassendes Verbot von personalisierter Werbung eingesetzt. Diese Forderung hat leider keine Mehrheit gefunden. Der DSA verbietet jedoch die Nutzung der Daten Minderjähriger für profilbasierte Werbung vollständig. Werbung, die auf Profiling unter Verwendung von besonderen Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DSGVO basiert, darf ebenso nicht angezeigt werden – in diesem Fall gilt das auch für die Daten von Erwachsenen. Schade ist, dass dieses Verbot nicht für Kleinst- und Kleinunternehmen gelten wird.

Auf Vorschlag des EU-Parlaments wurde auch ein Verbot von sogenannten „dark patterns" im DSA aufgenommen. Dieses Verbot habe ich ausdrücklich unterstützt, da hierdurch verhindert werden kann, dass Nutzende durch die Gestaltung von Apps und Websites manipuliert werden und so unter Umständen Daten preisgeben, die sie bei einer anderen Gestaltung des Angebots nicht weitergegeben hätten. Gewisse manipulative Praktiken sind zwar bereits nach der DSGVO untersagt, durch die Regelungen im DSA wird dieser Schutz aber noch erweitert.

Auch ermöglicht der DSA Forschungseinrichtungen Zugang zu Daten großer Online-Plattformen, um die Algorithmen analysieren zu können, die dafür verantwortlich sind, welche Inhalte den Nutzenden angezeigt werden. So ist es nun erstmals möglich zu erkennen, wie bestimmte zum Teil für die Gesellschaft schädliche Vorgänge in sozialen Netzwerken funktionieren, um diese ggf. zu bekämpfen. Natürlich habe ich bei der entsprechenden Regelung darauf geachtet, dass der Datenschutz gewahrt werden muss und eine nicht notwendige Verarbeitung personenbezogener Daten unterbleibt.

Schlussendlich ist für die Wirksamkeit des DSA die Aufsicht über die Unternehmen von zentraler Bedeutung, die in den Mitgliedsstaaten der „Digitale-Dienste-Koordinator" (Digital Services Coordinator, kurz: DSC) haben wird. Daher setze ich mich bei der Schaffung des deutschen Aufsichtsrahmens für den DSA dafür ein, dass die Datenschutzaufsichtsbehörden ihre Expertise zur Profilbildung möglichst effizient einbringen können und datenschutzrechtliche Wertungen zwingend von der unabhängigen Datenschutzaufsicht getroffen werden, um eine einheitliche Aufsicht zu gewährleisten.

Wie effektiv der DSA in der Praxis sein und welche Auswirkungen er konkret auf Unternehmen und Verbraucher haben wird, ist noch offen. Ich denke jedoch, dass der DSA ein wichtiger grundlegender Schritt ist, damit Online-Plattformen, Online-Marktplätze und Suchma-

schinen sicherer sowie datenschutz- und verbraucherfreundlicher werden.

4.2.3 Digital Markets Act

Der Digital Markets Act (DMA), der als zweiter Teil des Legislativpakets Digitale Dienste der EU-Kommission durch die Regulierung von großen digitalen Plattformen einen fairen Wettbewerb herstellen soll, ist am 1. November 2022 in Kraft getreten und ab 2. Mai 2023 anzuwenden. Im Gesetzgebungsprozess wurden von mir unterstützte datenschutzrechtliche Kernforderungen in den DMA aufgenommen, die die Kooperation zwischen Wettbewerbs- und Datenschutzaufsicht weiter stärken.

Wie bereits im 30. TB (Nr. 5.9) berichtet, war mir bei meiner Beratung im Rahmen des Gesetzgebungsverfahrens zum DMA die Kooperation der Aufsichtsbehörden ein wichtiges Anliegen, um eine einheitliche Aufsicht in Datenschutzfragen sicherzustellen. Denn der DMA beinhaltet sowohl unmittelbar anwendbare Verhaltensregeln mit Datenschutzbezug für große zentrale Plattformdienste, die sog. Gatekeeper, als auch Regelungen zu Profiling und Datenportabilität.

Daher freut es mich, dass im DMA nun auch datenschutzrechtliche Kernforderungen an entscheidenden Stellen verankert wurden, für die ich mich eingesetzt habe.

Mit der europäischen hochrangigen (Experten-)Gruppe wird ein Gremium geschaffen, in dem sich die Europäische Kommission als Vollzugsbehörde mit beteiligten europäischen Gremien und Netzwerken abstimmen soll. Hier können u. a. der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) die Europäische Kommission bei der kohärenten Anwendung des DMA und der Überwachung seiner Einhaltung unterstützen. Insbesondere dadurch soll sichergestellt werden, dass das Schutzniveau der DSGVO erhalten bleibt. Diese Kooperation ist aus meiner Sicht unerlässlich und daher sehr zu begrüßen, genauso wie etwa die Verpflichtung, die Beschreibung der Gatekeeper von Techniken zur Erstellung von Verbraucherprofilen (Profiling) auch dem EDSA zur Verfügung zu stellen.

Außerdem wird im DMA die Interoperabilität von Messengerdiensten geregelt. Neben Ende-zu-Ende verschlüsselten Textnachrichten sind grundsätzlich auch der Austausch von Bildern, Sprachnachrichten, Videos und anderer angehängter Dateien in der Ende-zu-Ende Kommunikation zwischen einzelnen Endnutzern verschiedener Messengerdienste sicherzustellen. Eine zeitlich nachgelagerte Erweiterung in Bezug auf Endnutzergruppen sowie Video- und Sprachanrufe erfolgt dann innerhalb von zwei bzw. vier Jahren nach Benennung des Messengerdienstes als Gatekeeper. Die ebenfalls von mir unterstützte Forderung nach Interoperabilität bei Diensten sozialer Netzwerke hat sich hingegen politisch leider nicht durchsetzen können.

Insgesamt bin ich zuversichtlich, dass die durch den DMA deutlich gestärkte Wettbewerbsaufsicht über große Plattformdienste sich auch auf den Datenschutz positiv auswirken wird.

4.2.4 Data Governance Act

Die Europäische-Kommission hat mit ihren Verordnungsvorschlägen zur Regulierung des europäischen Binnenmarkts für Daten weitere Schritte zu einem EU-weiten Regelwerk für den Digitalen Raum vorgelegt. Eine dieser Verordnungen ist der Data Governance Act (DGA).

Der DGA ist am 23. Juni 2022 in Kraft getreten und wird ab dem 24. September 2023 anzuwenden sein. Der DGA verfolgt in unterschiedlichen Handlungsfeldern die Schaffung von Rahmenbedingungen für eine sog. Datenökonomie (vgl. 30. TB, Nr. 5.9). Er zielt darauf ab, das Vertrauen in die gemeinsame Nutzung von Daten zu stärken.

Zum einen werden Voraussetzungen für die Weitergabe von Daten durch öffentliche Stellen zur allgemeinen Nutzung (Open Data) geschaffen. Dadurch sollen zukünftig Behörden u. a. auch personenbezogene Daten etwa zur kommerziellen Weiterverwendung freigeben. Die Schaffung von Rechtsgrundlagen für die zulässige Weitergabe soll allerdings den Mitgliedstaaten überlassen und die DSGVO insgesamt unberührt bleiben. Letzteres ist aus meiner Sicht zu begrüßen.

Zum anderen definiert der DGA Dienste für die gemeinsame Datennutzung, sog. Vermittlungsdienste. Unter neutraler Vermittlung sollen diese entsprechenden Dienste Datenanbietende und Datennutzende zusammenbringen. Darüber hinaus werden Rahmenbedingungen geschaffen, die Mitgliedstaaten zur Schaffung von sog. datenaltruistischen Organisationen ermutigen sollen. Das Vertrauen in solche Organisationen soll derart gestärkt werden, dass Bürgerinnen und Bürger freiwillig ihre personenbezogenen Daten für gemeinwohlbezogene Ziele, wie etwa zu Forschungszwecken, hergeben.

Bei allen Regelungsansätzen des DGA stellt sich das Problem, dass neben der Datenschutzaufsicht eine eigene Aufsichtsstruktur geschaffen werden soll, obwohl in der Sache überlappende Zuständigkeiten bestehen werden. Hierzu sowie zu weiteren kritischen Punkten habe ich gemeinsam mit meinen europäischen Kolleginnen und Kollegen und dem Europäischen Datenschutzbeauftrag-

ten (EDSB) im EDSA bereits im letzten Berichtsjahr eine umfangreiche Stellungnahme verfasst.[44]

4.2.5 Data Act

Meine Behörde begleitet die Verhandlungen zu europäischen Rechtsakten sowohl national im Rahmen von Ressortabstimmungen, als auch durch Initiativen im Europäischen Datenschutzausschuss (EDSA). Der Entwurf einer Verordnung für ein Datengesetz (Data Act, DA) steht im Fokus, weil es hier insbesondere um die Daten geht, die Nutzende auf ihren vernetzten Geräten erzeugen.

Am 23. Februar 2022 stellte die Europäische Kommission ihren Entwurf für den Data Act vor. Erklärtes Ziel des DA ist, neue Vorschriften darüber zu etablieren, wer die in den Wirtschaftssektoren in der EU erzeugten Daten nutzen darf und wer Zugriff darauf hat. Der Vorschlag sieht unter anderem vor, Nutzenden Zugang zu den von ihren vernetzten Geräten erzeugten Daten zu garantieren, die häufig ausschließlich von Herstellern gesammelt werden. Daneben sollen Maßnahmen zur Wiederherstellung einer ausgewogenen Verhandlungsmacht für kleine und mittelständische Unternehmen durch die Verhinderung von Ungleichgewichten in Verträgen über die gemeinsame Datennutzung etabliert werden. Und Behörden soll in besonderen Konstellationen Zugang zu und die Nutzung von Daten im Besitz des Privatsektors ermöglicht werden.

Deutlich wird sowohl beim Data Governance Act (DGA) als auch DA, dass verbesserte Rahmenbedingungen für digitale Geschäftsmodelle und Verarbeitungsformen im Mittelpunkt der Anstrengungen des EU-Gesetzgebers stehen. Beide Gesetzgebungsakte stellen allerdings das bisherige Schutzkonzept des Datenschutzes vor erhebliche Herausforderungen. Umso mehr gilt es, diese geplanten Rahmenregelungen für sog. Datenmärkte im Hinblick auf die Risiken in Gestalt eines massenhaften Austausches von auch personenbeziehbaren Daten und deren Auswertung insbesondere zu rein kommerziellen Zwecken sorgfältig im Blick zu behalten.

Ich habe mich wiederholt dafür eingesetzt, dass die Grundsätze der DSGVO weder durch den DA noch durch den DGA unterlaufen werden. Zwar soll die DSGVO nach Vorstellung der EU-Kommission von den neuen Rechtsakten unberührt bleiben. Es bestehen aber viele Unklarheiten im Verhältnis zur und bezüglich der Auswirkungen auf die DSGVO.

Darüber hinaus haben sowohl DGA als auch DA weitere Schnittstellen, die sich auf den Datenschutz in der EU insgesamt ganz erheblich auswirken werden. Ziel meiner Beratung ist es, auf diese Problempunkte aufmerksam zu machen und auf eine möglichst datenschutzfreundliche Regulierung hinzuwirken. Wichtig ist, im Blick zu behalten, ob und inwieweit aus diesen neuen, weitreichenden EU-Rechtsakten auch weiterer gesetzlicher Regelungsbedarf zum Schutz der Datenschutzrechte der Bürgerinnen und Bürger erwachsen könnte. Hierzu sowie zu weiteren kritischen Punkten, wie etwa die vorgesehene Aufsichtsstruktur im Data Act, habe ich gemeinsam mit meinen europäischen Kolleginnen und Kollegen und dem EDSB im EDSA eine umfängliche Stellungnahme verfasst.[45]

Im Berichtsjahr wurden nun zwischenzeitlich mehrere aktualisierte Kompromissvorschläge zum DA vorgelegt. Aktuell verhandeln das EU-Parlament und der EU-Rat jeweils intern den von der EU-Kommission verfassten Gesetzentwurf, gefolgt von den Trilog-Verhandlungen. Die Debatten über die Details der Verordnung gestalten sich aufgrund der hohen Komplexität der Thematik erwartungsgemäß schwierig. Selbstverständlich begleite ich diese Entwicklungen sowohl auf der europäischen als auch auf der nationalen Ebene. Über die finale Ausgestaltung des DA wird voraussichtlich bis zum Ende der laufenden Legislaturperiode des EU-Parlaments (2024) entschieden.

Querverweise:

4.2.4 Data Governance Act

4.2.6 Verordnung Politische Werbung

Die Europäische-Kommission hat einen Vorschlag über die Transparenz und die Ausrichtung von politischer Werbung vorgelegt, der ebenfalls für den Bereich des Datenschutzrechts relevant ist.

Am 25. November 2021 stellte die Europäische Kommission ihren Vorschlag für eine Verordnung über die Transparenz und das Targeting politischer Werbung vor (Verordnung politische Werbung). Ziel der Kommission ist, durch die Verordnung neue europaweite Regeln zum Schutz der Wahlintegrität und zur Förderung der demokratischen Teilhabe zu etablieren. Die vorgesehenen Regelungen betreffen auch datenschutzrechtliche Gesichtspunkte.

---

44 Stellungnahme 3/2021, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_de

45 Stellungnahme 2/2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en.

Der Entwurf schlägt unter anderem ein „Transparenzsiegel“ vor, wonach bezahlte politische Werbung eindeutig gekennzeichnet sein und eine Reihe wichtiger Informationen enthalten muss. Darüber hinaus sieht der Vorschlag für eine Verordnung strengere Auflagen für das Targeting und Amplifizieren von politischer Werbung vor, bei denen sensible personenbezogene Daten wie ethnische Herkunft, religiöse Überzeugungen oder sexuelle Orientierung verwendet oder abgeleitet werden. Nach Vorstellung der Kommission sollen diese Techniken in solchen Fällen nur mit Einwilligung der betroffenen Person zulässig sein.

Aus meiner Sicht geht das vorgesehene Verbot von Targeting und Amplifizieren im Rahmen politischer Werbung nicht weit genug. Ich habe mich wiederholt für ein komplettes Verbot der Nutzung jeglicher Form personenbezogener Daten für Targeting, Amplifizieren und Ad Delivery in Bezug zu politischer Werbung eingesetzt. Ein solches Verbot dient insbesondere dem Schutz der Nutzerinnen und Nutzer im Online-Raum, die sich einer solchen Verwendung ihrer Daten oftmals gar nicht bewusst sind. Darüber hinaus dient ein solches Verbot dem Schutz der Integrität von freien Wahlen und stellt sicher, dass eine offene, plurale Debatte als Säule der europäischen Demokratie gewährleistet wird. Natürlich setze ich mich auch dafür ein, dass die Grundsätze der DSGVO und die Regelungen des Digital Services Act (DSA) zu personalisierter Werbung durch die Verordnung nicht unterlaufen werden.

Im Berichtsjahr wurden nun auch bezüglich der Verordnung politische Werbung mehrere aktualisierte Kompromissvorschläge vorgelegt. Selbstverständlich begleite ich diese Entwicklungen sowohl auf der europäischen als auch auf der nationalen Ebene. Wann eine finale Ausgestaltung der Verordnung vorliegen wird, ist noch nicht abzusehen.

Querverweise:

4.2.2 Digital Services Act

4.3 Digitale Medien

Digitale Medien und Angebote sind aus unserem Alltag längst nicht mehr wegzudenken. Entscheidend aus Datenschutzsicht ist, dass diese Angebote rechtskonform gemacht werden. Das gilt für Behörden umso mehr, da sie Vorbilder in ihrem Verhalten sein sollen. Gerade deswegen erreichen mich immer wieder Eingaben und Beschwerden von Bürgerinnen und Bürgern, wenn es nicht so ist. Die Datenschutzaufsichtsbehörden in Deutschland und der EU erzwingen mittlerweile Entscheidungen, um Rechtsunsicherheiten und nicht rechtskonformes Verhalten zu beseitigen.

4.3.1 Verfahren Facebook Fanpages

Im Mai 2022 leitete der BfDI ein Verfahren zur Abhilfe wegen datenschutzrechtlicher Probleme im Zusammenhang mit dem Betrieb der Facebook-Fanpage für die Bundesregierung gegen das Bundespresseamt ein.

Bei einer Fanpage (auch „Facebook-Seiten“) handelt es sich um eine Art Homepage, die durch Facebook publiziert wird. Der Inhalt stammt nicht von Facebook, sondern von den Betreiberinnen und Betreibern der Fanpage. Bei dem Besuch einer Facebook-Fanpage werden umfassend personenbezogene Daten über das Surfverhalten der Nutzerinnen und Nutzer gesammelt, um diese Informationen über Werbung zu monetarisieren. Diese Überwachung trifft nicht nur angemeldete Nutzerinnen und Nutzer von Facebook, sondern auch Personen, die kein Facebook Konto haben.

Mir ist die Bedeutung sozialer Netzwerke für die Öffentlichkeitsarbeit der Bundesbehörden bewusst. Gleichwohl sind Behörden besonders gefordert, rechtskonform zu handeln. Die wichtige Aufgabe der Öffentlichkeitsarbeit kann nicht die Profilbildung und Verarbeitung personenbezogener Daten zu Marketingzwecken rechtfertigen. Daher und aufgrund ihrer Vorbildfunktion nehmen die Datenschutzaufsichtsbehörden diese nun vorrangig in die Pflicht.

Ich habe die öffentlichen Stellen des Bundes bereits mehrfach auf die datenschutzrechtlichen Bedenken gegen den Betrieb von Facebook-Fanpages aufmerksam gemacht und vergeblich zur Abhilfe aufgefordert. Die Ergebnisse des Kurzgutachtens zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages vom 18. März 2022 einer seitens der DSK eingesetzten Taskforce bestätigten die Ansicht, dass ein datenschutzkonformer Betrieb von Fanpages nicht möglich ist. Nach vorheriger Ankündigung, die Nutzung von Facebook-Fanpages durch die Bundesbehörden zu prüfen, leitete ich im Mai 2022 ein Abhilfeverfahren gegen das Presse- und Informationsamt der Bundesregierung (Bundespresseamt) ein. In einem ersten Schritt habe ich dem Bundespresseamt ein Anhörungsschreiben geschickt mit Fragen zum Betrieb der Facebook-Fanpage der Bundesregierung. Die Antworten des Bundespresseamts habe ich geprüft. Zum Redaktionsschluss habe ich noch keine Entscheidung über eine mögliche Abhilfe-

maßnahme getroffen, gehe aber davon aus, dass dies im ersten Quartal 2023 geschehen wird.

Anlässlich von Änderungen der Datenschutzrichtlinie und der Nutzungsbedingungen sowie des Cookie-Banners von Facebook überarbeitete die Taskforce Facebook-Fanpages das Kurzgutachten.[46]

Diese Aktualisierung ändert aber nichts an meiner datenschutzrechtlichen Bewertung des Betriebs von Facebook-Fanpages.

Eine datenschutzkonforme Nutzung von Facebook Fanpages ist h. E. weiterhin nicht möglich. Ich empfehle daher, die Fanpages abzuschalten.

4.3.2 Entscheidungen europäischen Aufsichtsbehörden zu Google Analytics

Seit dem Jahreswechsel 2021/22 haben verschiedene europäische Aufsichtsbehörden (AB) Entscheidungen zum Trackingtool „Google Analytics“ getroffen.

Unmittelbar nach dem sogenannten Schrems II-Urteil des EuGH[47] hatte der Europäische Datenschutzausschuss (EDSA) eine Taskforce (TF) eingesetzt, die sich mit 101 Beschwerden befassen sollte, die durch die NGO „Non-of-your-business (NOYB)“ bei verschiedenen EU- und EWR-Aufsichtsbehörden eingereicht wurden. Die Beschwerden bezogen sich sämtlich auf die Frage von Datenübermittlungen bei der Nutzung von Google-Analytics und Facebook-Connect durch unterschiedliche Webseitenbetreibende. NOYB beanstandete, die Nutzung führe zur Übermittlung personenbezogener Daten an die USA. Gemäß den Feststellungen des Schrems II-Urteils sei dies nicht als datenschutzkonform zu bewerten. Die eingerichtete TF nahm kurz nach Eingang der Beschwerden ihre Arbeit auf. Deutschland ist mit verschiedenen Aufsichtsbehörden in dieser TF vertreten.

Mittlerweile haben verschiedene europäische Aufsichtsbehörden Entscheidungen zu den bei ihnen eingereichten Beschwerden erlassen. Neben der österreichischen AB haben die französische und die italienische AB ihre Entscheidungen zu Google Analytics veröffentlicht[48]. In den Entscheidungen stellten die Behörden fest, dass die

46 Kurzgutachten vom 10. November 2022, abrufbar unter www.bfdi.bund.de/entschliessungen

47 Schrems II Urteil d. EuGH (C-311/18) v.16.07.20, abrufbar unter: https://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=40595668

48 Entscheidung der AB AT abrufbar unter: https://www.dsb.gv.at/download-links/bekanntmachungen.html; Entscheidung der AB FR abrufbar unter: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply; Entscheidung der AB IT, abrufbar unter https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782874#english ; https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9782890

jeweils vorgelegten Sachverhalte nicht im Einklang mit der DSGVO stehen. In der Begründung führten sie aus, dass die Anforderungen des Kapitel V der DSGVO an ein angemessenes Datenschutzniveau in den USA im Lichte der Maßgaben des Schrems II-Urteils nicht eingehalten würden. Auch die vom EuGH geforderten zusätzlichen Maßnahmen (sogenannte „supplementary measures“) wurden durch die AB als nicht ausreichend effektiv bewertet, da sie nicht gewährleisten könnten, mögliche Zugriffe von Sicherheitsbehörden zu verhindern. Die Implementierung derartiger zusätzlicher Maßnahmen hatte der EuGH im Schrems II-Urteil gefordert, um im Einzelfall ein dem Unionsrecht im Wesentlichen gleichwertiges Schutzniveau zu gewährleisten. Die französische und die italienische AB setzten den jeweiligen Webseitenbetreiber Fristen, innerhalb derer die Verarbeitungen in Einklang mit der DSGVO zu bringen waren. Die österreichische AB traf keine abschließende Entscheidung, da sie den Fall wegen einer Zuständigkeitsveränderung an eine deutsche AB abgegeben hat. Auch der EDPS hatte eine Entscheidung im Zusammenhang mit Google Analytics veröffentlicht und in dieser die Verwendung von Google Analytics ebenfalls als rechtswidrig erachtet.[49]

4.3.3 Einsatz eines Content-Distribution-Network (CDN) für die Website des Zensus 2022

Im Frühjahr 2022 habe ich eine größere Anzahl von Beschwerden von Bürgerinnen und Bürgern erhalten, die bemängelten, dass das Statistische Bundesamt für die Homepage des Zensus 2022 einen US-basierten Dienstleister für das Content-Distribution-Network einsetzte. In Zusammenarbeit mit dem Statistischen Bundesamt und dem Informatiktechnikzentrum Bund (ITZ-Bund) konnte ich sicherstellen, dass keine sensiblen Zensusdaten über das Netz dieses Dienstleisters übertragen wurden und somit auch das Risiko eines Zugriffs ausländischer Sicherheitsbehörden auf Zensusdaten ausgeräumt wurde.

Seit der Schrems-II Entscheidung des Europäischen Gerichtshofs (Rechtssache C-311/18) erhalten mögliche Übermittlungen personenbezogener Daten in Drittstaaten, in denen kein dem europäischen Datenschutzniveau vergleichbares Schutzniveau gewährleistet ist, verstärkt die Aufmerksamkeit der Öffentlichkeit. Der Europäische Datenschutzausschuss hat zu diesem Thema bereits im Jahr 2020 Empfehlungen erarbeitet und veröffentlicht. Diese geben Datenexporteuren (Verantwortlichen oder Auftragsverarbeitern) Hinweise, wie sie bei laufenden oder geplanten Verarbeitungen personenbezogener Daten ermitteln können, ob etwaige Datenübermittlungen an Drittstaaten den Anforderungen der Datenschutz-Grundverordnung (DSGVO) genügen, wenn für die betreffenden Drittstaaten kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Dazu hatte ich bereits im Herbst 2020 ein entsprechendes Informationsschreiben an die öffentlichen Stellen des Bundes sowie die meiner Aufsicht unterliegenden Unternehmen verschickt. Über den Themenkomplex Drittlandsübermittlungen habe ich bereits in meinem letzten Tätigkeitsbericht berichtet (vgl. 30. TB, Nr. 3.2.2).

Im Frühjahr 2022 erreichte mich eine größere Anzahl von Anfragen und Beschwerden von Bürgerinnen und Bürgern, denen aufgefallen war, dass die Homepage des Zensus 2022 bei einem US-basierten Content-Distribution-Netzwerk gehostet war. Die Anfragen bezogen sich dabei häufig auf die Veröffentlichung des IT-Sicherheitsforschers Mike Kuketz.[50] CDN- Dienste werden eingesetzt, wenn für bestimmte Webseiten ein besonders hohes Nachfragevolumen erwartet wird, so dass der Betreiber der Website befürchtet, dass die Bandbreite seiner eigenen Netzanbindung oder die Leistungsfähigkeit seiner eigenen Systeme nicht ausreichend sein könnte, die hohe Anzahl an Anfragen zu beantworten. In diesem Zug werden die Inhalte der Webseiten nicht mehr vom eigentlichen Betreiber ausgeliefert, sondern lagern beim Betreiber des CDN und werden von diesem an die Browser der Nutzerinnen und Nutzer übertragen. Je nach Art des Webangebots werden auch etwaige Rückmeldungen wie Formulareingaben oder hochgeladene Dokumente zunächst über das Netz des CDN übertragen oder dort verarbeitet.

Für die Website des Zensus 2022 hatte das ITZ-Bund im Auftrag des Statistischen Bundesamtes in Erwartung eines hohen Anfragevolumens einen US-basierten Anbieter von CDN-Diensten mit dem Hosting beauftragt. Ich konnte nach der Untersuchung des Sachverhalts in Zusammenarbeit mit dem ITZ-Bund kurzfristig erreichen, dass Anmeldeinformationen und Formulardaten in jedem Fall direkt zum ITZ-Bund übermittelt wurden, ohne Netze des CDN-Dienstleisters zu durchlaufen. Die Einstiegsseite selbst wurde noch eine Zeitlang durch den CDN-Dienstleister ausgeliefert, so dass beim Aufruf der Startseite des Zensus 2022 noch die IP-Adresse des Browsers durch den CDN-Anbieter verarbeitet wurde. Nach dem Ende dieses Übergangszeitraums ist die Startseite des Zensus 2022 seit Herbst 2022 vollständig direkt über das ITZ-Bund angebunden.

49 Entscheidung des EDPS abrufbar unter: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf
50 Blogbeitrag zu CDN-Diensten, abrufbar unter: https://www.kuketz-blog.de/zensus-2022-statistisches-bundesamt-hostet-bei-cloudflare/

In diesem Zusammenhang habe ich außerdem das ITZ-Bund und das Beschaffungsamt des Bundesministeriums des Innern bei der Vorbereitung einer Ausschreibung für CDN-Dienstleistungen beraten.[51] Das Ziel war hier, durch eine geeignete Formulierung der Ausschreibung sicher zu stellen, dass eingereichte Angebote von vorne herein auch den Anforderungen des Datenschutzes entsprechen.

Querverweise:

8.8 Zensus 2020

4.4 Einsatz von KI im Sicherheitsbereich

Künstliche Intelligenz (KI) wird oft als das wichtigste Zukunftsthema genannt. Dabei gibt es schon heute Prozesse, in denen KI längst eine zentrale Rolle spielt, auch wenn viele Aspekte überhaupt nicht reguliert sind. Gerade im Sicherheitsbereich, wo viele, teilweise sensible Daten verarbeitet werden, muss beim Einsatz von KI sehr genau hingesehen werden. Denn hier drohen Konsequenzen, die direkten und erheblichen Einfluss auf das Leben der Bürgerinnen und Bürger haben. Das zeigen die Themen, mit denen sich meine Behörde im Berichtszeitraum auseinandergesetzt hat.

4.4.1 CSAM-Verordnung

Der europäische Gesetzgeber plant, Anbietende von Messenger- und Hostingdiensten zum Auffinden von Materialien des sexuellen Online-Kindesmissbrauchs (CSAM) zu verpflichten und dazu sämtliche private Kommunikation und Dateien zu durchleuchten. Aus datenschutzrechtlicher Sicht ist das Vorhaben höchst problematisch.

Die Europäische Kommission hat am 11. Mai 2022 einen Verordnungsentwurf zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt. Anbietende von Messenger- und Hostingdiensten sollen verpflichtet werden, sämtliche Kommunikation bzw. Daten ihrer Nutzenden auf Material, das sexuellen Kindesmissbrauch zeigt (sog. CSA-Material), zu durchleuchten. Außerdem sollen durch Scannen von Nachrichten Annäherungsversuche von Erwachsenen gegenüber Kindern in sexueller Missbrauchsabsicht (sog. Grooming) aufgedeckt werden. Neben dem Auslesen von Textnachrichten sieht der Entwurf auch das Abhören von Audiokommunikation vor.

Auch wenn das Ziel, die Online-Verbreitung des sexuellen Kindesmissbrauchs zu stoppen, ein überaus wichtiges Ziel ist, schießt der Gesetzgebende der Europäischen Union (EU) mit seinem Vorschlag deutlich über dieses Ziel hinaus. Denn die sogenannte „Chatkontrolle“ bietet kaum Schutz für Kinder, wäre aber Europas Einstieg in eine anlasslose und flächendeckende Überwachung der privaten Kommunikation.

Der Verordnungsentwurf respektiert meines Erachtens weder die Vorgaben zur Verhältnismäßigkeit noch die Grundrechte, die deutschen Bürgerinnen und Bürgern nach der EU-Grundrechte-Charta (Charta) und nach dem Grundgesetz (GG) zustehen. Der Vorschlag droht die Ende-zu-Ende-Verschlüsselung zu durchbrechen, indem Inhalte privater Kommunikation derjenigen Dienste, die von der zuständigen Behörde eine sog. Aufdeckungsanordnung erhalten haben, flächendeckend gescannt werden sollen. Von einem solchen Scannen sind keine Ausnahmen vorgesehen, auch nicht für Berufsgeheimnisträger. Das heißt, es würde z. B. auch die vertrauliche Kommunikation zwischen Anwältinnen und Anwälten und ihren Mandantinnen und Mandaten oder zwischen Ärztinnen und Ärzten und ihren Patientinnen und Patienten erfasst. Durch eine Durchbrechung der Ende-zu-Ende-Verschlüsselung drohen Sicherheitslücken, die auch von Kriminellen genutzt werden könnten. Als alternative Möglichkeit sollen Dienste direkt auf dem jeweiligen Gerät der Nutzenden Inhalte auslesen können (sog. Client-Side-Scanning). Dies führt zu eklatanten Verstößen gegen die Achtung des Privatlebens nach Art. 7 der Charta und gegen das Fernmeldegeheimnis nach Art. 10 Absatz 1 GG.

Weiterhin weisen die Technologien, die zum Auffinden des CSA-Materials eingesetzt werden sollen, zum Teil noch Fehlerquoten von bis zu 12 Prozent auf. Dadurch könnten bei einem Dienst wie beispielsweise WhatsApp mit insgesamt circa zwei Milliarden Nutzenden bis zu 240 Millionen Nutzende zu Unrecht der Verbreitung von CSA-Material beschuldigt werden.

Datenschutzaufsichtsbehörden sollen sich vor dem Einsatz der jeweiligen Technologien nur mit unverbindlichen Stellungnahmen beteiligen können. Sobald eine Technologie einmal eingesetzt wird, ist eine Beteiligung jedoch nicht mehr vorgesehen. Diese eingeschränkte Rolle der Datenschutzbehörden halte ich bei derart schwerwiegenden, drohenden Grundrechtseingriffen für unzureichend.

Ein noch zu errichtendes EU-Zentrum soll eine Datenbank mit Verdachtsfällen führen, in der es erhaltene

51 Stellungnahme des BfDI vom 26. August 2022, abrufbar unter: www.bfdi.bund.de/stellungnahmen

Missbrauchsberichte sammelt. Diese werden vom EU-Zentrum geprüft und an die nationalen Strafverfolgungsbehörden weitergeleitet.

Schließlich sieht der Verordnungsentwurf auch verpflichtende Alterskontrollen durch App-und Software-Stores und teilweise sogar den Ausschluss bestimmter Altersgruppen von Software-Anwendungen vor. Dies führt im Ergebnis zu einer ungewollten Zensur und macht es teilweise unmöglich, das Internet anonym oder pseudonym zu nutzen. Ein Aufheben der Anonymität hätte insbesondere für Oppositionelle oder Whistleblower schwerwiegende Folgen.

Der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDPS) haben den Verordnungsentwurf bereits in einer gemeinsamen Stellungnahme im Juli 2022 sehr scharf kritisiert.[52] Dem schließe ich mich an und setze mich gemeinsam mit meinen europäischen Kolleginnen und Kollegen für eine deutliche Nachbesserung der Verordnung ein. Grundrechte müssen gewahrt werden und auch stets beim Datenschutz und dem Schutz des Fernmeldegeheimnisses gelten. Sofern der EU-Gesetzgeber den Verordnungsentwurf nicht deutlich nachbessert, werde ich mich dafür einsetzen, dass die Verordnung in dieser Form nicht verabschiedet wird.

Ich empfehle der Bundesregierung, auf eine erhebliche, grundrechtskonforme Überarbeitung des VO-Entwurfs zur Chat-Kontrolle zu drängen und ansonsten den Verordnungsentwurf insgesamt abzulehnen.

Querverweise:

3.3.1 Allgemeiner Bericht aus dem EDSA

4.4.2 Ergebnisse Konsultationsverfahren zur Künstlichen Intelligenz

Im Berichtsjahr habe ich den Bericht über die Ergebnisse des Konsultationsverfahrens veröffentlicht – ein Schritt in die Richtung einer notwendigen öffentlichen Debatte. Weitere konkrete Maßnahmen müssen folgen.

Die Ergebnisse des von mir durchgeführten Konsultationsverfahrens zum Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr liegen nunmehr vor. Den Konsultationsbericht mit meiner Bewertung der Sach- und Rechtslage habe ich samt den eingegangenen Stellungnahmen auf meiner Website veröffentlicht.[53] Bei allen Konsultationsteilnehmenden möchte ich mich an dieser Stelle ausdrücklich für den wichtigen Input bedanken.

Zum Bericht über das öffentliche Konsultationsverfahren geht's hier:

(QR-Code scannen oder klicken)

Die Konsultation hat ergeben, dass KI im Bereich der Strafverfolgung und Gefahrenabwehr bereits jetzt im Einsatz ist und angesichts der stetig wachsenden Datenmengen zunehmend an Bedeutung gewinnt.

Die Materie ist sehr komplex. Vor allem kann sich der Einsatz von KI erheblich auf die grundrechtlichen Freiheiten der Bürgerinnen und Bürger auswirken. Deshalb muss das Thema dringend in der Öffentlichkeit diskutiert werden. Darüber waren sich die Konsultationsteilnehmenden weitestgehend einig. Einigkeit bestand auch darüber, dass das Thema differenziert angegangen werden muss.

Der Gesetzgeber ist gehalten, den Einsatz von KI rechtlich zu „umhegen". Dafür ist eine umfassende, empirische und interdisziplinäre Bestandsaufnahme durch den Gesetzgeber unabdingbar. Ich rege an, eine Sachverständigenkommission einzusetzen, in der ich meine Expertise gerne einbringen würde.

Auf meinen Vorschlag hin hat Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Arbeitskreis Sicherheit mit einer Bestandsaufnahme beauftragt, wie KI in der aktuellen Praxis der Strafverfolgung und der Gefahrenabwehr in Deutschland eingesetzt wird.

Um den Einsatz von KI im Bereich der Strafverfolgung und Gefahrenabwehr rechtlich abzusichern, empfehle ich dem Gesetzgeber, eine umfassende, empirische und interdisziplinäre Bestandsaufnahme durch eine Expertenkommission durchzuführen.

52 Stellungnahme des EDSA zum Entwurf einer CSAM-Verordnung, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

53 Informationen zum Konsultationsverfahren, abrufbar unter: https://bfdi.bund.de/konsultation-2021

4.4.3 EDSA-Richtlinien zum Einsatz von Gesichtserkennungstechnologie

Der Europäische Datenschutzausschuss (EDSA) hat Richtlinien für den Einsatz von Gesichtserkennungstechnologie durch Gefahrenabwehr- und Strafverfolgungsbehörden veröffentlicht. Die Ergebnisse der öffentlichen Konsultation erlauben eine positive Zwischenbilanz.

Der EDSA hat im Mai 2022 umfangreiche Richtlinien zum Einsatz von Gesichtserkennungstechnologie durch Gefahrenabwehr- und Strafverfolgungsbehörden zur öffentlichen Konsultation bekannt gemacht. Sie sind über die Website des EDSA und zunächst nur in englischer Sprache verfügbar („Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement"). Ebenso sind dort sämtliche Beiträge aus der öffentlichen Konsultation abrufbar.

Die Richtlinien führen zunächst in die Funktionsweise und die Anwendungsfelder von Gesichtserkennungstechnologie ein und gehen sodann auf die relevanten rechtlichen Grundlagen ein. Hierbei liegt der Fokus auf den Besonderheiten, die in diesem Kontext für Gefahrenabwehr- und Polizeibehörden gelten. Außerdem enthalten die Richtlinien ergänzende Arbeitshilfen, etwa für die Planung und Durchführung von Projekten mit Gesichtserkennungstechnologie, und eine Darstellung von praxisnahen Beispielen.

Die Nutzung automatisierter Gesichtserkennung durch Gefahrenabwehr- und Strafverfolgungsbehörden wie etwa die Polizei birgt – neben den bekannten Problemen falscher Ergebnisse und möglicher Diskriminierung – auch ein enormes Missbrauchspotential (30. TB Nr. 4.2). Ich unterstütze daher ausdrücklich, dass der EDSA in diesen Richtlinien erneut seine Forderungen bekräftigt, die er bereits in seiner Stellungnahme zum KI-Regulierungsentwurf der EU-Kommission vertreten hat (30. TB Nr. 4.2.1). Hierzu gehören insbesondere das allgemeine Verbot der biometrischen Fern-Identifikation in öffentlich-zugänglichen Räumen und die Anwendung von Gesichtserkennungstechnologie auf unterschiedslos erhobene Massendatensammlungen.

Im Wege der Öffentlichkeitsbeteiligung haben nun zahlreiche NGOs und mitgliedstaatliche Polizei- und Regierungsstellen, aber auch Akteure aus Wissenschaft und Wirtschaft, zu diesem ersten Entwurf der Richtlinien Stellung genommen. Das Gesamtbild der Beiträge erlaubt eine positive Zwischenbilanz und zeigt, dass die Richtlinien bereits in der aktuellen Form im Wesentlichen unterstützt und gutgeheißen werden. Die Beiträge beleuchten den Entwurf aus unterschiedlichsten Perspektiven und bieten so eine wertvolle Quelle für die weitere Verbesserung der Richtlinien.

In diesem Sinne werde ich mich beim EDSA weiter für die Berücksichtigung der Erkenntnisse aus der öffentlichen Konsultation und die Finalisierung der Richtlinien einsetzen. An der Erstellung der Richtlinien war ich federführend beteiligt.

Querverweise:

4.4.2 Ergebnisse Konsultationsverfahren zur Künstlichen Intelligenz

4.5 Evaluierung der JI-Richtlinie und unzureichende Abhilfebefugnisse des BfDI in den Bereichen der Gefahrenabwehr und der Strafverfolgung

Am 25. Juli 2022 hat die Europäische Kommission ihren ersten Bericht zur Evaluierung der JI-Richtlinie veröffentlicht. Hierzu hatte sie den EDSA vorab konsultiert. Insgesamt zieht die Kommission eine positive Bilanz. Gleichwohl stellt sie auch Defizite bei der Umsetzung, z. B. in Deutschland, fest. In diesem Zusammenhang wurden im Sommer 2022 zwei Vertragsverletzungsverfahren gegen die Bundesrepublik eröffnet.

Knapp sechs Jahre nach dem Inkrafttreten der JI-Richtlinie legte die Europäische Kommission dem Europäischen Parlament und dem Rat Ende 2021 erstmals einen Bericht über die Umsetzung der JI-Richtlinie in den Mitgliedstaaten vor.[54] Bei dessen Vorbereitung hatte die Kommission im vergangenen Jahr u. a. den EDSA beteiligt. Unter meiner Mitwirkung ist ein Beitrag des EDSA zur Evaluierung erarbeitet worden, der im Dezember 2021 vom EDSA-Plenum verabschiedet wurde.[55] Die Europäische Kommission griff zahlreiche Empfehlungen des EDSA in ihrem Bericht auf. So wurde z. B. übereinstimmend darauf hingewiesen, dass die wirksame Umsetzung der in der JI-Richtlinie vorgesehenen Aufgaben die Verfügbarkeit ausreichender personeller und technischer Ressourcen voraussetzt. Außerdem müssten die Mitgliedstaaten dafür Sorge tragen, dass die

54 Bericht zur Umsetzung der JI-Richtlinie, abrufbar unter https://ec.europa.eu/info/files/communication-first-report-application-and-functioning-data-protection-law-enforcement-directive-eu-2016-680-led_en

55 Evaluierung durch den EDSA, abrufbar unter: https://edpb.europa.eu/news/news/2021/edpb-adopts-contribution-evaluation-law-enforcement-directive-spe-project-plan_de

Ressourcen der Aufsichtsbehörden entsprechend ihrer Arbeitslast aufgestockt werden.

Auch wenn die Erfahrungswerte aufgrund der kurzen Zeit seit ihrem Inkrafttreten noch begrenzt seien, stellt die Europäische Kommission insgesamt fest, dass die JI-Richtlinie in einem hohen Maß zur Sensibilisierung und Stärkung des Bewusstseins für den Datenschutz bei den zuständigen Behörden beigetragen habe und grundsätzlich ein hohes Datenschutzniveau gewährleiste.

Im Hinblick auf die im Rahmen grenzüberschreitender Zusammenarbeit von Strafverfolgungsbehörden zunehmende Zahl an Datenübermittlung in Drittländer wird die Bedeutung der JI-Richtlinie für den Schutz personenbezogener Daten hervorgehoben. Insbesondere die laufenden Arbeiten an den Leitlinien zu Art. 37 JI-Richtlinie (Datenübermittlung vorbehaltlich geeigneter Garantien), an denen ich als Hauptberichterstatter beteiligt bin, werden als wichtige Hilfestellung für die zuständigen Behörden erwähnt. Zum Teil bestünden jedoch noch Defizite bei der Umsetzung in nationale Rechtsvorschriften. Die Kommission kündigt diesbezüglich an, die Umsetzung der JI-Richtlinie in den Mitgliedstaaten weiter fortlaufend zu überwachen und auf eine vollständige Umsetzung in den Mitgliedstaaten mit den ihr zur Verfügung stehenden Mitteln hinzuwirken. Auch der EDSA hatte in seinem Evaluierungsbeitrag darauf hingewiesen, dass die Umsetzung der JI-Richtlinie noch nicht in allen Mitgliedstaaten abgeschlossen ist bzw. nationale Vorschriften die Vorgaben der JI-Richtlinie nur unzureichend umsetzen.

In diesem Zusammenhang hat die Europäische Kommission gegen Deutschland zwei Vertragsverletzungsverfahren eingeleitet.

Das erste Verfahren wurde im April 2022 eröffnet. Die Europäische Kommission moniert hierin, dass eine Umsetzung der JI-Richtlinie im Bereich der Bundespolizei bisher vollständig unterblieben ist. Das geltende Bundespolizeigesetz wird derzeit überarbeitet und soll durch eine Neufassung abgelöst werden. Der Gesetzgebungsprozess hierzu ist bei Redaktionsschluss noch nicht abgeschlossen.

Das zweite Verfahren wurde im Mai 2022 eröffnet. Die Europäische Kommission moniert hier die mangelhafte Umsetzung des Art. 47 Abs. 2 JI-Richtlinie. Dieser sieht vor, dass Datenschutzaufsichtsbehörden über wirksame Abhilfebefugnisse verfügen müssen. Diesen Anforderungen würden die Vorschriften, die der Umsetzung der JI-Richtlinie auf Bundesebene dienen, insgesamt nicht gerecht. Gleiches gelte für die Umsetzung in einer Vielzahl von Bundesländern.

Meiner bereits im 26. Tätigkeitsbericht 2015 – 2016 ausgesprochenen Empfehlung, die Befugnisse der Aufsichtsbehörden im Anwendungsbereich der JI-Richtlinie analog der DSGVO zu regeln (vgl. 26. TB Nr. 1.2.2), ist der Gesetzgeber auf Bundesebene bisher nicht gefolgt. So wurden in § 16 Abs. 2 BDSG zwar Informations- und Untersuchungsbefugnisse vorgesehen. Bei der Abhilfe bleibe ich nach dieser Vorschrift jedoch auf eine präventive Warnung gegenüber dem Verantwortlichen oder einer rechtlich nicht verbindlichen Beanstandung gegenüber der zuständigen obersten Bundesbehörde beschränkt. Die aktuellen Fassungen des Bundeskriminalamtsgesetzes (BKAG) und des Zollfahndungsdienstgesetzes (ZfDG) sehen zwar ergänzend zu den Vorschriften des BDSG eine Anordnungsbefugnis vor. Diese kann jedoch erst nach Beanstandung und nur bei „erheblichen Datenschutzverstößen“ erfolgen. Das Bundesinnenministerium bestreitet unter Bezugnahme auf die jeweiligen Gesetzesbegründungen zudem, dass die Anordnungsbefugnis auch die Löschung von rechtswidrig verarbeiteten personenbezogenen Daten umfasst (vgl. Begründung, BT-Drucksache 18/11163, S. 130).

Ich begrüße daher die Initiativen der Europäischen Kommission, mit denen sie auf eine richtlinienkonforme Umsetzung in Deutschland hinwirkt. Dabei kommt es mir insbesondere auf eine Umsetzung der Aufsichtsbefugnisse im deutschen Recht an, die rechtssicher gewährleistet, dass ich als Aufsichtsbehörde bei rechtswidrigen Datenverarbeitungen umfassend und wirksam Abhilfe schaffen kann.

5 Gesetzgebung

Auch im Jahr 2022 stand die Gesetzgebung nicht still. Nach der Geschäftsordnung der Bundesministerien bin ich als Bundesbeauftragter frühzeitig an allen Vorhaben zu beteiligen, die meinen Aufgabenbereich, also die Verarbeitung personenbezogener Daten, betreffen. Leider erfolgte eine Einbeziehung oft nicht zeitnah, was ich wiederholt in Fällen kritisieren musste. Dabei liegt es auf der Hand, dass eine frühe Einbindung meines Hauses nicht nur mir Möglichkeit gibt, schon in der Entwurfsphase auf grundrechtsfreundliche Regelungen hinzuwirken, sondern auch die Verfasser vor falschen Vorab-Grundsatzentscheidungen schützt, die später nur mit viel zeitlichem und finanziellem Aufwand korrigiert werden können.

Insbesondere infolge der Digitalisierung nahm die Gesetzgebungsaktivität und damit meine Beratungstätigkeit weiter zu:

So hat sich meine Behörde im Jahr 2022 mit 119 Gesetzentwürfen, 109 Verordnungen, 33 Richtlinien und 12 sonstigen Vorhaben befasst, die national, aber auch durch die EU, auf den Weg gebracht wurden. Die Beratung reicht dabei von einem ersten Austausch zu Eckpunkten über Referentenentwürfe bis hin zur Begleitung im parlamentarischen Beratungsverfahren mit ausführlichen Stellungnahmen an den Bundestag einschließlich der Mitwirkung bei Öffentlichen Anhörungen. Eine Beratung erfolgt dabei je nach Stadium und Beratungswunsch informell bzw. vertraulich, wie auch öffentlich. Die nachfolgenden Beispiele besonders relevanter Gesetzgebungsberatungen sind exemplarisch und bilden hierbei nur einen sehr kleinen Teil der täglichen Beratungsarbeit meines Hauses ab.

5.1 European Health Data Space

Mit dem European Health Data Space (EHDS) soll ein gemeinsamer europäischer Regelungsrahmen für die Nutzung und den Austausch von Gesundheitsdaten geschaffen werden. Er birgt Chancen für die Stärkung der Gesundheitsversorgung sowie der medizinischen Forschung, ist aber auch eine datenschutzrechtliche Herausforderung.

Die EU-Kommission hat am 3. Mai 2022 ihren Entwurf für einen „Rechtsakt über einen europäischen Raum für Gesundheitsdaten“ vorgestellt. Der EHDS soll der erste von mehreren sektorspezifischen Datenräumen im Rahmen der europäischen Datenstrategie werden. Mit ihm sollen Bürgerinnen und Bürger über ein digitales interoperables Format die Kontrolle über ihre Gesundheitsdaten erhalten. So sollen sie selbst u. a. auf Rezepte, Laborergebnisse, Entlassungsberichte sowie Impfnachweise zugreifen können. Zudem soll es für sie möglich werden, den Zugang zu ihren Daten gegenüber Leistungserbringern wie Ärzten, Krankenhäusern und Apothekern zu gewähren oder zu beschränken. Das Vorhaben betrifft elektronische Patientenakten, medizinische Softwareprodukte und Wellness-Apps. Daneben sieht der Verordnungsentwurf zahlreiche Regelungen für eine sekundäre Nutzung der Gesundheitsdaten für Forschung und Innovation vor.

Nach der DSGVO unterliegen Gesundheitsdaten einem grundsätzlichen Verarbeitungsverbot, für das jedoch Ausnahmetatbestände vorgesehen sind. Aus datenschutzrechtlicher Sicht ist der EHDS daher von höchster Relevanz.

Innerhalb der EU-Mitgliedstaaten bestehen vollkommen unterschiedliche Gesundheitssysteme, nicht nur im Hinblick auf den Stand der Digitalisierung. Um die Rechte der Bürgerinnen und Bürger sicherzustellen, müssen daher gleichermaßen einheitliche datenschutzrechtliche Standards geschaffen werden. Dies gilt aufgrund des föderalen Systems in Deutschland beispielsweise für die diversen Landeskrankenhausgesetze der einzelnen Bundesländer. Auch in technischer Hinsicht bedarf es einheitlicher Standards, um etwa Interoperabilität zu ermöglichen.

Mit der Stärkung der medizinischen Forschung durch den EHDS bietet sich die Chance der Verbesserung von Behandlungsmöglichkeiten insbesondere schwerer Er-

krankungen. Allerdings muss hierfür den Freiheitsrechten der Bürgerinnen und Bürger ausreichend Rechnung getragen werden, was bislang im EHDS-Verordnungsentwurf nicht hinreichend geschieht. In meinen bisherigen Stellungnahmen zum Verordnungsentwurf (Stand 3. Mai 2022) habe ich deshalb insbesondere auf folgende Punkte hingewiesen:

- Bürgerinnen und Bürgern muss das Wahlrecht eingeräumt werden, inwieweit sie digitalen Dienste überhaupt nutzen möchten.
- Der EHDS muss vollständig im Einklang zu den Vorschriften der DSGVO stehen; dies betrifft insbesondere die Betroffenenrechte und die Grundsätze der Verhältnismäßigkeit und Datenminimierung.
- Die Sekundärnutzung von Gesundheitsdaten für Forschung und Innovation erfordert die aktive Mitwirkung der Betroffenen. Es ist also entweder ihre Einwilligung einzuholen oder ihnen muss zumindest ein bedingungsloses Widerspruchsrecht eingeräumt werden.
- Der Verordnungsentwurf benötigt überdies dringend inhaltlicher Anpassungen. Hierbei geht es um die Legaldefinitionen, die Mindestkategorien von Gesundheitsdaten für die Sekundärnutzung und die Rolle der datenschutzrechtlichen Aufsichtsbehörden.

Das Gesetzgebungsverfahren soll mit Zustimmung des Rates und Billigung durch das EU-Parlament im Jahr 2024 abgeschlossen sein und der EHDS dann im Jahr 2025 in Kraft treten. Ich werde mich auch weiterhin dafür einsetzen, dass das Recht auf informationelle Selbstbestimmung gerade im Bereich sensibler Verarbeitungen gewahrt bleibt.

5.2 Regelungen zur Bewältigung der COVID-19-Pandemie

Auch im „Jahr 3" der Pandemie gab es neue Regelungen zur Pandemiebekämpfung mit neuen datenschutzrechtlichen Herausforderungen. In den Verfahren waren Stellungnahmefristen oft viel zu kurz. Die Zahl stetiger Änderungen und Anpassungen sowie teils rudimentäre Begründungen erschwerten es mir zusätzlich, die Bundesregierung sachgerecht zu beraten und gefährdeten auch die Qualität der Gesetzgebung.

Im Juni 2022 übersandte das Bundesministerium für Gesundheit (BMG) in Vorbereitung auf die COVID-19-Situation im bevorstehenden Herbst und Winter einen ersten Entwurf einer Formulierungshilfe zum Gesetz zur Stärkung des Schutzes der Bevölkerung und insbesondere vulnerabler Personengruppen vor COVID-19 (COVID-19-SchG). Verschiedene Änderungen und Überarbeitungen erreichten mich im Laufe des Verfahrens zwar regelmäßig, allerdings waren die Stellungnahmefristen oft viel zu kurz. Eine Unsitte, die ich schon im Vorjahr kritisierte; für dieses Jahr hatte ich allerdings auf eine Rückkehr zu einem ordentlichen Verfahren mit angemessenen Fristsetzungen gehofft – leider vergeblich. Zu den Ärgernissen, die mir eine Prüfung und Beratung erheblich erschwerten, gehörte beispielsweise, dass das BMG in Einzelfällen Anpassungen am Wochenende oder mitten in der Nacht und ohne Vorankündigung mit Fristen von nur wenigen Stunden versandte. Hinzu kam, dass in den aktualisierten Entwurfsfassungen die Hintergründe der Anpassungen oft nicht nachvollziehbar dargestellt wurden.

Die Bewältigung der COVID-19-Epidemie kommt nicht ohne pandemische Maßnahmen wie beispielsweise das Impfen und Testen und damit einhergehender zahlreicher Erhebungen, Speicherungen, Übermittlungen und Auswertungen von Gesundheitsdaten aus. Diese unterliegen aus gutem Grunde einem besonderen Schutz gemäß der Datenschutz-Grundverordnung. Für die notwendige Rechtssicherheit, gebotene datenschutzrechtliche Integrität und letztlich Akzeptanz der Prozesse sollte deshalb eine frühzeitige, transparente und konstruktive Einbindung meines Hauses eigentlich selbstverständlich und originäres Interesse Aller sein. Bei sachgemäßen Fristen ist es auch möglich, rechtskonforme und datenschutzfreundlichere Alternativen zu kritischen Vorschlägen zu entwickeln und anzubieten, die dann auch einer möglichen gerichtlichen Überprüfung standhalten.

Beschäftigtendatenschutz

Zumindest beim Beschäftigtendatenschutz ist erfreulich, dass meine Kritik wegen ursprünglich zu unbestimmter und weiter Formulierungen in §§ 34 ff. Infektionsschutzgesetz (IfSG) des ersten Entwurfes des COVID-19-SchG letztlich aufgegriffen wurde. So sollte § 23a IfSG zunächst gestrichen werden und durch allgemeine, zu umfassende Arbeitgeberbefugnisse zur Verarbeitung von sowohl Testdaten als auch Daten zum Impf- und Zerostatus von Beschäftigten in Bezug auf nicht hinreichend bestimmte Krankheiten ersetzt werden. In der Endfassung des Änderungsgesetzes wurde diese Verarbeitungsbefugnis schließlich auf Einrichtungen der Pflege und Eingliederungshilfe begrenzt, bestimmter formuliert und auf 2G-Daten beschränkt. Die Vorschrift des § 23a IfSG wurde zudem beibehalten.

Die allgemeine Befugnis von Arbeitgeberinnen und Arbeitgeber zur Verarbeitung von 3G-Daten („geimpft, genesen, getestet") vor Zutritt zur Arbeitsstätte gemäß § 28b IfSG, die mit dem Gesetz zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze anlässlich der

Aufhebung der Feststellung der epidemischen Lage von nationaler Tragweite“ vom 22. November 2021 (29. TB Nr. 4.1.4). eingefügt worden war, ist überdies weggefallen. Sie galt nur bis einschließlich 19. März 2022. Alle bisher auf dieser Grundlage erhobenen 3G-Daten waren zu löschen. Seitdem sind allgemeine 3 G-Zutrittskontrollen auf der Grundlage des Infektionsschutzgesetzes nicht mehr zulässig. In Einzelfällen bestehen indes weiterhin spezifische gesetzliche Ermächtigungsgrundlagen zur Verarbeitung beispielsweise von 2G-Daten der Beschäftigten durch Arbeitgeberinnen und Arbeitgeber, wie im Rahmen des § 23a InfSG oder bei der einrichtungsbezogenen Impfpflicht nach § 20a InfSG.

Ich habe stets darauf hingewiesen, dass die Verarbeitung sensibler 3G-Daten Beschäftigter nur in den gesetzlich geregelten Fällen zulässig ist. Aus der Fürsorgepflicht des Arbeitgebers in Verbindung mit § 26 Abs. 3 BDSG ergibt sich keine Möglichkeit, Gesundheitsdaten Beschäftigter zu verarbeiten.

Bei der Meldung der Corona-Tests befand sich im Gesetzentwurf zunächst eine fallbezogene Meldepflicht für negative Testergebnisse. Eine solche Meldung mit Pseudonym war bereits mit dem Zweiten Pandemie-Schutz-Gesetz – entgegen meiner Empfehlung – eingeführt und mit dem Dritten Pandemie-Schutz-Gesetz wieder aufgehoben worden (29. TB Nr. 4.1.4). Auch im aktuellen Anlauf konnten die rein statistischen Erwägungen in der Begründung lediglich eine Erhebung der Anzahl erklären, nicht aber eine zuordenbare, fallbezogene Erfassung. Tatsächlich wurde dann auf die Angabe einer fallbezogenen Pseudonymisierung aber verzichtet.

Die Bundesregierung nutzte das COVID-19-SchG leider nicht, um wesentliche Maßnahmen und grundlegende Regelungen im Zusammenhang mit den Herausforderungen mit COVID-19 auf gesetzliche Regelungen stützen zu können. So wurde mit der Novellierung des Infektionsschutzgesetzes die Möglichkeit geschaffen, Zutrittsbeschränkungen in Verbindung mit Kontrollen von 3G-Nachweisen zu ermöglichen, sofern eine epidemische Lage von nationaler Bedeutung vom Bundestag festgestellt wurde. Ich hatte empfohlen, die situative Zulässigkeit von Zutrittsbeschränkungen infolge von 3G-Nachweiskontrollen im Gesetz zu regeln, da dies aus Gründen der Rechtsklarheit und Rechtssicherheit zweckmäßig ist und insbesondere für öffentliche Stellen erforderlich sein kann. Daran anknüpfend wären fehlende, aber aus datenschutzrechtlicher Sicht zwingende Vorgaben zur Vertraulichkeit für die entsprechenden Datenverarbeitungsvorgänge durch Private in der Gesetzesnovellierung vorzusehen gewesen.

Wie der Bericht des Sachverständigenausschusses nach § 5 Abs. 9 IfSG – Evaluation der Rechtsgrundlagen und Maßnahmen der Pandemiepolitik – hatte auch ich anlässlich des Erlasses von Rechtsverordnungen wiederholt gesetzliche anstelle von Regelungen im Verordnungswege gefordert. Aus dem verfassungsrechtlichen Wesentlichkeitsgebot ergibt sich, dass der Gesetzgeber selbst Zweck, Umfang und Art der Eingriffe in das informationelle Selbstbestimmungsrecht regelt. So hätte ich es mehr als begrüßt, wenn die Bundesregierung etwa die Gelegenheit mit dem COVID-19-SchG genutzt hätte, die maßgeblichen Regelungen aus der Verordnung zum Schutz vor einreisebedingten Infektionsgefahren in Bezug auf das Coronavirus SARS-CoV-2, welche Einreisende zur Übermittlung der 3G-Nachweise an Beförderer verpflichtete und den Beförderern eine entsprechende Kontrollpflicht auferlegte, in gesetzliche Regelungen zu überführen. Vorgaben zur Vertraulichkeit hinsichtlich der Datenverarbeitungen im Zusammenhang mit den 3G-Nachweisen wurden den Befördern dabei nicht gemacht. Hier wurde dem erhöhten Schutzniveau dieser Gesundheitsdaten erneut nicht angemessen Rechnung getragen. Auch im Zusammenspiel mit den Prüfungen der 3G-Nachweise durch die Bundespolizei sowie der elektronischen Einreiseanmeldungen ergaben sich doppelte Datenerhebungen und -speicherungen, welche durchaus datenschutzkonform hätten gefasst werden können.

Ich erneuere an dieser Stelle mein wiederholt geäußertes Angebot, aber auch meine Erwartung an die Bundesregierung, mich frühzeitig zu beteiligen und mir nicht kursorische Prüfungen, sondern eine umfassende, verlässliche Beratung getreu meinem gesetzlichen Auftrag zu ermöglichen.

5.3 Änderungen bei der Geldwäschebekämpfung und der Durchsetzung von Sanktionen

In den letzten Jahren beschäftigten mich mehrere Gesetzgebungsverfahren zum Geldwäschegesetz (GwG) mit Befugniserweiterungen für die Financial Intelligence Unit (FIU). Mit dem Sanktionsdurchsetzungsgesetz II soll nun eine Zentralstelle für Sanktionsdurchsetzung mit umfangreichen Befugnissen zur Verarbeitung personenbezogener Daten errichtet werden. Datenschutzvorgaben wurden dabei allerdings wie zuvor nur unzureichend berücksichtigt.

Die Bekämpfung von Geldwäsche und Terrorismusfinanzierung stellt einen legitimen Zweck dar, der grundsätzlich geeignet ist, auch schwerwiegende Grundrechtseingriffe zu rechtfertigen. Allerdings hat das GwG in den letzten Jahren eine Reihe von Änderungen erfahren, die

gegen wesentliche Grundsätze des Datenschutzrechtes verstoßen.

Durch das Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG) vom 2. Juni 2021 wurde der FIU die Befugnis eingeräumt, steuerliche Grunddaten, die sie bislang nur im Wege von Einzelersuchen bei den Finanzbehörden erfragen konnte, automatisiert abzurufen. Im Rahmen des Gesetzgebungsverfahrens habe ich mich kritisch hierzu geäußert. Die durch das FISG geänderte Regelung des § 30 Abs. 5 GwG verstößt aus meiner Sicht gegen den Verhältnismäßigkeitsgrundsatz, da sie pauschal allein auf die Aufgabenwahrnehmung der FIU abstellt und darüber hinaus keinerlei begrenzende Eingriffsschwellen aufstellt.

Auch das Ziel der effektiven Durchsetzung von Sanktionen hat nicht zuletzt wegen des Angriffskrieges gegen die Ukraine meine volle Unterstützung. Allerdings enthielt das Sanktionsdurchsetzungsgesetz I nochmals eine problematische Befugniserweiterung der FIU. Diese kann nun auch unabhängig vom Vorliegen einer Geldwäscheverdachtsmeldung nach eigenem Ermessen weitere Analysen durchführen. Die nähere Ausgestaltung der geplanten Auswertungen, mögliche Anlässe, die einzubeziehenden Daten und die zulässigen Zwecke bleiben im Gesetz unklar, was mit dem Gebot der Normenklarheit- und -Bestimmtheit nicht zu vereinbaren ist. Eine konsequente Anpassung des GwG an die Vorgaben der Richtlinie (EU) 2016/680 (JI-Richtlinie) und die verfassungsgerichtliche Rechtsprechung zum Recht auf informationelle Selbstbestimmung ist dagegen bisher ausgeblieben. Da die Frist zur Umsetzung der JI-Richtlinie bereits im Mai 2018 abgelaufen ist, sehe ich eine Umsetzung im GwG auch im Interesse der Bundesregierung.

Mit dem Sanktionsdurchsetzungsgesetz II wurde jüngst eine Zentralstelle für Sanktionsdurchsetzung (ZfS) geschaffen, die eine Vielzahl personenbezogener Daten verarbeiten darf. Sie erhält u. a. Zugang zu polizeilichen und nachrichtendienstlichen Informationen. Zudem sollen personenbezogene Immobiliendaten mithilfe des Transparenzregisters verfügbar werden. Bei diesem befürchte ich, dass es zweckwidrig genutzt werden könnte, um die Fertigstellung des länderseitigen elektronischen Datenbankgrundbuchs zu überbrücken. Zwar konnten im Rahmen des Gesetzgebungsverfahrens einige Verbesserungen beim Datenschutz erreicht werden. So darf beispielsweise eine Zusammenarbeit der ZfS mit den Nachrichtendiensten nur noch dann erfolgen, wenn tatsächliche Anhaltspunkte für bestimmte, besonders schwere Straftaten vorliegen. Insgesamt weist das am 1. Dezember 2022 beschlossene Gesetz aber noch immer erhebliche datenschutzrechtliche Defizite auf.

Insgesamt empfehle ich dringend, sowohl das GwG als auch das Sanktionsdurchsetzungsgesetz datenschutzrechtlichen Vorgaben anzupassen.

5.4 Hinweisgeberschutzgesetz

Der Bundestag hat am 16. Dezember 2022 einen besseren Schutz hinweisgebender Personen im beruflichen Umfeld (sog. Whistleblower) beschlossen.

Mit dem am 16. Dezember 2022 verabschiedeten Gesetz wurde die Richtlinie 2019/1937 RL (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblowing-RL – WBRL) in nationales Recht umgesetzt. Die Richtlinie schafft erstmals unionsweite Mindeststandards zum individuellen Schutz von Whistleblowern und zum institutionellen Umgang mit den von ihnen weitergegebenen Insider-Informationen. Die Bundesregierung will damit Hinweisgeberinnen und Hinweisgeber (Whistleblower) im beruflichen Umfeld besser schützen. Wer verfassungsfeindliche Äußerungen oder sonstige Verstöße gegen nationale oder europäische Rechtsvorschriften im Zusammenhang mit der beruflichen Tätigkeit meldet, fällt nun unter das Hinweisgeberschutzgesetz und wird damit vor Repressalien geschützt. Im Mittelpunkt des Gesetzes steht die Ausgestaltung der internen und externen Meldestellen, die hinweisgebenden Personen wahlweise eine Anlaufstelle für ihre Meldungen bieten. Die Identität der hinweisgebenden Person ist in beiden Fällen vertraulich zu behandeln. Dabei soll zwar auch die Möglichkeit bestehen, anonyme Hinweise abzugeben. Sollte die Meldestelle den Hinweis nicht innerhalb einer bestimmten Frist bearbeitet haben oder der Hinweisgeber begründet davon ausgehen können, dass die Informationen eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses darstellen können, greifen die neu geschaffenen Schutzregelungen auch dann, wenn die hinweisgebende Person die Information öffentlich bekannt gibt.

Bei einem Verstoß gegen das Verbot von Repressalien besteht künftig eine Schadensersatzpflicht durch den Verursacher. Geahndet wird auch, wenn ein Unternehmen trotz gesetzlicher Verpflichtung keine interne Meldestelle einrichtet oder die Kommunikation zwischen Hinweisgeber und Meldestelle behindert wird.

Ich begrüße die Umsetzung der WBRL. Privatpersonen, die bereit sind, aus eigenem Antrieb Rechtsverstöße und gravierende Missstände aus ihrem beruflichen Arbeitsumfeld zu melden, handeln im Interesse demokratischer und rechtsstaatlicher Gesellschaften. Hinweisgeberinnen und Hinweisgeber leisten damit

einen Beitrag zu mehr Transparenz und zur Stärkung der Informationsfreiheit in für die Öffentlichkeit weitgehend intransparenten, aber für zentrale gesellschaftliche Ziele und Werte oft außerordentlich folgenreichen Beschäftigungsbereichen. Dies betrifft auch und gerade Missstände im Umgang mit persönlichen Informationen und Daten der Bürgerinnen und Bürger bei staatlichen wie auch nicht-staatlichen Stellen gleichermaßen. Bei den Meldungen durch die Hinweisgeber werden eine Reihe von personenbezogenen Daten verarbeitet.

Ich begrüße, dass der sachliche Anwendungsbereich zumindest in begrenztem Umfang auf korrespondierendes nationales Recht ausgeweitet und dabei insbesondere Hinweise auf Verstöße gegen sämtliche Verbotsnormen des Strafrechts und das Recht der Ordnungswidrigkeiten mit aufgenommen wurden. Damit werden Wertungswidersprüche vermieden und die praktische Anwendung des Gesetzes für hinweisgebende Personen handhabbarer gestaltet.

5.5 Dienste zur Einwilligungsverwaltung

Auch über ein Jahr nach dem Inkrafttreten des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) gibt es keine Rechtsverordnung über „Anerkannte Dienste zur Einwilligungsverwaltung", mit denen Internetnutzende ihre Einwilligungen z. B. in Cookies nutzerfreundlich verwalten können sollen.

In meinem letzten Tätigkeitsbericht (30. TB Nr. 5.1) habe ich über das Inkrafttreten des TTDSG am 1. Dezember 2021 berichtet. Erfreulich ist, dass mit § 25 TTDSG die Vorgabe der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) richtlinienkonform umgesetzt wurde, wonach eine Speicherung von Informationen auf Endgeräten oder der Zugriff auf dort bereits gespeicherte Informationen – etwa durch Cookies – grundsätzlich einer Einwilligung bedürfen. Mit § 26 TTDSG wurde zugleich die Möglichkeit der Nutzung anerkannter Dienste zur Einwilligungsverwaltung eingeführt. Mit ihnen sollen Internetnutzende Einwilligungen (und damit auch Verweigerung von Einwilligungen) nutzerfreundlich verwalten können. Den damit verfolgten Ansatz, „Cookie-Banner" einzudämmen, begrüße ich ausdrücklich. Eine Herabsetzung von Datenschutzstandards darf mit solchen Diensten aber nicht einhergehen und sie dürfen nicht als Mittel gesehen werden, mehr und eigentlich ungewollte Einwilligungen zu erreichen.

Bevor anerkannte Dienste zur Einwilligungsverwaltung auf den Markt kommen können, muss eine Rechtsverordnung die Anforderungen an solche Dienste und das Verfahren ihrer Anerkennung regeln. Im Sommer dieses Jahres wurde zwar ein erster Entwurf vorgelegt. Noch bevor es allerdings zu einer Ressortabstimmung kam, haben mehrere Ressorts und auch ich wegen erheblicher Bedenken eindringlich eine umfassende Überarbeitung gefordert. In Anbetracht dessen, dass mehrere Datenschutzgrundsätze in Frage gestellt wurden, habe ich mich zugleich gegen eine Veröffentlichung des unzureichenden Entwurfs ausgesprochen.

Als unionsrechtswidrig habe ich eine Abweichung von zwingenden Anforderungen der DSGVO kritisiert. Untauglich zur Eindämmung von Cookie-Bannern ist überdies die Verortung der anerkannten Dienste zur Einwilligungsverwaltung im TTDSG, weil eine solche Rechtsverordnung naturgemäß allein Einwilligungen nach § 25 TTDSG regeln kann. Nicht regelbar bleiben dabei Einwilligungen nach Art. 6 Abs. 1 lit. a) DSGVO, wie sie für eine Weiterverarbeitung der durch Cookies erhobenen Daten etwa zu Marketingzwecken erforderlich sein können.

Meine Empfehlung für Bundesbehörden, aber nicht nur diese, lautet daher weiterhin, Cookies und ähnliche Technologien nur dann einzusetzen, wenn dies technisch unabdingbar ist, um den von Nutzenden ausdrücklich gewünschten Telemediendienst zur Verfügung zu stellen. In diesem Fall ist nach § 25 Abs. 2 Nr. 2 TTDSG weder eine Einwilligung noch ein „Cookie-Banner" erforderlich. Leider muss ich immer wieder feststellen, dass auf den Websites von Bundesbehörden – und noch häufiger auf Subsites für Sondersituationen und Kampagnen – u. a. Cookies zu finden sind, weil diese Websites und Subsites aus Baukastensystemen zusammengestellt wurden.

Weitere Informationen zu den rechtlichen Anforderungen des Einsatzes von Cookies und ähnlicher Technologien sind in der „Orientierungshilfe Telemedien" der DSK zu finden.[56]

Ich empfehle die Einführung von Datentreuhändern auf Basis des TTDSG grundsätzlich zu überarbeiten und DSGVO-konform umzusetzen.

56 Orientierungshilfe vom 7. Dezember 2022, abrufbar unter: https://www.bfdi.bund.de/orientierungshilfen

5.6 Neues EES- und ETIAS-Durchführungsgesetz

Zur Umsetzung der EES- und der ETIAS-Verordnungen hat die Bundesregierung einen Gesetzentwurf vorgelegt, wodurch zahlreiche bestehende Gesetze geändert und neue Gesetze geschaffen werden. Auch Nachrichtendienste sollen auf die künftigen EU-Großsysteme zugreifen können.

Auf EU-Ebene sollen im Jahr 2023 zwei neue IT-Großsysteme in Betrieb genommen werden. Das ist einerseits das europäische Ein- und Ausreisesystem (EES) und andererseits das europäische Reiseinformations- und -genehmigungssystem (ETIAS). Hierfür sind auf nationaler Ebene zahlreiche Durchführungsvorschriften erforderlich, wie etwa zur Klärung von Zuständigkeiten und Befugnissen. Geregelt werden müssen aber auch etwa die Übermittlung personenbezogener Daten zwischen den zuständigen Behörden und die Sicherstellung, dass Datensätze rechtzeitig aus EES und ETIAS gelöscht werden.

Die Bundesregierung hat im Dezember 2022 den *„Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2017/2226 und der Verordnung (EU) 2018/1240 sowie zur Änderung des Aufenthaltsgesetzes, des Freizügigkeitsgesetzes/EU, des Gesetzes über das Ausländerzentralregister und der Verordnung zur Durchführung des Gesetzes über das Ausländerzentralregister“* im Kabinett angenommen. Dieses sog. EES- und ETIAS-Durchführungsgesetz (EEDG) enthält auch zwei neue Gesetze, das EES-Durchführungsgesetz (EESDG) und das ETIAS-Durchführungsgesetz (ETIASDG).

In der Ressortabstimmung habe ich einige datenschutzrechtliche Verbesserungen erreichen können. Positiv zu erwähnen ist in diesem Verfahren die konstante und konstruktive Beteiligung durch das federführende Bundesinnenministerium. Einige meiner Bedenken konnten allerdings nicht bzw. nicht vollständig ausgeräumt werden. So sieht der Entwurf vor, dass auch die Nachrichtendienste Zugriff auf EES und ETIAS erhalten sollten. Aus meiner Sicht ist jedenfalls fraglich, inwieweit diese Behörden nach deutschem Recht tatsächlich Aufgaben von Gefahrenabwehr- und Strafverfolgungsbehörden im Sinne der beiden EU-Verordnungen wahrnehmen dürfen und sollten. Denn nur für die Erfüllung dieser Aufgaben lassen die europäischen Rechtsakte nach meinem Verständnis eine Zugriffsmöglichkeit von Sicherheitsbehörden zu. In dem noch laufenden Gesetzgebungsverfahren werde ich mich daher weiter aktiv einbringen.

6 Informationsfreiheit

6.1 Konferenz der Informationsfreiheitsbeauftragten

Im Berichtsjahr hatte die Landesbeauftragte für Datenschutz Schleswig-Holstein den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten (IFK) inne. Unter ihrer Ägide widmete sich die IFK im Schwerpunkt technischen Aspekten der Weiterentwicklung staatlicher Transparenz.

Zu den Hauptaufgaben der IFK gehören die Förderung und die Weiterentwicklung des Informationszugangs bei öffentlichen Stellen. In ihrer 42. Sitzung am 30. Juni 2022 in Kiel verabschiedete die IFK zwei Entschließungen.[57]

Zu allen Entschließungen der IFK geht's hier:

(QR-Code scannen oder klicken)

In der Entschließung „SMS in die Akte" wiesen die Informationsfreiheitsbeauftragten darauf hin, dass Behörden mittlerweile vermehrt Kommunikationsformen wie Kurznachrichtendienste, Messenger Dienste, soziale Medien, aber auch SMS nutzen. Auch diese Behördenkommunikation kann eine amtliche Information sein. Laut IFK müssen öffentliche Stellen bei der Nutzung von Kommunikationsmedien stets ihre Dokumentations- und Informationspflichten erfüllen. Die IFK fordert die Verwaltungen in Bund und Ländern auf, auch diese Art der Kommunikation zu dokumentieren, um den Informationszugang zu garantieren.

Mit dem Zugang zu Informationen über die „Stiftung Klima- und Umweltschutz MV" befasste sich die Entschließung „Keine Umgehung der Informationsfreiheit durch Errichtung von Stiftungen bürgerlichen Rechts!". Für die Durchführung und Förderung von Maßnahmen des Umwelt- und Klimaschutzes wurde diese Stiftung durch die Landesregierung Mecklenburg-Vorpommern gegründet. Ein weiteres Ziel war die Fertigstellung der Erdgaspipeline Nord Stream 2. Neben der teilweisen öffentlichen Finanzierung hatte die Landesregierung auch Einfluss auf die personelle Besetzung der Stiftungsgremien. Die Landesregierung und die Stiftung verweigerten der Öffentlichkeit den vollständigen Zugang zu angefragten Informationen. Aus diesem Grunde bekräftigte die IFK, dass auch im Falle der Wahrnehmung öffentlicher Aufgaben durch Stiftungen des bürgerlichen Rechts nach allgemeinem Informationszugangsrecht Transparenz gewährleistet werden muss.

In der Entschließung „Niedersachsen: Die Zeit für ein Transparenzgesetz ist gekommen!" forderte die IFK die an den Koalitionsverhandlungen Beteiligten in Niedersachsen auf, den Erlass eines Transparenzgesetzes in den Koalitionsvertrag aufzunehmen. Das ist geschehen. Neben Bayern ist Niedersachen das letzte Bundesland, in dem es noch keinen voraussetzungslosen Anspruch auf Zugang zu amtlichen Informationen öffentlicher Stellen gibt. Dazu führte die IFK aus, dass öffentliche Stellen in Niedersachsen vergleichbaren Transparenzpflichten unterliegen müssten wie die öffentlichen Stellen anderer Länder und des Bundes.

Darüber hinaus haben sich der Arbeitskreis Informationsfreiheit und die IFK in allen Sitzungen im Berichtsjahr intensiv mit den Themen „Informationsfreiheit by desgin" und der technischen sowie rechtlichen Ausgestaltung von staatlichen Transparenz- und Informationsfreiheitsportalen beschäftigt.

6.2 Erfahrungsaustausch der obersten Bundesbehörden

Am 6. September 2022 hatte ich seit Beginn der Pandemie erstmals wieder zu einem Erfahrungsaustausch der obersten Bundesbehörden zur Praxis der Informationsfreiheit in Präsenz eingeladen.

57 Alle Entschließungen der IFK sind abrufbar unter: www.bfdi.bund.de/ifk-entschließungen

Wir informierten uns gegenseitig über die aktuelle Rechtsprechung, diskutierten praxisrelevante Fragen und boten eine Plattform für den Austausch innerhalb der Kollegenschaft. Gleichzeitig nutzten die Mitarbeiterinnen und Mitarbeiter des in meiner Behörde neu zugeschnittenen Referats Informationsfreiheit diesen Termin, um sich den Kolleginnen und Kollegen aus den obersten Bundesbehörden vorzustellen.

Die Beteiligten haben vereinbart, den Austausch künftig zu intensivieren. Hierfür wird in einem einjährigen Pilotversuch ein quartalweiser Erfahrungsaustausch angeboten. Dieser soll einmal in Jahr in Präsenz in Berlin stattfinden und drei Mal im Jahr in einem verkürzten Format als Videokonferenz. Der erste Erfahrungsaustausch im verkürzten Format fand im Dezember 2022 statt. Ich habe mich sehr über das Interesse an diesem Angebot und über die gehaltvollen Diskussionen gefreut.

6.3 Transparenzgesetz

Seit vielen Jahren fordere ich in meinen Tätigkeitsberichten, das Informationsfreiheitsgesetz (IFG) zu einem Transparenzgesetz weiterzuentwickeln. Dieses Ziel haben SPD, Bündnis 90/Die Grünen und FDP 2021 in ihrem Koalitionsvertrag verankert.

Zugleich sollten das IFG und das Umweltinformationsgesetz (UIG) sowie ggf. das Verbraucherinformationsgesetz zu einem Gesetz mit proaktiven Veröffentlichungspflichten zusammengeführt werden. In einem ersten sinnvollen und überfälligen Schritt müsste dem Recht auf voraussetzungslosen Zugang zu Informationen öffentlicher Stellen Verfassungsrang eingeräumt werden.

Ein Bundestransparenzgesetz kann meines Erachtens heute nur gemeinsam mit der Digitalisierung der Verwaltung gedacht und realisiert werden. Schon bevor Informationen verlangt werden, planen Behörden ihre inneren Abläufe und Strukturen dann so, dass die Informationsbereitstellung innerhalb kürzester Zeit möglich ist. Wenn sie sinnvoll verschlagwortet und maschinenlesbar sind, lassen sich digitalisierte Informationsbestände ohne großen Zeitaufwand durchsuchen. Aus meiner Beratungs- und Kontrollpraxis weiß ich aber, dass nicht wenige Behörden noch immer die klassische Papierakte führen.

Behördliche Informationen und ihre Vorgänge müssen manipulationssicher und vollständig sein. Hier helfen Metadaten, Hinweise zur Datenqualität sowie die Manipulationssicherheit von Daten und Informationen. Ein behördlicher Informationsfreiheitsbeauftragter könnte als zentraler Ansprechpartner beraten und unterstützen. Demnach sollten durch das Transparenzgesetz meiner Meinung nach behördliche Informationsfreiheitsbeauftragte etabliert werden. Letztlich bedeutet „Informationsfreiheit by design“ eine behördliche Kultur der Offenheit und ein klares gesetzgeberisches Bekenntnis dazu.

Kern jedes Transparenzgesetzes ist ein Transparenzportal, auf dem behördliche Informationen ohne Registrierung barrierefrei und mit offenen Lizenzen erlangt werden können. Das Bundestransparenzgesetz braucht einen Katalog veröffentlichungspflichtiger Informationen, der einen Mindeststandard definiert und Raum für die Veröffentlichung weiterer geeigneter Informationen lässt. Weitere zentrale Voraussetzungen sind die Durchsuchbarkeit des Datenbestandes im Transparenzportal, dokumentierte Schnittstellen und die Weiterverwendbarkeit der Informationen.

Entsprechend dem Grundsatz „access for one – access for all“ sollten Informationen, die auf individuellen Antrag hin zugänglich gemacht wurden, grundsätzlich auch im Informationsregister veröffentlicht werden. Weiterhin halte ich eine allgemeine Güterabwägung zwischen Informations- und Geheimhaltungsinteresse, die es im UIG bereits gibt, als zusätzliches Korrektiv für notwendig.

Unabdingbar ist für mich der Gleichklang mit dem Datenschutz und dessen Regelungen und Durchsetzungsmöglichkeiten. Deshalb benötigt der Informationsfreiheitsbeauftragte in einem Bundestransparenzgesetz Anordnungs- und Durchsetzungsbefugnisse. Im Konfliktfall muss der Informationsfreiheitsbeauftragte handlungsfähig sein. Es dem Informationssuchenden zu überlassen, stets den zeit- und kostenintensiven Rechtsweg zu beschreiten, konterkariert die Idee, die hinter allen Informationsfreiheitsgesetzen steht. Im meinen Augen besteht jetzt die Chance für ein modernes, wegweisendes Gesetz, mit dem Deutschland auch in Europa Maßstäbe setzen könnte.

Ich empfehle die Zusammenlegung von Informationsfreiheitsgesetz und Umweltinformationsgesetz (und möglichst auch des Verbraucherinformationsgesetzes) sowie die Weiterentwicklung zu einem Bundestransparenzgesetz mit proaktiven Veröffentlichungspflichten. Der Informationsfreiheitsbeauftragte benötigt in einem Bundestransparenzgesetz Anordnungs- und Durchsetzungsbefugnisse, um im Konfliktfall handlungsfähig zu sein.

6.4 Beratungs- und Kontrollbesuch beim BSI

Anträge unter Berufung auf das Informationsfreiheitsgesetz (IFG) an das Bundesamt für die Sicherheit in der Informationstechnik (BSI) sind häufig auf komplexe technische Sachverhalte gerichtet.

Im November 2022 führte ich einen Beratungs- und Kontrollbesuch beim BSI durch. Aufgrund der großem Zahl an IFG-Anträgen wurde eine umfangreiche Überprüfung der Verfahren aus den Jahren 2018 bis 2022 vorgenommen. Die an das BSI gestellten IFG-Anträge sind häufig auf komplexe technische Aspekte gerichtet. Regelmäßig erfordern die IFG-Anträge die Durchführung eines Drittbeteiligungsverfahrens, da Rechte Dritter betroffen sein können. Zu Details der Verfahrensweise habe ich Hinweise und Anregungen gegeben. Die materiellen sowie die formellen Anforderungen des IFG wurden beachtet. Den Besonderheiten des BSI als Sicherheitsbehörde wurde bei der Beurteilung des Vorliegens von Ausschlussgründen angemessen Rechnung getragen. Die Bearbeitung der IFG-Anträgen erfolgt zentral. Die Auswertung der geprüften Vorgänge zeigte eine effektive und zielgerichtete Zusammenarbeit mit den Fachreferaten. Die Bearbeitung der IFG-Anträge erfolgte insgesamt bürger- und serviceorientiert. Dabei war eine offene Haltung gegenüber der Informationsfreiheit ersichtlich.

6.5 IFG-Vermittlungsverfahren

Jeder kann sich an mich wenden, wenn er sein Recht auf Informationsfreiheit als verletzt ansieht. Im Rahmen meiner Vermittlungstätigkeit erreichten mich im Berichtsjahr deshalb auch eine Vielzahl von Eingaben. Die Vermittlungsverfahren bezogen sich auf vielfältige Themen. Unter anderem hatte ich mich mit der Frage zu beschäftigen, welche Anforderungen an die Bestimmtheit eines IFG-Antrages zu stellen sind. In einem anderen Verfahren war zu klären, ob ein Antrag nach dem Informationsfreiheitsgesetz (IFG) oder dem Umweltinformationsgesetz (UIG) zu bearbeiten war. Aber auch an meine Behörde werden regelmäßig IFG-Anträge gestellt. Einen Antrag musste ich ablehnen, da die Bereichsausnahme für die Geheimdienste auch für meine Behörde gilt. Die im Folgenden angeführten Vermittlungsverfahren stehen beispielhaft für die Arbeit meiner Behörde und sollen spezielle Aspekte beleuchten.

6.5.1 Kampagne zum Lobbyregister

Im Zusammenhang mit einer von dem Verein „Open Knowledge Foundation Deutschland e.V." zusammen mit „abgeordnetenwatch.de" auf der Online-Plattform „Frag den Staat" durchgeführten Kampagne „Lobbyregister selbst gemacht" erreichten mich viele Anrufungen.

Im Rahmen der Kampagne konnten IFG-Anträge zu Treffen von Lobbyverbänden mit Vertretern der Bundesregierung über die Online-Plattform gestellt werden. Diese Plattform hatte vorformulierte Anträge zur Verfügung gestellt, in denen die Adressaten und der Antragsgegenstand bereits vorgegeben waren. Ebenso war eine freie Antragstellung möglich.

Die im Rahmen der Kampagne gestellten IFG-Anträge wurden zum überwiegenden Teil abgelehnt. Im Rahmen meiner Vermittlungstätigkeit stellte ich wiederkehrende Begründungen seitens der angefragten Behörden fest. Unter anderem wurden häufig der Einwand der unzulässigen Rechtsausübung, der Schutz des Kernbereichs exekutiver Eigenverantwortung und die Anforderungen an die Bestimmtheit des Antrages herangezogen. Aus diesem Grund hatte ich mich im Februar 2022 mit einem Rundschreiben an mehrere oberste Bundesbehörden gewandt und Hinweise zum Umgang mit IFG-Anträgen im Rahmen der Kampagne gegeben.[58]

6.5.2 Die Bestimmtheit eines IFG-Antrages

An die Bestimmtheit eines Antrages nach Informationsfreiheitsgesetz (IFG) sind keine zu hohen Anforderungen zu stellen. Im Zweifelsfall ist die Behörde gehalten, den Antragsteller zu unterstützen.

Mit der Bitte um Vermittlung wandte sich ein Petent hinsichtlich eines beim Bundesministerium der Finanzen (BMF) gestellten IFG-Antrages an mich. Der Petent hatte einen weitreichenden Zugangsantrag zu Unterlagen und Informationen über die Mittel aus der Europäischen Aufbau- und Resilienzfazilität gestellt. Das BMF gab dem Petenten den Hinweis, dass nach Auslegung des Antragsbegehrens nicht nur von einem, sondern von vier einzelnen zu unbestimmten Anträgen auszugehen sei. Der Petent nahm eine Präzisierung vor und reduzierte den Antragsgegenstand auf Informationen zu der Vorbereitung der Beratung des Deutschen Aufbau- und Resilienzplans (DARP) im Koalitionsausschuss sowie auf den Konkretisierungs- und Entscheidungsprozess. Sofern das BMF den Antrag des Petenten nicht in zwei Anträge aufspalten sollte, lag seine Bereitschaft zur Kostenübername für die Bearbeitung des Antrages vor.

58 Das Rundschreiben ist abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2022/Rundschreiben-Lobbyregister-selbst-gemacht.pdf

Das BMF lehnte den Antrag schließlich wegen fehlender Bestimmtheit ab und fasste das Begehren als zwei separate Anträge auf. Nach Ansicht des BMF war der Antrag unter einer unzulässigen gebührenrechtlichen Bedingung gestellt worden. Ein nochmals präzisierter Antrag des Petenten wurde unter Hinweis auf die Bestandskraft des zuvor ergangenen Bescheides abgelehnt.

Die Ablehnung des BMF wegen fehlender Bestimmtheit konnte ich nicht nachvollziehen. Es leuchtete nicht ein, dass der Antrag gleichzeitig zu unbestimmt gestellt sein kann, während die inhaltliche Bewertung des BMF mehrere Anträge definierte. Es wäre hier wünschenswert gewesen, dass das BMF dem Petenten konkrete Hinweise erteilt hätte, wie eine Konkretisierung erfolgen könnte. Mangels Kenntnis der einschlägigen Dokumente ist es Antragstellenden oft nicht möglich, Dokumente konkret zu benennen. Deshalb sind keine zu hohen Anforderungen an die Bestimmtheit zu stellen.

Die Ablehnung des Antrages hinsichtlich einer unzulässigen gebührenrechtlichen Bedingung ist aus meiner Sicht diskussionswürdig. Eine für den Petenten günstige Auslegung des Antrages hätte hier zu dem Ergebnis geführt, dass sich der Petent vorsorglich gegen eine gesetzeswidrige (weil abschreckende) Aufspaltung seines Antrages zu wehren gedachte. Das Verbot abschreckender Wirkung ist nicht allein bei der Bemessung der Gebührenhöhe, sondern bereits bei der Bestimmung der einzelnen gebührenpflichtigen Amtshandlung zu beachten. Das BMF folgte meinen Empfehlungen in dieser Vermittlungssache nicht und verweigerte den Informationszugang.

6.5.3 Recht aus Auskunft nach dem Umweltinformationsrecht

Nach dem Umweltinformationsrecht (UIG) haben Bürgerinnen und Bürger Zugang zur Liste der Flüge, die der Bundespräsident in Ausübung seiner Tätigkeit durchgeführt hat.

Ein Petent bat mich bei seinem Antrag an das Bundespräsidialamt um Vermittlung. Gestützt auf das Umweltinformationsrecht hatte er um die Übersendung einer Liste der Flüge des Bundespräsidenten gebeten, die dieser in der Ausübung seines Amtes durchgeführt hat.

Das Bundespräsidialamt legte den Antrag zuerst nach dem Informationsfreiheitsgesetz (IFG) aus und lehnte ihn dann ab. Jedoch findet das IFG bei Informationen, die im Zusammenhang mit den Aufgaben des Bundespräsidenten als Staatsoberhaupt stehen (präsidiale Akte), keine Anwendung. Dabei handelt es sich um spezifisch verfassungsrechtliche Aufgaben. Nach meinem Hinweis an das Bundespräsidialamt, dass es sich bei den Flügen des Bundespräsidenten um Umweltinformationen handeln dürfte und der Antrag entsprechend nach dem UIG zu bewerten wäre, wurde der ursprüngliche Bescheid aufgehoben. Nach dem UIG gibt es weniger Bereichsausnahmen für bestimmte Bundesbehörden oder Bundesorgane. Präsidiale Akte sind im UIG nicht per se vom Informationszugang ausgeschlossen. Andere Ausschlussgründe wurden von dem Bundespräsidialamt nicht angeführt. Dem Petenten wurden die gewünschten Informationen nach dem UIG vollumfänglich zur Verfügung gestellt.

6.5.4 Bahnunfälle auf Schweizer Gebiet – erfolgreiche Vermittlung für eine Petentin

Ein Antrag nach dem Informationsfreiheitsgesetz (IFG) an den Beauftragten für die deutschen Eisenbahnstrecken auf Schweizer Gebiet wurde nach meiner Vermittlung zügig beantwortet.

Im Rahmen eines IFG-Antrags an den Beauftragten für die deutschen Eisenbahnstrecken auf Schweizer Gebiet konnte ich eine erfolgreiche Vermittlung durchführen. Die Petentin bat um Auskunft zu der Anzahl der Eisenbahnbetriebsunfälle, die sich in den Jahren 2017 bis 2022 auf deutschen Eisenbahnstrecken auf Schweizer Gebiet ereignet hatten. Der Beauftragte für die deutschen Eisenbahnstrecken auf Schweizer Gebiet unterliegt als Einrichtung des Bundes dem IFG (§ 1 Abs. 1 Satz 2 IFG). Er ist der Dienststelle Süd des Bundeseisenbahnvermögens zugeordnet. Den Antrag hatte die Petentin über eine Online-Plattform gestellt. Hierbei werden E-Mails mit automatisch generierten Absenderadressen erstellt, die teilweise aus zufälligen Zahlen und Buchstaben bestehen. Die hier auskunftspflichtige Stelle war mit diesen nicht vertraut. Die E-Mail der Petentin wurde deshalb als „verdächtig“ eingestuft und nicht weiter bearbeitet. Entsprechend erreichten auch Nachfragen zum Bearbeitungsstand den Empfänger nicht. Aufgrund meiner Vermittlung bei dem Beauftragten für die deutschen Eisenbahnstrecken auf Schweizer Gebiet konnten Bedenken hinsichtlich der E-Mail-Adresse und des Inhalts rasch ausgeräumt werden. Die gewünschten Informationen wurden der Petentin in der Folge zur Verfügung gestellt.

6.5.5 Die Bereichsausnahme für Nachrichtendienste gilt auch für den BfDI

Soweit meine Funktion als datenschutzrechtliche Kontroll- und Aufsichtsbehörde über die Nachrichtendienste des Bundes betroffen ist, muss auch ich den Informationszugang verweigern.

Nach dem Informationsfreiheitsgesetz (IFG) wurde bei meiner Behörde die Übersendung aller in den Jahren 2008 bis 2021 angefallenen Prüfberichte der Systeme NADIS – „Nachrichtendienstliches Informationssystem“ bzw. seit 2011 NADIS-WN „Nachrichtendienstliches Informationssystem und Wissensnetz“ sowie sämtliche

damit in Verbindung stehende Kommunikation und Dokumente beantragt. Der Antrag wurde abgelehnt.

Ich habe mich dabei darauf berufen, dass nach § 3 Nr. 8 IFG der Anspruch auf Informationszugang gegenüber den Nachrichtendiensten sowie den Behörden und sonstigen öffentlichen Stellen des Bundes nicht besteht, soweit sie Aufgaben im Sinne des § 10 Nr. 3 des Sicherheitsüberprüfungsgesetzes wahrnehmen. Nach mehreren Urteilen des Bundesverwaltungsgerichts sind auch solche Behörden von der Bereichsausnahme erfasst, die aufgrund ihrer Aufgabenstellung in einer besonders engen Beziehung zu den Nachrichtendiensten stehen.[59]

Diese Voraussetzungen sind bezüglich meiner Rolle als datenschutzrechtliche Kontroll- und Aufsichtsbehörde über die Nachrichtendienste des Bundes erfüllt. Mit der Aufgabe als Kontroll- und Aufsichtsbehörde über das Bundesamt für Verfassungsschutz (BfV) ist die Prüfung der Dateien NADIS bzw. NADIS-WN verbunden. Aus diesem Grund sind in meiner Behörde typischerweise eine Vielzahl von Dokumenten vorhanden, die nicht nur Erkenntnisse und Bewertungen des BfV, sondern auch Interna über Aufbau und Arbeitsweisen des BfV enthalten können.

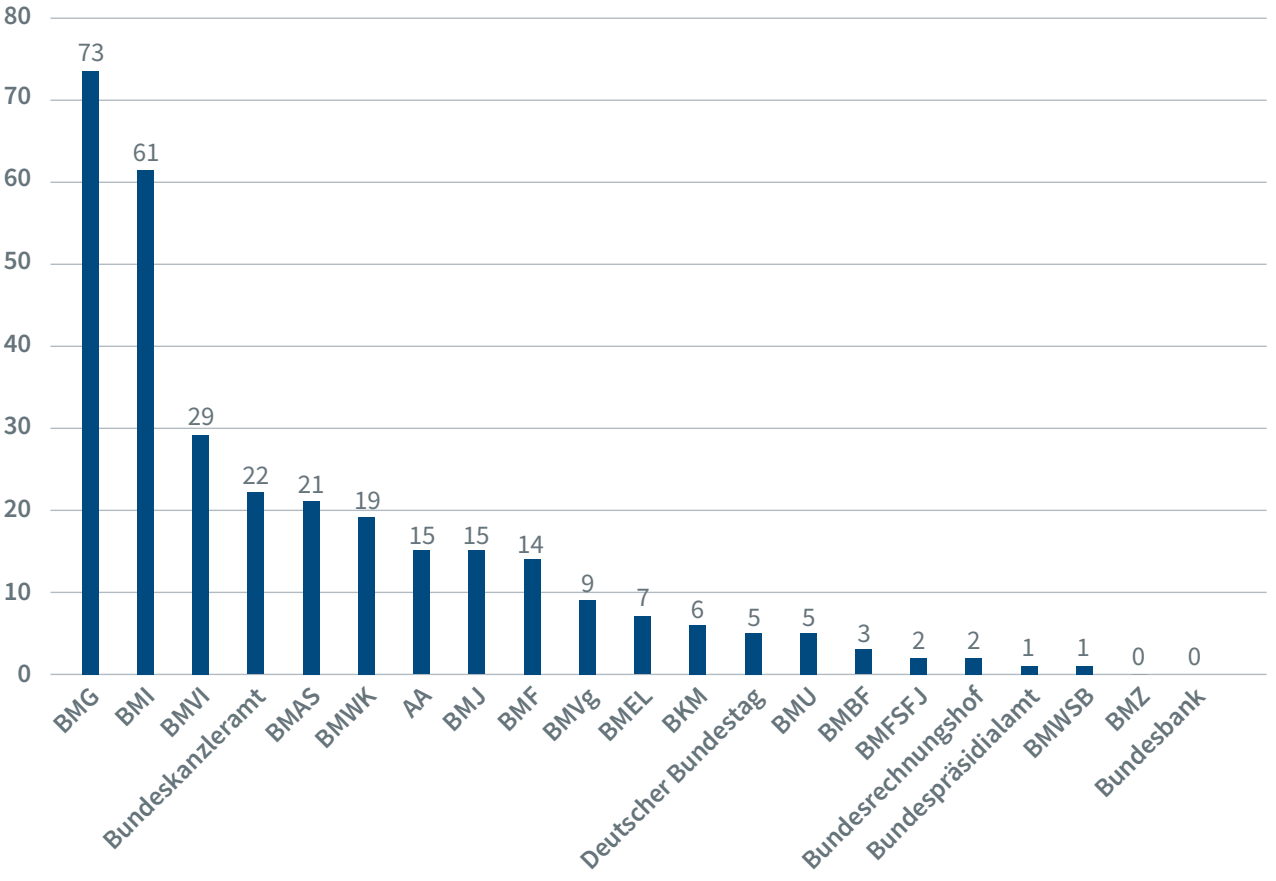
Die Informationsfreiheitsbeauftragten fordern die Abschaffung der Bereichsausnahme für den Verfassungsschutz im Generellen.[60] Solange der Gesetzgeber nichts ändert, ist die Regelung weiterhin zu beachten. Aber auch nach einer Abschaffung der Bereichsausnahme würden zahlreiche Dokumente und Vorgänge als nicht veröffentlichbar eingestuft werden müssen.

6.6 Statistische Auswertungen IFG für 2022

Eingaben mit Bezug zum Informationsfreiheitsgesetz (IFG) und zum Umweltinformationsgesetz (UIG)

Mich erreichten im Berichtszeitraum insgesamt 491 Eingaben. Damit ist die Zahl der Eingaben im Vergleich zu den Vorjahren gesunken.

Statistik der Anrufungen nach § 12 Abs. 1 IFG



59 BVerwG, Urteil vom 25. Februar 2016, 7 C 18/14; bestätigt durch: Urteil vom 22. März 2018, 7 C 21/16
60 Siehe hierzu die Entschließung der IFK vom 2. Juni 2021, abrufbar unter: www.bfdi.bund.de/ifk-entschließungen

In 310 Fällen riefen mich Petenten nach § 12 Abs. 1 IFG an und rügten eine Verletzung ihres Rechts auf Informationszugang nach dem IFG. Seit der Novellierung des UIG im März 2021 wurde meine bisher bestehende Ombudsfunktion für das IFG auf das UIG erweitert. Damit kann jede Person den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit anrufen, wenn sie ihr Recht auf Informationszugang nach dem Umweltinformationsgesetz des Bundes als verletzt ansieht.

Im Berichtszeitraum erreichten mich acht Bitten um Vermittlung bei Anträgen nach dem UIG. Im Vergleich zum Vorjahr bewegt sich die Zahl der Vermittlungsbitten weiterhin auf niedrigem Niveau. Neben den Anrufungen wegen einer Verletzung des Rechts auf Informationszugang wurden im Berichtszeitraum auch allgemeine Anfragen gestellt, in denen es um Rechtsauskünfte zum IFG ging, um Bürgeranfragen oder um Vermittlungen außerhalb meiner Zuständigkeit.

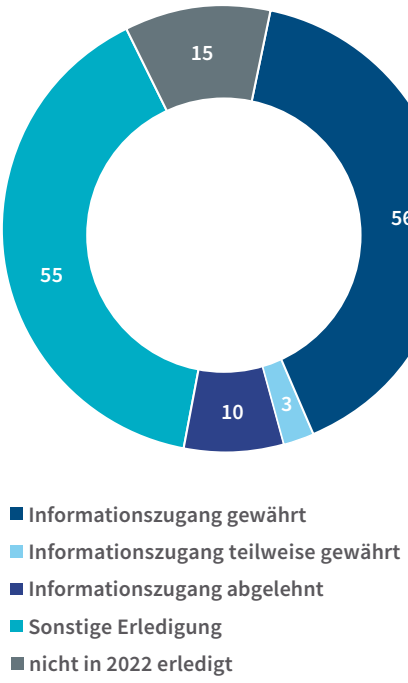
Bezogen auf die Ressorts und ihrer Geschäftsbereiche verteilen sich die Eingaben wie aus der nachfolgenden Grafik ersichtlich. Die höchste Zahl der Eingaben betraf das Bundesministerium für Gesundheit und seinen Geschäftsbereich, was – wie in den Vorjahren – am starken Interesse der Antragsteller an Informationen im Zusammenhang mit der Corona-Pandemie liegt. Antragsinhalte waren unter anderem Anfragen im Zusammenhang mit Nebenwirkungen von Impfungen, Qualitätsprüfung bei Impfstoffen und Impfeffektivität.

In zwei Vermittlungsfällen im Berichtszeitraum musste ich eine Beanstandung androhen, da der Informationszugang unrechtmäßig verweigert bzw. weil die Mitwirkungspflicht nach § 12 IFG iVm § 24 Abs. 4 BDSG a. F. verletzt wurde. Dies betraf – wie im Vorjahr – das Bundesministerium für Digitales und Verkehr wegen Unterlagen im Zusammenhang mit der „Maut-Affäre“ und zudem das Bundesarchiv im Zusammenhang mit der virtuellen Rekonstruktion von Stasi-Unterlagen.

IFG-Anträge an meine Behörde

Im Berichtszeitraum gingen insgesamt 139 Anträge auf Informationszugang bei mir ein. Diese Anträge richteten sich sowohl auf den Zugang zu Akteninhalten im Rahmen von eigenen, an den BfDI gerichteten Vermittlungsbitten nach deren Abschluss, als auch auf Stellungnahmen des BfDI zu Gesetzesvorhaben. Im Vergleich zu den Vorjahren ist das Antragsaufkommen rückläufig und entspricht daher in etwa wieder dem Antragsaufkommen der Jahre 2016 und 2017. Die proaktive Veröffentlichung von Rundschreiben an die beaufsichtigten Stellen bzw. an die obersten Bundesbehörden auf meiner Internetseite sowie die Veröffentlichung von ausgewählten Kontrollberichten u. a. Kontrollen zum Thema Sicherheitsüberprüfungsrecht und im Zusammenhang mit Kontrollen bei Postdienstleistern hat aus meiner Sicht dazu beitragen, dass das Antragsaufkommen insgesamt rückläufig ist.

IFG-Anträge meine Behörde im Jahr 2022



Aus der Abbildung ergibt sich die Verteilung der (teilweisen) Zugangsgewährung, der Zugangsablehnung und der sonstigen Erledigung im Jahr 2022. Fälle der sonstigen Erledigung umfassen beispielsweise Vorgänge, bei denen der Antrag wegen voraussichtlicher Gebührenpflichtigkeit nicht weiter verfolgt wird oder Vorgänge, bei denen der Antragsteller nicht hinreichend mitwirkt. Gründe für Ablehnungen waren im Wesentlichen weiterhin andauernde Beratungen oder die Tatsache, dass die erbetene Information beim BfDI nicht vorliegen.

7 Sicherheitsbereich

Auch im Jahr 2022 hat sich meine Behörde wieder mit einer Vielzahl von Themen im Sicherheitsbereich beschäftigt. Die Themenliste ist allerdings längst nicht abschließend. Über weite Teile meiner Arbeit im Kontext der Sicherheitsbehörden kann ich nicht öffentlich berichten.

Grund hierfür sind in erster Linie geheimschutzrechtliche Vorgaben. Diese schützen Informationen und Vorgänge, deren Bekanntwerden die Sicherheit oder die Interessen des Bundes oder der Länder gefährden oder schädigen können. Naturgemäß komme ich im Rahmen meiner Kontroll- und Beratungstätigkeit im Sicherheitsbereich immer wieder mit solchen Vorgängen und Informationen in Berührung. Meine Mitarbeitenden müssen sich daher vorab einer umfassenden Sicherheitsüberprüfung unterziehen und im Anschluss durch den Geheimschutzbeauftragten meiner Behörde für den Umgang mit solchen Verschlusssachen speziell ermächtigt werden.

Neben zwingenden gesetzlichen Vorgaben können aber auch Gründe der vertrauensvollen Zusammenarbeit einer öffentlichen Berichterstattung entgegenstehen. Für viele Projekte der Sicherheitsbehörden bin ich auf eine aktive und möglichst frühzeitige Beteiligung durch diese Stellen angewiesen. Auf diese Weise kann ich beispielsweise bei der Einführung neuer IT-Systeme oder Dateien im Sicherheitsbereich datenschutzrechtlichen Missständen bereits weit im Vorfeld entgegenwirken. Gerade wenn diese Behörden im Rahmen ihres gesetzlichen Auftrages heimlich tätig werden, sind diese Informationen jedoch nicht für die Öffentlichkeit bestimmt. Daher stimme ich mich mit den jeweils zuständigen Sicherheitsbehörden ab, ob aus ihrer Sicht Aspekte des Geheimschutzes gegen eine Veröffentlichung sprechen. Diese Vorgehensweise hat sich im Hinblick auf die vertrauensvolle Zusammenarbeit bewährt und bereits an vielen Stellen zu datenschutzrechtlichen Erfolgen geführt (s. Kap. 12).

7. 1 Passenger Name Records (PNR) – Grundsatzurteil des EuGH bestätigt Handlungsbedarf

Nun steht es fest: Die Verarbeitung von PNR-Daten muss grundlegend geändert werden. Die wegweisende Entscheidung des Europäischen Gerichtshofs (EuGH) betraf zwar eine Vorlage des belgischen Verfassungsgerichts. Seine Auslegung der sog. PNR-Richtlinie ist aber auch für Deutschland bindend. In meinem zweijährlichen Bericht an die Bundesregierung komme ich – wie schon mehrfach zuvor – ebenfalls zu einem kritischen Ergebnis.

Auf Basis der 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) haben die Mitgliedstaaten Vorschriften erlassen, die Luftfahrtunternehmen verpflichten, Informationen über die Fluggäste an sog. Fluggastdatenzentralstellen zu übermitteln. Diese ist in Deutschland beim Bundeskriminalamt eingerichtet. Sie speichert diese Daten und gleicht sie auch mit polizeilichen Datenbanken und vorher erstellten Mustern ab (z. B. Art der Buchung, gewählte Flugroute etc.). In Deutschland sind diese Vorgaben im Fluggastdatengesetz (FlugDaG) geregelt.

In meinen bisherigen Tätigkeitsberichten habe ich regelmäßig auf die unverhältnismäßige Verarbeitung von Fluggastdaten durch Sicherheitsbehörden hingewiesen (vgl. 22. TB Nr. 13.5.4, 26. TB Nr. 2.3.2, 27. TB Nr. 1.3, 28. TB Nr. 6.4, 29. TB Nr. 6.6, 30. TB Nr. 6.24). Auch dem EuGH lagen mehrere Verfahren vor, die die Rechtmäßigkeit der PNR-RL betrafen.

Die Große Kammer des EuGH hat nun auf eine Vorlage des belgischen Verfassungsgerichts hin eine Grundsatzentscheidung getroffen. Die PNR-RL hat danach zwar weiterhin Bestand. Der EuGH zieht aber deutliche Grenzen für die Auslegung der Richtlinie. Diese Grenzen sind nicht nur in Belgien zu beachten, sondern gelten auch

für die Art und Weise, wie die PNR-RL in Deutschland und in allen anderen Mitgliedstaaten umzusetzen ist.

Der EuGH hatte über zahlreiche Aspekte zu entscheiden, von denen viele auch für das deutsche FlugDaG direkt relevant sind. So erteilt der EuGH der pauschalen Einbeziehung von Intra-EU-Flügen, also Flügen ohne Drittstaatsbezug, in das PNR-System eine deutliche Absage. Dies sei nur zulässig, wenn hinreichend konkrete Umstände für die Annahme vorlägen, dass ein Mitgliedstaat mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert sei. Zudem dürfe dies auch nur für begrenzte Zeit gelten. Ebenso überschreite es die Grenze des absolut Notwendigen, wenn Datensätze von Personen länger als sechs Monate gespeichert würden, obwohl keine objektiven Anhaltspunkte für eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität mit einem jedenfalls mittelbaren Zusammenhang mit der Flugreise bestünden. Auch ich hatte die im FlugDaG vorgesehene Einbeziehung der Intra-EU-Flüge und die einer Vorratsdatenspeicherung gleichkommende fünfjährige Speicherdauer seit langem kritisiert.

Zudem betont der EuGH die strikte Zweckbindung der PNR-Daten. Eine Verarbeitung zu anderen Zwecken als der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität sei unzulässig. Insbesondere müssten die Mitgliedstaaten sicherstellen, dass nicht auch gewöhnliche Kriminalität oder Bagatelldelikte umfasst sind. Auch mit Blick auf die im PNR-System vorgesehene Musterfunktion, also der Nutzung von im Voraus festgelegten Kriterien, hat der EuGH klar Position bezogen: „Im Voraus festgelegt" stehe der Nutzung von sog. Machine-Learning-Systemen entgegen, die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die ergebnisrelevanten Bewertungskriterien sowie die Gewichtung der Kriterien ändern kann. Es müsse erkennbar bleiben, warum ein Treffer erzielt wurde.

Diese Musterfunktionalität ist auch Gegenstand des Berichts, den ich der Bundesregierung alle zwei Jahre gemäß § 4 Abs. 3 S. 9 FlugDaG erstatte. Erstmalig übersandte ich diesen Bericht im Februar 2022. Darin teilte ich meine begründeten Zweifel an der Verhältnismäßigkeit der Grundrechtseingriffe mit. Allein im deutschen PNR-System wird ein umfangreicher Datenkranz über viele Millionen Passagiere gespeichert und verarbeitet. Trotzdem konnten im o.g. zweijährlichen Berichtszeitraum die zahllosen Musterabgleiche das gesetzliche Ziel nicht fördern (vgl. 30. TB Nr. 6.24). Explizit wies ich zudem auf die nach EU-Recht nicht erforderliche allgemeine Erfassung der Intra-EU-Flüge und die zahlreichen dadurch veranlassten Grundrechtseingriffe hin.

All dies sind deutliche Hinweise darauf, dass das deutsche PNR-System dringend und grundlegend überarbeitet werden muss. Auch in anderen Mitgliedstaaten werden spätestens jetzt Anpassungen erforderlich sein. Dafür setze mich sowohl national als auch im Europäischen Datenschutzausschuss weiterhin ein.

7.2 Polizei 20/20 – P 20

Erste Softwareanwendungen des gemeinsamen „Datenhauses" der Polizeibehörden des Bundes und der Länder wurden programmiert. Aber auch die verfahrensübergreifende Recherche und Analyse innerhalb von P 20 spielt eine Rolle in meinem Berichtszeitraum.

Über das Gesamtprogramm P 20 als IT-Großprojekt der Polizeibehörden des Bundes und der Länder berichte ich regelmäßig. Zuletzt in meinem 30. Tätigkeitsbericht.

Entwicklung des Gesamtprojekts

Ein Entwicklungsschwerpunkt des letzten Jahres lag– wie auch im Vorjahr – darin, die Fallbearbeitungs-, die Vorgangsbearbeitungs-, und die Verbundsysteme zu vereinheitlichen (vgl. 30. TB Nr. 6.14). Aber auch zu dem gemeinsamen „Datenhaus" der Polizeibehörden des Bundes und der Länder gibt es Projektfortschritte. Zunächst liegt hier der Fokus auf der Auswahl einer geeigneten Technologie. In diesem Zusammenhang haben bereits erste Produkttests stattgefunden. Bis zum Ende des Jahres 2022 sollen drei Testinstallationen mit fiktiven Datensätzen befüllt werden. Ende 2024 ist dann die Verwendung von Echtdaten beabsichtigt. Mit dem Datenhaus wird auch ein Altdatenqualifizierungsdienst entwickelt. Dieser dient unter anderem dazu, den Grundsatz der hypothetischen Datenneuerhebung umzusetzen bzw. automatisiert zu unterstützen.

Hypothetische Datenneuerhebung als Spezialfall der Zweckbindung

Der vom Bundesverfassungsgericht entwickelte Grundsatz der hypothetischen Datenneuerhebung konkretisiert den Verhältnismäßigkeitsgrundsatz. Er formuliert verfassungsrechtliche Anforderungen, die der Gesetzgeber zu beachten hat, wenn er es den Sicherheitsbehörden ermöglicht, bereits erhobene Daten zweckändernd zu nutzen. Diese Rechtsfigur darf nicht dahingehend missverstanden werden, dass sie eine eindeutige Festlegung der Verarbeitungszwecke entbehrlich machen würde. Ebenso wenig ist die pauschale Heranziehung des Grundsatzes der hypothetischen Datenneuerhebung als Begründung für die Schaffung eines Verbundinformationssystems mit weitreichenden Abfrage- und Recherchemöglichkeiten sachgerecht.

Auszug aus meinem Positionspapier zum Grundsatz der Zweckbindung in polizeilichen Informationssystemen vom 6. April 2021. Abrufbar unter: www.bfdi.bund.de/stellungnahmen

Mir liegt zu dem gemeinsamen „Datenhaus“ ein erstes technisches Konzeptpapier vor. Die Projektgruppe im Bundesministerium des Innern und für Heimat (BMI) hat mir aber auch ein datenschutzrechtliches Fachkonzept in Aussicht gestellt. Dieses lag mir bei Redaktionsschluss jedoch noch nicht vor. Ohne ein solches Dokument ist eine datenschutzrechtliche Bewertung des gemeinsamen „Datenhauses“ nicht möglich.

Verfahrensübergreifende Recherche und Analyse

Seit dem Jahr 2022 verfügt das Bayerische Landeskriminalamt über ein „Verfahrensübergreifendes Recherche- und Analysesystem“ (VeRA). Nach einem europaweiten Ausschreibungsverfahren hat die Firma Palantir Technologies GmbH den Zuschlag erhalten. Der Rahmenvertrag ermöglicht es auch anderen Polizeibehörden des Bundes und der Länder, das System VeRA zu nutzen. Derzeit prüft das BMI, ob auch die Bundesbehörden von dem in Bayern betriebenen Softwareprodukt Gebrauch machen werden. Eine Entscheidung sei jedoch noch nicht getroffen. Das BMI hat mir eine Beteiligung zugesagt. In der Vergangenheit habe ich immer wieder auf die datenschutzrechtlichen Risiken und Anforderungen im Hinblick auf die Auswertung und Analyse von personenbezogenen Daten hingewiesen. Es handelt sich um erhebliche Grundrechtseingriffe. Zudem darf durch derartige Analysesysteme die Zweckbindung gespeicherter Daten nicht unterlaufen werden. Mein Haus hat zu dem Thema „KI in Strafverfolgung und Gefahrenabwehr“ vor diesem Hintergrund ein Konsultationsverfahren initiiert (vgl. 30. TB Nr. 4.2.2) und das o. g. Positionspapier zur Zweckbindung in polizeilichen Datenbanken veröffentlicht.

Proof of Concept (PoC) Datenkonsolidierung

Bereits in der Vergangenheit hatte ich über dieses Teilprojekt berichtet. Mit dem PoC soll ein weiteres Verbundsystem außerhalb des polizeilichen Informationsverbunds nach dem Bundeskriminalamtsgesetz (BKAG) betrieben werden (30. TB Nr. 6.14, 29. TB Nr. 6.1). Anfang des Jahres 2021 hatte ich formell eine Warnung nach § 16 Abs. 2 Satz 4 Bundesdatenschutzgesetz (BDSG) gegen die mit der PoC beabsichtigte Datenverarbeitung gegenüber dem Bundeskriminalamt (BKA) ausgesprochen. Einige Landesdatenschutzaufsichtsbehörden haben ihre Landespolizeibehörden ebenfalls vor dieser Datenverarbeitung gewarnt. Anfang des Jahres 2022 habe ich mich in einem mit der AG INPOL (einer Arbeitsgruppe des Arbeitskreises Sicherheit der DSK) abgestimmten Schreiben noch einmal ausführlich gegen den PoC ausgesprochen. Das BMI antwortete auf diese Stellungnahme Ende des Jahres und hält die mit dem PoC beabsichtigte Datenverarbeitung weiterhin für rechtmäßig. Es bleibt nun abzuwarten, ob bzw. wie sich das Teilprojekt weiter entwickeln wird. Ich werde über den Fortgang berichten.

European Police Records Index System (EPRIS)

Als Teilprojekt von P 20 führt das BMI EPRIS-ADEP auf. Ziel des Projektes sei es, ein EU-weites Fundstellennachweissystem für polizeiliche Kriminalakten zu schaffen. Zu diesem Zweck sei von ausgewählten EU-Mitgliedstaaten der Prototyp einer dezentralen Softwarelösung (ADEP-Technologie) entwickelt worden. Die technischen Vorgaben sollen es ermöglichen, bestimmte personenbezogene Daten nach einheitlichen Regelungen mit dezentral gespeicherten Datenbeständen in standardisierter Form abzugleichen. Die europarechtlichen Rechtsgrundlagen für ein solches EU-weites Fundstellennachweissystem wurden noch nicht geschaffen. Da das BKA europaweit die Projektleitung übernommen hat, habe ich es um eine datenschutzrechtliche Stellungnahme gebeten. Mich interessiert besonders, auf welcher rechtlichen Grundlage das Pilotprojekt EPRIS-ADEP derzeit betrieben und wie sichergestellt wird, dass rechtliche Vorgaben des BKAG beachtet werden. Eine Antwort des BKA lag mir bei Redaktionsschluss noch nicht vor. Generell ist mir auch bei diesem Projekt wichtig, dass grundrechtliche Vorgaben nicht unterlaufen werden. Dazu gehört insbesondere, anzuerkennen, dass die polizeiliche Datenbevorratung ein Grundrechtseingriff ist, der sich für die betroffenen Personen erheblich

auswirken kann. Dies gilt auch deshalb, weil in den Kriminalakten Personen oft nur auf einer Verdachtsbasis gespeichert sind. Der Eingriff wird hier vertieft, weil diese Personen und Verdachtsmomente dann europaweit abrufbar sind. Mindestens die für diese Datenbevorratung im BKAG vorgesehenen Schwellen dürfen nicht unterschritten werden.

Verzeichnis von Verarbeitungstätigkeiten

Meiner Beratungs- und Kontrollaufgabe unterliegt nicht nur P 20, sondern auch die „alte“ polizeiliche Informationsordnung im BKA. Seit 2019 hatte ich das BKA um das Verzeichnis von Verarbeitungstätigkeiten gebeten. Da ein solches nicht vorgelegt wurde, habe ich gegenüber dem BMI als Fachaufsichtsbehörde eine Beanstandung nach § 16 Abs. 2 BDSG ausgesprochen.

Das BMI teilte mir nun mit, nach einer europaweiten Ausschreibung würde das Managementsystem QSEC eingeführt werden. Dieses ermögliche auch die Abbildung von Datenschutz-Folgeabschätzungen. Da die BKA-weite Einführung des Systems erst für das dritte Quartal 2023 vorgesehen ist, habe ich das BMI um eine Interimslösung gebeten. An einer solchen Überbrückungslösung wird im BKA derzeit gearbeitet. Allerdings wurde mir das vorläufige Verzeichnis von Verarbeitungstätigkeiten bis zum Redaktionsschluss noch nicht vorgelegt.

7.3 Einschaltung Dritter bei Quellen-TKÜ und Onlinedurchsuchung

Polizeibehörden und Nachrichtendienste setzen IT-Produkte von Drittherstellern ein. Bei eingriffsintensiven Maßnahmen wie Quellen-TKÜ und Online-Durchsuchung dürfen sie Produkte von Dritten jedoch nur in engen rechtlichen Grenzen nutzen.

Heimliche Überwachungsmaßnahmen bieten immer wieder Stoff für kontroverse Diskussionen. Die Sicherheitsbehörden müssen einerseits die ihnen zugewiesenen Aufgaben effektiv wahrnehmen können. Andererseits müssen sie dabei die rechtlichen Grenzen einhalten bzw. die Rechte der betroffenen Personen wahren.

Eingriffsintensive Überwachungsmaßnahmen durchzuführen, gehört zum genuinen Bereich staatlicher Verantwortung. Beziehen die Ermittlungsbehörden Dritte ein, ist hier größte Zurückhaltung geboten. Dies gilt insbesondere dann, wenn die Sicherheitsbehörden und Nachrichtendienste Aufgaben mithilfe von IT-Produkten Dritter wahrnehmen.

Im Berichtszeitraum habe ich hierzu ein Positionspapier veröffentlicht.[61] Darin habe ich aufgezeigt, wo aus meiner Sicht in denkbaren Fällen des Einsatzes Dritter die rechtlichen Grenzen verlaufen. Maßgeblich bleiben natürlich die Umstände des jeweiligen Einzelfalls.

Aufgrund der dort aufgezeigten rechtlichen Leitplanken habe ich zum Einsatz Dritter bei eingriffsintensiven Maßnahmen vor allem folgende Forderungen formuliert:

- Entscheidungsbefugnisse hinsichtlich des „Ob“ und „Wie“ der Durchführung einzelner Überwachungsmaßnahmen dürfen nicht auf private Dritte übertragen werden.
- Die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen im Kontext der Durchführung eingriffsintensiver Maßnahmen sollte auf ein Mindestmaß begrenzt sein. Die Möglichkeit einer unkontrollierten Speicherung oder sonstigen missbräuchlichen Verwendung personenbezogener Daten ist auszuschließen.
- Eigenentwicklungen sind den von privaten Dritten entwickelten Software-Lösungen vorzuziehen (vgl. schon 28. TB 2019, S. 57).
- Die mithilfe von IT-Produkten Dritter verarbeiteten Daten dürfen nicht dem Einfluss und der Kontrolle des Verantwortlichen entzogen sein. Die Beherrschbarkeit der Hard- und Software durch den Verantwortlichen muss vollumfänglich gewährleistet sein.
- Die Einschaltung (privater) Dritter darf die Kontrollbefugnisse der Datenschutzaufsichtsbehörden nicht einschränken.

7.4 Kennzeichenerfassung Bundespolizei

Die Bundespolizei setzte 2022 erstmals Systeme zur automatischen Erfassung von KfZ-Kennzeichen und deren Abgleich mit Fahndungsdatenbanken ein. Sie dürfen nach der Rechtsprechung des Bundesverfassungsgerichtes (BVerfG) wegen ihres überwachungsstaatlichen Charakters nur restriktiv genutzt werden. Obwohl ich seit 2020 immer wieder aktiv um Sachstandsmitteilung gebeten hatte, wurde ich erst kurzfristig vor dem ersten Einsatz in das Verfahren einbezogen.

61 Stellungnahme vom 28. März 2022, abrufbar unter: www.bfdi.bund.de/stellungnahmen

Die anlassbezogene automatische Kennzeichenerfassung ist ein verhältnismäßig neues Instrument, das nur zur Abwehr gegenwärtiger Gefahren für Leib, Leben oder Freiheit einer Person oder zur Verhinderung und Verfolgung schwerer Straftaten eingesetzt werden kann. Dabei werden die Kennzeichen von sämtlichen Fahrzeugen, die eine Erfassungsanlage passieren, ausgelesen und mit einem zuvor festgelegten Datenbestand abgeglichen.

In Abkehr von seiner früheren Rechtsprechung entschied das BVerfG 2018 (Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15), dass schon die Erfassung der Nummernschilder und damit erst recht der Abgleich mit Fahndungsdateien einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Rechtsgrundlagen, die einen solchen Eingriff ermöglichen, sind daher zwar verfassungsrechtlich nicht gänzlich ausgeschlossen, müssen aber strengen Anforderungen an ihre Verhältnismäßigkeit genügen.

Nachdem 2017 im Bundespolizeigesetz (BPolG) und 2021 in der Strafprozessordnung (StPO) entsprechende Rechtsgrundlagen geschaffen wurden, werden solche Systeme nun seit 2022 bei der Bundespolizei eingesetzt. Da die betroffenen Personen über die Durchführung der Maßnahme regelmäßig nicht benachrichtigt werden, kommt meiner Kontrollfunktion eine besondere Bedeutung zu. Obwohl ich seit 2020 wiederholt nach dem Sachstand zu Kennzeichenerfassungsanlagen bei der Bundespolizei gefragt hatte, erfuhr ich erst eine Woche vorher von dem geplanten Einsatz. Gleichzeitig hatte das Bundesministerium des Innern und für Heimat (BMI) ohne meine vorherige Anhörung eine Errichtungsanordnung (sog. „Sofortanordnung“) erlassen, obwohl aus meiner Sicht die erforderliche Dringlichkeit für die Aufgabenerfüllung, gerade nach der langen Vorlaufzeit, nicht vorlag. Auch die nach meiner Einschätzung notwendige Datenschutzfolgenabschätzung wurde nicht durchgeführt.

Durch die nunmehr erfolgte nachträgliche Anhörung zur Errichtungsanordnung habe ich eine Prüfung des Verfahrens aufgenommen und werde auf eine datenschutzkonforme Ausgestaltung hinwirken.

7.5 Verstärkte Tätigkeiten im Bereich der Strafjustizbehörden

Dank des Personalaufwuchses meiner Behörde konnte ich im letzten Jahr meine Tätigkeiten im Bereich der Strafjustizbehörden erheblich ausbauen.

Meine Zuständigkeit umfasst auch die datenschutzrechtliche Aufsicht über den Generalbundesanwalt beim Bundesgerichtshof (GBA) sowie das Bundeszentralregister (BZR) und das Zentrale Staatsanwaltliche Verfahrensregister (ZStV), die beide beim Bundesamt für Justiz (BfJ) geführt werden.

Beim GBA habe ich die Einführung der elektronischen Strafakte beratend begleitet und führe dies auch fort. Zudem habe ich mich bei einem Informationsbesuch intensiv darüber unterrichten lassen, wie die Bearbeitung sogenannter Strukturermittlungsverfahren seitens des GBA gehandhabt wird und welche rechtlichen Überlegungen dabei zu beachten sind. Bei Strukturermittlungsverfahren handelt es sich zum Beispiel um Verfahren, in denen noch unbekannte Mitglieder bekannter terroristischer Organisationen identifiziert werden sollen.

Beim BfJ war ich bei verschiedenen Gelegenheiten beratend tätig. Dies betraf zum einen die nationale Umsetzung von ECRIS-TCN (European Criminal Record Information System for Third Country Nationals), also das Europäische Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose. Zum anderen konnte ich meinem Beratungsauftrag bei der Neukonzeption der Protokollierung im ZStV sowie bei der Erstellung Europäischer Führungszeugnisse nachkommen. Im letzteren Fall bestand die Problematik darin, dass aufgrund falscher Personenidentifizierungen im EU-Ausland die Führungszeugnisbeiträge dieser Länder andere Personen betrafen als die antragstellende Person. Zudem führte ich eine Kontrolle bezüglich der Bearbeitung von Zeugenschutzfällen im BZR nach § 44a Bundeszentralregistergesetz durch.

7.6 Der Verfassungsschutz und das Bundesverfassungsgericht

Erneut hat das Bundesverfassungsgericht (BVerfG) grundlegende und weitreichende Änderungen im Nachrichtendienstrecht eingefordert. Viele Normen des bayerischen Gesetzes müssen wegen Verfassungswidrigkeit geändert werden. Ähnliches gilt für das Bundesverfassungsschutzgesetz (BVerfSchG). Spannend dürfte vor allem die Anpassung der Übermittlungsvorschriften an die Vorgaben des Urteils werden. In einer zweiten Entscheidung im Verlauf des Jahres hat das BVerfG die Verfassungswidrigkeit einzelner Normen des Bundesgesetzes ausdrücklich bestätigt.

Am 26. April 2022 hat das BVerfG anlässlich einer Verfassungsbeschwerde zum Bayerischen Verfassungsschutzgesetz (BayVSG) ein Urteil gefällt, dessen Auswirkungen weit über Bayern hinausreichen. Es hat viele Vorschriften des Landesrechts für verfassungswidrig erklärt und dem dortigen Gesetzgeber bis zum 31. Juli 2023 Zeit gegeben, Abhilfe zu schaffen. Viele andere Landesverfassungsschutzgesetze und auch das Bundesver-

fassungsschutzgesetz (BVerfSchG) beinhalten ähnliche oder sogar identische Regelungen wie die des BayVSG, so dass auch dort ein Handeln geboten ist. Die Entscheidung des BVerfG hatte sich aufgrund der früheren Rechtsprechung bereits abgezeichnet. Ich hatte daher bereits mehrfach eine umfassende Reform des BVerfSchG eingefordert (vgl. 29. TB Nr. 5.5).

Unterschiede und Gemeinsamkeiten zwischen Verfassungsschutzbehörden und Polizeibehörden bei Anforderungen an Grundrechtseingriffe

Das Gericht hat auf der einen Seite das Tätigwerden der Verfassungsschutzbehörden für den Erhalt der Demokratie anerkannt, weil sie zum Schutz besonders wichtiger Rechtsgüter wie dem Schutz der freiheitlich demokratischen Grundordnung tätig werden. Es hat auf der anderen Seite aber auch deutlich gemacht, unter welchen Voraussetzungen der Verfassungsschutz Bestrebungen beobachten darf. Die Schwellen, ab denen der Verfassungsschutz tätig werden und damit auch in Grundrechte eingreifen darf, sind in der Regel zulässigerweise geringer als beispielsweise die von Polizeibehörden. Verfassungsschutzbehörden können aus einer Überwachungsmaßnahme keine unmittelbaren operativen Konsequenzen für den Einzelnen ziehen, wie z. B. Durchsuchungen, Beschlagnahmen oder Festnahmen. Höher sind diese Schwellen allerdings dann, wenn die Eingriffsintensität deutlich zunimmt. Dies ist beispielsweise dann der Fall, wenn durch Überwachungsmaßnahmen besonders umfangreiche Informationen gewonnen werden können, durch die eine Erfassung der Persönlichkeit ermöglicht wird. In solchen Fällen sind dieselben Maßstäbe anzulegen wie bei vergleichbaren polizeilichen Maßnahmen, namentlich die Online-Durchsuchung und die Wohnraumüberwachung. Dazu muss für die Anordnung der gerade genannten Maßnahmen eine dringende Gefahr für die öffentliche Sicherheit vorliegen und darüber hinaus geeignete polizeiliche Hilfe ansonsten nicht rechtzeitig erlangt werden können. Vor allem mit dem letztgenannten Erfordernis der Subsidiarität sind beide Maßnahmen – für die Wohnraumüberwachung galt dies ohnehin schon – für die Verfassungsschutzbehörden nur noch in der Theorie einsetzbar. Denn dass die Polizei in derartigen Fällen nicht rechtzeitig zur Stelle ist, ist kaum vorstellbar.

Gericht definiert Anforderungen u. a. an die Übermittlungen von Daten durch Verfassungsschutzbehörden

Das Gericht trifft viele weitere wichtige Aussagen, z. B. unter welchen Voraussetzungen Dritte ausnahmsweise mittelbar oder unmittelbar in eine Überwachungsmaßnahme einbezogen werden dürfen. Ferner stellt das Gericht Anforderungen an die Bestimmtheit und Klarheit von Eingriffsnormen im Bereich des Nachrichtendienstrechts auf. Bei bestimmten eingriffsintensiven Maßnahmen statuiert es das Erfordernis einer Vorabkontrolle durch eine unabhängige Stelle, wie dies im Bereich der Strafverfolgung durch den Richtervorbehalt vorgesehen ist. Vor allem aber äußert es sich auch dazu, unter welchen Voraussetzungen personenbezogene Daten vom Verfassungsschutz an verschiedene Stellen im In- und Ausland übermittelt werden dürfen.

Erste Überlegungen von Bund und Ländern zur Umsetzung des Urteils

Unmittelbar im Anschluss an die Gerichtsentscheidung haben sich Bund und Länder in einer Arbeitsgruppe zusammengefunden, um über die Auswirkungen des Urteils zu diskutieren und Vorschläge für die notwendigen Anpassungen an den Vorschriften zu erarbeiten. Dieser Bericht, inklusive mehrerer Anlagen, wurde mit Beschluss der Innenministerkonferenz vom 27. September 2022 veröffentlicht. Daraus geht hervor, dass die Mitwirkenden in vielen Punkten unterschiedlicher Auffassung sind. Zum einen, wie bestimmte Aussagen des Gerichts zu verstehen sind und zum anderen, wie Änderungen in den Gesetzen aussehen könnten. Dies betrifft u. a. die Frage, unter welchen Voraussetzungen Verfassungsschutzbehörden künftig Informationen an Behörden mit sog. operativen Zwangsbefugnissen sowie auch an Strafverfolgungsbehörden übermitteln dürfen. Für Übermittlungen an diese Stellen gelten nach dem BVerfG erhöhte Anforderungen, weil die Informationen von der Verfassungsschutzbehörde für derartige Maßnahmen gerade nicht genutzt werden können. Im Gegensatz zu den vorgenannten Behörden besitzt der Verfassungsschutz nämlich keine solchen Zwangsbefugnisse.

Was ist eine „Behörde mit operativen Zwangsbefugnissen“?

Das Gericht hat den Begriff der operativen Zwangsbefugnisse neu eingeführt, ohne ihn eindeutig zu definieren. Es nennt sie allerdings lediglich im Vergleich mit Polizeibehörden. Daraus wird überwiegend geschlossen, dass es sich um Befugnisse handeln muss, gegen die der Betroffene vorab keinen Rechtsschutz erlangen kann, wie z. B. im Fall von Beschlagnahme, Festnahme oder Durchsuchung. Fraglich ist dann weiterhin, ob die erhöhten Übermittlungsanforderungen generell bei Übermittlungen an solche Behörden gelten oder ob die konkrete Übermittlung darauf gerichtet sein muss, die Information zur Anwendung operativen Zwangs zu benutzen.

Offene Fragen hinsichtlich der Datenübermittlung an Strafverfolgungsbehörden

Eine Übermittlung an Strafverfolgungsbehörden darf nach dem Urteil des Gerichts nur zur Verfolgung besonders schwerer Straftaten erfolgen. Dieser Begriff ist einfachrechtlich geprägt durch den Straftatenkatalog des § 100b Abs. 2 Strafprozessordnung (StPO). Danach dürfen Strafverfolgungsbehörden die eingriffsintensive Maßnahme der Online-Durchsuchung nur bei den dort in Rede stehenden Straftaten einsetzen. Auch das BVerfG selbst hat sich in einem früheren Urteil daran orientiert. Hauptaufgabe von Verfassungsschutzbehörden ist der Schutz der freiheitlich-demokratischen Grundordnung sowie der Schutz der Sicherheit und des Bestandes der Bundesrepublik. Würde man Übermittlungen allein für die in § 100b Abs. 2 StPO genannten Straftaten erlauben, würden einige Straftaten, die dem Verfassungsschutz bei seiner Arbeit bekannt werden, nicht an Strafverfolgungsbehörden übermittelt werden dürfen. Beispielhaft zu nennen sind in diesem Kontext Körperverletzungsdelikte mit antisemitischem Hintergrund oder bestimmte Staatsschutzdelikte wie die geheimdienstliche Agententätigkeit nach § 99 Strafgesetzbuch. Im Bund-Länder-Bericht wird daher teilweise bezweifelt, dass das Gericht dieses Ergebnis gewollt haben kann und versucht, Alternativen zu finden. Teilweise wird gefordert, einen eigenen, verfassungsschutzspezifischen Begriff der besonders schweren Straftat einzuführen. Denkbar wäre auch, den Strafrahmen für solche Straftatbestände deutlich zu erhöhen. Hier sind noch viele Fragen offen. Besonderes Augenmerk wird dabei auch auf die unten genannte zweite Entscheidung des BVerfG aus dem September 2022 zu legen sein, in der sich das Gericht ebenfalls zu diesem Themenkomplex äußert.

Notwendig sind auch Regelungen für eine umfassende Kontrolle über nachrichtendienstliche Tätigkeiten

Hinsichtlich der notwendigen Änderungen im BVerfSchG bin ich frühzeitig an das Bundesministerium des Innern und für Heimat (BMI) herangetreten. Auf diese Weise konnte ich schon vor dem offiziellen Beginn des Gesetzgebungsverfahrens Kenntnis von den Überlegungen des BMI nehmen. Ich habe deutlich gemacht, dass aus meiner Sicht nicht nur dieses Urteil, sondern auch bereits ältere Urteile den Gesetzgeber zum Handeln aufgefordert haben und dass das BVerfSchG einer grundlegenden Reform bedarf. Zudem sehe ich auch durch meine Kontrollpraxis an einigen Stellen die Notwendigkeit von Präzisierungen, so z. B. bei der Speicherung von Daten unbekannter bzw. unbeteiligter Personen sowie beim Auskunftsanspruch.

Wichtig ist mir bei der Anpassung des Gesetzes auch, dass die Zusammenarbeit zwischen derjenigen Stelle, die künftig die Vorabkontrolle für eingriffsintensive Maßnahmen durchführt, und dem BfDI sichergestellt ist. Nur so wird eine umfassende Kontrolle und auch ein umfassender Austausch möglich sein. Den Bereich der Observation, den das BVerfG im Urteil u. a. als eine solche Maßnahme ansieht und künftig einer unabhängigen Vorabkontrolle unterwirft, habe ich z. B. 2021 sowohl beim Bundesamt für Verfassungsschutz (BfV) als auch beim Bundesamt für den Militärischen Abschirmdienst (MAD) kontrolliert. Diese Ergebnisse könnten für die neue Kontrollinstanz hilfreich sein. Weitere vielfältige Überschneidungspunkte sind denkbar.

Weitere Entscheidung des BVerfG im September 2022

Mit Beschluss vom 28. September 2022 (1BvR 2354/13) hat das Gericht Teile seiner Festlegungen aus dem April-Urteil ausdrücklich auf das BVerfSchG übertragen. Bereits seit 2013 war eine Verfassungsbeschwerde gegen die §§ 19 – 21 BVerfSchG anhängig gewesen. Die Übermittlungsnormen der §§ 20 und § 21 BVerfSchG in Verbindung mit dem Rechtsextremismusdatei-Gesetz wurden für verfassungswidrig erklärt. § 20 BVerfSchG normiert Übermittlungspflichten des BfV an die Strafverfolgungs- und Sicherheitsbehörden zur Verhinderung oder Verfolgung von Staatsschutzdelikten. § 21 BVerfSchG regelt diese Übermittlungspflichten für die Landesämter für Verfassungsschutz. In Bezug auf § 19 BVerfSchG war die Verfassungsbeschwerde unzulässig, so dass insoweit keine inhaltliche Entscheidung erging. Ich habe in diesem Verfahren mehrere Stellungnahmen abgegeben, weil auch ich die in Rede stehenden Normen für zu unbestimmt und für unverhältnismäßig halte. Meine Forderung einer Dokumentation der Übermittlung von Erkenntnissen, die durch nachrichtendienstliche Mittel erhoben worden sind, hat das Gericht aufgegriffen und die Protokollierung von Übermittlungen angemahnt. Zudem ist es meiner Ansicht gefolgt, dass dies auch im Gesetz verankert sein muss. Durch die Vorgabe, die verfassungswidrigen Normen bis zum 31. Dezember 2023 anzupassen, ist der Gesetzgeber nun auch hier zu besonderer Eile aufgefordert. Es ist daher zu befürchten, dass meine langjährigen Forderungen nach einer umfassenden Reform des BVerfSchG angesichts der zur Verfügung stehenden Zeit nicht berücksichtigt werden können.

7.7 Beanstandungen des BAMAD und des BfV aufgrund der Verletzung der Unterstützungspflicht

In der Vergangenheit kam es sowohl im Verantwortungsbereich des Bundesministeriums der Verteidigung (BMVg) als auch im Datenschutzreferat des Bundesamtes für Verfassungsschutz (BfV) zu erheblichen Verzögerungen in der Beteiligung meiner Behörde. Dies stellt eine Verletzung der Pflicht dar, mich bei meiner Kontrolltätigkeit in sämtlichen datenschutzrechtlichen Belangen rechtzeitig zu informieren und umfassend zu unterstützen. Ich habe dies jeweils beanstandet.

BAMAD

Das Bundesamt für den Militärischen Abschirmdienst (BAMAD) ist gesetzlich verpflichtet, für jede automatisierte Datei eine Dateianordnung (DAO) zu erstellen und mich vor Erlass anzuhören. Besteht im Hinblick auf die Aufgabenerfüllung eine besondere Dringlichkeit, hat das BAMAD die Möglichkeit, die Datei mittels einer Sofortanordnung zu erlassen (§ 8 MAD-Gesetz i. V. m. § 14 Abs. 3 BVerfSchG). Die Anhörung ist dann aber unverzüglich nachzuholen. Wie ich im Berichtszeitraum erfahren habe, hat das BAMAD bereits im September 2021 eine neue Datei mittels Sofortanordnung erlassen. Es wurde jedoch versäumt sicherzustellen, dass die in den Postausgang gegebene Anordnung meine Behörde zur unverzüglichen Nachholung des vorgeschriebenen Verfahrens auch tatsächlich erreicht. Erst auf meine Aufforderung hin wurde ich über ein Jahr später angehört.

Ich habe dies beanstandet und klargestellt, dass für das BAMAD die ausdrückliche gesetzliche Pflicht besteht, meine Behörde bei der Erfüllung ihrer Aufgaben zu unterstützen. Das BMVg hat mir im Rahmen seiner Stellungnahme zwischenzetlich mitgeteilt, dass die gegenständliche Datei durch das BAMAD schon seit Oktober 2021 nicht mehr fachlich genutzt wird.

BfV

Im Frühjahr 2021 tauschte ich mich mit dem BfV erstmals über mögliche Änderungen bei der Zusammenarbeit zwischen dem BfV und der Financial Intelligence Unit (FIU) aus (30. TB Nr. 8.2.7). Ein besonderes Augenmerk lag auf der Schaffung von technischen Schnittstellen, durch die ein vereinfachter Datentransfer im Rahmen der Regelungen des Geldwäschegesetzes umgesetzt werden sollte. Ende April 2021 legte mir das BfV seinen bis dato geltenden Planungsstand schriftlich dar. Das Vorhaben warf diverse datenschutzrechtliche Fragen, insbesondere zu automatisierten Verarbeitungsprozessen, auf. Daher richtete ich Anfang Juni 2021 ein Schreiben mit meinen Bedenken und Fragen zur Umsetzung der geplanten Schnittstellen an das BfV. In den folgenden Monaten kündigte mir das BfV mehrfach die Beantwortung des Schreibens an, ohne dies tatsächlich umzusetzen. Nach mehrfachen Erinnerungen beanstandete ich dies schließlich mit Schreiben vom 4. Mai 2022 wegen Verletzung seiner Unterstützungspflicht. Diese Pflicht beinhaltet, u. a. Auskünfte zu meinen Fragen zu gewähren (§ 28 Abs. 3 Satz 2 Nr. 1 BVerfSchG).

In der Stellungnahme bedauerte das für die Fachaufsicht zuständige Bundesministerium des Inneren und für Heimat die Verzögerung. Das BfV habe zugesagt, Prozesse zu etablieren, um die Kommunikation mit mir zu verbessern. Die geforderten Informationen erhielt ich schließlich am 31. Mai 2022. Das BfV hat die Pläne zur Einführung von Schnittstellen demnach weitestgehend auf Eis gelegt. Die zuvor bedenklichen Vorhaben werden nicht weiterverfolgt.

In den letzten Jahren kommt es beim BfV immer wieder zu Fällen mit überlanger Bearbeitungszeit. Dies füh-

re ich auf den Umstand zurück, dass der zuständige Datenschutzbereich nicht im selben Umfang personell gewachsen ist wie der Rest des Hauses.

Ich setze mich daher auch weiter für eine bessere personelle Ausstattung der Datenschutzbereiche der Behörden ein, damit die Aufgaben zeit- und sachgerecht bearbeitet werden können. Dies verbessert im Ergebnis auch die Kommunikation mit meinem Haus.

7.8 Personenbezogene Daten in Informationsschreiben des BfV

Wenn der Austausch des Bundesamtes für Verfassungsschutz (BfV) mit anderen Behörden und die Information der Bundesregierung über Trends personenbezogene Daten enthält, stellt auch das eine Übermittlung dar, für die eine Rechtsgrundlage erforderlich ist. Im Einzelfällen fehlt diese aus meiner Sicht, daher muss das Verfahren umgestellt werden.

Der allgemeine Austausch über Erkenntnisse, Historie und Trends in den verschiedenen Aufgabenbereichen des BfV mit anderen Behörden, insbesondere mit den Verfassungsschutzbehörden der Länder, aber auch die Information der Regierung, stellen einen wichtigen Teil der Arbeit des BfV dar. Dieser Austausch geschieht nicht nur anlassbezogen, sondern auch regelmäßig institutionalisiert. Seit vielen Jahren versendet das BfV wöchentlich einen Bericht mit Entwicklungen zu verschiedenen aktuellen Themen an eine Reihe vom Behörden.

Diente dieser Bericht zunächst in erster Linie der Information der Landesverfassungsschutzbehörden und später auch der Information der Bundesregierung, wurde der Adressatenkreis über die Jahre immer größer. Diese Entwicklung wäre an sich unproblematisch, wenn die Berichte nicht auch ab und zu personenbezogene Daten zu einzelnen Personen aus den jeweiligen Aufgabenbereichen des BfV wie Links- oder Rechtsextremismus, Ausländerextremismus oder Spionageabwehr beinhalten würden. Denn mit dem Versenden dieser Informationen ist rechtlich eine Datenübermittlung verbunden, die einer entsprechenden Rechtsgrundlage bedarf.

Hierfür kommen zwar verschiedene Übermittlungsvorschriften aus dem Bundesverfassungsschutzgesetz in Betracht, die in einer Vielzahl der Fälle einschlägig sein können. Allerdings stellt sich mir angesichts des großen Verteilers in Einzelfällen die Frage, ob tatsächlich immer eine einschlägige Befugnis vorliegt.

Es wird nicht deutlich genug danach unterschieden, ob alle Empfänger die jeweiligen personenbezogenen Daten für ihre Aufgabe benötigen. Behörden, deren Aufgabenbereiche nur Bezug zu einem einzigen der oben genannten Aufgabenbereiche des Verfassungsschutzes haben, benötigen in der Regel personenbezogene Daten aus anderen Phänomenbereichen nicht. Bei einigen Empfängern stelle ich die Übermittlungsbefugnis generell in Frage.

Ich erwarte seitens des BfV für Anfang 2023 einen mit der Fachaufsicht abgestimmten datenschutzkonformen Lösungsvorschlag. Aus meiner Sicht könnte dieser z. B. aus einem verkleinerten Adressatenkreis oder verschiedenen Teilberichten für einzelne Empfängerkreise bestehen.

7.9 Endlich: eine gesetzliche Grundlage für die ZITiS

Die Zentrale Stelle für die Informationstechnik im Sicherheitsbereich (ZITiS) wurde 2017 ohne jegliche gesetzliche Grundlage geschaffen. Die Bundesregierung will dieses Projekt nun endlich angehen. Ich werde sie dabei eng begleiten.

Die ZITiS wurde 2017 per ministeriellem Erlass, also ohne Schaffung einer gesetzlichen Grundlage, errichtet. Seither erfuhr die ZITiS jedes Jahr einen deutlichen Personalaufwuchs. Im aktuellen Koalitionsvertrag ist festgelegt, dass eine Rechtsgrundlage für die Arbeit der ZITiS geschaffen werden soll. Dies sehe ich mit Blick auf die Bedeutung der technischen Unterstützung der Sicherheitsbehörden als überfällig an.

Der Haushaltsausschuss hatte die Bundesregierung im Sommer 2022 zur Festlegung von Eckpunkten für das künftige Gesetz verpflichtet. Bei der Erarbeitung dieser Eckpunkte hat mich das BMI, zu dessen Geschäftsbereich die ZITiS gehört, beteiligt. Die Eckpunkte sind relativ allgemein gehalten und orientieren sich im Wesentlichen am Errichtungserlass aus dem Jahr 2017. Danach soll zumindest die Schaffung einer Befugnis der ZITiS, personenbezogene Daten zu verarbeiten, geprüft werden. Dies gilt insbesondere für solche personenbezogenen Daten, die sie von ihren Bedarfsträgern zwecks Testung oder Training von IT-Systemen erhalten hat. Eine solche Rechtsgrundlage ist aus meiner Sicht notwendig, weil es sich bei dieser Datenverarbeitung um eine Zweckänderung handelt. Zu diesem Zweck sind die Daten ursprünglich nicht erhoben worden, sondern zu polizeilichen oder nachrichtendienstlichen Zwecken. Jede Zweckänderung stellt einen neuen Grundrechtseingriff dar und bedarf daher einer rechtlichen Grundlage. Bislang war von der ZITiS sowie der Bundesregierung immer konstatiert worden, dass die ZITiS keine personenbezogenen Daten verarbeitet.

Die Eckpunkte definieren noch nicht die sog. Behörden des Bundes mit Sicherheitsaufgaben, für die die ZITiS tätig sein soll. Lediglich das Bundespolizeipräsidium, das Bundeskriminalamt und das Bundesamt für Verfassungsschutz werden als unmittelbare Bedarfsträger genannt. Ich werde im Gesetzgebungsverfahren darauf drängen, dass die Behörden des Bundes mit Sicherheitsaufgaben abschließend genannt werden.

Wichtig ist auch, dass im Falle der Schaffung einer spezifischen Rechtgrundlage für die Verarbeitung personenbezogener Daten im ZITiS-Gesetz meiner Behörde Abhilfebefugnisse gegen die ZITiS unmittelbar eingeräumt werden. Außerdem müssen im Fall der Einschränkung von Betroffenenrechten meine Kontroll- und Kompensationsfunktionen gesetzlich verankert werden.

Kritisch sehe ich schließlich die Ankündigung, alle neu einzustellenden Mitarbeitenden der ZITiS einer Sicherheitsüberprüfung unterziehen zu wollen. Das Sicherheitsüberprüfungsgesetz sieht vor, dass nur solche Personen einer Sicherheitsüberprüfung unterzogen werden, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen. Das heißt, die Personen müssten Zugang zu Verschlusssachen haben oder sich verschaffen können oder an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung beschäftigt sein. Die Betrauung mit einer sicherheitsempfindlichen Tätigkeit muss absehbar sein. Eine Sicherheitsüberprüfung auf Vorrat ist unzulässig. Eine Begründung, wonach das gesamte Personal der ZITiS (z. B. auch Personen, die in der Verwaltung arbeiten) mit einer sicherheitsempfindlichen Tätigkeit betraut werden muss, liegt mir bislang nicht vor. Die Tendenz, pauschal alle Neueinstellungen in bestimmten Behörden zu sicherheitsempfindlichen Tätigkeiten zu deklarieren, halte ich für bedenklich.

Querverweise:

Nr.7.10 „Wildwuchs“ bei Überprüfungsverfahren

7.10 Wildwuchs bei Überprüfungsverfahren

Immer mehr Menschen müssen sich in ihrem Berufsleben einer Personenüberprüfung unterziehen, Tendenz steigend. Den sich hieraus ergebenden Problemen stellt man sich ganz nach dem Motto: Was nicht passt, wird passend gemacht!

Die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes sind im Sicherheitsüberprüfungsgesetz (SÜG) geregelt. Die Sicherheitsüberprüfung soll es dem Staat ermöglichen festzustellen, welchen Personen er besonders sensible Dienst- und Staatsgeheimnisse anvertrauen bzw. Zugang zu sicherheitsempfindlichen Stellen innerhalb einer lebens- oder verteidigungswichtigen Stelle ermöglichen kann.

Bereits in meinem 22. Tätigkeitsbericht habe ich von einem zunehmenden Wildwuchs bei Sicherheits- und Zuverlässigkeitsüberprüfungen berichtet (22. TB Nr. 4.8). Neben dem SÜG existieren diverse Regelungen über Zuverlässigkeitsüberprüfungen, z. B. im Atomgesetz und Luftsicherheitsgesetz. Aber auch andere Vorschriften ordnen durch einen Verweis auf das SÜG die Notwendigkeit zur Durchführung einer Sicherheitsüberprüfung an. Zu nennen sind hier das Satellitendatensicherheitsgesetz, das Soldatengesetz, das Reservistengesetz oder das Bundeskriminalamtsgesetz. Die weite Formulierung in § 1 Abs. 2 Nr. 4 SÜG bietet hierfür das Einfallstor. Danach übt eine sicherheitsempfindliche Tätigkeit auch aus, wer nach anderen Vorschriften einer Sicherheitsüberprüfung unterliegt, soweit auf das SÜG verwiesen wird. Aktuelle Vorhaben zeigen, dass der Gesetzgeber auch künftig verstärkt von der Verweismöglichkeit auf das SÜG Gebrauch machen wird und immer mehr Tätigkeitsfelder identifiziert, in denen das Erfordernis einer Sicherheitsüberprüfung existiert. Die Folge sind tausende Neuüberprüfungen und eine zunehmende Unübersichtlichkeit.

Problematisch ist aus meiner Sicht, dass der Gesetzgeber hierbei keine großen Hürden überwinden muss. Es reicht aus, dass die Verweisnorm die Sicherheitsüberprüfung nach dem SÜG anordnet. Hierbei findet jedoch eine Abkehr vom eigentlichen Zweck des SÜG, nämlich dem Geheim- und Sabotageschutz, statt. Andererseits ist im Hinblick auf das aktuelle Weltgeschehen nicht von der Hand zu weisen, dass sich die Bundesrepublik gegen eine steigende Bedrohungslage durch Unterwanderung von extremistischen Gruppierungen oder ausländischen Nachrichtendiensten wappnen muss. Sofern also die Definition der „sicherheitsempfindlichen Stelle oder Tätigkeit“ im Sinne des SÜG nicht mehr im Einklang mit der Lebenswirklichkeit steht, könnte eine Anpassung im Gesetzeswortlaut des SÜG zielführender sein als die vermehrte Anordnung von Sicherheitsüberprüfungen für die gesamte (künftige) Belegschaft einzelner Behörden. Die jeweiligen zuständigen Stellen hätten so die Möglichkeit, die sicherheitsrelevanten Tätigkeitsfelder in Ihrer Behörde zu identifizieren und nur den dort beschäftigten Personenkreis zu überprüfen.

Die derzeitige Vorgehensweise führt an vielen Stellen aufgrund von Überschneidungen mit den vorhandenen Sabotageschutzregelungen zu Mehrfachüberprüfungen betroffener Personen nach § 1 Abs. 2 Nr. 4 SÜG einerseits und § 1 Abs. 4 SÜG andererseits. Dies liegt daran,

dass aktuell die erweiterte Sicherheitsüberprüfung im Sabotageschutz (Ü2-Sab) die einfache Sicherheitsüberprüfung (Ü1) wegen eines abweichenden Prüfumfanges nicht ersetzt. Ziel sollte jedoch sein, jede Person möglichst nur einer Überprüfung nach der höchsten für sie erforderlichen Stufe zu unterziehen.

Zusätzlich verschärft wird die Problematik der Mehrfachüberprüfungen dadurch, dass für einzelne Personen Überprüfungen nach Landesrecht hinzukommen. Im Berichtsjahr hat sich beispielsweise ein Wirtschaftsunternehmen an mich gewandt, das bundesweit Aufträge im Zusammenhang mit Verschlusssachen bearbeitet. Die Mitarbeitenden dieses Unternehmens sind gezwungen, in mehreren Bundesländern (teilweise bis zu vier) Sicherheitsüberprüfungen zu durchlaufen. Der Grund hierfür ist, dass einige Bundesländer die Sicherheitsüberprüfungen anderer Bundesländer nicht als gleichwertig anerkennen. Dies ist aus meiner Sicht verwunderlich, da alle Landesbestimmungen eine Regelung enthalten, die den Verzicht einer Sicherheitsüberprüfung ermöglicht, wenn bereits vor weniger als 5 Jahren eine gleich- oder höherwertige Sicherheitsüberprüfung erfolgreich abgeschlossen wurde. Unnötige Mehrfachüberprüfungen sollen hierdurch gerade verhindert werden. Die Praxis sieht jedoch anders aus. Ich habe die Thematik beim „Arbeitskreis Sicherheit“ der Datenschutzkonferenz zum Erfahrungsaustausch und zur Sensibilisierung vorgetragen. Wünschenswert wäre hier künftig eine genaue und einzelfallbezogene Prüfung anhand der Angaben in der Sicherheitserklärung und den durchgeführten Maßnahmen zur Feststellung, ob die vorhandene Sicherheitsüberprüfung des Mitarbeitenden anerkannt werden kann. Noch besser wäre ein zwischen Bund und Ländern abgestimmtes Gesamtsystem.

Darüber hinaus führt die steigende Anzahl von Sicherheitsüberprüfungen zu Folgeproblemen. So ist auch die Verfahrensdauer in den vergangenen Jahren merklich angestiegen. Dies ist insbesondere in Sicherheitsbehörden ein Problem. Zeit spielt hier eine übergeordnete Rolle. Der Einsatz von sicherheitsüberprüftem Personal ist dort zuweilen von heute auf morgen erforderlich. In einer meiner Kontrollen musste ich feststellen, dass man sich dieses Problems ganz pragmatisch entledigt hat, indem durch eine hauseigene Überprüfung der (freien) Mitarbeitenden auch Erkenntnisse weiterer Stellen abgefragt werden. Eine verfassungsgemäße, gesetzliche Grundlage hierfür existiert nach meinem Dafürhalten nicht. Die zuständige Stelle hat mich um Beratung zur rechtskonformen Ausgestaltung gebeten. Die Beratungen dauern noch an.

Anlässlich der anstehenden Fußball-Europameisterschaft 2024 gewinnt auch das Thema von Personenüberprüfungen ohne bundesweit einheitliche gesetzliche Grundlage erneut Aktualität.

Dem aktuellen und künftig steigenden „Wildwuchs“ von Sicherheitsüberprüfungen in den verschiedenen Geschäftsbereichen sollte entgegengesteuert werden. Der Gesetzgeber sollte die verschiedenen Vorschriften über Zuverlässigkeitsüberprüfungen zusammenführen und eine für alle Überprüfungsarten geltende einheitliche gesetzliche Grundlage schaffen. Insbesondere das Verhältnis zwischen personellem Geheimschutz, vorbeugendem personellen Sabotageschutz und Überprüfungen nach anderen Gesetzen sollte hierbei stimmig geregelt werden. Auf diese Weise ließen sich Mehrfachüberprüfungen von betroffenen Personen vermeiden.

Ich empfehle dem Gesetzgeber, die anstehende Evaluierung des SÜG zu nutzen, um ein schlüssiges Gesamtkonzept für Personenüberprüfungen auf Bundesebene zu entwickeln. Anstelle einer ausufernden Anwendung der Öffnungsklausel auf ganze Behörden, verschiedene Überprüfungsformate außerhalb des SÜG sowie Mehrfachüberprüfungen aufgrund verschiedener Tätigkeiten sollte der Anwendungsbereich des Gesetzes neu definiert werden.

8 Weitere Einzelthemen

8.1 Aktuelles aus der Telematikinfrastruktur und von ihren Anwendungen

Die Telematikinfrastruktur (TI) und auch ihre Anwendungen wie das E-Rezept oder die elektronische Patientenakte (ePA) entwickeln sich stetig weiter. Dabei gewinnt die datenschutzkonforme Umsetzung mehr und mehr an Bedeutung.

E-Rezept

Bereits im Jahr 2020 wurde mit dem Patientendaten-Schutz-Gesetz in den §§ 360 und 361 SGB V festgelegt, dass ärztliche Verordnungen ab dem 1. Januar 2022 elektronisch über die TI übermittelt werden müssen. Das sogenannte E-Rezept ist damit eine Pflichtanwendung – und zwar die erste medizinische überhaupt. Gestartet werden sollte die Anwendung E-Rezept tatsächlich am 1. September 2022 zunächst in der Testregion Westfalen-Lippe. Sie wurde von der Kassenärztlichen Vereinigung Westfalen-Lippe wieder gestoppt.

Rezepte im Rahmen der vertragsärztlichen Versorgung werden in der Anwendung E-Rezept immer in einem zentralen Speicher in der TI abgelegt. Patientinnen und Patienten können dann nur wählen, ob sie die Zugangsinformationen dazu in elektronischer Form oder – nach dem Vorbild eines Bahn- oder Flugtickets – als Papierausdruck mit einem Code-Block zur Einlösung in einer Apotheke ausgehändigt bekommen wollen. Die Vorteile der Digitalisierung ergeben sich, wenn Patientinnen und Patienten auf den Papierausdruck verzichten können, weil sie ihre Rezepte mit der E-Rezept-App über die TI abrufen können und dann auch sicher an die Apotheken zuweisen können. Dazu müssen sie sich mit ihrer elektronischen Gesundheitskarte (eGK) in der TI anmelden. Die dazu benötigten NFC-fähigen eGKs sind schon verbreitet, allerdings ist den meisten Versicherten die ebenfalls benötigte PIN noch nicht von ihren Krankenkassen zugestellt worden. Ich appelliere an die Verantwortlichen, mehr Versicherte mit NFC-fähiger eGK und PIN auszustatten.

Damit bis dahin Versicherte die E-Rezepte nicht unverschlüsselt per E-Mail an die Apotheken senden, hat die gematik das Verfahren „Versenden von E-Rezepten ohne Anmelden in der TI“ spezifiziert: Versicherte können ihre E-Rezepte-Codes durch Abfotografieren in ihre E-Rezept-App hinzufügen. Von da können sie sie dann verschlüsselt mittels eines speziellen Dienstleisters über das Internet an die Apotheke ihrer Wahl senden. Dieser Versand erfolgt zwar nicht über die TI und es ergeben sich gewisse Nachteile, da keine Protokollierung der Zuweisung im Fachdienst stattfindet, meine Prüfung hat aber keine grundsätzlichen datenschutzrechtlichen Hinderungsgründe ergeben.

Parallel habe ich ein durch die gematik vorgeschlagenes Verfahren geprüft, bei dem Versicherte in den Apotheken ihre eGK in das Kartenlesegerät (ohne PIN-Eingabe) stecken und die Apotheke so alle E-Rezepte vom zentralen E-Rezepte-Server abrufen kann. Ich begrüße eine barrierearme Möglichkeit, E-Rezepte in den Apotheken einzulösen, die die bestehenden Möglichkeiten ergänzt. Ein Medienbruch durch einen Ausdruck oder das Installieren einer App auf dem Smartphone wären so nicht nötig. Über die TI könnten die Rezepte auch sicher zur Apotheke gelangen. Die konkrete, von der gematik vorgeschlagene technische Umsetzung zeigte allerdings erhebliche Mängel auf, die ein hohes Risiko für alle Versicherten bedeuten würden, dass Unbefugte auf ihre Rezeptdaten zugreifen, selbst wenn diese nicht diesen Einlösungsweg selbst nutzen. Deshalb habe ich der gematik mitgeteilt, dass ich der Lösung so nicht zustimmen kann. Gleichzeitig habe ich Vorschläge unterbreitet, wie die Funktion „Einlösen durch Stecken der eGK“ sicher umgesetzt werden kann, ohne Komfort für Versicherte einzubüßen. Hierzu befinde ich mich aktuell in Gesprächen mit der gematik.

Alternatives Authentifizierungsverfahren

Bereits in meinem Tätigkeitsbericht für das Jahr 2020 (29. TB Nr. 4.2) habe ich das nicht den Vorgaben der DSGVO entsprechende Authentifizierungsverfahren der ePA kritisiert. Konkret bezog sich meine Kritik auf das Verfahren der „Alternativen Versichertenidentität (al.vi)“,

mit dem Versicherte sich entsprechend dem § 336 Abs. 2 SGB V auch ohne Einsatz ihrer eGK an ihrer ePA anmelden können. Weil Gesundheitsdaten besonders sensibel sind, bedürfen Zugriffe auf die ePA immer hochsicherer Authentifizierungsverfahren, die stets dem aktuellen Stand der Technik entsprechen müssen. Für einen datenschutzkonformen Zustand bedarf es auch bei al.vi der Gewährleistung eines höchstmöglichen Sicherheitsniveaus, das al.vi allerdings nicht bietet. Somit wurde al.vi von mir lediglich für einen Zeitraum von zwei Jahren geduldet, um der gematik die Gelegenheit zu bieten, al.vi bis zum 31. Dezember 2022 durch ein geeignetes sicheres Authentifizierungsverfahren abzulösen.

Da ein solches Authentifizierungsverfahren noch nicht spezifiziert ist, hat gematik mich gebeten, meine Duldung um ein Jahr bis zum 31. Dezember 2023 zu verlängern. Hierzu habe ich diverse Gespräche mit der gematik geführt, in denen die gematik verbindlich versichert hat, dass al.vi zum 31. Dezember 2023 in jedem Fall abgeschaltet werden soll. Unter dieser Maßgabe und den Bedingungen, dass die gesetzlichen Krankenkassen alle Versicherten, die bis zum 31. Dezember 2022 eine ePA beantragt haben, verbindlich bis spätestens zum 30. Juni 2023 sowie alle Versicherten, die eine ePA nach dem 31. Dezember 2022 beantragen, gleichzeitig mit einer eGK mit NFC-Schnittstelle und PIN ausstatten werden, habe ich mein befristetes Einvernehmen zu al.vi bis zum 31. Dezember 2023 verlängert.

Sachstand zum Gerichtsverfahren zur elektronischen Patientenakte

In meinem 30. Tätigkeitsbericht (Nr. 6.1) habe ich darüber berichtet, dass fünf Krankenkassen gegen von mir verhängte datenschutzaufsichtsrechtliche Maßnahmen zur Durchsetzung einer europarechtskonformen Ausgestaltung der elektronischen Patientenakte (ePA) geklagt haben. In der Zwischenzeit haben die meiner Aufsicht unterliegenden Krankenkassen die gesetzlichen Vorgaben des § 342 Abs. 2 Nr. 2 lit. b) SGB V fristgerecht umgesetzt und ihren Versicherten eine von der gematik GmbH zugelassene ePA der Stufe 2 zum 1. Januar 2022 zur Verfügung gestellt. Damit können zumindest Frontend-Nutzer und von Frontend-Nichtnutzern befugte Vertreter eine Einwilligung gegenüber Zugriffsberechtigten in den Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der ePA barrierefrei erteilen („feingranulares Zugriffsmanagement“). Für die Frontend-Nichtnutzer, die keinen Vertreter einsetzen können oder möchten, bleibt es jedoch dabei, dass Ihnen über die Nutzung der dezentralen Infrastruktur der Leistungserbringer nur ein eingeschränktes, sog. mittelgranulares Zugriffsmanagement zur Verfügung steht. Zudem hat diese Nutzergruppe mangels Terminal- oder anderweitiger Lösung weiterhin keine Möglichkeit, Einsicht in die eigene ePA zu nehmen.

Die betroffenen Krankenkassen wehren sich weiterhin – unter Einsatz von Versichertengeldern – gegen die von mir erteilten Weisungen. Die Klageverfahren, die vor vier Kammern des Sozialgerichts Köln rechtshängig sind, dauern dementsprechend an.

Datenschutzrechtliche Verantwortlichkeit bei den Konnektoren

Leistungserbringer wie Arztpraxen und Krankenhäuser verfügen über sichere Zugangsrouter zur TI. Auf diesen sogenannten Konnektoren werden technische Protokolle gespeichert. In bestimmten Fällen kam es dabei zu Datenschutzverletzungen aufgrund einer fehlerhaften Speicherung von Seriennummern der eGK-Zertifikate in den Konnektoren eines Herstellers.[62] Dies hat gezeigt, dass die gesetzlich festgelegte Zuweisung der datenschutzrechtlichen Verantwortung an die Nutzer von dezentralen Komponenten der TI wie den Konnektoren nicht zufriedenstellend ist. Nach § 307 Abs. 1 SGB V sind für die Konnektoren diejenigen datenschutzrechtlich verantwortlich, die diese für gesetzlich beschriebene Zwecke nutzen, soweit sie über die Mittel der Datenverarbeitung mitentscheiden. Diese Verantwortlichkeit erstreckt sich insbesondere auf die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Konnektoren.

Die Datenschutzverletzungen verdeutlichten, dass die Nutzer von Konnektoren, mithin die Leistungserbringer, dem Fehlverhalten machtlos gegenüberstanden. Sie waren und werden nicht in der Lage sein, selbst Veränderungen an den Konnektoren zu bewirken oder zu veranlassen. Sie sind davon abhängig, dass die Konnektoren ordnungsgemäß arbeiten und müssen sich dabei auf Andere wie z. B. die Hersteller der Konnektoren und auf die Zulassung durch die gematik verlassen.

Den Datenschutzvorfall habe ich zum Anlass genommen, gegenüber dem Bundesministerium für Gesundheit eine Neuregelung des § 307 Abs. 1 SGB V anzuregen. Diese könnte eine gemeinsame Verantwortung der gematik mit den Nutzern entsprechend dem Datenschutzkonferenz-Beschluss vom 12. September 2019 (s. 28. TB Nr. 4.2.1) vorsehen.

Opt-out Debatte bei der elektronischen Patientenakte

Die elektronische Patientenakte, ePA, wie sie mit dem Patientendaten-Schutz-Gesetz in den §§ 341 ff. SGB V

62 siehe auch meinen FAQ, abrufbar unter www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/01_FAQ-TI-Konnektoren.htm

geregelt wurde, ist eine versichertengeführte elektronische Akte und stellt insbesondere auf die Patientensouveränität ab. Die Nutzung ist für Versicherte freiwillig. Sie entscheiden von Anfang an, welche Daten gespeichert werden, wer zugreifen darf und ob Daten wieder gelöscht werden. Diese ePA spiegelt eine vollständige Opt-in-Lösung wieder.

Im Koalitionsvertrag 2021-2025 zwischen SPD, Bündnis 90/Die Grünen und FDP erklärten die Regierungsparteien, die Einführung der ePA beschleunigen zu wollen. Alle Versicherten sollten DSGVO-konform eine ePA zur Verfügung gestellt bekommen; ihre Nutzung sei freiwillig (Opt-out). Durch diese Aussage im Koalitionsvertrag wurde die Debatte um eine Opt-out-Lösung bei der ePA ausgelöst bzw. verstärkt.

Unklar ist allerdings bis jetzt, wie die Opt-out-Lösung im Detail aussehen soll. Ob jedem der ca. 73 Mio. gesetzlich Versicherten ein leerer digitaler Aktenordner mit rein administrativen Daten zur Verfügung gestellt werden soll oder ob bereits eine automatische Befüllung der ePA mit medizinischen Daten erfolgen soll. Ferner, ob alle Leistungserbringer auf alle Gesundheitsdaten in der ePA zugreifen dürfen oder ob sogar die Gesundheitsdaten der ePA direkt der medizinischen Forschung zur Verfügung gestellt werden. Es sind viele unterschiedliche Gestaltungsmöglichkeiten denkbar, gegen die die Versicherten nur nachträglich einen Widerspruch, also ein Opt-out, aussprechen könnten.

Grundsätzlich sehe ich keine Notwendigkeit für den angestrebten Paradigmenwechsel zu einer Opt-out-ePA. Auch eine versichertengeführte ePA hat das Potenzial, Nutzen für die Gesundheitsversorgung zu bringen, wenn die Akzeptanz und das Vertrauen in ePA bei den Versicherten durch vermehrte Information und Werbung über die Vorteile einer ePA stärker gefördert würde. Die bisherige geringe Nutzung ist auf den noch nicht ersichtlichen Mehrwert für die Versicherten zurückzuführen, nicht auf die Umsetzung einer Opt-in-Lösung.

Auch wenn aus meiner Sicht eine ePA-Opt-out-Lösung nicht erforderlich ist, begrüße ich, dass die Koalitionäre eine DSGVO-konforme Lösung anstreben und werde hierzu beraten. Erste Gespräche haben bereits stattgefunden.

8.2 Digitale Gesundheitsanwendungen

Der Prozess, für die erstattungsfähigen digitalen Gesundheitsanwendungen den Nachweis der Datenschutzkonformität durch ein Zertifikat nachweisen zu können, schreitet deutlich voran und ist auf einem guten Weg, das bisherige, unzureichende Verfahren der Selbsterklärung der Hersteller, abzulösen.

Im Hinblick auf das vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) gemäß § 139e Abs. 1 SGB V geführte Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen (DiGA) nach § 33a SGB V konnte das Einvernehmen hinsichtlich der Festlegung der Prüfkriterien fristgemäß zum 31. März 2022 durch mich erklärt werden (vgl. 30. TB Nr. 6.9).

Damit wurde ein großer Schritt zur Ablösung des bisherigen Verfahrens, der Nachweisführung der Erfüllung der datenschutzrechtlichen Anforderungen unter Verwendung einer Selbsterklärung der Hersteller, erfolgreich abgeschlossen.

Perspektivisch soll der Nachweis der Erfüllung der datenschutzrechtlichen Anforderungen unter Verwendung eines Zertifikates nach Art. 42 DSGVO geführt werden (vgl. Nr. 8.16).

Für die Zertifizierung der digitalen Gesundheitsanwendungen strebt das BfArM auch die Rolle des Programmeigners an. Dies bedeutet, dass das BfArM neben den materiellen Prüfkriterien auch festlegt, wie die jeweiligen Kriterien im Zertifizierungsverfahren zu prüfen und nachzuweisen sind.

Als Programmeigner stellt das BfArM das Prüfprogramm nach dessen Fertigstellung Dritten, welche die eigentliche Zertifizierung durchführen, mittels der Gewährung von Lizenzen zur Nutzung zur Verfügung. Ich begleite das noch laufende Verfahren zur Erstellung des Prüfprogramms beratend und gehe von einer Fertigstellung im Laufe des Jahres 2023 aus.

Querverweise:

8.16 Zertifizierung und Akkreditierung

8.3 Sormas (follow up)

Die Weiterentwicklung des Programms SORMAS zur digitalen Kontaktnachverfolgung in den Gesundheitsämtern erforderte auch in diesem Jahr eine engmaschige Begleitung durch die Datenschutzaufsichtsbehörden.

Auch in diesem Jahr habe ich gemeinsam mit mehreren Landesbeauftragten das vom Bundesministerium für Gesundheit (BMG) geförderte und von der Helmholtz-Zentrum für Infektionsforschung GmbH (HZI) durchgeführte Forschungsprojekt SORMAS@DEMIS, bei dem es sich um die Entwicklung einer Software zur digitalen Kontaktnachverfolgung in den Gesundheitsämtern handelt, datenschutzrechtlich begleitet (30. TB Nr. 4.1.2).

Aufgrund dieser intensiven Beratung konnten deutliche Verbesserungen insbesondere in der technischen Umsetzung erreicht werden. Diese Verbesserungen wurden unter anderem durch die konkreten Anpassungen und Ergänzungen beim Kryptografiekonzept, im Pseudonymisierungskonzept, im IT-Sicherheitskonzept sowie in der Datenschutz-Folgenabschätzung erzielt.

Da die Förderung des Projektes durch das BMG zum 31. Dezember 2022 ausgelaufen ist, wurde bereits im Sommer 2022 zur Gewährleistung der Weiterführung des Projektes und des Angebotes der Software für die Gesundheitsämter die gemeinnützige SORMAS-Stiftung (SORMAS Foundation) gegründet. Diese hat ab Januar 2023 die Aufgabe, die Bereitstellung und Weiterentwicklung von SORMAS zu unterstützen. Der eigentliche Betrieb der Software wird weiterhin durch die Netzlink GmbH betrieben. Im Hinblick auf das Hosting der Daten ist mittelfristig auch eine Migration der Daten vom ITZBund zu einem von der Netzlink GmbH betriebenen Server geplant. Dies soll voraussichtlich bis Juni 2023 abgeschlossen sein.

Aufgrund dieser Neuausrichtung ist auch die datenschutzrechtliche Beratung im Rahmen des zum 31. Dezember 2022 auslaufenden Forschungsprojektes durch mehrere Landesbeauftragte für den Datenschutz und mir abgeschlossen worden. Diese wird zukünftig durch die jeweils zuständigen Landesbeauftragten erfolgen.

8.4 Nutzung der Krankenversichertennummer (follow up)

Der Gesetzgeber schafft die notwendige gesetzliche Grundlage zur Nutzung der Krankenversichertennummer in der Telematikinfrastruktur.

Im 30. Tätigkeitsbericht (Nr. 6.5) habe ich meine Forderung nach einer eindeutigen Legitimationsgrundlage für die Nutzung der Krankenversichertennummer (KVNR) in der Telematikinfrastruktur dargelegt. Dieser Forderung ist der Gesetzgeber mit dem Gesetz zur Pflegepersonalbemessung im Krankenhaus sowie zur Anpassung weiterer Regelungen im Krankenhauswesen und in der Digitalisierung (Krankenhauspflegeentlastungsgesetz – KHPflEG) nachgekommen. So sieht § 290 Abs. 4 SGB nunmehr die Befugnis zur Verwendung der KVNR im Rahmen der Telematikinfrastruktur von Anbietern und Nutzern von Anwendungen und Diensten im Sinne von § 306 Abs. 4 Satz 1 und 2 zur eindeutigen Identifikation des Versicherten vor, soweit dies für die eindeutige Zuordnung von Daten und Diensten bei der Nutzung dieser Anwendungen und Dienste erforderlich ist.

Die ebenfalls von mir geforderte Rechtsgrundlage für die Einbeziehung der Unternehmen der privaten Krankenversicherung (PKV) sowie weiterer Kostenträger in das Clearing-Verfahren zum Ausschluss einer Doppelvergabe der KVNR wurde durch eine Ergänzung des § 290 Abs. 3 SGB V mit dem Gesetz zur Stärkung des Schutzes der Bevölkerung und insbesondere vulnerabler Personengruppen vor COVID-19 (COVID-19-Schutzgesetz) geschaffen und ist am 17. September 2022 in Kraft getreten (vgl. BGBl. I S. 1454).

8.5 Corona-Warn-App: Änderungen 2022

Nicht alle Veränderungen in der Corona-Warn-App finde ich gelungen

Auch im Jahr 2022 habe ich meine Beratungen zur Corona-Warn-App (CWA) fortgesetzt. Aufgrund der bereits etablierten Prozesse in der CWA und des Rückgangs der Infektionen wurden wenige Änderungen angegangen. Da laut Einschätzung des Projektteams viele Releases ohne datenschutzrechtliche Veränderungen auskamen, wurde meine Beratung nur in einigen Fällen genutzt. Und so erfuhr ich von mancher Veränderung dann leider auch nur über die Presse. Dies betraf auch die Neuerungen zu einer veränderten farblichen Ausgestaltung der Zertifikatsansicht. Durch eine Anzeige in grüner Färbung sollte erkennbar sein, ob die Voraussetzungen zur Ausnahme von einer Maskenpflicht vorliegen – sofern ein Bundesland diese anordnen

würde. Erst auf meine kritische Nachfrage hin wurden mir diese Pläne dann durch das Bundesministerium für Gesundheit und das Robert Koch-Institut vorgestellt. Leider fanden nicht alle im Rahmen meiner Beratung eingebrachten Empfehlungen in diesem Fall Gehör. Vielmehr wurde die CWA entgegen meiner Empfehlung mit einer automatischen Berechnung und farblichen Darstellung der Maskenpflicht in der Zertifikatsansicht ausgestattet. Natürlich kann es für einen Nutzer sehr hilfreich sein, sich die jeweils gültige Maskenpflicht zum jeweiligen Bundesland berechnen zu lassen. Präsentiert die nutzende Person das Zertifikat, kann auch eine prüfende Instanz (Gastwirt etc.) dann direkt in der App ablesen, ob eine Maskenpflicht besteht oder nicht. Die Berechnung hätte jedoch auch erst auf Verlangen der nutzenden Person durchgeführt und das Ergebnis der Berechnung auch abseits der Zertifikatsansicht in der CWA angezeigt werden können. Für die datensparsame Prüfung der Zertifikate ist explizit die CovPassCheck-App entwickelt worden. Folgerichtig hätte eine Bewertung der Maskenpflicht für die prüfende Instanz nur in dieser App umgesetzt werden müssen – und nicht in der CWA!

Auch hier gilt also, dass die datenschutzkonforme Umsetzung bereits bei der Formulierung von Vorschriften im Blick sein sollte. Die Nachweispflicht greift in das Grundrecht auf informationelle Selbstbestimmung ein und bedarf der sorgfältigen Begründung. Ist der Nachweis aus Gründen des Gesundheitsschutzes unabdingbar, muss eine zielführende Kontrolle möglich sein. Ein knapper Blick auf eine farbige Anzeige im Display erfüllt die Anforderungen nicht.

Allerdings hat meines Wissens bisher (bis zum Redaktionsschluss dieses Tätigkeitsberichts) kein Bundesland eine entsprechende Regelung der Maskenpflicht erlassen, so dass dieses Feature keine Anwendung findet.

Insgesamt bleibt anzumerken, dass bei möglichen Weiterentwicklungen der CWA darauf zu achten ist, das hohe Vertrauen der Bürgerinnen und Bürger in die App nicht durch Hinzunahme weiterer, datenschutzrechtlich komplexerer Funktionen zu beeinträchtigen.

8.6 Registermodernisierung/ OZG-Umsetzung

Die Registermodernisierung zwischen neuem Aufbruch und Detailarbeit: Kann das Recht auf informationelle Selbstbestimmung auch dann gewährleistet werden, wenn der Staat die Fäden zur Datenzusammenführung in der Hand hält?

Mit Verkündung des Registermodernisierungsgesetz (RegMoG) am 6. April 2021 im Bundesgesetzblatt begann eine neue Phase dieses Großprojektes der Verwaltungsdigitalisierung. Die Federführung im BMI sowie in Bayern, Hamburg, Nordrhein-Westfalen und Baden-Württemberg haben gemeinsam im Oktober 2021 die Gesamtsteuerung Registermodernisierung eingerichtet, um die zahlreichen Anforderungen aus verschiedenen Rechtsbereichen erfüllen zu können. Zu den Anforderungen gehören u. a. die Umsetzung des Once-Only-Prinzips, sowohl im Sinne des Onlinezugangsgesetz (OZG) als auch im Sinne der DSGVO, sowie die Einführung eines registerbasierten Zensus. Selbstgesetztes Ziel der Gesamtsteuerung ist es hierfür, ein umfassendes interbehördliches Kommunikationssystem (OOTS) zu schaffen. Dieses System soll den direkten Nachweisaustausch sowohl zwischen nationalen wie auch europäischen Behörden gewährleisten. Die nunmehr – entgegen meinem Rat – als Identifikationsnummer eingesetzte Steuer-ID bildet dabei das zentrale Rückgrat.

Once-Only-Prinzip

Ziel des Once-Only-Prinzips ist es, dass Bürger und Unternehmen bestimmte Standardinformationen den Behörden und Verwaltungen nur noch einmal mitteilen müssen. Unter Einbeziehung von Datenschutzbestimmungen und der expliziten Zustimmung der Nutzer ist es der öffentlichen Verwaltung erlaubt, die Daten wiederzuverwenden und untereinander auszutauschen.

Wie bereits in meinen vorangegangenen Tätigkeitsberichten (siehe 29. TB Nr. 5.1, 28. TB Nr. 5.5, 27. TB Nr. 9.2.2) dargelegt, halte ich die derzeitige Ausgestaltung der IDNr für nicht vereinbar mit dem Grundrecht auf informationelle Selbstbestimmung und damit das IDNrG als Teil des RegMoG für verfassungswidrig. Zusammen mit der Datenschutzkonferenz habe ich ausdrücklich davor gewarnt, auf die Steuer-ID als einheitliches, bereichsübergreifendes Personenkennzeichen zu setzen. Es besteht weiterhin die Gefahr, dass das technische Rückgrat der bürgernahen Verwaltungsdigitalisierung auf verfassungsrechtlichem Sand gebaut wurde. Eine Gefahr, die neben dem Bundesrat und dem Wissenschaftlichen Dienst des Bundestags auch die aktuelle Bundesregierung erkannt hat, indem sie selbst eine verfassungsfeste Registermodernisierung fordert (siehe Koalitionsvertrag, S. 15).

Diese fundamentale Problematik hat sich mit der Implementierung der Gesamtsteuerung Registermodernisierung nicht erledigt. Sie schwebt viel mehr wie ein Damoklesschwert über dieser Phase, die sich eigentlich ganz der Umsetzung dieses wichtigen Bausteins widmen sollte. Diese Situation hat auch Auswirkungen auf meine beratende Tätigkeit. Auf der einen Seite arbeite ich weiterhin mit leitenden Stellen und Entscheidungsträgern daran, einen alternativen Ansatz zur bisherigen IDNr zu entwickeln. Im Gespräch sind dabei sowohl bekannte datenschutzfreundliche Modelle, wie der Einsatz von bereichsspezifischen Kennzeichen, als auch gänzlich neue Ansätze. Das oberste Ziel bleibt dabei die Herstellung der Augenhöhe zwischen Staat und Bürger. Hierfür bleiben Transparenz, Beteiligung und strukturelle Zusammenführungshindernisse die entscheidenden Faktoren, die auch jede diskutierte Alternative gewährleisten muss.

Auf der anderen Seite beteilige ich mich, gemeinsam mit Vertretern der DSK, trotz der grundsätzlichen Bedenken gerne und seit Beginn an der Gesamtsteuerung Registermodernisierung. Meine Behörde und ich sind dabei aktuell auf mehreren Ebenen aktiv und wirken hinsichtlich übrigen Elemente neben der IDNr darauf hin, die informationelle Augenhöhe soweit wie möglich auch dort herzustellen. Diese Ebenen der Gesamtsteuerung gliedern sich in die strategische Steuerung (Lenkungskreis, Transformationseinheit), die operative Steuerung (Projekteboard, Beiräte und Kompetenzteams) sowie einzelne Unterprojekte. Der Lenkungskreis berichtet direkt an den IT-PLR. Der IT-PLR bleibt die politische Steuerung der Registermodernisierung. In beratender Tätigkeit bin ich derzeit vorwiegend im Lenkungskreis sowie im sog. Kompetenzteam Recht / Datenschutz aktiv.

Meine Beratungen konzentrieren sich aktuell insbesondere auf die Konzeptionierung des bereits erwähnten OOTS. Dieses Kommunikationssystem soll die technische und architektonische Grundlage dafür werden, den Once-Only-Ansatz in Deutschland umsetzen zu können. Das OOTS gliedert sich dabei in den nationalen und den europäischen Teil. Der nationale Teil soll die Kommunikation zwischen nationalen Behörden und Registern in der Art ermöglichen, dass ohne nochmalige direkte Erhebung beim Bürger, relevante Nachweise für (z. B. im Rahmen des OZG) digitalisierte Verwaltungsprozesse direkt ausgetauscht werden können.

In gemeinsamer Arbeit mit den federführenden Stellen wurden dabei die Grundlagen des geplanten Prozesses entwickelt, mit einem besonderen Fokus auf die Gewährleistung der Transparenz. Zeitgleich beriet ich das Kompetenzteam Recht / Datenschutz zu Fragen der geplanten gesetzlichen Umsetzung (sog. Once-Only-Generalklausel). Insbesondere begrüße ich dabei die geplante Einrichtung einer technischen Vorschaufunktion, die dem Bürger im Rahmen seines digitalen Antragsprozesses den vorgesehenen Nachweis vor der tatsächlichen Übermittlung bildlich darstellen soll. Eine Funktion, die meines Erachtens zwingend notwendig ist, um das für hergebrachte Verwaltungsprozesse bestehende verfassungsrechtliche Gleichgewicht zwischen dem Recht auf informationelle Selbstbestimmung und dem staatlichen Interesse an Verwaltungseffizienz in die digitale Zeit hinüberzutragen.

Darüber hinaus soll die geplante Generalklausel auch die Nutzung der IDNr für Stellen ermöglichen, die bisher nicht vom IDNrG direkt erfasst wurden (in der Regel nicht-registerführende Stellen, die OZG-Leistungen anbieten). Die Idee eines derart ganzheitlichen Gesetzesansatzes ist dabei nicht zwingend datenschutzrechtlich bedenklich. Besonders wichtig ist meines Erachtens dabei jedoch, dass wenigstens die bereits im IDNrG geltenden Anforderungen an die Verarbeitung der IDNr dann ebenso zentral für die neu erfassten Stellen verpflichtend gemacht werden. Die besonderen Ausgleichsmaßnahmen, wie u. a. das Datenschutzcockpit, der IDNr

haben dieser stets zu folgen. Dieser Grundsatz gilt auch, wenn ich die bisher geregelten Maßnahmen, wie bereits erwähnt, für an sich nicht ausreichend erachte.

Das Datenschutzcockpit als mit der Gesamtsteuerung Registermodernisierung assoziiertes Unterprojekt ist Gegenstand intensiver Beratung. Das Projekt befindet sich seit September 2021 in der Umsetzungsphase. Die DSK und ich haben zusammen mit den Federführern Bremen sowie dem BMI vor allem zur technischen Ausgestaltung, inklusive dem Datenübermittlungsstandard, sowie zu verschiedenen Rechtsfragen aus dem IDNrG beraten. Insbesondere fällt meines Erachtens bereits die erstmalige Einspeicherung der IDNr in die Register / öffentliche Stellen als „Nutzung" unter die Pflicht zur Protokollierung im Sinne des § 9 IDNrG und Anzeige im Datenschutzcockpit. Den Bürgerinnen und Bürgern muss von Anfang an die notwendige Transparenz gewährt werden, um den Lauf ihrer durch die IDNr einfacherer erfassbaren personenbezogenen Daten problemlos nachvollziehen zu können.

Nur durch einen ganzheitlichen Ansatz, der das Recht auf informationelle Selbstbestimmung auch in einer neuen, digitalen Umgebung zur Entfaltung kommen lässt, kann das Ziel der Registermodernisierung nachhaltig erreicht werden.

8.7. Betriebliches Eingliederungsmanagement (BEM)

Gerade für das BEM-Verfahren unabdingbar: eine vertrauensvolle Zusammenarbeit zwischen Beschäftigungsstelle und den betroffenen Beschäftigten auf Basis einer transparenten Datenverarbeitung. Vor diesem Hintergrund ist die Frage zu bewerten, ob die Gleichstellungsbeauftragte eine Kopie des Einladungsschreibens erhalten darf.

Das BEM ist ein Instrument, um Beschäftigte mit längeren Arbeitsunfähigkeitszeiten den Wiedereinstieg in das Arbeitsleben zu erleichtern. Das Verfahren verfolgt den Zweck, die Ursachen von Arbeitsunfähigkeit zu ergründen und gemeinsam nach einer Möglichkeit zu suchen, künftige Arbeitsunfähigkeitszeiten zu vermeiden oder zu verringern. Da in dem Verfahren regelmäßig Daten über Erkrankungen als sensible Daten im Sinne des Art. 9 DSGVO verarbeitet werden und dies gemäß § 167 Abs. 2 Sozialgesetzbuch Neuntes Buch (SGB IX) nur auf der Grundlage einer informierten und freiwilligen Zustimmung der oder des Beschäftigten erfolgen darf, ist dieser Aspekt immer wieder ein Thema in meiner praktischen Arbeit.

Damit das BEM-Verfahren zum Erfolg führen kann, ist eine vertrauensvolle Kommunikation und Zusammenarbeit zwischen allen Beteiligten unabdingbar. Nur wenn eine Vertrauensbasis geschaffen und die beschäftigte Person darüber aufgeklärt wurde, welche ihrer personenbezogenen Daten von wem und für welchen Zweck verwendet werden, kann sie sich angstfrei auf das BEM einlassen.

Wie das BMI in seiner Personalaktenrichtlinie festgelegt hat, ist es daher geboten, dass das BEM-Verfahren nicht von Beschäftigten, die mit Aufgaben der Laufbahnbetreuung betraut sind, durchgeführt wird. Alle Daten, die im Rahmen eines BEM erhoben wurden, sind außerhalb der Personalakte aufzubewahren. Hierfür ist eine gesonderte BEM-Akte anzulegen, die als Sachakte außerhalb der personalverwaltenden Stelle zu führen ist. Beschäftigte der Personalverwaltung dürfen auf diese Akte nicht zugreifen.

Aufgrund einer Beratungsbitte habe ich mich aktuell mit der Frage auseinandergesetzt, ob die Gleichstellungsbeauftragte (GleiB) bei Einleitung eines BEM-Verfahrens standardmäßig eine Kopie des Einladungsschreibens an die oder den Beschäftigten erhalten kann. Soweit ersichtlich, ist diese Frage höchstrichterlich bislang noch nicht entschieden worden.

Meines Erachtens ist hier bei der aktuellen Gesetzeslage entscheidend, wie das Verhältnis der Vorschriften § 25 Abs. 2 Nr. 2 i.V.m. § 27 Abs. 2 Nr. 2 Bundesgleichstellungsgesetz (BGleiG) und § 167 Abs. 2 SGB IX zueinander ausgelegt wird. Grundsystematisch besteht zwischen der Regelungsmaterie des BGleiG und der des SGB IX kein genereller Vorrang für eine der beiden Materien. Gleichberechtigung sowie Rehabilitation und Teilhabe von Menschen stehen zunächst einmal als Rechtsgüter gleichberechtigt nebeneinander.

Rein vom Wortlaut her kann man das BEM-Verfahren unter den Begriff der „sozialen Angelegenheiten" subsumieren mit der Folge, dass es Aufgabe der GleiB wäre, diese Verfahren zu überwachen und ihr gemäß § 27 Abs. 2 Nr. 2 BGleiG frühzeitig alle Informationen dazu zur Verfügung zu stellen. Allerdings ist die Bezeichnung „soziale Angelegenheit" schon für sich genommen ein relativ unbestimmter Begriff, der nicht nahelegt, dass beim Erlass der betreffenden Vorschriften der Gesetzgeber sich spezifische Gedanken zum BEM-Verfahren gemacht hat und dazu bewusst Regelungen treffen wollte.

Demgegenüber enthält § 167 Abs. 2 SGB IX spezifische und detaillierte Einzelregelungen zum BEM-Verfahren. Insbesondere legt die Vorschrift fest, wer Beteiligter, zum Teil mit welchen Vorgaben, des Verfahrens sein kann. Eine Überwachungsaufgabe wird explizit dem Personalrat zugewiesen. Dass sich die Vorschrift sehr

dezidiert mit unterschiedlichen Teilnehmern (Personalrat, Schwerbehindertenvertretung, Betriebs-/Werksarzt usw.) und deren Aufgaben beschäftigt und gleichzeitig zur Gleichstellungsbeauftragten nichts sagt, spricht dafür, dass der Gesetzgeber der Gleichstellungsbeauftragten keine Aufgabe innerhalb dieses speziellen Verfahrens zuweisen will.

Es kommt hinzu, dass der Gesetzgeber sich im Kontext des Teilhabestärkungsgesetzes vom 2. Juni 2021 erneut mit dem Teilnehmerkreis beschäftigt und mit § 167 Abs. 2 Satz 2 SGB IX für die betroffene Person die neue Möglichkeit geschaffen hat, zusätzlich eine eigene Vertrauensperson hinzuziehen zu können. Die GleiB hat er weiterhin nicht gesondert in die spezifische BEM-Verfahrensregelung aufgenommen.

Insgesamt ist § 167 Abs. 2 SGB IX damit aus meiner Sicht bei der derzeitigen Gesetzeslage als lex specialis anzusehen, der den Rückgriff auf die allgemeineren Vorschriften der §§ 25 Abs. 2 Nr. 2, 27 Abs. 2 Nr. 2 BGleiG als Rechtsgrundlage sperrt. Es fehlt damit an einer hinreichenden Rechtsgrundlage, die eine standardmäßige Übermittlung von personenbezogenen Daten im Zusammenhang mit dem BEM-Verfahren an die GleiB ermöglicht.

8.8 Zensus 2022

Die Durchführung des Zensus hat auch in diesem Jahr zu zahlreichen Eingaben von Bürgerinnen und Bürgern geführt. Insbesondere die Einbindung eines US-amerikanischen IT-Dienstleisters in den Betrieb der Internetseite zum Zensus hat die Zahl der Beschwerden in die Höhe schießen lassen.

Nach Verlegung um ein Jahr ist im Mai 2022 der offizielle Startschuss für den Zensus gefallen. Die statistischen Landesämter und ihre Erhebungsstellen haben die Gebäude- und Wohnungszählung sowie die Haushaltebefragung durchgeführt. Unter den Eingaben und Beschwerden zur konkreten Durchführung dieser Erhebungen gab es auch immer wieder Fragen und Kritik zu den gesetzlichen Bestimmungen. So äußerten viele Einsender und Anrufer etwa ihr Unverständnis über die geforderte Angabe der Namen von Wohnungsinhabern als Hilfsmerkmale der Gebäude- und Wohnungszählung. Insoweit ist zumindest eine unzureichende Aufklärung der statistischen Ämter über die Erforderlichkeit dieser Angaben festzustellen.

In weiteren Einsendungen an mich wurde auch ein Ausschluss der Betroffenenrechte nach der DSGVO thematisiert und meine Hilfe erbeten. Da solche nach der DSGVO grundsätzlich zulässigen Einschränkungen auf landesrechtliche Regelungen zurückzuführen sind, musste ich in diesen Fällen auf die Zuständigkeit der Kolleginnen und Kollegen der Datenschutzaufsichtsbehörden der Länder verweisen. Diese haben ihrerseits wiederum zahlreiche Eingaben zu dem vom Statistischen Bundesamt erstmalig angebotenen Online-Verfahren zum Zensus zuständigkeitshalber an mich weitergeleiteten müssen. Diesen unfreiwilligen „Austausch“ zwischen den Aufsichtsbehörden von Bund und Ländern werte ich als Beleg für die von mir schon im Gesetzgebungsverfahren als unzureichend kritisierte Festlegung der konkreten Verantwortlichkeiten der beteiligten datenverarbeitenden Stellen von Bund und Ländern.

Die Mehrzahl der Anfragen und Beschwerden in meinem Zuständigkeitsbereich erreichte mich seit Mitte Mai 2022. Hauptgegenstand dieser Eingaben war die Einbindung eines US-amerikanischen IT-Dienstleisters im Zusammenhang mit der Bereitstellung der Internetseiten zum Zensus 2022 und die darauf bezogene Befürchtung eines nicht autorisierten Abflusses von persönlichen Daten zum Zensus in die USA. Das vom Statistischen Bundesamt mit dem Betrieb der Internetseiten beauftragte Informationstechnikzentrum Bund (ITZBund) hatte seinerseits den Dienstleister mit der Absicherung gegen Angriffe und der Verbesserung der Performance beauftragt. Ich habe den Sachverhalt unverzüglich eingehend geprüft und als Sofortmaßnahme dafür gesorgt, dass die problematische Einbindung ausgesetzt wird. Im Ergebnis habe ich zudem gegen das ITZBund ein datenschutzaufsichtsbehördliches Verfahren eingeleitet.

Auch wenn sich früh herausstellte, dass ein Zugriff auf die über das Online-Portal eingegebenen Zugangsdaten und Inhaltsangaben zu den Zensuserhebungen technisch nicht möglich war, habe ich die vereinbarten Vorkehrungen gegen die dienstleistungstypisch unvermeidbare Übermittlung der IP-Adresse der Nutzergeräte als personenbezogenes Datum, soweit sie auch Empfänger außerhalb des Schutzbereichs der DSGVO beinhalten konnte, als nicht ausreichend bewertet. Das ITZBund nimmt die Dienstleistungen des besagten Unternehmens daraufhin seit etwa Mitte Oktober nicht mehr in Anspruch.

Querverweise:

4.3.3 Einsatz eines Content-Distribution-Network (CDN) für die Website des Zensus 2022

8.9 Datenschutz bei Onlinevirenscannern

Vor dem Einsatz eines Onlinedienstes zum Viren- oder Malwareschutz ist dieser auch daraufhin zu überprüfen, ob man ihm personenbezogene Daten anvertrauen darf.

Im Berichtsjahr habe ich mich mit den datenschutzrechtlichen Aspekten des Einsatzes von Onlinevirenscannern befasst. Die Erkennung und Abwehr von Computer-Viren und sonstigen Schadprogrammen ist nicht nur eine wichtige Aufgabe der Informationssicherheit, sondern auch des Datenschutzes. Um ein angemessenes Schutzniveau der Verarbeitung personenbezogener Daten zu gewährleisten, sind Unternehmen und Behörden nach Art. 32 DSGVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen. Der Einsatz von Viren- und Malwarescannern gehört dabei zum Standard bei der elektronischen Datenverarbeitung. Entsprechende Produkte, Verfahren und Dienstleistungen werden in vielfältigen Formen sowohl als Desktop- oder Serverapplikationen als auch über Onlinedienste angeboten.

Allen Lösungen ist regelmäßig gemein, dass sie nicht nur der Informationssicherheit und dem Datenschutz dienen, sondern vor und bei ihrem Einsatz der Datenschutz beachtet werden muss. Denn typischerweise müssen gerade auch Dateien auf Viren und sonstige Schadprogramme überprüft werden, die personenbezogene Daten enthalten. Dabei ist unerheblich, ob die Texte, Bilder, Metadaten oder sonstigen Inhalte sich auf identifizierte oder identifizierbare Menschen beziehen.

Besonders wichtig ist es daher, vor dem Einsatz neuer Schutzinstrumente diese selbst daraufhin zu überprüfen, wie personenbezogene Daten verarbeitet werden, ob dies datenschutzkonform erfolgt und welche Risiken damit einhergehen. Sofern die Überprüfung ergibt, dass zwar ein datenschutzkonformer Einsatz grundsätzlich möglich, aber von einem hohen Risiko auszugehen ist, ist eine Datenschutz-Folgenabschätzung durchzuführen. Werden keine Maßnahmen zu Eindämmung getroffen, ist die Aufsichtsbehörde zu konsultieren. Kann ein Schutzinstrument nicht datenschutzgemäß eingesetzt werden, muss sein Einsatz unterbleiben. Wo dies schwierig erscheint, stehen die Aufsichtsbehörden beratend zur Seite. Auch Ausnahmesituationen, wie z. B. die Einschränkungen aufgrund der Corona-Pandemie, dürfen nicht dazu führen, dass eine datenschutzrechtliche Überprüfung neuer Schutzinstrumente unterbleibt, nicht mit gebotener Sorgfalt durchgeführt wird oder keine angemessenen Konsequenzen daraus gezogen werden.

Im Berichtsjahr veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Warnmeldung[63], die auch datenschutzrechtlich relevant ist. Im Rahmen eines Vorfalls wurde entdeckt, dass in einer Institution verdächtige E-Mail-Anhänge zu einem Online-Virenscanner zwecks Viren-/ Malware-Überprüfung hochgeladen wurden. Dabei handelte es sich um einen Online-Dienst, der hochgeladene Dateien zur Verbesserung der Erkennung durch eine Vielzahl verschiedener Antivirenprogramme und Malwarescanner überprüfen lässt. Bei manchen solcher – mitunter für die Nutzer kostenlos angebotener – Online-Dienste erhalten allerdings neben IT- und IT-Security-Dienstleistern auch weitere Kunden Zugriff auf alle hochgeladenen Dateien. Zu den Kunden, die Zugriff auf die Daten erhalten, können z. B. Wissenschaftler, Journalisten, diverse Unternehmen und sogar Geheimdienste zählen, die auch außerhalb der Europäischen Union ansässig sind.

Ein Beispiel für einen solchen Online-Dienst ist der von Google Inc. betriebene Online-Dienst „VirusTotal“, dessen Arbeitsweise in seinen Servicebedingungen beschrieben wird und der auf seiner Uploadseite eine klare Warnung enthält, dass keine persönlichen Informationen hochgeladen werden sollen. Die Warnung ist ernst zu nehmen.

Die Inhalte vertraulicher Dokumente, die hochgeladen werden, müssen als nun mehr öffentlich angesehen werden. Personenbezogene Daten werden einem unbestimmten Personenkreis offengelegt. Das Hochladen personenbezogener Daten Dritter ist daher in der Regel ein Datenschutzverstoß, sofern nicht ausnahmsweise eine ausreichende Rechtsgrundlage die Verarbeitung rechtfertigt. Da der Upload insoweit zu einem unbefugten Zugang zu personenbezogenen Daten führt, ist dieser als meldepflichtige Verletzung des Schutzes personenbezogener Daten anzusehen.

Gerade vor dem Hintergrund der angespannten geopolitischen Lage sollte die Warnung des BSI zum Anlass genommen werden, sich der möglichen Risiken von Online-Virenscannern bewusst zu werden. Eine besondere Sorgfalt ist bei deren Auswahl, Bewertung, Implementierung und Einsatz nicht nur zum Schutz vertraulicher Daten geboten, sondern auch datenschutzrechtliche Pflicht.

63 Cybersicherheitswarnung, CSW-Nr. 2022-206270-1032, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2022/2022-206270-1032_csw.html

8.10 Digitale Datenräume und Mobilitätsdaten im Verkehrssektor

Die Bundesregierung plant ein Mobilitätsdatengesetz. Gemeinsam mit der „acatech – Deutsche Akademie der Technikwissenschaften“ hat das Bundesverkehrsministerium eine Plattform für den Handel mit Mobilitätsdaten geschaffen. Dabei wird es auch um Echtzeitdaten aus fahrenden Kfz gehen. Diese verraten unter Umständen auch viel über gefahrene Strecken und das Fahrverhalten.

Die Europäische Kommission wie auch die Mitgliedstaaten der EU setzen große Hoffnungen auf die Wertschöpfungsmöglichkeiten in einer datengetriebenen digitalen Ökonomie. Die EU-Kommission hat dazu im Februar 2022 einen Verordnungsentwurf über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Data Act“) vorgelegt, um die wirtschaftliche Verwertung von Daten rechtssicher zu ermöglichen. Gemeinsam mit meinen europäischen Kollegen habe ich dazu im Europäischen Datenschutzausschuss kritisch Stellung bezogen. Ausdrücklich sind davon auch die Daten aus den vielen smarten Gerätschaften des „Internet of Things (IoT)“ umfasst, die eine Fülle personenbezogener Daten produzieren, wenn sie von Personen genutzt werden oder sich in privaten Haushalten befinden. Dazu zählen grundsätzlich auch moderne vernetzte Fahrzeuge. Speziell für Fahrzeuge hat die Kommission für das zweite Quartal 2023 eine spezialgesetzliche Vorschrift angekündigt, mit der Hersteller verpflichtet werden, Wettbewerbern einen fairen Zugang zu Daten, Funktionen und Ressourcen in Fahrzeugen zu ermöglichen.

Die datengetriebene Wertschöpfung setzt vertrauenswürdige Datenräume voraus., In diesen können Anbieter ihre Daten anderen Teilnehmern des Datenraums für wohlbestimmte Verarbeitungszwecke auf Vertragsbasis zur Verfügung stellen, ohne einen Missbrauch durch unbefugte Dritte befürchten zu müssen. Ein solcher Datenraum wurde auf Betreiben der Bundesregierung für den Mobilitätssektor eingerichtet. Die „DRM Datenraum Mobilität GmbH“ wurde 2021 mit dem Ziel gegründet, Behörden, Unternehmen und wissenschaftlichen Institutionen die Verfügbarmachung von Mobilitätsdaten für die Entfaltung datengetriebener Geschäftsmodelle in einem IT-technisch geschützten Umfeld zu ermöglichen. An dem Gründungsprozess wurde ich beteiligt und habe bei der Erstellung der Musterverträge beraten. Teilnehmer dieses so geschaffenen vertrauenswürdigen Datenraums sind neben Behörden, wie etwa dem Deutschen Wetterdienst (DWD), auch deutsche Autohersteller und ihre Zulieferer.

Die Teilnahme von Privatpersonen als Datenliefernde ist zunächst nicht vorgesehen und personenbezogene Daten stehen nicht im Fokus. Insoweit konnte ich mich auch bisher nicht mit meinem Anliegen durchsetzen, die Chancen der Digitalisierung im Fall personenbezogener Daten auch dafür zu nutzen, betroffene Privatpersonen unmittelbar an den Vertragsbeziehungen zu beteiligen und auch dafür Musterverträge vorzusehen. Der so geschaffene Datenraum dient damit vornehmlich dem Schutz von Geschäftsinteressen und nicht dem Schutz der Interessen möglicherweise betroffener Privatpersonen. Das wird seine Nutzung erschweren, wenn es um die Verwertung von Daten aus fahrenden Fahrzeugen geht. Eine Verwertung dieser Daten wird im Regelfall nur möglich sein, wenn die Daten zuvor anonymisiert wurden. Dabei ist zu berücksichtigen, dass eine Fülle unterschiedlicher Daten oder in dichter zeitlicher Folge erhobene Daten in der Regel nur schwer zu anonymisieren sind. Zur Orientierung über mögliche Maßnahmen habe ich hierzu bereits im Zusammenhang mit der Verwendung von Telekommunikationsdaten eine Position bezogen.[64]

Soweit es um den Zugriff auf Daten, Funktionen und Ressourcen aus Fahrzeugen für Mobilitätsdienste aller Art geht, müssen auch deshalb Fahrzeugnutzenden vergleichbare Möglichkeiten für die Nutzungskontrolle eingeräumt werden, wie wir sie aus der Welt der Smartphones und Tablets kennen. Ob die Fahrzeugsensoren auch für den Parkplatzfinder des Fahrzeugherstellers oder eines anderen Dritten genutzt werden, darf sich nicht der Kontrolle durch die Fahrzeugnutzenden entziehen. Zusammen mit meinen Kolleginnen und Kollegen aus den Ländern setze ich mich dafür ein, für Fahrzeugnutzende praktikable Möglichkeiten vorzusehen, jederzeit die Kontrolle über den digitalen Zugang zu ihren Fahrzeugen zu erhalten. Fahrzeugnutzende müssen einfache Möglichkeiten haben herauszufinden und zu kontrollieren, für welchen Mobilitätsdienst welche Daten, Funktionen und Ressourcen gerade genutzt werden. Allgemeine Nutzungsbedingungen oder Vertragsklauseln werden dafür nicht der richtige Ort sein. In den zu schaffenden Datenräumen muss dem Schutz der Interessen von Privatpersonen die gleiche Priorität eingeräumt werden wie dem Schutz von Geschäftsinteressen.

Aufgrund der aktuellen Bedeutung des Themas habe ich am 18. Oktober 2022 ein politisches Forum mit dem Titel

64 Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, abrufbar unter: www.bfdi.bund.de/konsultation

„Mein Auto. Meine Daten!“ ausgerichtet, auf dem ich mit Vertreterinnen und Vertretern der Automobilindustrie, des Verbraucherschutzes und des Bundesministeriums für Verkehr und Digitale Infrastruktur diskutiert habe. Dabei habe ich deutlich gemacht, dass nur jene souverän über die Nutzung ihrer Daten entscheiden können, denen man auch die Mittel an die Hand gibt, deren Verwertung jederzeit kontrollieren zu können. Das setzt voraus, dass auch die Schutzinteressen dieser Personen in den Datenräumen auf technisch hohem Niveau geschützt werden und insbesondere keine Cyberrisiken durch die Vernetzung von Fahrzeugen für das Heil einer Digitalökonomie entstehen.

Querverweise:

4.2.4 Data Governance Act, 4.2.5 Data Act

8.11 TrustPid – neue Wege der personalisierten Werbung

Bislang funktioniert personalisierte Werbung im Internet mit Werbe-Cookies. Diese ermöglichen die Nachverfolgung von Internetnutzenden und ihrem Verhalten, um Werbung zielgerichtet auszuspielen. Viele Browser erschweren zum Glück mittlerweile aber die Nutzung dieser Cookies. In einem Piloten haben sich deutsche Mobilfunkanbieter nun etwas Neues einfallen lassen, um eine Alternative zu den altbekannten Werbemodellen anzubieten.

Dieses Projekt namens „TrustPID“ erregte im letzten Jahr in unterschiedlichen Beiträgen mediale Aufmerksamkeit. Es dient der Wiedererkennung von Mobilfunk-Nutzern auf Webseiten. Im Berichtszeitraum arbeiten zwei Mobilfunknetzbetreiber (Vodafone und Deutsche Telekom) an einem Machbarkeitstest, der in Deutschland u. a. gemeinsam mit großen Nachrichten-Webseiten durchgeführt wurde.

Wie erfolgt die Datenverarbeitung im Detail?

Bei TrustPID werden die IP-Adressen und die Mobilfunknummern der Nutzer verwendet, um eine pseudonyme Kennung zu generieren. Rechtliche Basis der Datenverarbeitung ist eine datenschutzrechtliche Einwilligung des Nutzers, die vom Webseitenbetreiber (in dem Pilotbetrieb z. B. bei Bild.de) eingeholt wird. Diese beinhaltet auch die Verarbeitung der Verkehrsdaten (hier dynamische IP-Adresse) beim Mobilfunk-Netzbetreiber.

Nur wenn diese Einwilligung abgegeben wurde, wird die IP-Adresse des Nutzers an seinen Mobilfunk-Netzbetreiber übertragen. Dies funktioniert natürlich auch nur, wenn der jeweilige Mobilfunkanbieter bei dem Testbetrieb mitmacht. Der jeweilige Netzbetreiber ermittelt dann anhand der IP-Adresse die Rufnummer und erstellt sodann aus dieser eine eindeutige, pseudonyme Netzwerkkennung für TrustPID.

Der Anbieter des Werbevermarktungsdienstes, die Vodafone Sales and Services Limited mit Sitz im Vereinigten Königreich, wiederum erzeugt aus diesem Pseudonym weitere – ebenfalls pseudonyme – Marketing-Kennungen. Diese Marketing-Kennungen ermöglichen Werbetreibenden ein personalisiertes Online-Marketing. Beispielsweise wird es Webseitenbetreibern so möglich, Nutzer bei einem erneuten Besuch ihrer Internetseite wiederzuerkennen. Werbeplattformen können ebenfalls Nutzer wiedererkennen, um passende Werbung zu deren Interessen zu vermarkten.

Verbesserungen nach meiner Beratung

Ich wurde von den teilnehmenden deutschen Mobilfunk-Netzbetreibern über das Projekt informiert. Für den Anbieter des Werbevermarktungsdienstes in dem Vereinigten Königreich bin ich nicht zuständig. Meine Aufsichtszuständigkeit erschöpft sich in der Projektbeteiligung der deutschen Mobilfunkanbieter.

In meiner Beratung habe ich insbesondere auf die datenschutzrechtlichen Anforderungen einer Einwilligung hingewiesen. Konkret muss hier in verständlicher, leicht zugänglicher Form und in klarer und einfacher Sprache erläutert werden, wie die Daten verarbeitet werden. Dabei geht es nicht nur um die Erstellung der dargestellten Kennungen anhand der IP-Adresse durch den jeweiligen Mobilfunkanbieter, sondern auch um die Nutzung dieser Kennungen, z. B. im Bereich der Werbevermarkter und durch alle anderen beteiligten Akteure.

Aufbauend auf meinen Hinweisen wurde die Einwilligung transparenter gestaltet und die Webseite www.trustpid.com grundlegend überarbeitet. Auch die Widerrufs- und Widerspruchsmöglichkeiten wurden bei TrustPID aufbauend auf meinen Hinweisen stark modifiziert. So sollte ein Widerspruch zunächst nur für 90 Tage gespeichert werden. Dies wurde nach meiner Remonstration angepasst: Ein Widerruf der Datenverarbeitung gilt nun unbefristet bis es vom Betroffenen eine gegenteilige Willensbekundung gibt.

Ausblick

Durch meine Beratung konnten viele relevante Bedenken bei TrustPID ausgeräumt werden. Datenschutzpolitisch kann man den Dienst durchaus zwiespältig sehen. Einerseits findet hier lediglich eine Verarbeitung pseudonymisierter Daten auf Basis einer datenschutzrechtlichen Einwilligung statt. Andererseits kommt gerade Telekommunikationsanbietern eine besondere Vertrauensstellung zu, die für mich nur schwer mit einem

Tracking ihrer Nutzer vereinbar ist. Außerdem müssen weitere Gefahren wie die Zusammenführung der pseudonymen Kennung und z. B. dem Log-in bei Diensten von Anbietern im Web, die zu einer Repersonalisierung führen würden, betrachtet und unterbunden werden.

Es bleibt abzuwarten, wie sich das Projekt nach Ende der aktiven Projektphase entwickeln wird. Im Falle einer europäischen Umsetzung des Projektes wird es auch maßgeblich auf die Bewertung der dann zuständigen europäischen Datenschutzaufsichtsbehörden ankommen. Mein Haus wird diesen Prozess weiter aktiv begleiten, um die Einhaltung aller datenschutzrechtlichen Vorgaben sicherzustellen.

8.12 Videokonferenzdienste

Videokonferenzdienste sind in unserer Lebens- und Arbeitswelt selbstverständlich geworden und es haben sich neue Formen des virtuellen und hybriden Zusammenarbeitens etabliert. Entsprechend werden in der Praxis viele Diskussionen über den Datenschutz bei Videokonferenzen geführt. Seit der Einführung des neuen Telekommunikationsgesetzes (TKG) am 1. Dezember 2021 sind kommerzielle Videokonferenzdienste rechtlich als Telekommunikationsdienste zu werten, so dass sie der datenschutzrechtlichen Zuständigkeit des BfDI unterliegen.

Zur Klärung datenschutzrechtlicher Fragen im Zusammenhang mit der Durchführung einer Videokonferenz müssen die verschiedenen rechtlichen Ebenen im Zusammenhang mit der Erbringung des Videokonferenzdienstes und die jeweils betroffenen datenschutzrechtlichen Verantwortlichkeiten gedanklich voneinander getrennt werden. Nur so kann man das für den jeweiligen Bereich anwendbare Datenschutzrecht und die danach bestehenden konkreten Verpflichtungen ermitteln. Im TKG vom 1. Dezember 2021 wurde der Begriff der Telekommunikation weit gefasst und umfasst in einem funktionellen Sinn nunmehr alle gewöhnlichen Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch ermöglichen (s. a. § 3 Nr. 24 TKG). Gemeint sind dabei Dienste, die für Dritte und gewöhnlich gegen Entgelt erbracht werden.

Die Erbringung eines Videokonferenzdienstes im Sinne des TKG

Damit ist auch der kommerzielle Anbieter eines Videokonferenzsystems ein Anbieter von Telekommunikationsdiensten im Sinne des TKG und deshalb zur Einhaltung der Datenschutzgrundsätze des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) und des TKG verpflichtet. Außerdem muss er die notwendigen technischen und organisatorischen Maßnahmen einhalten und die allgemeinen datenschutzrechtlichen Erfordernisse nach der Datenschutz-Grundverordnung (DSGVO) beachten, soweit sie nicht durch die speziellen Regelungen des TTDSG verdrängt werden. Dazu zählt beispielsweise, dass der Anbieter des Videokonferenzsystems die personenbezogenen Daten, die im Rahmen der Durchführung der Videokonferenz erhoben werden, nur für eigene Zwecke verarbeitet, wenn es hierfür eine Rechtsgrundlage gibt. Es dürfen ohne Einwilligung keine Aufzeichnungen erfolgen und bei der Übermittlung ins Drittland sind die Vorschriften der Art. 44 ff. DSGVO zu beachten. Weitere Einzelheiten dazu, wie die Orientierungshilfe der Datenschutzkonferenz (DSK) zu Videokonferenzsystemen und eine Checkliste, finden sich auf meiner Webseite.[65]

Die datenschutzrechtliche Zuständigkeit liegt gemäß § 29 TTDSG grundsätzlich beim BfDI, das One-Stop-Shop-Verfahren der DSGVO findet damit keine Anwendung. Bei grenzüberschreitenden Konstellationen kommt es darauf an, ob im Inland ein Telekommunikationsdienst erbracht wird (vgl. § 1 Abs. 3 TTDSG).

Datenschutzrechtliche Pflichten für Anwender von Videokonferenzdiensten

Welche Inhalte und personenbezogenen Daten Gegenstand einer Videokommunikation sind, wird von den jeweiligen Anwendern des Systems bestimmt. Soweit ein Unternehmen oder eine Behörde personenbezogene Daten im Rahmen einer Videokonferenz verarbeitet, ist sie insoweit die datenschutzrechtlich verantwortliche Stelle. Betroffene Daten können hier sowohl Namen und ggfls. E-Mail-Adressen der eingeladenen Teilnehmerinnen und Teilnehmer sein als auch Inhalte, die in der Videokonferenz besprochen werden, sofern es sich um personenbezogene Daten handelt.

Dem Unternehmen oder der Behörde obliegt die Risikoabwägung, ob eine Videokonferenz überhaupt stattfindet, welches Videokonferenzsystem verwendet wird (z. B. eigenes oder externes System) und welche besonderen Einstellungen die Sicherheit der personenbezogenen Daten zusätzlich gewährleisten können.

Für die Abwägung ist das Gesamtgefährdungspotential der konkret betroffenen personenbezogenen Daten von besonderer Bedeutung. Hier gibt es verschiedene Parameter. So ist z. B. ein besonders hohes Gefähr-

65 Informationen des BfDI, abrufbar unter: www.bfdi.bund.de/videokonferenzen

dungspotential darin zu sehen, wenn besonders sensible Daten im Sinne von Art. 9 DSGVO betroffen sind, also der Verarbeitung besonderer Kategorien personenbezogener Daten.

8.13 Neues von der E-Mail – Zuständigkeitswechsel zum BfDI

Während die Anbieter von E-Mail-Diensten jedenfalls nach dem Google Gmail-Urteil des Europäischen Gerichtshof (EuGH, 13. Juni 2019, Rechtssache C-193/18) nicht als Anbieter von Telekommunikationsdiensten im Sinn des (alten) Telekommunikationsgesetzes anzusehen waren, hat sich die rechtliche Situation mit der Einführung des neuen Telekommunikationsgesetzes (TKG) vom 1. Dezember 2021 grundlegend geändert. Nunmehr sind die Anbieter von E-Mail-Diensten auch nach dem TKG als Anbieter von Telekommunikationsdiensten zu qualifizieren. Damit werden sie von meiner Sonderzuständigkeit für den Bereich Telekommunikation erfasst.

Im TKG vom 1. Dezember 2021 wurde der Begriff der Telekommunikation weit definiert und umfasst in einem funktionellen Sinn nunmehr alle gewöhnlichen Dienste, die einen direkten interpersonellen und interaktiven Informationsaustausch zwischen Personen ermöglichen (s. § 3 Nr. 24 TKG). Darunter fallen also auch E-Mails, Voice-Over-IP und Videokonferenzen (so genannte Over-the-top (OTT)-Anwendungen).

Datenschutzrechtliche Anforderungen

Der Anbieter eines E-Mail-Dienstes ist damit zur Einhaltung der Datenschutzgrundsätze des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) und des TKG verpflichtet. Außerdem muss er die notwendigen technischen und organisatorischen Maßnahmen nach § 165 TKG und Art. 32 DSGVO einhalten. Die datenschutzrechtliche Zuständigkeit liegt gemäß § 29 TTDSG grundsätzlich beim BfDI.

Unabhängig davon können auch datenschutzrechtliche Pflichten für die Versenderin oder den Versender einer E-Mail bestehen. Hier ist je nach Konstellation im Einzelfall eine datenschutzrechtliche Risikoabwägung durchzuführen, ob eine E-Mail in Bezug auf die konkret betroffenen Daten überhaupt das geeignete Medium ist, welche Verschlüsselung gewählt werden soll und welcher E-Mail-Anbieter dafür in Betracht kommt.

Aus der Beratungspraxis des BfDI

In letzter Zeit wurden an mich zahlreiche Fragen von Bürgerinnen und Bürgern gerichtet, die ihre Login-Daten für ihren E-Mail Account vergessen und nun keinen Zugriff auf ihre E-Mails mehr haben. Auch wenn ich in diesen Fällen nicht weiterhelfen konnte, zeigt sich darin für mich, dass die Anbieter von E-Mail-Accounts offenbar ihre datenschutzrechtlichen Verpflichtungen ernst nehmen und die E-Mail-Accounts wirksam vor unbefugten Zugriffen schützen. Ein Zugriff auf das E-Mail-Konto ist nur möglich, wenn die jeweilige Person sich als Berechtigte gerade in Bezug auf das E-Mail-Konto authentifizieren kann. Es genügt nicht, nur einen Nachweis darüber zu erbringen, die Person zu sein, auf deren Namen möglicherweise die E-Mail-Adresse lautet.

Dieses strikte Verhalten der E-Mail-Anbieter ist aus datenschutzrechtlicher Sicht gut und richtig. Vielfach speichern Bürgerinnen und Bürger in ihrem E-Mail-Konto viele E-Mails, aus denen sich zahllose persönliche Informationen und Querverbindungen ergeben. Es ist daher wichtig, den Zugriff auf dieses Konto zu sichern. Dies bedeutet für die Bürgerinnen und Bürger auf der anderen Seite, dass sie die Zugriffsinformationen zu ihrem Konto wie beispielsweise auch ihren Haustürschlüssel nicht „verlegen“ sollten. Sonst droht auch hier die Gefahr, sich „auszusperren“.

Ebenfalls als ungünstig kann sich erweisen, wenn man für die alternativ vorgesehenen Sicherheitsabfragen – vielleicht sogar „zur Sicherheit“ – falsche Angaben macht, an die man sich dann später nicht mehr erinnern kann. Wirksamer Datenschutz setzt damit auch entsprechende Digitalkompetenzen bei allen Akteuren sowie ein Bewusstsein für den Schutz der eigenen Daten voraus. Hier werde ich mich weiterhin sowohl für einfache und verständliche aber sichere Systeme als auch für ein breiteres Datenschutzbewusstsein einsetzen.

8.14 Datenschutz bei digitalen Identitäten

Der Bedarf für sichere Identifizierungen und Authentifizierung im digitalen Raum ist gewachsen, wie die Debatte um VideoIdent (Nr. 8.1) zeigt. Ich habe in einer Anhörung des Ausschusses für Digitales des Deutschen Bundestages für den verstärkten Einsatz der Onlinefunktion des Personalausweises (nPA) als datenschutzfreundliche Lösung plädiert. Auf europäischer und völkerrechtlicher Ebene habe ich mich für den Schutz von Bürgerinnen und Bürgern vor Profilbildung und Überidentifikation eingesetzt.

Übergreifend betrachtet spielt die Etablierung sicherer digitaler Identitäten eine Schlüsselrolle für die erfolgreiche Umsetzung wichtiger Digitalisierungsvorhaben im Gesundheitssektor oder der Digitalisierung der Verwaltung. Nutzerfreundliche digitale Identitäten stellen eine Möglichkeit zur digitalen Teilhabe dar und stehen

in einem Spannungsfeld zum verfassungsrechtlich verbürgtem Recht auf informationelle Selbstbestimmung. Grundlage meiner Anhörung im Ausschuss für Digitales war ein Verordnungsvorschlag des Europäischen Parlaments und des Rates zur Änderung der „eIDAS"-EU-Verordnung (910/2014) im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. In der Anhörung des Bundestagsausschusses für Digitales (ADi) vom 4. Juli 2022 habe ich Datenschutzrisiken App-gestützter mobiler ID-Wallet-Lösungen (Brieftasche für digitale Identitäten) aufgezeigt. Solche Risiken sind insbesondere Profilbildung durch Verhaltens- und Standorttracking, die Gefahr einer „Überidentifikation", also das Erfordernis einer Identifikation für Rechtsgeschäfte im Netz, für die üblicherweise die Anmeldung mit einem Pseudonym ausreichend wäre und neue Angriffsflächen für Identitätsdiebstahl. Die Anhörung hat das auch von mir geteilte Bild ergeben, dass der nPA eine sichere und auch komfortablere Lösung zur Identifizierung von Personen in Fällen, in denen dies gesetzlich vorgeschrieben ist, bietet. Für die Nutzung des nPA habe ich mich bereits in meinem 30. TB (Nr. 6.19) ausgesprochen.

Die EU-Kommission sieht die Einführung einer europäischen ID-Wallet als priorisiertes Vorhaben zur Stärkung des digitalen europäischen Binnenmarktes. Für die eIDAS-Verordnung habe ich vertreten, dass Wallets für den Identitätsabgleich von Nutzern nicht mit einem einheitlichen Personenkennzeichen verknüpft werden sollten, da eine Gefahr der Profilbildung von Nutzenden besteht. In diesem Punkt habe ich mich mit Unterstützung der Bundesregierung für eine Nachbesserung des Entwurfes der EU-Kommission eingesetzt. Die Bundesregierung konnte diese Position im Rat nicht durchsetzen, insbesondere da andere Mitgliedstaaten nicht über ähnlich fortschrittliche Systeme wie den nPA verfügen. Jedoch wurde nach dem momentanen Stand des Verordnungsentwurfes ein Kompromiss erzielt. Dieser Kompromiss beinhaltet eine datenschutzfreundliche dienst- und sektorspezifische Lösung, die an die Lebensdauer des Gerätes, mit welchem die Wallet genutzt wird, gebunden ist. Außerdem wurden Erwägungsgründe zu „Ledger-Technologien" in den Verordnungsentwurf aufgenommen. Hier habe ich mich für eine technologieneutrale Fassung des Verordnungsentwurfes eingesetzt. Diese konnte ich leider nicht durchsetzen, da sich in der Bundesregierung die Meinung durchgesetzt hat, die Erwägungsgründe zu „Ledger-Technologien" lediglich nachzubessern statt auf deren Streichung zu bestehen

Das Projekt Digitale Identitäten hatte, wie bereits in meinem 30. TB (Nr. 6.19) dargestellt, geplant, eine ID-Wallet zu entwickeln, die teilweise auf einer Blockchain-Technologie basieren sollte. Daraus ergaben sich komplexe datenschutzrechtliche Fragen, die bislang noch nicht hinreichend geklärt werden konnten. Daher sehe ich es als positiv an, dass dieser Ansatz zugunsten des existierenden datenschutzfreundlichen und sicherheitstechnisch hochwertigen Systems für digitale Identitäten nicht weiterverfolgt wird und die Nutzung des nPA stärker gefördert werden soll. Das Projekt digitale Identitäten wurde in das interministerielle und behördenübergreifende Format „Governance Labratory" Digitale Identitäten („GovLab DE") überführt. Ein „Governance Labratory" ist ein Innovationslabor für die Verwaltung, das neue Technologien, Arbeitsweisen und Prozesse erprobt. Ich berate das „Governance Labratory" weiterhin zu datenschutzrechtlichen Aspekten deutscher Lösungen für digitale Identitäten.

Auf völkerrechtlicher Ebene hat der Europarat Guidelines National Digital Identity zur Ergänzung des Protokolls zur Datenschutzkonvention 108 („Convention 108+") beschlossen. Das Bundesministerium des Innern und für Heimat (BMI) hat mich an deren Kommentierung beteiligt. Erfreulicherweise wurde ein Hinweis meinerseits zur Vermeidung von Profilbildung durch globale und permanente Identifikationsnummern in den Konventionstext aufgenommen.

Nutzerfreundliche digitale Identitäten stellen eine Möglichkeit zur digitalen Teilhabe dar, sie existieren jedoch in einem Spannungsfeld zum verfassungsrechtlich verbürgtem Recht auf informationelle Selbstbestimmung. Gestaltungsanforderungen können durch datenschutzfreundliche Ausgestaltung des rechtlichen und technischen Rahmens bewältigt werden, wofür ich mich weiterhin einsetzen werde.

Querverweise:

8.1 Aktuelles aus der Telematikinfrastruktur und von ihren Anwendungen

8.15 Datenschutz im Smart Home

Der Rollout intelligenter Messsysteme nach § 2 Nr. 7 Messstellenbetriebsgesetz hat begonnen. Stromzähler werden dadurch bei Einhaltung höchster Cybersicherheits-Standards fernauslesbar. Auch wird dadurch eine unterjährige Verbrauchserfassung möglich, die Verbrauchenden jederzeit einen Überblick über ihren Stromverbrauch gewährt. Die intelligenten Messsysteme sind auch für die Gas-, Wasser- und Wärmezählung einsetzbar, jedoch besteht dazu nur in Einzelfällen eine gesetzliche Verpflichtung. Überdies wird es durch eine Übergangsregelung möglich, etwa für die Wärmezählung die Privacy-Management-Funktionen des intelligenten Messsystems zu umgehen.

Mit der Digitalisierung im Energiesektor ergeben sich auch dort neue Möglichkeiten für digitale Geschäftsmodelle. Bei der Energiezählung im Haushalt wird nun nicht mehr nur ein Jahresarbeitswert erhoben, sondern im Fall elektrischer Energie ein Arbeitswert im Viertelstundentakt, also etwa 36.500 Arbeitswerte jährlich. Aufgrund des dadurch entstehenden Risikos für den Schutz der Privatsphäre durch Nutzerprofile wurde 2016 mit dem Gesetz zur Digitalisierung der Energiewende das Messstellenbetriebsgesetz (MsbG) geschaffen, mit dem Belange der Cybersicherheit und des Datenschutzes mustergültig berücksichtigt wurden. Insbesondere die sogenannten Smart-Meter-Gateways (SMGW), die eine Vernetzung der Energiezähler mit dem Internet ermöglichen, setzen nicht nur Maßstäbe für die Cybersicherheit, sie haben auch zugleich die Funktion eines Privacy-Information-Management-Systems (PIMS). Sie gewähren Verbrauchenden die größtmögliche Kontrolle über die Verwendung der zuweilen im Millisekundentakt aus intelligenten Zählern (Smart Meter) verfügbaren Daten. Für den Bereich der Messung elektrischer Energie wird mit dem MsbG datenschutzrechtlich umfassend geregelt, welche Stelle welche Daten für welchen Zweck erhalten und verarbeiten darf. Insbesondere regelt das Gesetz, dass für die Fernauslesung der Stromzähler nur intelligente Messsysteme verwendet werden dürfen, bei denen intelligente Zähler über ein nach den strengen technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) zugelassenes Smart-Meter-Gateway kommunizieren.

Leider erstrecken sich die für Verbrauchende vorteilhaften Regelungen nicht auf andere Sparten im Energiesektor. Die 2021 novellierte Heizkostenverordnung (HKV) sieht - vor dem Hintergrund der Kosten für die Nutzung eines Smart-Meter-Gateways nachvollziehbar – aus wirtschaftlichen Gründen eine verpflichtende Nutzung von Smart-Meter-Gateways nur im Rahmen der sogenannten Mehrsparten-Messung vor, wenn ein Messstellenbetreiber sowohl für die Strom- als auch für die Wärmezählung und ggf. für weitere Sparten zuständig ist. Im Bereich der Wasserzählung ist keine Novellierung der gesetzlichen Grundlagen vorgesehen. Auch für die Gaszählung bleibt die Nutzung von Smart-Meter-Gateways optional.

Mit einer Novellierung des MsbG im Rahmen des im Juli 2021 beschlossenen Gesetzes zur Änderung des Energiewirtschaftsrechts (BT-Drucksache 20/2402) wurde es möglich, die in Bezug auf funktionale Sicherheit noch nicht ausreichend spezifizierte, für die Fernsteuerung von Anlagen im Heimnetz der Anschlussnutzenden nach § 14a Energiewirtschaftsgesetz vorgesehene Schnittstelle eines Smart-Meter-Gateways bereits zu nutzen. Diese Möglichkeit wurde geschaffen, weil diese Schnittstelle durch sichere Verschlüsselung der Kommunikation sowie kryptographisch abgesicherte Identifizierung der Zugangsnutzenden ausgezeichnet ist und deshalb die Nutzung insbesondere für Steuerungszwecke möglich werden sollte, ohne dass Anforderungen für die funktionale Sicherheit der Fernsteuerung erfüllt werden müssten. Damit wird zwar das Risiko minimiert, dass Unbefugte die Schnittstelle nutzen können. Eine unbefugte Nutzung der Schnittstelle durch berechtigte Stellen bleibt jedoch technisch möglich.

Wie sich inzwischen herausgestellt hat, ist die Eigenschaft einer funktional noch unbestimmten, aber sicheren Verbindung auch für die Sparten der Energiewirtschaft attraktiv, die gesetzlich nicht zur Nutzung intelligenter Messsysteme verpflichtet sind. Das ist einerseits zu begrüßen, weil so zumindest eine sichere Übermittlung an zuvor identifizierte Stellen gewährleistet werden kann. Andererseits entspräche eine solche Anbindung für Energiezählungszwecke aber nicht dem Stand der Technik, weil damit die Vorkehrungen für eine datenschutzgerechte Messwertverarbeitung auf dem Gateway umgangen werden können. So ist etwa für die Wärmezählung nicht gewährleistet, dass eine Übermittlung von Zählwerten nur im erforderlichen Umfang erfolgt. In den vom BSI im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) durchgeführten Branchenanhörungen zur Weiterentwicklung des Smart-Meter-Gateways habe ich deshalb deutlich gemacht, dass eine Nutzung der für Steuerung gedachten Schnittstelle für Messzwecke nicht dem Stand der Technik entspricht. Ich begrüße außerdem den Ansatz des BSI, durch eine zusätzliche technische Richtlinie auch Sicherheitsanforderungen für die Geräte zu formulieren, die über diese Schnittstelle angebunden werden sollen.

Gesetzliche Vereinfachungen zur Beschleunigung der Energiewende dürfen und brauchen auch nicht zu Lasten des Datenschutzes und der Cybersicherheit vorgenommen werden. Das Smart-Meter-Gateway ermöglicht Verbrauchenden grundsätzlich ein hohes Maß an Kontrolle über in ihrer Privatsphäre erhobene Zählwerte. Die Möglichkeiten zur Kontrolle über die Verwendung der Zählwerte müssen auch vor dem Hintergrund aktueller Bemühungen der EU-Kommission zur Nutzbarkeit der Daten von datenproduzierenden IoT-Geräten (Internet of Things) für die Wertschöpfung in der Digitalökonomie ausgebaut werden. Dahingehend werde ich die Bundesregierung auch bei der anstehenden Novellierung des MsbG zur Beschleunigung der Energiewende beraten.

Querverweise:

4.2.4 Data Governace Act, 4.2.5 Data Act

8.16 Zertifizierung und Akkreditierung

Die DSGVO ermöglicht datenschutzrechtlich Verantwortlichen eine freiwillige Überprüfung der Einhaltung ihrer Vorgaben, die durch Zertifikate bzw. Datenschutzsiegel nachgewiesen werden kann und gibt dafür einen grundsätzlichen rechtlichen Rahmen in den Artikeln 42 und 43 vor. Vertrauen und Transparenz sollen so erhöht und eine überprüfbare Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet werden. Die Grundlagen dafür sind in den genannten Artikeln relativ offengehalten, um den nationalen Besonderheiten Raum zu lassen. Das hat dazu geführt, dass die Prozesse der Ausgestaltung einen hohen zeitlichen Aufwand in Anspruch genommen haben, weil sowohl auf nationaler als auch auf EU-Ebene zunächst Grundsatzarbeit geleistet werden musste, damit die komplexe Umsetzung gelingen kann. Erste Verfahren auf EU-Ebene sind jetzt aber abgeschlossen, so dass mit Zertifizierungen im Laufe dieses Jahres zu rechnen ist.

DSGVO-Zertifizierungen sollen als Nachweis zur Einhaltung der Vorgaben der Verordnung dienen. Zertifikate darf dabei nur erteilen, wer zuvor in einem festgelegten Verfahren als Zertifizierungsstelle akkreditiert wurde. Sinn und Zweck dieser Prozedur ist es, eine besonders hohe Qualität der Zertifikate zu erreichen, die am Ende des Prozesses stehen.

Akkreditierung als Qualitätsmerkmal

Nach § 39 Bundesdatenschutzgesetz (BDSG) entscheiden die zuständigen Datenschutzaufsichtsbehörden, ob eine Stelle als Zertifizierungsstelle tätig werden darf. Das tun sie in Zusammenarbeit mit der deutschen Akkreditierungsstelle (DAkkS) (vgl. § 4 Abs. 3 AkkStelleG). Der Prozess der Akkreditierung ist durchaus komplex und zeitaufwendig[66]. Er erfordert die Einhaltung festgelegter Kriterien. Diese wurden von den unabhängigen Aufsichtsbehörden von Bund und Ländern im Arbeitskreis Zertifizierung, einer Untergruppe der Datenschutzkonferenz (DSK), konkretisiert und gemäß ISO/IEC 17065 mit einer speziellen Ausrichtung auf den Bereich des Datenschutzes erarbeitet[67].

Wesentlich für die Akkreditierung einer Zertifizierungsstelle ist das Vorliegen eines Zertifizierungsprogramms, das entsprechende Zertifizierungskriterien enthält – auch diese müssen zuerst genehmigt werden. Der Arbeitskreis Zertifizierung hat dazu ebenfalls Orientierungsvorgaben entwickelt[68], die im Berichtsjahr einer erneuten Überprüfung unterzogen und im Sommer 2022 in einer aktualisierten Version veröffentlicht wurden.

Für das Durchlaufen eines erfolgreichen Akkreditierungsprozesses ist insgesamt eine Vielzahl an Schritten auf europäischer und nationaler Ebene erforderlich, bevor eine Zertifizierungsstelle auf Grundlage ihres Zertifizierungsprogramms tätig werden kann. Diese hohen Standards sollen im Ergebnis aber auch zu besonders vertrauenswürdigen Nachweisen beitragen und es den Antragstellern mit möglichst klaren Vorgaben erleichtern, den Weg hin zu einer Zertifizierung einzuschlagen.

Nationale Zertifizierungskriterien genehmigt

Als erste deutsche Datenschutzaufsichtsbehörde hat die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW) im Berichtsjahr nationale Zertifizierungskriterien genehmigt. Das Zertifikat „European Privacy Seal“ (EuroPriSe) soll Unternehmen künftig attestieren, dass ihre Auftragsverarbeitungen den Anforderungen des europäischen Datenschutzrechts entsprechen. An diesem Genehmigungsverfahren und bei weiteren Verfahren für nationale Zertifizierungskriterien, wie etwa dem luxemburgischen Zertifizierungsverfahren GDPR-CARPA, habe ich mich intensiv in den Gremien des Europäischen Datenschutzausschusses (EDSA) beteiligt. Bei zahlreichen deutschen und bei anderen europäischen Aufsichtsbehörden liegen entsprechende neue Anträge vor, die sich in unterschiedlichen Stadien der Bearbeitung auf nationaler und EDSA-Ebene befinden. Insgesamt lässt sich feststellen: Es kommt Bewegung in den Bereich der Datenschutz-Zertifizierung.

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) ist eine der ersten Behörden, die ein spezielles Zertifizierungsprogramm entwickeln, um die Rechte von Patientinnen und Patienten bei digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) mit Blick auf den Datenschutz gezielt zu stärken. In die Umsetzung der gesetzlichen Regelungen

66 Eine Übersicht der einzelnen Prozessschritte des Akkreditierungsprozesses finden Sie unter: https://www.dakks.de/content/projekt-datenschutz
67 Kriterien der DSK, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf
68 Zertifizierungskriterien der DSK, abrufbar unter. https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_V2_0_Stand_21062022.pdf

in konkrete Prüfkriterien[69] und die Ausarbeitung eines entsprechenden Programms ist meine Behörde beratend eingebunden. Diesen Prozess werde ich auch weiterhin intensiv begleiten (8.2. Digitale Gesundheitsanwendungen)

Erstes EU-Datenschutzsiegel startet

Über die Zertifizierungen auf nationaler Ebene hinaus besteht die Möglichkeit, ein europäisches Datenschutzsiegel zu erlangen. Auch hier müssen die Kriterien vom EDSA gebilligt werden. Im Oktober 2022 hat der EDSA das erste europäische Datenschutzsiegel genehmigt. In der Stellungnahme[70] zu den von der luxemburgischen Datenschutzbehörde (CNPD) vorgelegten Europrivacy-Zertifizierungskriterien vertrat der EDSA die Auffassung, dass die eingereichten Zertifizierungskriterien mit der DSGVO im Einklang stehen. Die unabhängigen Aufsichtsbehörden von Bund und Ländern haben die positive Stellungnahme innerhalb des EDSA nicht unterstützt, weil aus deutscher Sicht noch Unklarheiten bei der Umsetzung bestehen. Ich hätte es begrüßt, wenn einzelne Aspekte des Siegels vor einer Verabschiedung nochmals eine Überarbeitung durchlaufen hätten. Jetzt, da das Siegel genehmigt ist, werde ich selbstverständlich auch die Umsetzung weiterhin im Sinne eines möglichst einheitlichen und hochwertigen Datenschutzniveaus begleiten.

Eine lebendige Zertifizierungslandschaft

Zertifizierungen sollen künftig als anerkannter Standard Vertrauen und Rechtssicherheit hinsichtlich einer rechtmäßigen Datenverarbeitung schaffen. Ziel ist es dabei unter anderem, dass ein Umfeld entsteht, in dem Datenschutzkonformität gefördert wird.

Auch für andere EU-Mitgliedsstaaten wurden bereits erste nationale Zertifizierungskriterien verabschiedet. Es liegen zahlreiche weitere Anträge vor, die eine lebendige Zertifizierungslandschaft erwarten lassen.

Vertrauenswürdige und qualitativ hochwertige Verfahren für Akkreditierung und Zertifizierung sind eine unerlässliche Voraussetzung für einen glaubwürdigen Nachweis, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern eingehalten wird. Gerade deshalb wurde sowohl auf nationaler als auch auf europäischer Ebene besonderer Wert auf die Ausgestaltung der Prozesse gelegt. Das Warten hat ein Ende – jetzt können die ersten Zertifikate an den Markt gehen und ihre Qualität unter Beweis stellen. Sie werden es auch Klein- und Mittelunternehmen erleichtern, mit der Auswahl von Anbietern bzw. Auftragsverarbeitern ihre eigene Datenverarbeitung rechtskonform auszugestalten.

Querverweise:

8.2 Digitale Gesundheitsanwendungen

69 Zertifizierungsprogramm des BfArM, abrufbar unter: https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutz-kriterien.pdf

70 Stellungnahem der CNPD, abrufbar unter: https://edpb.europa.eu/system/files/2022-10/edpb_opinion_202228_approval_of_europrivacy_certification_criteria_as_eu_data_protection_seal_en.pdf

9 Kontrollen und Beratungsbesuche

Eine meiner wesentlichen Aufgaben ist die Durchführung von Kontrollen bei den meiner Zuständigkeit unterfallenden datenverarbeitenden Stellen. Kontrollen können sowohl anlassbezogen – etwa aufgrund von Hinweisen von Bürgerinnen und Bürgern oder Medienberichten – als auch anlasslos erfolgen. Auch in der Durchführung und bezüglich des Themenspektrums gibt es eine Vielzahl von verschiedenen Kontrollarten; von der allgemeinen Querschnitts- bis zur spezifischen Schwerpunktkontrolle und von der schriftlichen Fragebogenkontrolle bis zur mehrtägigen Vor-Ort-Kontrolle besteht eine dem jeweiligen Bedarf angepasste Varianz bei der Auswahl der richtigen Kontrollart.

Besonders im Sicherheitsbereich, wo – wie schon vom Bundesverfassungsgericht festgestellt – die Datenschutzkontrollen eine Art Kompensationsfunktion für die grundsätzlich für die Betroffenen nicht erkennbar erfolgenden Eingriffe in das Grundrecht auf informationelle Selbstbestimmung erfüllt, sind Kontrollen besonders wichtig. Aus diesem Grund sehen viele Gesetze in diesem Bereich auch sogenannte Pflichtkontrollen vor. Diese verpflichten mich schon von Gesetzes wegen, in regelmäßigen Abständen besonders eingriffsintensive Datenverarbeitungen zu kontrollieren.

Ungeachtet der jeweiligen Art ist ein wesentliches Element meiner Kontrollen immer auch meine Beratungsfunktion gegenüber der verantwortlichen Stelle. Auf diese Weise lassen sich Datenschutzverstöße bereits weit im Vorfeld vermeiden. Denn Ziel ist es nicht, möglichst viele Datenschutzverstöße aufzudecken und zu sanktionieren, sondern durch eine regelmäßige Kontrollpraxis das Datenschutzbewusstsein in der praktischen Anwendung zu festigen und dadurch dazu beizutragen, die Personen, deren Daten verarbeitet werden, nachhaltig zu schützen.

In diesem Sinne habe ich – trotz der nach wie vor durch Corona bestehenden Einschränkungen – auch wieder in diesem Berichtszeitraum eine Vielzahl von Kontrollmaßnahmen durchgeführt.

9.1. Corona-angepasste Kontrollen

Die Corona-Pandemie erforderte auch in diesem Berichtsjahr ein gewisses Maß an Flexibilität und Kreativität bei meiner Kontrolltätigkeit. Das bisher am häufigsten genutzte Instrument der Vor-Ort-Kontrolle wurde pandemiebedingt um Fragebogen- und mit Videokonferenzen kombinierte Kontrollen erweitert. Die positiven Ergebnisse werden meine Kontrolltätigkeit auch mit Wirkung für die Zukunft verändern.

Die Kontrolle der Einhaltung gesetzlicher Vorgaben und die Überprüfung von aufsichtsbehördlichen Anweisungen sind zwei meiner Kerntätigkeiten. Bis vor wenigen Jahren bedeutete dies, dass meine Mitarbeitenden anlassbezogen oder anlasslos die von mir beaufsichtigten Stellen aufsuchten und vor Ort teilweise mehrtätige Kontrollen durchführten.

Unter den Voraussetzungen der Corona-Pandemie mussten bedingt durch Reise- und Kontaktbeschränkungen sowie die Obliegenheit zum Schutz meiner Mitarbeitenden trotzdem geeignete Wege gefunden werden, eine angemessene Kontrolldichte auch sicherzustellen. Hinzu kam, dass viele der zu kontrollierenden Stellen ihre Mitarbeitenden ebenfalls großflächig von zu Hause arbeiten ließen, was die Durchführung effektiver Vor-Ort-Kontrollen weiter erschwerte.

Eine Lösung für diese neue Herausforderung fand sich in Form von Kontrollen aus der Ferne. Zum einen habe ich verstärkt Kontrollen durchgeführt, bei denen die kontrollierten Stellen einen strukturierten Fragebogen erhielten, den sie bis zu einer bestimmten Frist beantworten und zurücksenden mussten. Über eine Vielzahl von geschlossenen und offenen Fragen habe ich Begebenheiten, Prozesse oder Handhabungen der kontrollierten Stellen erfragt.

Ein großer Vorteil einer Fragebogenkontrolle ist, dass sie sich leicht skalieren lässt, also inhaltsgleich an mehrere beaufsichtigte Stellen geschickt werden kann. Werden die gegebenen Antworten mehrerer kontrollierter Stellen nebeneinandergelegt, so ist ein Quervergleich möglich, über den sich auf das allgemeine Datenschutzniveau in einem Bereich schließen lässt.

Folgefragen können jedoch nicht unmittelbar, sondern erst nach Auswertung der ersten Antworten gesammelt und gemeinsam schriftlich gestellt werden, was die Erstellung von Kontrollberichten verzögern kann. Ich habe zudem festgestellt, dass nicht alle kontrollierten Stellen bei der schriftlichen Kontrolle auf Anhieb ausreichend antworten, was oft Nachfragen erforderlich machte.

Das Zurückhalten von Informationen ist wohlgemerkt nie eine Möglichkeit für eine kontrollierte Stelle: Der BfDI als Aufsichtsbehörde verfügt über entsprechende Untersuchungsbefugnisse nach der Datenschutz-Grundverordnung, die es ihm ermöglichen, sein Informationsinteresse auch durchzusetzen.

Im Gegensatz zur Fragebogenkontrolle können bei einer Kombination aus schriftlicher Kontrolle und Videokonferenzen kurzfristig auch weitere, nicht vorab von mir vorgegebene Themen, kontrolliert werden. Bei dieser Kontrollform habe ich den kontrollierten Stellen vorab Fragen und Inhalte vorgegeben, die dann ausführlich in einer Videokonferenz erläutert wurden.

Unter Nutzung von Videokonferenztools mit der Möglichkeit zur Wiedergabe von Präsentationen oder Visualisierung von Prozessen ergab sich ein konstruktiver Austausch, der auch über die vorgegebenen Inhalte hinausging. Eine solche Kontrolle ermöglicht der kontrollierten Stelle eine gute inhaltliche Vorbereitung und ist für meine Mitarbeitenden höchst effizient, da diese auf die moderne Kommunikationsinfrastruktur der Dienststelle zurückgreifen können und Reisezeiten eingespart werden.

Zusammenfassend ergänzen sich die verschiedenen Kontrollarten hervorragend und ermöglichen es mir, unter Berücksichtigung von technischen, ökologischen und weiteren Aspekten eine angemessene Kontrolldichte sicherzustellen – auch losgelöst von pandemischen Beschränkungen. So wird es auch in Zukunft, abhängig vom Inhalt der Kontrolle, keine ausschließliche Rückkehr zur klassischen Vor-Ort-Kontrolle geben, sondern jeweils die bestgeeignetste Kontrollform gewählt werden.

9.2 Kontrolle Aufbewahrungsvorschriften in der Finanzverwaltung

Insgesamt schreitet die Digitalisierung in der Finanzverwaltung weiter voran und befindet sich aus Datenschutzsicht überwiegend auf einem Weg in die richtige Richtung. Um auf diesem Pfad zu bleiben, habe ich den Finanzministerien Empfehlungen und Hinweise an die Hand gegeben. Bleibt zu hoffen, dass die einzelnen Nachzügler den Weg nicht verlassen und zügig aufschließen.

Im Jahr 2020 habe ich eine Prüfung der Regelungen zur Aufbewahrung und Speicherung personenbezogener Daten im Anwendungsbereich der Abgabenordnung (AO) in allen 16 Bundesländern begonnen. Diese Kontrolle konnte ich in diesem Berichtsjahr abschließen. Besonderer Schwerpunkt waren die Aufbewahrungsbestimmungen des Bundesministeriums der Finanzen und die jeweilige landesrechtliche Umsetzung durch die Finanzministerien der Länder.

Im Rahmen meiner Prüfung habe ich insgesamt einen positiven Gesamteindruck gewinnen können. Dennoch habe ich zu den einzelnen Prüfungsschwerpunkten Empfehlungen und Hinweise ausgesprochen, um den Datenschutz weiter zu stärken und das erreichte Grundniveau anzuheben. Insbesondere bei der Umstellung auf eine vollständige elektronische Vorgangsbearbeitung gibt es noch viel Verbesserungspotential.

Zwar haben die Bundesländer bereits elektronische Vorgangsbearbeitungen in unterschiedlichen Ausprägungen eingeführt, dennoch empfehle ich dringend, eine zeitnahe und vollständige Umstellung aller Finanzämter auf elektronische Akten und auf eine digitale Bearbeitung. Auf diese Weise können die Prinzipien der Datenminimierung und ggf. Auskunftsansprüche von Betroffenen praktisch wirksam und effizient umgesetzt werden.

Außerdem wäre es so leicht möglich, alle Dauersachverhalte (z. B. Übersichten über Sonderabschreibungen und erhöhte Absetzungen), die über die üblichen Aufbewahrungsfristen hinaus gespeichert werden, standardisiert in elektronischer Form aufzunehmen und zu erfassen.

Aus datenschutzrechtlicher Sicht wäre es zudem zu begrüßen, wenn in den Bundesländern einheitliche Regelungen zu jährlichen Stichtagen, an denen tatsächlich eine Aussonderung von Schriftgut in Papierform erfolgt, getroffen und den Beschäftigten geeignete unterstützende Programme zur Verfügung gestellt werden. Damit könnte eine fristgerechte Aussonderung leicht sichergestellt werden.

Bei der bereits laufenden Entwicklung, Umstellung und Einführung der koordinierten neuen Software-Entwicklung der Steuerverwaltung (KONSENS-Programme) empfehle ich dringend, einfache und naheliegende Möglichkeiten wie zum Beispiel regelmäßig, insbesondere größenunabhängige Löschdurchläufe von Steuerdateien durchzuführen, um bis zum Abschluss der Entwicklung und Implementierung der KONSENS-Gesamtfalladministration eine rechtzeitige, datenschutzkonforme Löschung elektronischer Daten zu gewährleisten. Darüber hinaus sehe ich es als notwendig an, die Entwicklung und Umset-

zung der KONSENS-Gesamtfalladministration entschiedener als bisher voranzutreiben und zu priorisieren.

Leider habe ich feststellen müssen, dass die grundsätzliche Aufbewahrungsfrist für Vorgänge der Einkommens-, der Körperschafts- und der Gewerbesteuer von 15 auf 20 Jahre angehoben wurde. Aus diesem Grund halte ich es für geboten, noch gezielter darauf zu achten, den Umfang der Akten auf die wirklich notwendigen Bestandteile zu begrenzen. Dies dürften insbesondere die (elektronisch gespeicherten) Festsetzungsdaten und ggf. die diesen zugrundeliegenden Erklärungsdaten sein.

Auch ist die Speicherung von personenbezogenen Daten über den tatsächlichen Abschluss einer Außenprüfung hinaus nur nach § 147 Abs. 6 Satz 2 AO gedeckt, soweit und solange die Daten noch für Zwecke des Besteuerungsverfahrens (z. B. bis zum Abschluss etwaiger Rechtsbehelfsverfahren) benötigt werden. Die zum Einsatz kommenden Löschlistenverfahren in der Außenprüfung mit Überprüfung durch den Sachgebietsleiter bzw. Innendienst begrüße ich daher sehr und empfehle diese ausdrücklich allen Bundesländern für alle Prüfungsdienste einzuführen.

Insgesamt zeigt sich, dass die fortschreitende Digitalisierung in der Finanzverwaltung die Steuerfallbearbeitung und Überwachung, insbesondere hinsichtlich der Aufbewahrung und Einhaltung der Aufbewahrungsfristen, positive und wünschenswerte Effekte hat, jedoch noch viel Verbesserungspotential in einigen Bereichen aufweist. Zu einzelnen Themenschwerpunkten plane ich daher in den kommenden Jahren, vertiefte Kontrollen und Beratungen durchzuführen.

9.3 Kontrollen in Auslandsvertretungen in Kasachstan

Die europäischen Datenschutzstandards sind auch für die deutschen Auslandsvertretungen außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums verbindliches Recht. Der BfDI prüft daher auch in den Botschaften und Konsulaten Deutschlands die Einhaltung dieser Standards.

Der Auswärtige Dienst besteht aus dem Auswärtigen Amt (AA) und den Auslandsvertretungen, die zusammen eine einheitliche Bundesbehörde unter Leitung der Bundesministerin des Auswärtigen bilden. Als Teil dieser Bundesbehörde unterliegen die Auslandsvertretungen damit meiner datenschutzrechtlichen Aufsicht.

In diesem Jahr führten meine Bediensteten einen Kontroll- und Beratungsbesuch in der deutschen Botschaft Astana und im Generalkonsulat Almaty durch. Schwerpunkte waren hierbei u. a. die Neustrukturierung der internen Datenschutzorganisation im AA sowie die Verarbeitung von personenbezogenen Daten im Rahmen der Visa-Beantragung/-Bearbeitung. In diesem Zusammenhang wurde auch die Einbindung eines für das AA tätigen externen Dienstleisters vor Ort geprüft.

Der Kontrollbericht wird aktuell noch abgestimmt, so dass mit einem formellen Abschluss der Kontrolle erst im Jahr 2023 zu rechnen ist.

9.4 Kontrollen im Sicherheitsbereich

Das Jahr 2022 war von einer Vielzahl von Kontrollen und Beratungen im Sicherheitsbereich geprägt. Viele meiner Kontrollen in diesem Bereich unterliegen dem Geheimschutz. Wegen der Natur der Sache darf ich über sie daher teilweise nur eingeschränkt oder gar nicht berichten. Es gilt der Grundsatz: „Kenntnis nur, wenn nötig“. Die nachfolgenden Kontrollen und Beratungen stellen daher nur einen kleinen Ausschnitt der tatsächlich geleisteten Arbeit dar.

9.4.1 Pflichtkontrolle: Verdeckte Maßnahmen beim BKA

Die Pflichtkontrolle hinterließ insgesamt einen sehr positiven Eindruck. Lediglich in einem Vorgang wurde ein datenschutzrechtlicher Verstoß festgestellt.

Aufgrund der Corona-Beschränkungen im Jahr 2021 konnte ich die Pflichtkontrolle erst in 2022 durchführen. Zu prüfen waren sechs Maßnahmen zur Eigensicherung nach § 34 Bundeskriminalamtgesetz (BKAG) sowie drei sehr umfangreiche sog. Gefahrenabwehrvorgänge, in denen Maßnahmen nach dem fünften Abschnitt des BKAG durchgeführt worden waren. Dabei handelt es sich um verdeckte Datenerhebungsmaßnahmen im Vorfeld bei Gefahren des internationalen Terrorismus.

Ich konnte alle Anordnungen und Beschlüsse einsehen und prüfen. Gleiches galt für die Dokumentation im Vorgangsbearbeitungssystem VBS und die Daten im einheitlichen Fallbearbeitungssystem eFBS. Auch eine Datenabfrage und Kontrolle im polizeilichen Informationssystem INPOL wurde mir ermöglicht.

Die Dokumentation fiel dabei insgesamt positiv auf. Fast alle Maßnahmen waren umfassend und nachvollziehbar festgehalten. Auch die erforderlichen Benachrichtigungen betroffener Personen und deren Dokumentation konnte überprüft werden und war generell sorgfältig umgesetzt worden.

Lediglich in einem Vorgang – bezüglich einer Maßnahme nach § 34 BKAG – ermöglichte die Dokumentation es

nicht, die Entscheidungen des BKA vollständig nachzuvollziehen. Zudem kam es in diesem Vorgang zu einem datenschutzrechtlichen Verstoß von jedoch eher formeller Natur. Im Vorfeld der Eigensicherungsmaßnahme fehlte der für die zu sichernde Strafverfolgungsmaßnahme einzuholende Gerichtsbeschluss.

Die Durchführung der Eigensicherungsmaßnahme ergab dann aber, dass die Strafverfolgungsmaßnahme voraussichtlich keine weiteren Erkenntnisse ergeben wird. Deshalb konnte von letzterer abgesehen werden. Es handelt es sich hierbei jedoch um einen Einzelfall. Auch bestand erheblicher Zeitdruck und ein Gerichtsbeschluss wäre mit sehr hoher Wahrscheinlichkeit erlangt worden, da aus meiner Sicht die gesetzlichen Voraussetzungen vorlagen. Daher habe ich von einer Beanstandung abgesehen.

9.4.2 Pflichtkontrolle eingriffsintensiver Maßnahmen im Zollfahndungsamt München

Das Zollfahndungsdienstgesetz erlaubt den Zollfahndungsämtern und dem Zollkriminalamt in ihrer Zuständigkeit den Einsatz besonderer Mittel der Datenerhebung, wenn Straftaten von erheblicher Bedeutung vermutet werden. Diese Mittel unterliegen meiner besonderen datenschutzrechtlichen Kontrollpflicht.

Besondere Mittel der Datenerhebung zeichnen sich dadurch aus, dass Daten auch verdeckt, also ohne Wissen der betroffenen Personen, erhoben werden können. Meine Datenschutzkontrollen sind in diesem Bereich besonders wichtig. Sie sollen ausgleichen, dass es den betroffenen Personen mangels Kenntnis der sie betreffenden Maßnahmen selbst nicht möglich ist, gerichtlichen Rechtschutz zu suchen. Seit 2021 bin ich daher durch das neue Zollfahndungsdienstgesetz verpflichtet, den Einsatz dieser Mittel regelmäßig zu kontrollieren.

Meinem Kontrollauftrag bin ich dieses Jahr im Zollfahndungsamt München nachgekommen. Im Zentrum der Kontrolle stand der Einsatz längerfristiger Observationen als ein besonderes Mittel der Datenerhebung.

Positiv ist zunächst der restriktive Einsatz der eingriffsintensiven Maßnahme hervorzuheben. Dieser führte dazu, dass ich in den mir zur Verfügung stehenden Kontrolltagen eine Vollkontrolle durchführen konnte, d. h. dass alle zu den längerfristigen Observationen vorhandenen Aktenbestände geprüft werden konnten.

Während meiner Kontrolle habe ich insbesondere bei der ordnungsgemäßen Aktenführung Defizite festgestellt, so dass ich in Folge dessen zwei Beanstandungen ausgesprochen habe. Dabei ging es zum einen um die Nachvollziehbarkeit der Ermittlungsarbeit und des Verfahrensablaufs, zum anderen um die Dokumentation der Nachhaltung der gesetzlichen Benachrichtigungspflichten.

Die Beanstandungen wurden durch das Bundesministerium der Finanzen und das Zollfahndungsamt München uneingeschränkt angenommen und die Versäumnisse eingeräumt. Gleichzeitig erfolgten umgehend Anpassungen interner Arbeitsanweisungen sowie die Etablierung neuer Arbeitsprozesse, um die ordnungsgemäße Aktenführung zukünftig sicherstellen zu können.

9.4.3 Datenübermittlung des BKA im internationalen Bereich

In dem Berichtszeitraum habe ich einen verpflichtenden Beratungs- und Kontrolltermin beim Bundeskriminalamt (BKA) wahrgenommen. Gegenstand der Kontrolle waren die Übermittlungen von personenbezogenen Daten Minderjähriger in Drittstaaten in den Jahren 2020 und 2021.

In insgesamt rund 280 Stichproben habe ich für die Jahre 2020 und 2021 im BKA geprüft, ob personenbezogene Daten Minderjähriger rechtmäßig in Drittstaaten übermittelt wurden.

Nur in einem Fall habe ich festgestellt, dass die Datenübermittlung nicht erforderlich gewesen ist und dies nach § 16 Abs. 2 Bundesdatenschutzgesetz (BDSG) beanstandet. Um einen Anschlussinhaber in einem strafrechtlichen Ermittlungsverfahren zu ermitteln, stellte das BKA eine Anfrage an Interpol Kasachstan. Dabei wurden auch personenbezogene Daten eines in Deutschland lebenden Verdächtigen übermittelt. Diese Übermittlung war nicht erforderlich, um den Anschlussinhaber festzustellen. Das BKA räumte diesen Verstoß während des Kontrolltermins ein.

In den übrigen Fällen konnte ich keine Verstöße gegen die datenschutzrechtlichen Regeln feststellen, nach denen das BKA in Drittstaaten übermittelt. Überwiegend waren Fälle Gegenstand meiner Prüfung, in denen das BKA in seiner sog. Korrespondenzfunktion den mit Drittstaaten erforderlichen Dienstverkehr für Landespolizeibehörden übernimmt. In diesen Fällen muss das BKA zwingend mindestens eine summarische materielle Rechtmäßigkeitsprüfung vornehmen. Das BKA bezeichnet diese Funktion hingegen als „Botenfunktion“ und hält eine formelle Rechtmäßigkeitsprüfung für ausreichend.

Diese Thematik war bereits Gegenstand meiner letzten Kontrolle (vgl. 29. TB Nr. 9.5.4). Laut eines Rundschreibens des BKA lässt sich dieses in Fallkonstellationen von Personenfeststellungsverfahren, die es in seiner Korrespondenzfunktion für die Länder durchführt, immer den Sachverhalt, die Delikte sowie weitere Angaben von den Landespolizeibehörden mitteilen, bevor es für diese Behörden tätig wird. Ich schließe daraus, dass sich das BKA seiner datenschutzrechtlichen Verantwortung bewusst ist und in der Praxis durchaus eine summari-

sche Prüfung vornimmt, die über eine reine formelle Rechtmäßigkeitsprüfung hinausgeht.

Die Dokumentation einiger der geprüften Fälle war für mich vor Ort allerdings nicht nachvollziehbar. In einer Nachbesprechung konnten mir die zuständigen Sachbearbeiter beim BKA die tatsächlichen und rechtlichen Grundlagen der Datenübermittlung erläutern. Ein solches Nachgespräch kann eine ordnungsgemäße Dokumentation jedoch nicht ersetzen.

Das BKA muss jede Einzelfallentscheidung polizeilichen Handelns gesondert verakten und die Grundsätze einer ordnungsgemäßen Aktenführung einhalten. Defizite in diesem Bereich hatte ich bereits in der Vergangenheit beanstandet (vgl. 28. TB Nr 6.7.3, 30. TB Nr. 8.2.2). Vor dem Hintergrund der aktuellen Prüfergebnisse halte ich an meinen Hinweisen auf Änderungsbedarf bei der Aktenführung beim BKA fest.

9.4.4 Pflichtkontrollen ATD/RED

Nach Durchführung der Pflichtkontrollen von Anti-Terror-Datei (ATD) und Rechtsextremismus-Datei (RED) bleibe ich bei meiner grundsätzlichen Einschätzung, dass der Nutzen dieser Dateien für die Sicherheitsbehörden – übrigens auch nach Meinung der teilnehmenden Behörden selbst – sehr gering ist bei gleichzeitig weitreichendem Grundrechtseingriff aufgrund der großen Anzahl der angeschlossenen Behörden und der sensiblen gespeicherten Daten. Insofern fordere ich weiterhin die Abschaffung beider Dateien in ihrer jetzigen Form.

Das Bundesministeriums des Innern und für Heimat (BMI) hat bisher auf meine in vergangenen Kontrollberichten (s. 30. TB, Nr. 8.1.1) geäußerten Kritik an der Art und Weise der automatisierten Einspeicherung in beiden Dateien, die nach meiner Bewertung meine Kontrolle der Datenhistorie erheblich erschwert, noch nicht mit einer Umgestaltung der technischen Lösung reagiert.

Sowohl ATD als auch RED werden mit teils sehr sensiblen personenbezogenen Daten gefüllt. Der entstehende Grundrechtseingriff wiegt auch deswegen schwer, weil eine große Zahl von Behörden prinzipiell Zugriff darauf nehmen kann. Die Dimension des Grundrechtseingriffs steht aber im Kontrast zur Geeignetheit des Konstrukts. Die unmittelbaren Eindrücke zur tatsächlichen Nutzung und dem Gewinn für die Arbeit der Sicherheitsbehörden bestätigen mich vielmehr in meiner Meinung, dass ATD und RED einer umfassenden Umgestaltung bedürfen, wenn sie nicht gar abgeschafft werden sollten.

Kontrolle beim Bundesnachrichtendienst (BND)

Die Kontrolle der ATD beim BND habe ich im Mai 2022 durchgeführt. Dabei wurden auch Datensätze geprüft, die in der pandemiebedingt schriftlich durchgeführten Kontrolle 2020 nicht zufriedenstellend erörtert werden konnten. Zu beanstandende wesentliche datenschutzrechtliche Defizite habe ich nicht festgestellt. Praxisempfehlungen habe ich jedoch u. a. zu Löschwiedervorlagen und zur Dokumentation der Entscheidung zur verdeckten oder beschränkten Speicherung gegeben. Diese wurden bereits umgesetzt, so dass die Kontrolle abgeschlossen werden konnte.

Kontrolle beim Bundesamt für Verfassungsschutz (BfV)

Ende des Jahres 2021 habe ich vor Ort im BfV die Kontrolle der Nutzung sowohl der ATD als auch der RED durchführen und abschließen können. Die aus meiner Sicht weiterbestehenden Schwächen bei den automatisierten Befüllungsschnittstellen habe ich hierbei nach intensiver Prüfung in den letzten Kontrollen nicht erneut zum Kontrollgegenstand gemacht, denn, wie bereits oben erläutert, hatte das BMI während der letzten Jahren trotz anderer Beteuerungen keine Verbesserungen der Technik veranlasst. Somit waren hier keine neuen Erkenntnisse zu erwarten. Der Stillstand bestätigt lediglich den Eindruck einer wenig beachteten Datei. Zwar habe ich in den aktuellen Kontrollen sowohl bei der ATD als auch der RED datenschutzrechtliche Mängel bei einzelnen Speicherungen festgestellt, die das BfV aber umgehend beseitigte. Deshalb konnte ich von einer Beanstandung in beiden Fällen absehen.

Kontrolle beim Bundesamt für den Militärischen Abschirmdienst (BAMAD)

Beim BAMAD führte ich im Berichtsjahr 2022 die regelmäßige Kontrolle der Nutzung der ATD durch. Dabei kritisierte ich die Speicherung von Datensätzen, die nach Abschluss eines Auslandseinsatzes der Bundeswehr ohne Grundlage weiter gespeichert wurden. Das BAMAD sagte daraufhin die Löschung dieser Daten zu. Diese letzten verbliebenen Datensätze des BAMAD in der ATD wurden tatsächlich unverzüglich gelöscht. Deshalb habe ich hier von einer Beanstandung abgesehen.

Kontrolle beim Bundeskriminalamt (BKA)

Ende 2021 habe ich die ATD beim BKA kontrolliert. Dabei musste ich feststellen, dass nicht alle Einspeicherungen mit dem Datenschutzrecht im Einklang standen. Ich habe daher neben zwei Anpassungsempfehlungen auch zwei Beanstandungen ausgesprochen.

Beanstandet habe ich die fehlende Möglichkeit einer – teilweise gesetzlich vorgesehenen – Einzelfallprüfung bei der automatisierten Übertragung von Daten aus der Quelldatei in die ATD. Ferner hatte das BKA die Daten zu einer Person erst drei Jahre nach Einstellung des Ermittlungsverfahrens und damit nicht unverzüglich im

Sinne des § 58 Abs. 2 Bundesdatenschutzgesetz (BDSG) gelöscht.

Des Weiteren habe ich bei meiner Kontrolle in mehreren Fällen Daten zu Personen vorgefunden, die mittlerweile verstorben sind. Ich möchte zwar im Einzelfall nicht ausschließen, dass es angesichts der Zielsetzung der ATD notwendig sein kann, auch Daten von Verstorbenen weiter zu speichern. Allerdings birgt dies auch die Gefahr, dass gesetzliche Vorgaben umgangen werden können. Ich habe daher empfohlen, die Löschung von Daten Verstorbener zu überprüfen. Im Übrigen habe ich eine gesonderte Dokumentation der Speichervoraussetzungen empfohlen.

Die Kontrolle der Speicherungen in der RED konnte bis zum Redaktionsschluss nicht abgeschlossen werden.

Kontrolle bei der Bundespolizei (BPol)

Die Pflichtkontrolle der ATD aus dem Jahr 2021 konnte im Berichtsjahr 2022 abgeschlossen werden. Einen Grund für eine Beanstandung gab es nicht. Da jedoch die Dokumentationsdefizite aus der vorhergehenden Kontrolle in 2019 noch nicht zur vollständigen Zufriedenheit abgestellt waren, musste ich erneut Empfehlungen zur Verbesserung aussprechen. Solange meine Empfehlung, die Dateien gänzlich aufzulösen, nicht umgesetzt wird, bleibt zu hoffen, dass so mit jeder Kontrolle zumindest ein weiterer Schritt zur Optimierung der Dokumentation und damit zur Wahrung des Rechtstaatsprinzips getan wird.

Auch die Ende 2021 begonnene Kontrolle der RED in einer ausgewählten Direktion der BPol konnte im Berichtsjahr 2022 abgeschlossen werden. Die BPol prüfte nach meiner Kontrollankündigung die Datei selbst und stellte einige Mängel fest. Meine Prüfung deckte darüber hinaus einen systemischen Fehler im Vorgangsbearbeitungssystem sowie kleinere Dokumentationsdefizite auf. Der systembedingte Fehler soll mit einem Update der Software behoben werden; den Dokumentationsdefiziten wurde zwischenzeitlich schon mit Anpassungen interner Regelungen begegnet.

Zusätzlich musste ich eine Beanstandung aussprechen, da nicht alle Datensätze die nötigen Speichervoraussetzungen erfüllten. Das Defizit wurde zwischenzeitlich abgestellt. Aufgrund meiner Kontrolle wurde ein erheblicher Anteil der Daten in der RED gelöscht.

Ich empfehle dem Gesetzgeber weiterhin, angesichts des festgestellten geringen Nutzwertes von Antiterrordatei und Rechtsextremismusdatei, diese abzuschaffen.

9.4.5 PIAV-Kontrolle

Infolge einer Bürgereingabe habe ich die anlassbezogene Löschung von Altdatensätzen des Zollfahndungsdienstes in der Verbunddatei Rauschgift des sog. Polizeilichen Informations- und Analyseverbund (PIAV) kontrolliert. Die Kontrolle führte im Ergebnis zur Löschung von 7.798 Datensätzen, für die das Fortbestehen der Speichervoraussetzungen nicht mehr ohne erheblichen Aufwand ermittelt werden konnte.

Im Jahr 2021 erreichte mich eine Bürgereingabe, bei deren Untersuchung eine Abweichung der Speicherung personenbezogener Daten zwischen dem internen Informationssystem des Zollfahndungsdienstes (INZOLL) und PIAV-Rauschgift aufgedeckt wurde. Während die Speicherung in INZOLL längst gelöscht war, war sie im PIAV weiterhin für alle Verbundteilnehmer auffindbar. Der Sachverhalt ließ darauf schließen, dass es sich um ein systematisches Problem im Zusammenhang mit der Übertragung des bisherigen Datenbestandes aus der Falldatei Rauschgift (FDR) in den PIAV handeln könnte.

Polizeilicher Informations- und Analyseverbund

Der PIAV ist ein Teil des gemeinsamen Informationssystems der deutschen Polizei. Im PIAV werden Daten des BKA, der Landespolizeidienststellen, der Bundespolizei und auch der Zollbehörden zusammengeführt, die diese jeweils aus ihren internen Systemen anliefern. Innerhalb des PIAVs ist die Komponente „Rauschgift“ eine deliktsbezogene Datei, in die Fälle der Rauschgiftkriminalität mit länderübergreifender Bedeutung eingetragen werden sollen. Sie hat Mitte 2018 die Falldatei Rauschgift (FDR) abgelöst. Der zu diesem Zeitpunkt in der FDR enthaltene Datenbestand wurde im Zuge der Ablösung in den PIAV migriert.

Aus diesem Anlass wurde im Jahr 2022 eine Kontrolle bei der Zollfahndung durchgeführt. Dabei wurde festgestellt, dass bei den Altdatensätzen aus der früheren FDR kein funktionierender Prozess für eine anlassbezogene Löschung im PIAV eingerichtet war. Daher waren in diesen Fällen erforderliche Löschungen, die in INZOLL vollzogen wurden, nicht an den PIAV weitergegeben worden.

Nachdem dieser Sachverhalt feststand, erkannte auch das ZKA den bestehenden Datenschutzverstoß und unterbreitete mir von sich aus einen konstruktiven Lösungsvorschlag. Da nur mit erheblichem Aufwand hätte ermittelt werden können, ob die Speichervoraus-

setzungen im Einzelfall jeweils fortbestehen, wurden als Ergebnis der Kontrolle sämtliche der 7.798 damals aus der FDR migrierten Datensätze aus dem PIAV gelöscht.

Die Aufgabenerfüllung des Zollfahndungsdienstes wurde dabei nicht beeinträchtigt. Datensätze, die für die Aufgabenerfüllung noch gebraucht werden, sind weiterhin in INZOLL vorhanden und können bei Bedarf nochmals an den PIAV übertragen werden. Eine Wiederholung des Fehlers kann ausgeschlossen werden. Seit Mitte 2018 werden relevante Datensätze aus INZOLL unmittelbar an den PIAV übermittelt. Dafür wurde eine neue, automatisierte Schnittstelle eingerichtet, welche einen Gleichlauf der Systeme sicherstellt.

9.4.6 Kontrolle der Abrufe von Daten im automatisierten Auskunftsverfahren

Das Bundeskriminalamt (BKA) hält technisch-organisatorische Vorkehrungen vor, um missbräuchliche Abfragen von Telekommunikationsdaten zu verhindern.

Die Befugnisse der Strafverfolgungsbehörden, auf Datenbestände zuzugreifen oder von öffentlichen und nichtöffentlichen Stellen Auskunft über personenbezogene Daten zu verlangen, bergen ein Potenzial für Datenmissbrauch. Wie eine Reihe von öffentlich bekannt gewordenen Fällen zeigen, können solche Befugnisse z. B. dazu missbraucht werden, um Menschen – wie Lebensgefährten, Ex-Freunde, Prominente oder Nachbarn – aus persönlichen Motiven auszuspionieren. Auch wenn diese nicht das BKA betrafen, habe ich dort anlassunabhängig eine Kontrolle zum Umgang mit personenbezogenen Daten im automatisierten Auskunftsverfahren nach § 173 des Telekommunikationsgesetzes durchgeführt.

Die Hemmschwelle für einen missbräuchlichen Abruf könnte bei dieser Art des Abrufverfahrens schon deshalb niedriger sein, weil die Abfrage personenbezogener Daten automatisiert durchgeführt werden kann. Betroffene Kundendaten sind vor allem Rufnummern, andere Anschlusskennungen, Namen und Anschrift des Anschlussinhabers oder der Anschlussinhaberin, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen auch die Anschrift des Anschlusses und in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie das Datum des Vertragsbeginns.

Geprüft habe ich die technisch-organisatorischen Vorkehrungen, die das BKA ergreift, um missbräuchliche Datenabfragen im automatisierten Auskunftsverfahren zu verhindern. Außerdem wurden stichprobenweise die gesetzlichen Voraussetzungen für die Datenabfragen im automatisierten Auskunftsverfahren in einer Reihe von Einzelfällen überprüft.

Die Kontrolle hat keine wesentlichen datenschutzrechtlichen Defizite ergeben. Es konnten allerdings datenschutzrechtliche Verbesserungen erzielt werden. Insbesondere konnte ein Softwarefehler gefunden und behoben werden, der zu einer zweifachen Verarbeitung personenbezogener Daten im Zuge des automatisierten Auskunftsverfahren führte.

9.4.7 Funkzellendatei des Bundeskriminalamts

Das Bundeskriminalamts (BKA) hat gegen von mir erlassene Maßnahmen gegen dessen Funkzellendatenbank Klage erhoben. Aufgrund einer gewollten Gesetzeslücke darf das BKA die Datenbank vorerst zumindest bis zu einer bestandskräftigen Gerichtsentscheidung weiter betreiben.

Im 30. Tätigkeitsbericht (8.2.4.) berichtete ich darüber, dass ich die Rechtswidrigkeit der Datenspeicherung und des Datenabgleichs in einer Funkzellendatenbank des BKA beanstandet hatte. In dieser Datenbank verarbeitet das BKA die durch die Polizeibehörden der Länder in diversen Ermittlungsverfahren erhobenen Funkzellendaten.

Nach meiner Auffassung hat das BKA für die tiefgreifenden Datenverarbeitungen, die ich in der beanstandeten Datenbank feststellen konnte, keine Rechtsgrundlage. Deshalb habe ich gegenüber dem BKA verbindlich angeordnet, keine weiteren personenbezogenen Daten in dieser Datenbank zu speichern und die dort gespeicherten personenbezogenen Daten zu löschen. Bis zur Löschung der personenbezogenen Daten habe ich dem BKA verboten, weitere Datenabgleiche vorzunehmen.

Das BKA und das Bundesministerium des Innern und für Heimat teilen meine Rechtsauffassung nicht. Daher hat das BKA gegen meine Anordnungsverfügung Klage erhoben. Aufgrund der aufschiebenden Wirkung dieser Klage muss das BKA meine Anordnung bis zu einer bestandskräftigen Gerichtsentscheidung nicht befolgen. Die im deutschen Verwaltungsrecht eigentlich übliche Möglichkeit einer Behörde, die sofortige Vollziehung des von ihr erlassenen Verwaltungsaktes anzuordnen, wenn die sofortige Vollziehung im öffentlichen Interesse oder im überwiegenden Interesse eines Beteiligten liegt, hat der Gesetzgeber in § 20 Abs. 7 BDSG ausdrücklich ausgeschlossen.

Die Beschränkung dieser Befugnis wurde isoliert und zielgerichtet nur im Hinblick auf die Durchsetzung des europäischen Datenschutzrechts eingeführt. Darin sehe ich eine erhebliche Beschränkung der effektiven Daten-

schutzaufsicht. Aus diesem Grund habe ich die Europäische Kommission gebeten, die Vereinbarkeit des § 20 Abs. 7 BDSG mit dem Europäischen Rechts zu prüfen.

9.4.8 Koordinierte Kontrollen zu Ausschreibungen zur verdeckten/gezielten Kontrolle im Schengener Informationssystem

Im Juni 2019 hatten sich europäische Datenschutzbehörden darauf geeinigt, Ausschreibungen zur verdeckten/gezielten Kontrolle im Schengener Informationssystem (SIS) systematisch zu prüfen. In Deutschland haben daraufhin die Datenschutzaufsichtsbehörden des Bundes und der Länder 27 Stellen bei Polizei und Nachrichtendiensten koordiniert kontrolliert. Mehrere formelle und materielle Rechtsverstöße wurden festgestellt. Die deutschen Aufsichtsbehörden haben verschiedene Maßnahmen und Empfehlungen ausgesprochen bzw. planen diese.

Europaweit ist die Zahl der Ausschreibungen zur verdeckten/gezielten Kontrolle nach Artikel 36 des Ratsbeschlusses 2007/533/JI vom 12. Juni 2007 im SIS in den letzten Jahren kontinuierlich angestiegen. Mit dieser Kategorie von Ausschreibungen können Personen oder Sachen zur Strafverfolgung oder Gefahrenabwehr ausgeschrieben und aufgrund dessen dann verdeckte bzw. gezielte Kontrollen durchgeführt und eine Reihe an Daten an die ausschreibende Stelle übermittelt werden. Aus den Treffermeldungen einer solchen Ausschreibung lassen sich umfassende Bewegungsbilder der betroffenen Person und ihrer Begleitpersonen generieren. Es handelt sich dementsprechend um einen intensiven Grundrechtseingriff.

Vor diesem Hintergrund beschloss die europäische Arbeitsgruppe zur koordinierten Aufsicht über das SIS, die SIS II Supervision Coordination Group (SIS SCG), die Thematik aufzugreifen und eine gemeinsame Kontrollaktivität durchzuführen. Ziel ist es, den steigenden Zahlen auf den Grund zu gehen und ein Gesamtbild über die Nutzung dieses Instruments und damit verbundene datenschutzrechtliche Fragen zu erhalten. Zugleich soll die Rechtmäßigkeit solcher Ausschreibungen in einer Stichprobe kontrolliert werden.

Die Koordinierungsgruppe des SIS II ("SIS II SCG") ist ein von der SIS II Verordnung und dem SIS II Rahmenbeschluss eingerichtetes Gremium, das den Schutz personenbezogener Daten im Informationssystem SIS II überwacht. Die Gruppe besteht aus Vertretern der nationalen Aufsichtsbehörden der Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten.

Obwohl die Zahl dieser Ausschreibungen in Deutschland im Vergleich zu anderen Mitgliedsstaaten nicht stark zugenommen hat, haben sich die Datenschutzbehörden des Bundes und der Länder darauf geeinigt, auch in Deutschland koordinierte Kontrollen durchzuführen.

Im Bereich der Polizeien habe ich deshalb auf Bundesebene zwei Kontrollen zu verdeckten/gezielten Ausschreibungen durchgeführt (27. TB Nr. 9.3.5). Zuletzt habe ich dieses Jahr die entsprechenden Ausschreibungen des Bundeskriminalamts geprüft und dabei keine Verstöße festgestellt. Allerdings habe ich empfohlen, die Dokumentation der Unterlagen zu verbessern.

Im Bereich der Nachrichtendienste habe ich in den letzten Jahren zudem drei Kontrollen zu Ausschreibungen nach Artikel 36 des Ratsbeschlusses 2007/533/JI vom 12. Juni 2007 vorgenommen (Nr. 9.2.9 und Nr. 9.2.10 sowie 30. TB Nr. 8.2.6 und Nr. 8.2.7). Darüber hinaus haben sich 11 Aufsichtsbehörden der Länder an den Kontrollen beteiligt, wodurch insgesamt 27 Stellen bei Bund und Ländern kontrolliert wurden. Weitere Prüfungen in diesem Bereich sind geplant.

Bei den Kontrollen von Bund und Ländern wurde eine Reihe an formellen und materiellen Verstößen festgestellt, so beispielsweise Fehler bei der Anordnung der Ausschreibung, der Fristberechnung, der Dokumentation und dem Aktenrückhalt. Entsprechende Maßnahmen und Empfehlungen wurden durch die jeweils zuständigen Aufsichtsbehörden ausgesprochen bzw. sind geplant. Abschließend ist zudem eine europaweite Auswertung der Ergebnisse in der SIS SCG vorgesehen.

Querverweise:

9.2.9 Datenschutzaufsicht und Beratung beim BfV; 9.2.10 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst

9.4.9 Datenschutzaufsicht und Beratung beim BfV

Im Berichtszeitraum habe ich diverse Kontrollen sowie Informations- und Beratungsbesuche beim Bundesamt für Verfassungsschutz (BfV) durchgeführt. Schwerpunkte lagen u. a. im Bereich der elektronischen Akte und deren Nachfolgesystem sowie im Bereich diverser Internetaktivitäten des BfV.

Elektronische Akte

Auch in diesem Jahr habe ich das BfV zum Großprojekt des einheitlichen Dokumentenmanagementsystems im Verfassungsschutzverbund (Verbund-DMS) beraten. Das Verbund-DMS soll eine einheitliche Vorgangsbearbeitung beim BfV, den Landesämtern für Verfassungsschutz und künftig auch beim Bundesamt für den Militärischen

Abschirmdienst (BAMAD) gewährleisten und hierfür verschiedene Schnittstellen bereitstellen. Die im vergangenen Jahr begonnene Beratung des BfV hierzu sowie der Austausch mit den Kolleginnen und Kollegen der Landesdatenschutzbehörden wurde fortgesetzt.

Die geplante Einführung des neuen Vorgangsbearbeitungssystems und die damit einhergehende große datenschutzrechtliche Bedeutung habe ich auch zum Anlass genommen, das aktuelle System DOMUS beim BfV zu kontrollieren. Im Fokus stand dabei die Funktionalität und technische Umsetzung der Volltextsuche nach Personen und die Einhaltung der gesetzlichen Grenzen gemäß § 13 Abs. 4 Satz 3 Bundesverfassungsschutzgesetz (BVerfSchG). Ziel der Kontrolle war es, mögliche datenschutzrechtliche Schwachstellen des bisherigen Systems zu identifizieren und die Ergebnisse frühzeitig in das sich noch im Entwicklungsstadium befindliche Verbund-DMS miteinzubeziehen.

Beanstandungen haben sich in der Kontrolle nicht ergeben. Allerdings habe ich weitere technische organisatorische Maßnahmen in Bezug auf beide Systeme mit dem BfV diskutiert. Eine dieser Maßnahmen betrifft die interne Datenschutzkontrolle. Diese hat in Bezug auf DOMUS erfreulicherweise zeitnah nach meinem Hinweis auf die Notwendigkeit der regelmäßigen Durchführung mit einem neuen Konzept begonnen, sodass die hiesige Kontrolle erfolgreich abgeschlossen werden konnte. Eine weitere Kontrolle meinerseits zusammen mit dem behördlichen Datenschutz des BfV ist für das kommende Jahr geplant. Dabei soll geprüft werden, ob die Suche nach Personen von den Mitarbeitenden des BfV ausschließlich innerhalb der rechtlich zulässigen Grenzen genutzt wird.

Erste Ergebnisse der beim BfV bereits begonnenen internen Kontrolle deuten leider darauf hin, dass bei vielen Mitarbeitenden des BfV Unklarheiten bei der Nutzung der Personensuche in DOMUS bestehen. Das lässt zwar nicht automatisch auf einen bewussten Missbrauch schließen. Allerdings sehe ich mich in der Notwendigkeit bestätigt, die geplante gemeinsame Kontrolle mit dem BfV im nächsten Jahr durchzuführen und die bereits begonnene interne Kontrolle sowie verpflichtende Schulungen der Mitarbeitenden als organisatorische Maßnahmen unbedingt weiter zu verfestigen. Die Ergebnisse der Kontrolle werden entscheidend sein, ob für das Verbund-DMS neben den bereits bei DOMUS implementierten organisatorischen Maßnahmen auch weitere technische Maßnahmen erforderlich sind.

Information und Beratung bei neuen Datenerfassungs- und Analysesystemen

Wie die meisten anderen Sicherheitsbehörden erschließt das BfV zunehmend Möglichkeiten der Informationsgewinnung im Internet. Hier gibt es verschiedene Arten der Vorgehensweise, in Fachkreisen z. B. mit Begriffen wie OSINT (Open Source Intelligence – die Informationsgewinnung aus offenen Quellen), SOCMINT (Social Media Intelligence – die Informationsgewinnung mittels sozialer Medien) oder ONI (Operative Nutzung des Internets durch verdeckte Informationserhebung durch Ausnutzung schutzwürdigen Vertrauens) bezeichnet.

Der Austausch und die Verbreitung von verfassungsfeindlichen Äußerungen, von Propaganda und Desinformation, aber auch die Mobilisierung bzw. der Aufruf zu potentiell verfassungsfeindlichen Aktionen verlagert sich seit Jahren immer mehr ins Internet, teils offen, teils konspirativ. Daher beobachtet der Verfassungsschutz insbesondere einschlägige Internetseiten, aber auch Social Media Plattformen, und wertet diese systematisch aus.

Zugleich werden neue technische Kompetenzen bei modernen Datenanalysemethoden aufgebaut. Das BfV stellt sich dabei organisatorisch neu auf und hat mir, wie in § 14 Abs. 1 BVerfSchG verpflichtend vorgegeben, zuletzt auch mehrere Dateianordnungen zu neuen Systemen aus diesem Themenbereich zur Anhörung vorgelegt.

In Folge eines sich stetig ändernden Kommunikationsverhaltens und technischer Fortentwicklungen in der Gesellschaft wächst die Menge der potentiell zu durchsuchenden bzw. zu analysierenden Daten exponentiell. Dem muss auch das BfV begegnen (siehe unten „Kontrolle Mediendateien“). Aus meiner Sicht ist es wichtig, diese Daten nur im absolut erforderlichen Umfang und für einen möglichst begrenzten Zeitraum zu speichern. Wenn sich keine tatsächlichen Anhaltspunkte für eine Zuständigkeit des BfV aus den Daten ergeben, müssen sie natürlich auch wieder umgehend gelöscht werden.

Ich befinde mich mit dem BfV und auch dem BMI in der Diskussion, wie weit die jetzigen Rechtsnormen für eine solche Datenverarbeitung noch tragfähig sind. In einigen Fällen sehe ich die Fortentwicklung von Datenerfassungs- und Analysesystemen durchaus problematisch.

Um die tatsächlichen fachlichen Bedürfnisse und Rahmenbedingungen der Datenverarbeitungen besser einschätzen zu können, habe ich neben Kontrollen auch Informations- und Beratungsbesuche durchgeführt, über deren genauen Inhalt ich aufgrund von Geheimhaltungsvorgaben hier nur sehr begrenzt berichten kann.

Im Berichtszeitraum besuchte ich beispielsweise eine relativ junge Organisationseinheit in der Abteilung Technische Analyseunterstützung und Datengewinnung sowie den Bereich der Cyberabwehr und beriet mich mit dem BfV gezielt zu einzelnen Verfahren der Informationsgewinnung im Internet. Mein Eindruck aus diesen

Kontakten ist, dass sich hier mit großer Dynamik neue methodische sowie technische Herausforderungen für das BfV ergeben. Möglicherweise muss darauf auch mit entsprechenden Änderungen des BVerfSchG reagiert werden. Daher werde ich die Entwicklungen auch weiterhin eng datenschutzrechtlich begleiten und den Austausch mit dem BfV und dem BMI zur Beratung suchen.

Kontrolle Mediendateien

Die gerade beschriebene Problematik zieht Folgeprobleme bei der Ablage von umfangreichen Mediendateien nach sich. Notwendig ist die Entwicklung und Implementierung von technischen Systemen, die Mediendateien im Internet (z. B. Audio-, Video oder Textdateien) systematisch aufbereiten, sortieren und auffindbar archivieren. Dazu bietet das BfV für den Verfassungsschutzverbund eine gemeinsame Datei für die Datenverarbeitung von Mediendateien an. Im Berichtszeitraum habe ich begonnen, diese Datei datenschutzrechtlich umfangreich zu kontrollieren. Im Vordergrund meiner Prüfung steht, neben der Prüfung der tatsächlichen Funktionsweise der Anwendung, dessen datenschutzrechtliche Einordnung in die Systemlandschaft des Verfassungsschutzverbundes, die Einhaltung von Speicher- und Löschfristen, die Rechte von Betroffenen und die Unkenntlichmachung von unbeteiligten Dritten in Mediendateien. Aus Geheimhaltungsgründen und des Fortdauerns meiner Prüfung kann ich hier keine weitergehenden Auskünfte machen.

Kontrolle verdeckter Ausschreibungen im SIS II beim BfV

Die bereits Anfang des Jahres 2020 beim BfV durchgeführte Kontrolle der verdeckten Ausschreibungen im Schengener Informationssystem der 2. Generation (SIS II) (vgl. 29. TB Nr. 9.5.1; 30. TB Nr. 8.2.7) konnte im Berichtsjahr 2022 abgeschlossen werden. Die Kontrolle hat einige diffizile Rechtsfragen ergeben, die im Nachgang umfassend mit dem BfV diskutiert wurden.

Meiner Auffassung nach war bei vielen Stichproben der Umfang der vom BfV im Rahmen des Ausschreibungsformulars an die nationale Zugangsstelle (Supplementary Information Request at the National Level –Büro, das sog. SIRENE-Büro) übermittelten Daten nicht vom SIS II-Beschluss gedeckt. Die Argumentation des BfV, dass die Übermittlungen nach dem SIRENE-Handbuch zulässig seien, konnte mich nicht überzeugen. Denn das SIRENE-Handbuch als Durchführungsrechtsakt kann die Bestimmungen des SIS II-Beschlusses nach der Hierarchie des EU-Sekundärrechts nicht überlagern und den Mitgliedsstaaten weitergehende Befugnisse einräumen.

Zum anderen habe ich den Umfang der aufgrund der Ausschreibung an das BfV übermittelten Daten nach Art. 37 Abs. 1 SIS II-Beschluss kritisiert. Die überwiegend von der Bundespolizei an das BfV übermittelten Daten konnten bei einer Vielzahl der Stichproben keiner Kategorie des abschließenden Katalogs des Art. 37 Abs. 1 SIS II-Beschluss zugeordnet werden. Für die Übermittlung der über diesen Katalog hinausgehenden Daten kann aufgrund des sog. europarechtlichen Anwendungsvorrangs auch nicht auf nationale Rechtsgrundlagen zurückgegriffen werden.

Obwohl damit die Voraussetzungen für eine Beanstandung gemäß § 16 Abs. 2 Satz 1 Bundesdatenschutzgesetz in beiden Fallkonstellationen vorlagen, habe ich auf eine solche verzichtet. Denn die in Rede stehende Datenverarbeitung ist nach der für März 2023 geplanten Inbetriebnahme des neuen, erweiterten Schengener Informationssystems der dritten Generation (SIS III) und der Anwendung der neuen Verordnung (EU) 2018/1862 des europäischen Parlaments und des Rates vom 28. November 2018 (SIS III-VO) nicht mehr als datenschutzwidrig zu bewerten. Durch diese Verordnung können künftig mehr Daten als bisher übermittelt werden; insbesondere hat das BfV künftig die Möglichkeit, im Einzelfall die Übermittlung von Daten zu beantragen, die im Katalog des Art. 37 Abs. 1 SIS III-VO nicht enthalten sind. Diese Befugnis sehe ich datenschutzrechtlich sehr kritisch. Ich habe dem BfV daher bereits angekündigt, dass ich bei künftigen Kontrollen insbesondere das Vorliegen der Ausschreibungsvoraussetzungen sowie die entsprechenden Dokumentationen umfassend prüfen werde.

9.4.10 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst

Im Berichtsjahr habe ich die Anbindung des Bundesamts für den Militärischen Abschirmdienst (BAMAD) an das Nachrichtendienstliche Informationssystem (NADIS) kritisch begleitet sowie die Verarbeitung von Daten zu Reservistinnen und Reservisten überprüft. Ich konnte zwei umfangreiche Kontrollen, die ich bereits im Vorjahr begonnen hatte, mit erfreulichem Ergebnis fortführen.

Anbindung des BAMAD an NADIS

Seit einer Gesetzesänderung des Gesetzes über den Militärischen Abschirmdienst (MAD-Gesetz) und des Bundesverfassungsschutzgesetzes im Juli 2021 sehen diese die Möglichkeit vor, Unterrichtungspflichten zwischen dem BAMAD und den Verfassungsschutzbehörden des Bundes und der Länder durch gemeinsam geführte Dateien zu erfüllen.

Im Verfassungsschutzverbund wird dazu das System NADIS genutzt, an das nun auch das BAMAD angebunden werden soll. Das Bundesamt für Verfassungsschutz

(BfV) und das BAMAD haben mir dafür entsprechende Änderungen ihrer Dateianordnungen zur Anhörung vorgelegt. Im Rahmen der Anhörungsverfahren habe ich die verfassungskonforme Umsetzung einer solchen Verflechtung der Dateiensysteme eingefordert.

Bereits im dazugehörigen Gesetzgebungsverfahren von 2020 hatte ich die Intensivierung des Informationsaustauschs zwischen den Behörden zwar als in der Sache richtig begrüßt, jedoch wiederholt auf die dafür notwendige Schaffung verfassungskonformer Übermittlungsregelungen gedrungen (vgl. 29. TB Nr. 5.5). Durch diesjährige Rechtsprechung des Bundesverfassungsgerichts zu den Gesetzen der Nachrichtendienste sind die zuständigen Ministerien nunmehr gefordert, die entsprechenden Vorschriften zu reformieren (vgl. Nr. 7.8). Zum Zeitpunkt des Redaktionsschlusses dauerte das Anhörungsverfahren noch an.

Überprüfung der Verarbeitung von Daten zu Reservistinnen und Reservisten

Die nachrichtendienstliche Bearbeitung von extremistischen Bestrebungen bei Reservistinnen und Reservisten ist aufgrund der wechselnden Zuständigkeiten zwischen dem BfV und BAMAD mit einer Vielzahl von Datenübermittlungen und -speicherungen verbunden. Für Personen mit Reservistenstatus ist grundsätzlich das BfV zuständig, nur für den Zeitraum des Reservisteneinsatzes wird das BAMAD zuständig.

Im Berichtszeitraum habe ich die hierfür geschaffenen Formen der Zusammenarbeit näher betrachtet und die Festlegung feststehender Vorgaben und Prozesse gefordert. Im Vordergrund steht hierbei für mich, die Wahrung der Betroffenenrechte – insbesondere des Rechts auf Auskunft – sicherzustellen. Meine Prüfung dauert zum Zeitpunkt des Redaktionsschlusses noch an. Selbst wenn zeitnah in der Praxis Verbesserungen erreicht werden sollten, ist aus meiner Sicht eine klarstellende Änderung des MAD-Gesetzes dringend angeraten, um auch für die handelnden verantwortlichen Personen in den Behörden Rechtssicherheit zu schaffen.

Kontrolle verdeckter Ausschreibungen im Schengener Informationssystem der 2. Generation (SIS II) beim BAMAD

Die im dritten Quartal 2021 beim BAMAD durchgeführte Kontrolle verdeckter Ausschreibungen im SIS II (vgl. 30. TB Nr. 8.2.6) konnte ich in diesem Berichtsjahr abschließen. Ich freue mich, dass meine im Kontrollbericht ausgesprochenen Praxisempfehlungen, die insbesondere die Implementierung oder Anpassung von Prozessabläufen sowie die Vorgaben zur Löschung von Ausschreibungen betrafen, vom BAMAD vollumfänglich umgesetzt wurden.

Kontrolle von Datenverarbeitungen im Bereich der Observation

Ende 2021 habe ich eine umfangreiche Kontrolle im Bereich der Observation des BAMAD begonnen (vgl. 30 TB Nr. 8.2.6) und im Berichtsjahr weitergeführt. Aufgrund des besonderen Umfangs des zu überprüfenden Datenbestandes konnte meine Prüfung noch nicht abgeschlossen werden.

Meine getroffenen Feststellungen sowie meine datenschutzrechtliche Bewertung zu den geprüften Observationsvorgängen habe ich nebst ergänzenden Praxishinweisen in meinem Kontrollbericht dem BAMAD mitgeteilt. Von einer Beanstandung konnte ich bisher absehen. Die Stellungnahme des BAMAD zu meinem Kontrollbericht erwarte ich im Jahr 2023.

Für den Fall, dass die von mir im Kontrollbericht festgehaltenen datenschutzrechtlichen Bedenken nicht fristgerecht beseitigt werden, habe ich mir die Möglichkeit der Beanstandung ausdrücklich vorbehalten. Aus Gründen der Geheimhaltung und des Fortdauerns meiner Kontrolle kann ich hier keine weitergehenden Ausführungen machen.

Ich empfehle dem Gesetzgeber, eine gesetzliche Klarstellung hinsichtlich der Zuständigkeit für Reservistinnen und Reservisten zwischen BAMAD und BfV vorzunehmen.

Querverweise:

7.6 Der Verfassungsschutz und das Bundesverfassungsgericht

9.4.11 Datenverarbeitung beim BND

In meinem 23. (Nr. 7.6.1) und 30. (Nr. 6.16) Tätigkeitsbericht habe ich über datenschutzrechtliche Verstöße im Rahmen des Betriebes einer Großdatei beim Bundesnachrichtendienst (BND) berichtet. In diesem Jahr habe ich dazu einen Kontrollbesuch durchgeführt, der zu Beanstandungen geführt hat.

Nach jahrelangen intensiven Beratungen zur datenschutzrechtlichen Problematik dieser Großdatei wurde im Jahr 2011 eine Archivlösung für die Datei etabliert (30. TB Nr. 6.16). In dieses Archiv wurden und werden bis 2025 immer noch die Datensätze verschoben, für die entgegen den gesetzlichen Regelungen keine Löschwiedervorlage implementiert wurde, die länger als 10 Jahre in der Großdatei gespeichert wurden und die keinen aktuellen Bezug mehr zu laufenden Vorgängen haben.

Im Archiv können diese Datensätze nur noch unter besonderen Voraussetzungen für aktuelle Zwecke genutzt werden, die der BND in einem Leitfaden festgeschrieben hat. Mein Besuch Ende August 2022 war auf die Kontrolle der Nutzung dieser Archivdaten ausgerichtet.

Das Archiv umfasste zum Zeitpunkt der Kontrolle einige Millionen Dokumente. Im Rahmen der Kontrolle eingesehene Dokumente mit personenbezogenen Daten reichten bis in die 1960er Jahre zurück.

Die seit 2011 durchgeführten Recherchen im Archiv richteten sich grundsätzlich nach den im Leitfaden festgelegten Bestimmungen. Die sowohl gesetzlich und als auch im Leitfaden vorgesehene Prüfung der Erforderlichkeit einer weiteren Speicherung der im Rahmen einer Archivrecherche eingesehenen personenbezogenen Daten wurde jedoch nicht durchgeführt. Eine nachrichtendienstliche Relevanz der Dokumente konnte während der Kontrolle nicht festgestellt werden.

Die ohne Prüfung auf Auftragsrelevanz erfolgende automatisierte Speicherung der zuvor bereits mehr als 10 Jahre in der Großdatei gespeicherten personenbezogenen Daten in einem Archiv und das Unterlassen der Erforderlichkeitsprüfung nach Zugriff auf personenbezogene Archivdaten habe ich beanstandet. Das Verfahren ist noch nicht abgeschlossen.

9.4.12 Datenschutzkontrollen im Sicherheitsüberprüfungsrecht – von vorbildlich bis mangelhaft

Immer wieder kommt es zu Verstößen und Mängeln bei der Verarbeitung personenbezogener Daten im Zusammenhang mit Sicherheitsüberprüfungen. Einige davon sind weit verbreitet und ziehen sich wie ein roter Faden durch meine Kontrollen. Aber es gibt auch immer wieder neue Problemkonstellationen. Einige kontrollierte Stellen zeigten aber auch: Eine datenschutzkonforme Führung von Sicherheitsakten und Dateien ist möglich.

In diesem Berichtsjahr kontrollierte ich bei insgesamt 16 Stellen, ob diese die datenschutzrechtlichen Bestimmungen des Sicherheitsüberprüfungsgesetzes (SÜG) einhalten. Ausgangspunkt meiner Kontrolltätigkeit ist eine neue Prüfstrategie, die es mir ermöglicht, einen repräsentativen Überblick über alle Stellen zu erhalten, die in den Anwendungsbereich des SÜG fallen. Dabei berücksichtige ich nicht nur große Akteure, sondern insbesondere auch die Stellen, bei denen das Recht auf informationelle Selbstbestimmung der betroffenen Personen erfahrungsgemäß in besonderen Maße herausgefordert wird. Gegenstand meiner Kontrolltätigkeit waren acht Wirtschaftsunternehmen und acht öffentliche Stellen.

Die kontrollierten Wirtschaftsunternehmen gehörten zu folgenden Sparten: Bewachung (1x), Forschung (1x), Telekommunikation (1x), Industrie (2x) und IT bzw. Elektronik (3x).

Bei den kontrollierten Behörden handelt es sich um:

- das Bundesamt für Wirtschaft und Ausfuhrkontrolle
- das Bundesamt für die Sicherheit der nuklearen Entsorgung
- das Bundesamt für Familie und zivilgesellschaftliche Aufgaben (BAFzA)
- die Zentrale Stelle für Informationstechnik im Sicherheitsbereich
- das Bundeskriminalamt
- das Bundesamt für Justiz (BfJ)
- das Bundesamt für Strahlenschutz
- das Bundesministerium für Wirtschaft und Klimaschutz (BMWK).

Das BMWK kontrollierte ich in seiner Funktion als zuständige Stelle für den nicht-öffentlichen Bereich. Das Ministerium ist zuständig für die Geheimschutzbetreuung der Wirtschaftsunternehmen und entscheidet darüber, ob Unternehmen eine überprüfte Person an sicherheitsempfindlicher Stelle einsetzen dürfen oder nicht.

Gegen sechs Behörden und sechs Unternehmen sprach ich eine oder mehrere Beanstandungen aus. Darüber hinaus stellte ich zahlreiche weitere Verstöße oder Mängel fest, bei denen ich jedoch aus Gründen der Verhältnismäßigkeit von einer Beanstandung absah. Im Ergebnis sah ich bei vier Kontrollen vollständig von Beanstandungen ab.

Verschiedene Fehlerquellen

Insgesamt stellte ich bei Wirtschaftsunternehmen im Verhältnis weniger Verstöße fest als bei Behörden. Zum Teil erfolgte die Verarbeitung personenbezogener Daten in der Wirtschaft vorbildlich. Einige meiner Feststellungen ziehen sich allerdings wie ein roter Faden durch die überwiegende Anzahl der Kontrollen (vgl. dazu bereits 28. TB Nr. 6.7.4, 29. TB Nr. 9.5.5, 30. TB Nr. 8.2.8). Insbesondere fand ich häufig personenbezogene Daten unbeteiligter Dritter und Dokumente vor, die nicht verarbeitet werden dürfen.

Die meisten Beanstandungen sprach ich gegenüber dem BfJ und dem BAFzA aus. Beim BAFzA hatte insbesondere das Arbeiten im Homeoffice während der Pandemie zu pragmatischen, jedoch nicht datenschutzkonformen Vorgehensweisen geführt. So beanstandete ich hier

unter anderem die unverschlüsselte E-Mail-Kommunikation mit externen Empfängern über ungesicherte Netze. Die Geheimschutzbeauftragte (GSB) versandte diverse Unterlagen aus der Sicherheitsüberprüfung an ihre private E-Mailadresse, um sie im Homeoffice ausdrucken und bearbeiten zu können. Des Weiteren verstieß das BAFzA gegen das Abschottungsgebot, indem zur Entlastung der GSB Mitarbeitende der personalverantwortlichen Stelle vor Ort die Prüfung der Sicherheitserklärung durchführten.

Beim BfJ beanstandete ich unter anderem fehlende organisatorische Maßnahmen. Die personelle Ausstattung im Bereich Geheimschutz war derart unzureichend, dass eine ordnungsgemäße Sicherstellung der datenschutzrechtlichen Vorgaben nicht gewährleistet war. Zusätzlich war der Informationsfluss gem. § 15a SÜG durch die personalverantwortliche Stelle an den Bereich Geheimschutz unzureichend. Auch dies beanstandete ich beim BfJ.

Häufig beachteten Behörden Lösch- und Vernichtungsfristen nicht und erhielten deshalb eine Beanstandung. Auch die Fortsetzung einer Sicherheitsüberprüfung, obwohl keine sicherheitsempfindliche Tätigkeit mehr aufgenommen werden sollte, beanstandete ich in einem Fall. In einem anderen Fall beanstandete ich die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage. Des Weiteren sprach ich wegen der unzulässigen Übermittlung von Daten aus der Sicherheitsüberprüfung an die personalverantwortliche Stelle eine Beanstandung aus.

Auch bei Wirtschaftsunternehmen stieß ich auf nicht beachtete Lösch- und Vernichtungsfristen und beanstandete dies. Eine weitere Beanstandung ergab sich aufgrund einer unvollständigen Aktenführung. Durch eine vorzeitige Vernichtung der Sicherheitserklärung konnte das Unternehmen die darauf dokumentierte Zustimmung der betroffenen Person zu ihrer Überprüfung und den damit verbundenen Datenverarbeitungen nicht mehr nachweisen. Des Weiteren beanstandete ich die fehlende Einwilligung der betroffenen Person zur Durchführung des sogenannten Besuchskontrollverfahrens, mit dem Unternehmen sicherheitsüberprüftes Personal bei anderen Unternehmen oder Behörden anmelden. Ebenfalls zu beanstanden war ein von der personalverwaltenden Stelle gegenüber dem Sicherheitsbevollmächtigten unzureichender Informationsfluss zu sicherheitsrelevanten Veränderungen, soweit sich diese auch auf den Datenschutz auswirken. Ein solcher liegt beispielsweise dann vor, wenn hierdurch Löschfristen ausgelöst werden.

Pragmatische Beratung

Trotz festgestellter Mängel und Verstöße standen fast alle geprüften Stellen meinen Kontrollen und der damit verbundenen Beratung positiv gegenüber. Zudem stellte ich fest, dass die umfassende Beratung im Vorfeld, insbesondere auch mit Blick auf die Digitalisierung der Sicherheitsüberprüfung, sich positiv in den Kontrollen widerspiegelt (vgl. u. Nr. 13.4).

Aufgrund einiger Unzulänglichkeiten des Gesetzes (vgl. 30. TB Nr. 6.20) sind die verantwortlichen Stellen – bis zur anstehenden Überarbeitung des SÜG durch den Gesetzgeber – gezwungen, pragmatische Lösungen zu finden und zugleich datenschutzrechtliche Vorgaben zu erfüllen. Das gilt gleichermaßen auch für meine Beratung.

Manchmal geht es hier um vermeintlich banale Fragen wie den „Doktortitel“ im Besuchskontrollverfahren. Die verwendeten Einwilligungsformulare sehen vor, dass Wirtschaftsunternehmen den Namen und andere personenbezogene Daten der eigenen Mitarbeiter an andere Unternehmen übermitteln dürfen, umfassen jedoch standardmäßig nicht den akademischen Titel. Für die Außendarstellung eines Unternehmens mag dies jedoch von erheblicher Bedeutung sein.

Eine kleine Ergänzung auf dem Standardformular kann hier helfen. Dennoch ist die bisherige gesetzliche Regelung bzw. fehlende Regelung des Besuchskontrollverfahren für alle Seiten aufwändig und insoweit unbefriedigend. Auch wenn ich mit meinem Lösungsvorschlag ein mehr an Datenverarbeitung ermögliche, dient dies im Ergebnis dem Datenschutz, denn es zeigt sich, dass Sicherheit und Wirtschaftsinteressen auch mit Datenschutz funktionieren.

Querverweise:

12.4 Beratung und fachlicher Austausch zum SÜG – Eine fruchtbare Ergänzung

10 BfDI Intern

10.1 Neue Strategie für den BfDI

Im Berichtszeitraum habe ich damit begonnen, die Strategie für mein Haus zu erweitern und die Umsetzung zu konkretisieren. In einem ersten Schritt wurden dabei eine Vision, Mission und die Handlungsfelder nebst strategischen Leitsätzen festgelegt.

Eine Hausstrategie spiegelt zum einen die grundlegenden Ziele und Werte der Behörde und ihrer Mitarbeitenden wider. Darüber hinaus stellt sie aber auch die Ausgangsbasis für die Entwicklung und Umsetzung der konkreten Organisations- und Arbeitssteuerung dar. Damit dient sie nicht einem reinen Selbstzweck, sondern schafft eine Struktur für die tägliche Arbeit und bietet damit neben einer besseren Transparenz auch dadurch einen echten Mehrwert für alle Mitarbeitenden, indem sie dabei unterstützt, die Arbeit und Aufgaben in Zukunft besser planen und aufeinander abstimmen zu können.

Daher war es mir wichtig, den Prozess der Strategieweiterentwicklung auch so zu gestalten, dass allen Kolleginnen und Kollegen mit Interesse die Möglichkeit gegeben wurde, sich aktiv daran zu beteiligen. Nachdem die Hausleitung sich auf eine aktualisierte Vision geeinigt hatte, wurden in insgesamt sieben ganztägigen Workshops mit Mitarbeitenden die daraus folgende Mission und die Handlungsfelder mit zugehörigen strategischen Leitsätzen entwickelt. Ich habe mich sehr darüber gefreut, dass das Mitwirkungsangebot von meinen Kolleginnen und Kollegen auf breiter Basis angenommen wurde und so Ideen und Input aus allen Bereichen des Hauses und Vertretern aller Laufbahngruppen in das Projekt einfließen konnte.

Vision

Wir sind gefragter Ansprechpartner zu Digitalisierung, bei Gesetzgebung und staatlichem Handeln.

Mission

Datenschutz schützt Menschen und nicht Daten. Deshalb steht bei all unserem Handeln – nach außen und innen – der Mensch im Mittelpunkt. Datenschutz ist ein Grundrecht. Um dieses zu wahren, informieren, sensibilisieren und beraten wir umfassend Bürgerinnen und Bürger, Politik, Verwaltungen, Unternehmen und alle anderen Interessengruppen in adressatengerechter Form und auf Augenhöhe. Wenn erforderlich, nutzen wir unsere aufsichtsrechtlichen Möglichkeiten, um den Datenschutz durchzusetzen.

Dies ist eine Aufgabe, die nur gemeinsam bewältigt werden kann. Darum arbeiten wir eng mit nationalen und internationalen Partnerbehörden und Interessengruppen zusammen, auch weil Datenflüsse nicht an Grenzen enden.

Die Digitalisierung bestimmt weitgehend unsere Lebens- und Arbeitswelt, so dass immer mehr personenbezogene Daten anfallen. Um den hiermit verbundenen neuen Herausforderungen gerecht werden zu können, begleiten wir digitale Entwicklungen aktiv und kompetent. Dafür halten wir uns auch technologisch auf dem aktuellen Stand.

Neben dem Datenschutz ist auch die Informationsfreiheit eine wichtige Voraussetzung für unser demokratisches Zusammenleben. Deshalb setzen wir uns für Transparenz ein und leben diese auch selbst vor.

Unsere Beschäftigten bilden das Fundament unserer erfolgreichen Arbeit. Um deren Zufriedenheit und Motivation zu sichern, unterstützen wir bei der Vereinbarkeit von Beruf und Familie und setzen auf eine Kultur der Transparenz und der offenen Kommunikation auf allen Ebenen, die Veränderungen und Kritik zulässt und fördert. Die Inklusion von Menschen mit Behinderungen sowie Wertschätzung und Respekt gegenüber allen Beschäftigten – unabhängig von Geschlecht, sexueller Orientierung, Herkunft, religiösen oder politischen Anschauungen – sind Leitlinien unseres Umgangs miteinander. Außerdem sehen wir nachhaltiges Handeln in ökologischer, sozialer und ökonomischer Hinsicht als wichtigen Teil unserer Verantwortung. Hierdurch schaffen wir eine Atmosphäre, in der wir gerne und gut arbeiten.

Am Ende des ersten Teils dieses Strategieprojekts stehen somit vor allem die aktuelle Vision und Mission meiner Behörde. Hinter der zwangsläufig abstrakt gehaltenen Vision steht der Gedanke, dass sich mein Haus in erster Linie als kompetenter Berater versteht, der aufgrund der großen Expertise in seinen Betätigungsfeldern für jedermann, von Bürgerinnen und Bürgern über Behörden und Unternehmen bis hin zu Presse, NGOs und der Politik Ansprechpartner sein will; egal ob national, europäisch und international. Die Mission beschreibt etwas konkreter, wie wir unserer Aufgaben angehen, um unser in der Vision dargelegtes Ziel konsequent und dauerhaft zu erreichen.

Im Jahr 2023 werden im zweiten Projektteil die einzelnen Arbeitseinheiten individuelle strategische Ziele und Maßnahmen zu deren messbaren Umsetzung festlegen, um damit die Gesamtstrategie zu finalisieren.

10.2 Aufbau Labor

Im Berichtsjahr wurde begonnen, eine erweiterte Labor-Umgebung zur technischen Untersuchung von IT-Anwendungen, -Diensten und Apps für meine Behörde zu schaffen, Erste Erfahrungen mit eigenen Laboruntersuchungen im Bereich der Telemedien waren bereits vorhanden. Der jetzt erfolgende Aufbau soll auch größere Untersuchungen in allen Bereichen meiner Zuständigkeit ermöglichen.

Durch das Fortschreiten der Digitalisierung in alltäglichen Lebenssituationen wie auch bei der Arbeit der Bundesbehörden spielen technische Aspekte des Datenschutzes eine immer stärkere Rolle. Ob digitale Gesundheitsanwendungen oder Nutzung digitaler Identitätsdokumente, ob Einsatz von smarten Stromzählern oder Web-Portalen zu Fachanwendungen in Bundesbehörden – es kommen zunehmend browsergestützte Verfahren, Smartphone-Apps und smarte Geräte zum Einsatz.

Um prüfen zu können, ob entsprechende Dienste, Anwendungen, Apps und Geräte die gesetzlichen Anforderungen des Datenschutzes berücksichtigen, sollten deren technischen Eigenschaften noch genauer und vor allem „unabhängig“ durch meine Behörde untersucht werden können. Erste Erfahrungen konnten mit einzelnen Untersuchungen von Webseiten und Apps im Bereich Telemedien gesammelt werden. Jetzt habe ich ein eigenständiges Referat eingerichtet, das für den Betrieb einer solchen Untersuchungsumgebung zuständig ist. Es wird eine virtualisierte Untersuchungsumgebung aufgebaut, in der zu unterschiedlichen Fragestellungen gleichzeitig Produkte untersucht werden können und deren Verhalten, etwa das Senden von Daten zum Hersteller, geprüft werden kann.

Funktionsweise

Mit Hilfe des aufgebauten Untersuchungssystems und geeigneter Software können die Datenflüsse von Produkten – wie Apps oder Web-Applikationen – untersucht werden. Zur Untersuchung werden virtuelle Maschinen genutzt, die jeweils einen Computer emulieren. Auf diesen virtuellen Computern können unterschiedliche Betriebssysteme zum Einsatz kommen, um dort lauffähige Produkte untersuchen zu können. Durch die Nutzung virtueller Maschinen können einfach und schnell verschiedene Szenarien gleichzeitig durchgespielt werden und auch Abhängigkeiten und Zusammenarbeit mehrerer Produktbestandteile auf verschiedenen Systemen nachgestellt und untersucht werden.

Auch ist vorgesehen, Möglichkeiten für die Durchführung größerer Untersuchungen von Anwendungen und Geräten – etwa Sensoren und Aktoren des IoT (Internet of Things) – gemeinsame mit externen Auftragnehmern unter Federführung meiner Behörde zu schaffen. Dabei können Dritte – wie z. B. das BSI – grundsätzlich um jede Form von Untersuchungen gebeten und zu deren Durchführung beauftragt werden. Um jedoch unabhängige Kontrollen durchführen zu können, muss ich auf eigene Laborkapazitäten zurückgreifen können.

Das Referat soll damit zukünftig technische Prüfungen bei meiner Kontrolltätigkeit ermöglichen, aber auch technische Fragestellungen aus der Zusammenarbeit mit der Zivilgesellschaft bearbeiten können oder bei der verständlichen Darstellung komplexer technischer Zusammenhänge in meinen Informationsmaterialien für die Öffentlichkeit mitwirken. Weiter soll die Zusammenarbeit mit Wissenschaft und Forschung im Bereich der technischen Entwicklung der elektronischen Datenverarbeitung befördert werden. Damit will ich auch die Attraktivität meiner Behörde für neue Mitarbeitende erhöhen und meinen Mitarbeitenden die Möglichkeit bieten, ihre Kompetenzen in diesen Themenfeldern zu erweitern.

Um bereits in der Datenschutz-Community vorhandenes Wissen zu Untersuchungswerkzeugen und –methoden zu nutzen und eigene Ergebnisse und Erkenntnisse zu streuen, stehe ich im aktiven Austausch mit anderen Behörden; der Austausch mit Nicht-Regierungsorganisationen ist ebenfalls geplant.

10.3 Nach der Organisationsuntersuchung – Anschlussprojekte

Die Ergebnisse der Organisationsuntersuchung werden stetig weiter umgesetzt. Nach der Organisationsuntersuchung führe ich derzeit diverse Anschlussprojekte durch, um mein Haus weiter zu optimieren. Es handelt sich um die Einführung eines zentralen Wissensmanagements, den Auf- und Ausbau eines zentralen Krisenmanagements, die Einführung eines zentralen Controllings inklusive der Erhebung von erforderlichen Kennzahlen. Darüber hinaus möchte ich das Berichtswesen weiter vereinheitlichen und die erlassenen Hausanordnungen optimieren.

Weiterer Aufbau zentrales Wissensmanagement

Im Rahmen der Organisationsuntersuchung wurden Optimierungspotentiale ermittelt, die unter anderem den Umgang mit Wissen beinhalten, so dass das Thema Wissensmanagement im Berichtsjahr aufgegriffen wurde und im Jahr 2023 im Rahmen eines Projekts fortgeführt wird.

Als eine Erkenntnis aus der in meiner Behörde durchgeführten Organisationsuntersuchung möchte ich den Umgang mit der Ressource Wissen verbessern. Auch wenn der Altersdurchschnitt in meiner Behörde ungewohnt niedrig ist, so bemerke aber auch ich den demographischen Wandel in der Belegschaft. Erfahrene Wissensträger gehen in Ruhestand und das eine Behörde tragende Erfahrungswissen könnte verloren gehen. Dem will ich genauso vorbeugen wie der mehrfachen Erarbeitung bestimmter Erkenntnisse und der Uneinheitlichkeit beim Vorgehen. Um weiterhin effizient arbeiten zu können, möchte ich das neue Personal am vorhandenen Erfahrungswissen meiner erfahrenen Mitarbeitenden teilhaben lassen. Im Berichtsjahr wurde deshalb in einem ersten Schritt bereits ein neues, optimiertes Intranet zur internen Information umgesetzt. Ziel ist es, im Rahmen eines Projekts ein ganzheitliches, strukturiertes Wissensmanagement in meiner Behörde zu etablieren, um zu einem umfassenden Wissenstransfer und -erhalt beizutragen. Hiermit wurde ebenfalls im Jahr 2022 begonnen, so dass im Laufe von 2023 dieses Ziel erreicht werden kann.

Aufbau zentrales Krisenmanagement

Spätestens der Umgang mit den Folgen der Covid-19 Pandemie hat gezeigt, wie wichtig in einer Behörde strukturierte Prozessabläufe in einer Krisensituation sind. Diese Prozessabläufe baut meine Behörde weiter aus.

Um die Resilienz gegen aufkommende Krisen, wie etwa die weitere Entwicklung der pandemischen Lage, sicherheitspolitische Veränderungen oder der Schutz der IT-Infrastruktur etc. zu stärken, werde ich den systematischen Aufbau eines übergreifenden behördlichen Krisenmanagements vorantreiben. Mit zusätzlicher externer fachlicher Unterstützung werden die strategischen und operativen Elemente des Krisenmanagements untersucht, ggf. geschärft und zu einheitlichen Soll-Prozessen ausgebaut. Die Definition einer Krise, die Beschreibung von Meldewegen, die Einrichtung einer institutionell besonderen Aufbauorganisation im Krisenfall (Krisenstab) und das Zusammenspiel zu bereits bestehenden Notfallregelungen werden dabei den Hauptbestandteil der Untersuchung bilden. Die Untersuchung zum Aufbau eines Krisenmanagements erfolgt in einer Projektstruktur. Der vorläufige Projektplan sieht erste Ergebnisse für das erste Halbjahr 2023 vor.

Weiterentwicklung Organisationsstruktur

Unter Berücksichtigung der Ergebnisse der im Jahr 2021 abgeschlossenen Organisationsuntersuchung und des Zulaufs an weiteren Aufgaben hat mein Haus seine Organisationsstruktur fortentwickelt.

Das Thema Informationsfreiheit ist namensgebender Bestandteil unserer Behörde und nunmehr auch in einem eigenständigen und erweiterten Referat außerhalb der Abteilungsorganisation unmittelbar bei der Hausleitung eingerichtet.

Die weiteren Veränderungen der Aufbauorganisation betreffen die Abteilungen 1 und 2. Das neu eingerichtete Referat 16 bündelt die Zuständigkeiten für die innere Verwaltung und den auswärtigen Dienst. Die Themen Telemedien und Telekommunikation sind in der Abteilung 2 nun in zwei eigenständigen Referaten verortet. Des Weiteren wird der technische Ausbau meiner Aufsichtsfunktion des BfDI durch die Einrichtung der Referate Technikentwicklung/Labor und Zusammenarbeit/Aufsicht über das Bundesamt für Sicherheit in der Informationstechnik weiter gestärkt.[71]

10.4 Personalentwicklung und Haushaltslage im Jahr 2022

Der Haushaltsgesetzgeber hat mir für meine Arbeit im Datenschutz und für die Informationsfreiheit im Haushaltsjahr 2022 Gesamtausgaben von 43.243.000 € bewilligt. Den weit überwiegenden Teil dieser Ausgaben binden die Personalausgaben. Ich danke dem Haushaltsgesetzgeber für die Bereitstellung der finanziellen

71 Siehe Organigramm in der Anlage

Mittel, um damit meine unabhängige Datenschutzaufsicht wahrnehmen zu können.

Meiner Behörde wurden im Jahr 2022 50 zusätzliche Stellen bewilligt, die sich aufgrund der in 2021 durchgeführten Organisationsuntersuchung als Mehrbedarf ergeben haben. Damit ist mein Personalhaushalt auf insgesamt 396,4 Stellen angestiegen, wovon 375,9 Planstellen für Beamtinnen und Beamten sowie 20,5 Stellen für Tarifbeschäftigte vorgesehen sind. Nach wie vor befinde ich mich auf einem guten Weg, um die mir zur Verfügung gestellten Stellen sukzessive zu besetzen. Im vergangenen Jahr konnte ich trotz anhaltender Corona-Pandemie und damit einhergehenden Kontaktbeschränkungen fast 80 % meiner Stellen besetzen.

Zum 31. Dezember 2022 beträgt die Personalstärke meines Hauses 301 Personen. Im Berichtsjahr 2022 hatte ich insgesamt nur sieben Personalabgänge zu verzeichnen. Gleichzeitig konnte ich mich über 33 Zugänge freuen, die nun als Nachwuchskräfte oder erfahrene Beschäftigte mein Haus verstärken. Darüber hinaus rechne ich noch mit weiteren 18 Personalzugängen aus im Jahr 2022 bereits abgeschlossenen Bewerbungsverfahren.

In meinem Hause biete ich interessante Karriereperspektiven und abwechslungsreiche Tätigkeitsfelder. Die Aufgaben sind komplex und haben häufig einen internationalen Bezug. Als Personalentwicklungsmaßnahme habe ich erstmalig ein Aufstiegsverfahren vom gehobenen in den höheren nichttechnischen Verwaltungsdienst angeboten. Hierdurch wird – nach erfolgreichem Auswahlverfahren – ab dem 1. Mai 2023 ein Studium an der Hochschule des Bundes (HS Bund) ermöglicht.

Ich habe 2022 wieder sieben Studierenden, elf Referendarinnen und Referendaren sowie sieben Anwärterinnen und Anwärtern die Gelegenheit gegeben, ihre Ausbildungsstage in meinem Haus zu absolvieren. Somit konnte ich auch während der Corona-Pandemie viele Nachwuchskräfte bei ihrem Einstieg in das Berufsleben unterstützen.

Meine Behörde legt besonderen Wert darauf, das Wissen und die Fähigkeiten ihrer Beschäftigten auszubauen und auf dem neuesten Stand zu halten: Dazu biete ich meinen Mitarbeiterinnen und Mitarbeitern ein umfangreiches Fortbildungsangebot, um sowohl deren Fachexpertise als auch Soft Skills zu stärken. Mit Entspannung der Corona-Situation konnten die Veranstaltungen wieder verstärkt in Präsenz oder außer Haus durchgeführt werden. Gleichzeitig wurden weiterhin viele Webinare angeboten.

Wichtig ist mir zudem, die Vereinbarkeit von Beruf und Familie zu fördern. Mein Haus bietet unter anderem sehr flexible Arbeitszeiten und umfangreiche Möglichkeiten zum mobilen Arbeiten.

Die Gewinnung neuer Mitarbeiterinnen und Mitarbeiter ist eine meiner Prioritäten. Den deutschlandweiten Fachkräftemangel und die große Konkurrenz um gute Bewerberinnen und Bewerber nehme ich stark wahr, insbesondere im technischen Bereich. Umso mehr hat es mich gefreut, dass die Teilnahme an Karrieremessen wieder möglich war. So konnte ich im August 2022 am Fachbereichstag der HS Bund, im Oktober und November 2022 an Karrieremessen in Bonn und Aachen mein Haus präsentieren und bekannt machen.

Im Berichtsjahr 2022 habe ich 42 Stellenbesetzungsverfahren (sowohl Einzel- als auch Sammelbesetzungsverfahren) durchgeführt. Insgesamt habe ich 326 Bewerbungen erhalten. Von diesen wurden 240 Bewerberinnen und Bewerber zu Vorstellungsgesprächen eingeladen, die sowohl mithilfe moderner hausinterner Videokonferenztechnik als auch in Präsenz durchgeführt worden sind. 45 Personen konnte ich eine Einstellungszusage geben.

10.5 Im Wachstum – das Verbindungsbüro des BfDI in Berlin

Größe und Konzept des aktuellen Verbindungsbüros des BfDI in Berlin spiegeln noch den Bedarf des Jahres 2008. Wie schon der Bonner Sitz meiner Behörde infolge zusätzlicher Aufgaben und Personals gewachsen ist, wird sich nun auch meine Hauptstadtrepräsentanz weiterentwickeln müssen. Mit der Anmietung einer neuen, größeren und vielseitiger nutzbaren Liegenschaft, die voraussichtlich im vierten Quartal 2023 bezugsfähig ist, wurde hierfür die Grundlage gelegt.

Bonn ist historisch und seit 2018 auch gesetzlicher Sitz des BfDI. Ohne eine örtliche Repräsentanz in der Bundeshauptstadt geht es aber nicht. Deshalb bestand schon vor meiner Amtszeit angesichts der räumlichen Distanz ein Berliner Verbindungsbüro, um meine Behörde bei ihren parlamentarischen und ressortbezogenen Beratungsaufgaben am Sitz von Bundestag, Bundesrat und Bundesregierung Vor-Ort zu unterstützen. Neben dem allgemeinen Berliner Politik- und Regierungsbetrieb erfordert auch die Teilhabe am sonstigen politischen, wirtschaftlichen, wissenschaftlichen und gesellschaftlichen Diskurs rund um den Datenschutz und die Informationsfreiheit eine adäquate örtliche Vertretung. Das derzeitige Berliner Verbindungsbüro ist baulich und konzeptionell bisher nicht mit dem Stammhaus und seinen Aufgaben und Organisationseinheiten mitgewachsen. Für eine sachgerechte Vertretung aller meiner Organisationsein-

heiten sind die bisher in der Friedrichstraße angemieteten Räumlichkeiten längst zu klein. Nach einer Bedarfsplanung durch das Bundesfinanzministerium, einer gemeinsamen Markterkundung mit der Bundesanstalt für Immobilienaufgaben und der Klärung der Konditionen von Umbau und Anmietung, freue ich mich nun auf einen Umzug in eine neue Liegenschaft am Spittelmarkt voraussichtlich im vierten Quartal 2023.

Das neue Berliner Verbindungsbüro bietet langfristig ausreichend Platz, damit jedes meiner Referate durch eine Mitarbeiterin oder einen Mitarbeiter in Berlin vertreten sein kann. Mangels Raumkapazitäten waren bisher nur einzelne Referate in Berlin vertreten. Zudem verfügt Berlin künftig über moderne variable Besprechungs- und Konferenzräume nutzbar auch für kleinere Veranstaltungen, ausgerüstet mit zeitgemäßer Präsentations-, Ton- und Videotechnik.

10.6 Bericht zu Presse- und Öffentlichkeitsarbeit

Bei der Pressearbeit meiner Behörde lag der Fokus im Berichtsjahr insbesondere auf Einzelthemen aus den Bereichen Gesundheit und Soziale Medien. Damit verbunden ist sicher auch der Erfolg unserer Mastodon-Instanz im Fediverse. Die von mir angebotenen Publikationen werden weiterhin stark nachgefragt. Deshalb gab es bei den Pixi-Büchern für Kinder bereits in diesem Jahr nicht nur eine zweite Auflage der ersten Reihe, sondern auch einen neuen Teil der Serie. Außerdem können interessierte Bürgerinnen und Bürger immer öfter an hybriden Veranstaltungen meiner Behörde teilnehmen.

Pressearbeit

Im Frühjahr 2022 gab es viele öffentliche Diskussionen zur möglichen Einführung eines Impfregisters. Dementsprechend erreichten meine Pressestelle im Berichtszeitraum hierzu viele Anfragen. Ich betonte immer wieder, dass ein Impfregister grundsätzlich datenschutzrechtlich vorstellbar wäre, wenn die entsprechenden gesetzlichen Voraussetzungen geschaffen würden. Dazu hätte vor allen Dingen die Definition eines Zwecks für die Schaffung des Registers gehört. Zu einer Umsetzung der Pläne kam es bisher nicht. Ein weiteres Projekt aus dem Bereich Gesundheit führte ebenfalls zu vielen Anfragen: Das E-Rezept. Hier war es insbesondere die Fachpresse, die nach Informationen fragte, wie die einzelnen Verbringungswege und das E-Rezept insgesamt datenschutzrechtlich zu bewerten seien.

Der zweite Bereich mit hohem Medieninteresse stand im Zusammenhang mit der Nutzung von sozialen Medien. So habe ich im Berichtszeitraum ein Anhörungsverfahren in Sachen Facebook Fanpages gegen das Bundespresseamt angestoßen, das zu vielen Presseanfragen führte.

Mit der Übernahme des Kurznachrichtendienstes Twitter durch Elon Musk im Oktober 2022 und den hiermit verbundenen Veränderungen nahm auch das Medieninteresse an alternativen Plattformen aus dem Fediverse zu. Gerade der Server meiner Behörde mit einer Instanz des dezentralen Kurznachrichtendienstes Mastodon (https://social.bund.de) und die darauf vertretenen Accounts erlebten im Oktober und November 2022 einen hohen Zulauf, sowohl von „Followern“ als auch von Behörden des Bundes und bundesnaher Institutionen, die dort selbst mit einem Account aktiv wurden. Meine Pressestelle erhielt sehr viele Anfragen, die sich insgesamt mit dem Komplex beschäftigten.

Ich habe im Berichtszeitraum – neben Kurzmeldungen und Veröffentlichungen – 13 Pressemitteilungen herausgegeben und war einmal zu Gast in der Bundespressekonferenz. Als Vorsitzender der Konferenz der unabhängigen Datenschutzaufsichtbehörden des Bundes und der Länder (DSK) habe ich außerdem acht Pressemitteilungen im Namen der DSK herausgegeben. Ich habe sechs Gastbeiträge bzw. Aufsätze für verschiedene Medien verfasst. Meine Pressestelle hat 413 Anfragen per Mail und 406 telefonische Anfragen beantwortet.

Social Media

Im April 2021 habe ich begonnen, selbst eine Instanz des dezentralen Kurznachrichtendienstes Mastodon zu betreiben. Was ursprünglich als Beweis für die Möglichkeit einer datenschutzfreundlichen Umsetzung sozialer Medien gedacht war, wuchs von einem Nischenangebot immer mehr zu einer ernsthaften Alternative heran.

Dem Account meiner Behörde (https://social.bund.de/@bfdi) folgen mittlerweile (Stand: 31. Dezember 2022) mehr als 40.000 interessierte Bürgerinnen und Bürger. Außerdem sind auf unserem Server Accounts von mehr als 40 anderen Behörden und Institutionen zu finden, darunter zahlreiche Bundesministerien.

Zum Mastodon-Account des BfDI geht’s hier:

(QR-Code scannen oder klicken)

Meine Mitarbeiterinnen und Mitarbeiter, die sich auch um den Mastodon-Account kümmern, versuchen immer ansprechbar zu sein und so viele Fragen wie möglich auf diesem Weg unkompliziert zu beantworten. Auch ich persönlich bringe mich mit Beiträgen immer wieder in die Diskussion ein, denn ich sehe im direkten Austausch

mit Bürgerinnen und Bürgern zu den von mir behandelten Themen einen großen Mehrwert. Diese Arbeit möchte ich zukünftig weiter ausbauen.

Darüber hinaus würde ich es begrüßen, wenn die Bundesregierung eigene Kapazitäten im Bereich der datenschutzfreundlichen sozialen Medien aufbaut und diese auch finanziell fördert. Das ITZBund sah sich bislang trotz meiner Bitte, die Bundesinstanz zentral zu hosten, nicht in der Lage, diese eigentlich in seinen Zuständigkeitsbereich fallende Aufgabe auszufüllen. Weil ich es allerdings für wichtig halte, dass gerade die obersten Bundesbehörden mit einem guten Beispiel vorangehen und rechtskonforme soziale Medien nutzen sollten, werde ich auch weiterhin versuchen, mein Angebot mit den mir zur Verfügung stehenden begrenzten Mitteln anzubieten, was angesichts von Moderationsaufgaben und der technischen Absicherung eines Kommunikationskanals für eine Vielzahl von Behörden eine große Herausforderung ist.

Neuerungen Internetseite

Eine zentrale Neuerung meiner Webseite betrifft die Zugänglichkeit für Menschen mit Beeinträchtigungen. So stehen nunmehr insgesamt drei Videos in Gebärdensprache und drei Artikel in leichter Sprache zur Verfügung. In diesen werden meine Aufgaben sowie die Funktionsweise der Webseite erklärt.

Im Berichtjahr habe ich außerdem begonnen, meine Flyer neu zu gestalten. Alle neu aufgelegten, gedruckten Flyer erhalten ein digitales, erweitertes Gegenstück auf meinem Internetauftritt. Zu diesem gelangen die Leserinnen und Leser durch einen QR-Code. Auf der Webseite finden alle Interessierten dann weiterführende Informationen, insbesondere auch Links zu verwandten Artikeln. Die gedruckte Version hingegen kann besser als früher die Bürgerinnen und Bürger über die grundlegenden Punkte informieren und diesen einen Überblick geben. Diese Verzahnung des Analogen mit dem Digitalen wird für alle zukünftigen Flyer angestrebt.

Informationsmaterial

Durch diese digitale Verknüpfung meines Webangebots mit und als Ergänzung zu Print-Medien, ist es mir möglich, die ständige Aktualität unserer Informationen noch besser zu gewährleisten. Interessierte Leserinnen und Leser können sich eigenständig, die für sie relevanten Themen anzeigen lassen und bekommen gleichzeitig Hinweise zu weiterführenden Themen angeboten.

Hinsichtlich der Zielgruppe lag bei der Weiterentwicklung meines Informationsangebots das Hauptaugenmerk in 2022 ganz klar bei Kindergartenkindern, Schülerinnen und Schülern der Grundschule sowie der Einstiegsklassen weiterführender Schulen. Nach wie vor ist eine frühzeitige Beratung und Sensibilisierung begleitend zur Digitalisierung wichtiger Bestandteil meiner Arbeit. Die anhaltend hohe Nachfrage und sehr positive Resonanz zu unseren ersten beiden Pixi-Büchern zeigt, dass das Thema Datenschutz bei Kinder, Jugendlichen, Eltern und Lehrkräften angekommen ist. Um allen Interessierten die Inhalte beider Bücher jederzeit zugänglich zu machen, habe ich die Bücher auch in Videos umsetzen lassen. Ungeachtet dessen war die Nachfrage nach Printexemplaren so hoch, dass ich bereits ein halbes Jahr nach Veröffentlichung eine 2. Auflage nachdrucken lassen musste.

Um den Kindern und Erwachsenen auch meine zweite große Aufgabe, die Informationsfreiheit, näher zu erklären, habe ich eine zweite Reihe der „Daten-Füchse“ mit dem Carlsen Verlag entworfen. Für Schülerinnen und Schüler gibt es seit Dezember 2022 das Pixi Wissen „Was ist Informationsfreiheit?“. Für Kita-Kinder erschien gleichzeitig das Pixi Buch „Aber warum?!“ zum Thema Transparenz.

Wie bereits in 2021 blinkte der Bestell-Button bei uns permanent. Mehr als 27.000 Bestellungen gingen allein in den beiden ersten Wochen ein. Auch diese beiden Bücher werden wieder in Videos umgesetzt, um die Informationen unabhängig von der Verfügbarkeit der Printexemplare unbegrenzt anzubieten zu können.

Anlässlich des Weltkindertages am 20. September 2022 habe ich einen Flyer für Eltern veröffentlicht. Hierin wird zu zwölf Fragen Stellung bezogen und Empfehlungen für Eltern zum Umgang mit Smartphones, Social Media, Games und mehr ausgesprochen. Um den Flyer einer breiten Zielgruppe zu eröffnen, biete ich diesen in Deutsch und in englischer Sprache an. Dieser Flyer ist eng verknüpft mit weiterführenden Informationen in unserem digitalen Angebot.

Veranstaltungen

Im Berichtszeitraum konnten wieder vermehrt Veranstaltungen durchgeführt werden, teilweise noch unter strikten Hygieneauflagen. Deshalb wurden alle Veranstaltungen, die meine Behörde selbst organisiert hat, in hybrider Form angeboten. Ich werde auch zukünftig versuchen, wo immer möglich einen Live-Stream und den späteren Abruf einer Aufzeichnung der Veranstaltung für interessierte Bürgerinnen und Bürger anzubieten.

Die „Bonner Tagen der Demokratie“ fanden im Mai statt. Zu der Frage: „Was Bürger*innen wissen dürfen“ organisierte ich für die Auftaktveranstaltung eine Diskussionsrunde zum Thema Transparenz und freien Zugang zu Informationen.

Im September durfte ich als Gastgeber im offiziellen G7-Rahmen meine Kolleginnen und Kollegen der Datenschutzaufsicht der übrigen G7-Staaten zur Data Protection Roundtable 2022 in Bonn begrüße.

Ebenfalls im September habe ich erstmals an der Veranstaltung zum Weltkindertag in Köln teilgenommen. Das feuchte Wetter hat die Kinder und Eltern nicht abgehalten, unseren Stand zu besuchen und an unserem Quiz teilzunehmen. Ich war sehr froh über die große Begeisterung der Kleinen sowie das Interesse der Erwachsenen. Auch in Zukunft will ich an solchen Veranstaltungen teilnehmen.

Im Oktober habe ich ein politisches Forum mit dem Titel „Mein Auto! Meine Daten?“ durchgeführt, das auf positive Resonanz stieß und den Auftakt zu einer Reihe von gleichgelagerten Veranstaltungen im politischen Berlin markieren soll.

Im November habe ich ein ganztägiges Symposium mit dem Titel „Forschung mit Gesundheitsdaten – Herausforderungen im Zeichen der Datenschutz-Grundverordnung“ veranstaltet. Das Format richtete sich vorrangig an ein Fachpublikum und wurde ebenfalls sehr gut angenommen. Auch hier plane ich eine Fortführung der Reihe im nächsten Jahr.

Ein Hauptfokus beim diesjährigen Veranstaltungsmanagement lag aber sicherlich auf den insgesamt zehn – teilweise mehrtägigen – Veranstaltungen der Datenschutzkonferenz (DSK), die ich als diesjähriger Vorsitz organisiert habe. Neben den geschlossenen Veranstaltungsteilen habe ich zudem zu je einer öffentlichen Veranstaltung am Vorabend der 103. und der 104. DSK in Bonn eingeladen. Ich bin überzeugt, dass diese Formate nicht nur ein guter Einstieg in unsere Arbeit sind, sondern auch wichtige Anregungen und Impulse für die zukünftigen Beratungen setzen.

Es ist mein erklärtes Ziel, dass meine Behörde weiterhin über solche und ähnliche Veranstaltungen für alle Interessierten nahbar bleibt und so der Kontakt zu Bürgerinnen und Bürgern gehalten wird.

Besuchergruppen

Auch dieser Berichtszeitraum war noch stark von den Beschränkungen der Corona-Pandemie geprägt. Das offizielle Besuchergruppenprogramm des Bundespresseamts war bis zum Mai 2022 ausgesetzt. Trotzdem konnte ich fünf Besuchergruppen mit bis zu 50 Teilnehmerinnen und Teilnehmern in der Bonner Liegenschaft sowie eine im Berliner Verbindungsbüro empfangen und betreuen.

Datenschutzgarten

Nach dem Umzug meiner Behörde in die Liegenschaft an der Graurheindorfer Straße in Bonn wurden die Grünflächen durch eine Gartenbaufirma insektenfreundlich umgestaltet. Insbesondere Bienen sollen in der etwa 800 m² großen Anlage nun über einen langen Zeitraum im Jahr Nahrung finden. Gleichzeitig wurde ein Informa-

Datenschutz-Garten an der Bonner Dienstelle des BfDI

tionspfad mit Details zu den Themen Datenschutz und Informationsfreiheit angelegt. Insgesamt sechs Informationstafeln sind im Datenschutzgarten verteilt. Der Garten mit seinen Sitzgelegenheiten steht der Öffentlichkeit zur Verfügung. Die Informationen zum Datenschutzpfad können auch online abgerufen werden.

Querverweise:

3.4 G7 Roundtable, 4.1.1 Symposium Forschung mit Gesundheitsdaten, 4.3.1 Verfahren Facebook Fanpages, 8.1 Aktuelles aus der Telematikinfrastruktur und von ihren Anwendungen, 8.10 Digitale Datenräume und Mobilitätsdaten im Verkehrssektor, 10.7 Gut vernetzt: Das Hauptstadtteam des BfDI

10.7 Gut vernetzt: Das Hauptstadtteam des BfDI

In meinem letzten Tätigkeitsbericht hatte ich vom Aufbau meines Hauptstadtteams berichtet (vgl. 30. TB Nr. 9.4). Mittlerweile hat es sich als wichtige Schnittstelle meiner Behörde in den politischen Raum etabliert.

Zu meinen gesetzlichen Aufgaben gehört die Beratung von Bundestag und Bundesrat, der Bundesregierung sowie anderer Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten. Neben der Teilhabe am datenschutzrechtlichen und -politischen Diskurs habe ich zudem relevante Entwicklungen technischer, wissenschaftlicher, gesellschaftlicher und wirtschaftlicher Art zu verfolgen sowie die Öffentlichkeit im Hinblick auf Risiken zu sensibilisieren.

Um diese Aufgaben effizient erfüllen zu können und dabei den durch eine Vielzahl an Akteuren und Einflussfaktoren geprägten Dynamik und der Komplexität politischer Prozesse in der Bundeshauptstadt Rechnung zu tragen, habe ich in meinem Berliner Verbindungbüro 2021 ein kleines Hauptstadtteam aus drei Personen gebildet. Angebunden an den Leitungsbereich koordiniert und bündelt es u. a. die politische Arbeit und Korrespondenz meiner Behörde, beobachtet Entwicklungen, sichert Informationsflüsse und pflegt den wechselseitigen Austausch mit allen relevanten Akteuren.

Dank der gut vernetzten Kolleginnen und Kollegen konnten Informationsflüsse verbessert sowie die Fachebene meines Hauses entlastet werden. Der politisch-parlamentarische Raum hat überdies durch mein Hauptstadtteam feste Ansprechpartnerinnen und Ansprechpartner gewonnen, die dem Dienstleistungsauftrag meiner Behörde entsprechend zentral und bei Bedarf auch kurzfristig erreichbar sind.

Positiv etabliert haben sich auch die verschiedenen Informations- und Austauschformate für den parlamentarischen Bereich: Der regelmäßig, mindestens vierteljährlich erscheinende Parlamentsbrief für Abgeordnete und deren Mitarbeitende wird gut angenommen. Er informiert in komprimierter Form zielgruppenorientiert über aktuelle politische Themen zu Datenschutz und Informationsfreiheit und ist öffentlich verfügbar (www.bfdi.bund.de/parlamentsbrief).

Zu den Parlamentsbriefen geht's hier:

(QR-Code scannen oder klicken)

Großer Beliebtheit erfreute sich zudem der zu Beginn der Legislatur mehrfach angebotene Workshop zu den Grundlagen des Datenschutzes. Er richtete sich speziell an neue Mitglieder und Mitarbeitende des Bundestages und soll die Sensibilität für datenschutzrechtliche Fragen erhöhen. Ich werde ihn auch weiterhin regelmäßig anbieten. Gleiches gilt für fachliche Themenworkshops zu ausgewählten, politisch bedeutsamen Datenschutzfragen.

Ebenso erfolgreich war der Auftakt meines ersten Politischen Forums in Berlin zum Thema „Mein Auto! Meine Daten?“, so dass ich auch hier regelmäßige Fortsetzungsveranstaltungen plane.

Insgesamt hat sich durch das Hauptstadtteam die politische Kommunikation mit meiner Behörde verbessert. In diesem Zusammenhang sehe ich auch das aktuelle Bestreben des Deutschen Bundestages, seine Geschäftsordnung zu ändern. Ich soll zukünftig bei Sachverständigenanhörungen stets hinzugezogen werden, wenn es in den Ausschüssen um Vorhaben geht, die in erheblicher Weise den Schutz personenbezogener Daten betreffen und eine Anwesenheit zumindest von einem Viertel der Ausschussmitglieder verlangt wird.

Querverweise:

8.10 Digitale Datenräume und Mobilitätsdaten im Verkehrssektor

10.8 Sichere Kommunikation Behördenpostfach

Sichere Übermittlungswege für die Zustellung elektronischer Dokumente sind gerade im Rahmen der Digitalisierung der Verwaltung besonders wichtig. Im Rahmen der Vorbild- und Vorreiterrolle hat meine Dienststelle hierzu bereits im September 2020 den

Zugang per sog. besonderem elektronischen Behördenpostfach eröffnet.

Die Digitalisierung der Verwaltung kann viele Vorteile sowohl für die Bürgerinnen und Bürger als auch für Behörden haben, wenn sie richtig umgesetzt wird. Dabei kann sie effektiver, nutzerfreundlicher und sicherer sein als die überkommenen analogen Verwaltungsprozesse. Für meine Dienststelle als Datenschutzaufsichtsbehörde des Bundes war es immer besonders wichtig, selbst eine Vorreiterrolle bei der Digitalisierung der Verwaltung einzunehmen und diese datenschutzkonform umzusetzen. So wurden Papierakten frühzeitig in ein elektronisches Dokumentenmanagement überführt, welches – von wenigen Ausnahmen, etwa im Bereich von bestimmten Verschlusssachen abgesehen – bereits vor Jahren in eine vollständige elektronische Aktenführung mündete. Die Alltagsarbeit der Mitarbeitenden wurde dadurch weitgehend papierlos. Kombiniert mit der notwendigen IT-Infrastruktur und modernen Möglichkeiten zum mobilen Arbeiten konnte der Dienstbetrieb meiner Behörde daher auch während der Pandemie problemlos aufrechterhalten werden.

Aber bei der Digitalisierung der Verwaltung ist es nicht nur wichtig, die interne Aktenbearbeitung, sondern auch die Kommunikation mit anderen Stellen digital und sicher zu gestalten. Beaufsichtigte Stellen und Bürgerinnen und Bürger konnten meine Dienststelle schon immer digital über Eingabeformulare auf meiner Webseite und per elektronischer Post erreichen, neben einem DE-Mail-Postfach auch per herkömmlicher E-Mail. Die entsprechenden PGP-Schlüssel zur verschlüsselten E-Mail-Kommunikation u. a. sind auf meiner Homepage hinterlegt.

Seit dem 1. Januar 2022 besteht für Behörden und juristische Personen des öffentlichen Rechts die Pflicht, am sog. elektronischen Rechtsverkehrs (ERV) teilzunehmen und hierfür bestimmte sichere Übermittlungswege für die Zustellung elektronischer Dokumente zu nutzen. Die Justiz empfiehlt hierzu die Verwendung des sog. „besonderen elektronischen Behördenpostfachs“ (beBPo). Tatsächlich hatte meine Dienststelle aber schon lange zuvor, d. h. bereits im September 2020, das beBPo eingerichtet und so auch für andere Stellen den Zugang elektronischer Dokumente über einen sicheren Übermittlungsweg eröffnet.

Meine Dienststelle hat mit Blick auf den ERV dabei drei Kommunikationskanäle eröffnet:

- BfDI – Poststelle – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- BfDI – Justitiariat – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- BfDI – Referat Z 1 (Personal) – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Hierdurch kann die Kommunikation mit Gerichten unmittelbar mit unserem Justitiariat erfolgen und auch für den besonders sensiblen Bereich der Personalverwaltung ist für Personalangelegenheiten ein gesonderter Kanal eingerichtet. Für alle anderen Fälle ist meine Dienststelle über den beBPo-Kanal der Poststelle erreichbar. Mit diesem kann das beBPo auch von anderen Teilnehmenden des ERV im Rahmen der sonstigen behördlichen Kommunikation als sicherer Übermittlungsweg verwendet werden. Dies betrifft beispielsweise andere Behörden, Krankenkassen und Rechtsanwälte, die u. a. auch bei Beratungsanfragen oder Aufsichtsverfahren gerne über das beBPo mit meiner Dienststelle in Kontakt treten können und sollen.

Als Bundesdatenschutzbehörde werde ich auch weiterhin auf eine bürgerfreundliche, grundrechtskonforme und sichere Digitalisierung der Verwaltung hinwirken, auch innerhalb der internen Verwaltungsvorhaben meiner eigenen Dienststelle. Die Vergangenheit meiner eigenen frühzeitig umgesetzten Digitalisierungsvorhaben sollte dabei hinreichend deutlich machen, dass die Bundesdatenschutzbehörde keine Digitalisierungsbremse, sondern Vorreiter einer digitalen und sicheren Verwaltung ist.

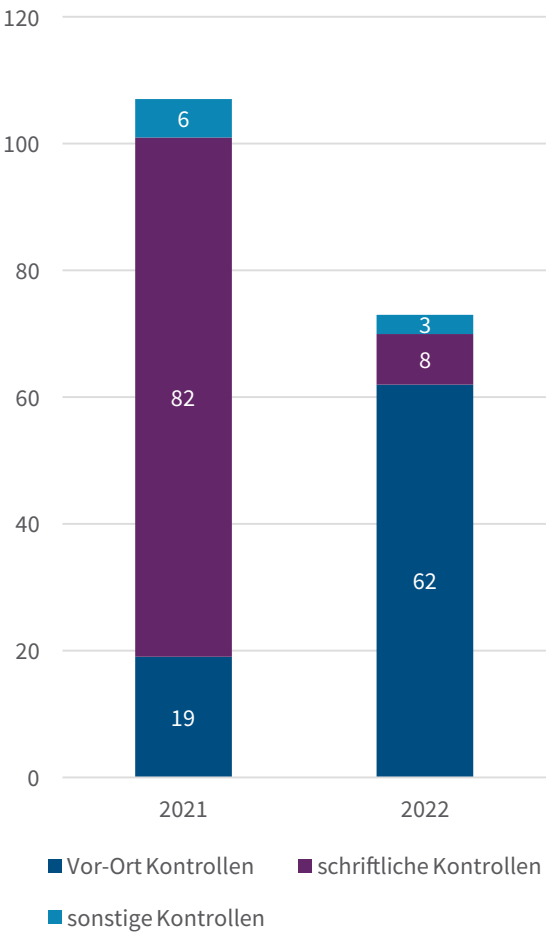
10.9 Statistik 2022

Neben den in den vielen vorausgehenden Beiträgen dargestellten inhaltlichen Einblicken liefert auch die Statistik einen aufschlussreichen Blick auf die Arbeit meiner Behörde. Für das Berichtsjahr lassen sich unter anderem einige Trends erkennen, die mit dem Abklingen der Corona-Pandemie in Verbindung stehen.

Beratung und Kontrolle

Als Aufsichtsbehörde stellen Beratung und Kontrolle wichtige Arbeitsbereiche dar, die mitunter stark vom persönlichen Kontakt mit den verantwortlichen Stellen abhängen. Vor diesem Hintergrund ist es erfreulich, dass meine Mitarbeiterinnen und Mitarbeiter im Jahresverlauf die Aufsichtstätigkeit wieder stärker bei Vor-Ort-Terminen wahrnehmen konnten. Insbesondere noch offene Pflichtkontrollen bei Sicherheitsbehörden konnten nachgeholt werden. Diese Vor-Ort-Kontrollen sind in der Regel inhaltlich sowie zeitlich wesentlich umfangreicher und gehen dabei komplexere Sachverhalte an als die schriftlichen Kontrollen, die oft eingesetzt werden, um einen Überblick über bestimmte Themen in einer Branche oder einer Gruppe von Behörden zu erhalten. Dies ist eine Erklärung dafür, dass die Gesamtzahl der durchgeführten Kontrollen im Vergleich zum Vorjahr gesunken ist, während die Zahl der Vor-Ort-Kontrollen sich mehr als verdreifacht hat.

Kontrollen im Rahmen meiner Aufsichtstätigkeit



Mit Blick auf die strategische Ausrichtung meiner Behörde als Beratungshaus ist es außerdem erfreulich, dass die Anzahl von Beratungsterminen mit beaufsichtigten Stellen stark angestiegen ist. Bei diesen Terminen werden konkrete Problemstellungen und datenschutzfreundliche Lösungsmöglichkeiten besprochen. Oftmals werden die Themen von den beaufsichtigten Stellen an mich herangetragen.

Anfragen, Beschwerden und Meldungen zu Datenschutzverstößen

Im Berichtsjahr richteten Bürgerinnen und Bürger insgesamt 6.619 Beschwerden und Anfragen an mich. Außerdem konnte ich 6.374 Personen telefonisch beraten. Das entspricht grob den Zahlen der Vorjahre, wobei eine leicht fallende Tendenz zu beobachten ist. Nach den vielen Beschwerden zum Start der DSGVO und den Anfragen rund um die Datenverarbeitung zur Pandemiebekämpfung scheint Beratungsbedarf von Bürgerinnen und Bürgern etwas rückläufig zu sein. Ich führe das auch auf die intensive Beratung z. B. bei Jobcentern und Finanzämtern zurück, die zur Verbesserung der Verarbeitungsprozesse und damit zu weniger Beschwerden geführt haben.

Eine leichte Zunahme beobachtete ich hingegen bei den eingehenden Meldungen von Datenschutzverstößen. Im Berichtsjahr habe ich 10.658 Meldungen entgegengenommen.

Beschwerden und Anfragen	2020	2021	2022
Allgemeine Anfrage	4.897	4.329	4.434
Beschwerde Art. 77 DSGVO	2.861	2.383	2.115
Beschwerde Art. 80 DSGVO	25	19	3
Beschwerde § 60 BDSG	56	54	29
Eingabe gegen Nachrichtendienste	39	44	38

Meldungen von Datenschutzverstößen	2020	2021	2022
Meldungen nach Art. 33 DSGVO	9.987	10.106	10.614
Meldungen nach § 169 TKG	37	51	44

Förmliche Begleitung von Rechtsetzungsvorhaben

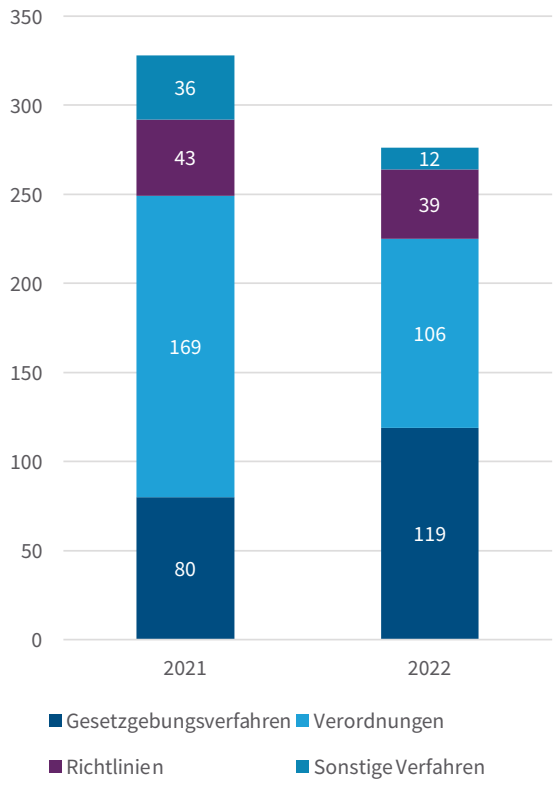
Gemäß § 21 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) haben die federführenden Ressorts mich bei der Erstellung von Gesetzesvorlagen frühzeitig zu beteiligen, soweit diese meine Aufgaben berühren. Wie an mehreren Stellen in diesem Bericht ausgeführt, funktioniert dies leider nicht immer reibungslos. Allerdings wurde ich insgesamt häufiger an förmlichen Gesetzgebungsverfahren beteiligt; die Steigerung lag bei knapp 50 Prozent im Vergleich zum Vorjahr. Bei Verordnungen dagegen sank die Zahl, was vermutlich auch damit zu tun hat, dass im ersten Jahr nach einem Regierungswechsel die Rechtsgrundlage für geplante Verordnungen noch nicht geschaffen werden konnten, so dass hier 2023 eine Steigerung zu erwarten ist.

Neben den in der Grafik aufgeführten 276 Beteiligungen nach § 21 GGO habe ich 99 Dateianordnungen sowie 6 EU-Rechtsakte geprüft und zu 12 Verfahren des Bundesverfassungsgerichts Stellung genommen. Außerdem konnte ich mich als Sachverständiger in 5 Anhörungen von Ausschüssen des Deutschen Bundestages einbringen.

Querverweise:

6.6 Statistische Auswertungen IFG für 2022

Beteiligungen nach § 21 GGO



11 Zentrale Anlaufstelle

Die Zentrale Anlaufstelle (ZASt) koordiniert die grenzüberschreitende Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder mit den anderen Mitgliedstaaten der Europäischen Union, dem Europäischen Datenschutzausschuss (EDSA) und der Europäischen Kommission.

Im europaweit einmaligen föderalen System ermöglicht sie es den Aufsichtsbehörden der EU-Mitgliedstaaten, dem Europäischen Datenschutzausschuss und der Europäischen Kommission ohne Kenntnis der deutschen Zuständigkeitsverteilung mit den deutschen Datenschutzaufsichtsbehörden zu kommunizieren und zusammenzuarbeiten.

Obgleich beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) angesiedelt, ist die ZASt organisatorisch von diesem getrennt. Diese organisatorische Trennung soll etwaigen Interessenkollisionen entgegenwirken und sicherstellen, dass die Datenschutzaufsichtsbehörden des Bundes und der Länder beim Informationsfluss von und nach Europa gleichbehandelt werden.

Die Aufgaben der ZASt beschränken sich darauf, die Datenschutzaufsichtsbehörden des Bundes und der Länder bei ihren Aufgaben zu unterstützen, ohne selbst Aufgaben der Datenschutzaufsicht wahrzunehmen.

11.1 ZASt Rückblick

Die Erledigung der grenzüberschreitenden Beschwerdeverfahren in der europäischen Verwaltungszusammenarbeit gewinnt an Fahrt. Einige Entwicklungen erscheinen jedoch vielschichtiger, als es die Zahlen zunächst nahelegen. Auch 2022 war die Zentrale Anlaufstelle (ZASt) hinter den Kulissen aktiv und hat ihren Teil zur verbesserten Zusammenarbeit beigetragen.

Rückgang der Einsprüche: zunehmende Harmonisierung beim Datenschutzvollzug

Die Zusammenarbeit der Aufsichtsbehörden erfolgt in grenzüberschreitenden Fällen zunehmend konsensual. Die Aufsichtsbehörden tauschen sich verstärkt untereinander aus, auch schon in frühen Verfahrensstadien, wo noch alle Entscheidungsmöglichkeiten offenstehen. Dies ist ein Ergebnis eines informellen Treffens der Leitungen der europäischen Aufsichtsbehörden Ende April 2022 in Wien mit dem Ziel einer verbesserten Zusammenarbeit.

Obschon die Verstetigung dieser Entwicklung abzuwarten bleibt, sind erste Auswirkungen bereits messbar. So ist die Anzahl der Einsprüche, die Aufsichtsbehörden gegen Entscheidungen ihrer europäischen Kollegen einlegen, stark rückläufig. Das Ziel der DSGVO, ein harmonisiertes hohes Datenschutzniveau zu schaffen, wird somit zunehmend erreicht. Viele der anfangs sehr streitigen prozeduralen Grundsatzfragen sind geklärt und die europäischen Aufsichtsbehörden wenden sich verstärkt den wichtigen materiell-rechtlichen Fragen zu. Auch ist der konsensuale Weg im Interesse aller Beteiligten, weil auf diese Weise schneller eine Entscheidung getroffen werden kann.

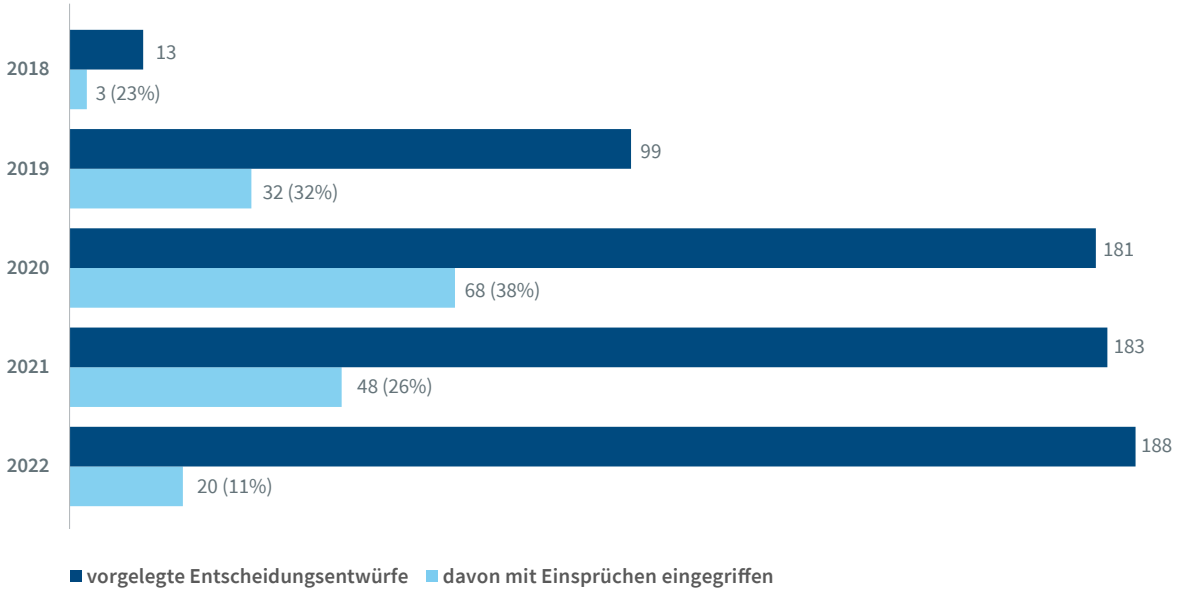
Die nachfolgende Grafik zeigt diese Entwicklung anhand der vorgelegten Entscheidungsentwürfe und der hiergegen erhobenen Einsprüche. Eine erste Plateaubildung bei den vorgelegten Entscheidungsentwürfen zeichnet sich ab.

Ausgenommen sind gütliche Einigungen, hierzu nun mehr im folgenden Abschnitt.

Mehr Verfahrensabschlüsse gleich mehr Datenschutz? Leider nicht immer.

Im Verfahren nach Art. 60 DSGVO sollen federführende und betroffene Aufsichtsbehörden sich grundsätzlich

Entscheidungsentwürfe & Einspruchseinlegung seit Anwendbarkeit der DSGVO am 25. Mai 2018



über die Art und Weise, wie ein konkreter Sachverhalt abgeschlossen wird, in vertrauensvoller und konstruktiver Zusammenarbeit einigen.

Im Berichtszeitraum 2022 werden für Deutschland 135 Beschlussentwürfe und für Irland 172 ausgewiesen. Alleine 160 irische Beschlussentwürfe wurden im Zeitraum von Juni 2022 bis Ende Dezember erstellt. Wie ist dieser signifikante Anstieg in so kurzer Zeit zu erklären?

Im Juni 2022 hat das 66. EDSA-Plenum die Leitlinie 06/2022 verabschiedet. Danach sollen Aufsichtsbehörden, die nach ihrem nationalen Verfahrensrecht Beschwerdefälle gütlich beilegen, den anderen betroffenen Aufsichtsbehörden in jedem Einzelfall vorab einen Beschlussentwurf „sui generis“ übermitteln.

Die Verfahrensentscheidungen werden hier nicht zwischen den beteiligten Aufsichtsbehörden, sondern allein zwischen federführender Aufsichtsbehörde, Verantwortlichen und betroffenen Personen verhandelt. Dabei werden die gerügten Datenverarbeitungen behördlicherseits nicht weiter aufgeklärt. Die Möglichkeiten anderer betroffener Aufsichtsbehörden, gegen einen derartigen verfahrensbeenden Beschlussentwurf vorzugehen und eine intensivere oder abweichende rechtliche Prüfung und Einschätzung durchzusetzen, sind stark verkürzt.

Verdienst der Leitlinie 06/2022 ist es, dass diese in äußerst unterschiedlichem Umfang praktizierte Art der Verfahrensbeendigung nunmehr sichtbar gemacht ist. Das Instrument der gütlichen Einigungen an sich kann hingegen aus unterschiedlichen Perspektiven betrachtet werden. Einerseits ermöglicht es, in kurzer Zeit eine große Anzahl von in der Regel einfachen und häufig auch ähnlich gelagerten Einzelfällen unter Einbindung von Beschwerdeführenden und verantwortlichen Stellen abzuschließen. Andererseits besteht bei diesen Beschlussentwürfen eine äußerst eingeschränkte Möglichkeit der betroffenen Aufsichtsbehörden, über die rechtlichen Erwägungen der federführenden Aufsichtsbehörde Kenntnis zu erlangen. Deswegen sowie erschwerend aus prozeduralen Gründen, ist die Möglichkeit zur Einflussnahme auf aufsichtsbehördliche Maßnahmen und eine rechtliche Überprüfung der Bewertung der federführenden Aufsichtsbehörde durch den EDSA äußerst eingeschränkt.

Es gilt nun weiter zu beobachten, welche Auswirkungen diese Arbeitsweise auf den auf transparenten Austausch zwischen den Aufsichtsbehörden angelegten Kooperationsmechanismus hat. Flankierend hat der EDSA im Rahmen seiner Strategieentwicklung gegenüber der EU-Kommission als Bestandteil einer „Wishlist“ angeregt, diese praktisch bedeutsame Form der Verfahrensbeendigung gesetzlich näher zu konturieren.

Angebot von Schulungen im Binnenmarktinformationssystem IMI durch die ZASt

Aufgrund der grenzüberschreitenden Fallbearbeitung im von der Europäischen Kommission bereitgestellten Binnenmarktinformationssystem IMI haben die deutschen Aufsichtsbehörden auch viereinhalb Jahre nach Inkrafttreten der DSGVO erheblichen Bedarf an Schulung in der praktischen Arbeit in diesem zentralen IT-System an die ZASt gemeldet.

Anknüpfend an die einführenden Schulungen durch das EDSA-Sekretariat und die Europäische Kommission

im Jahre 2018 sowie zuletzt Anfang 2020 hat die ZASt daher ein Schulungskonzept in Eigenregie entwickelt. Darauf aufbauend wurden im Herbst des Jahres 2022 Beschäftige von fast allen deutschen Aufsichtsbehörden im Umgang mit IMI geschult. In einer Grundlagenschulung im Oktober 2022 wurde zunächst das erforderliche Basiswissen zur Bearbeitung der grenzüberschreitenden Fälle im IMI vermittelt und in praktischen Übungseinheiten vertieft. Hierbei wurden auch die mittlerweile zahlreichen Ausarbeitungen des EDSA mit formellen und prozeduralen Vorgaben der grenzüberschreitenden Beschwerdebearbeitung in den Blick genommen.

Ein Fortgeschrittenenworkshop fand im November 2022 statt. Mit der Schaffung dieses Forums durch die ZASt konnten sich die Expertinnen und Experten der deutschen Aufsichtsbehörden in Sachen IMI-Anwendung über besonders schwierige Fallgestaltungen austauschen. Ergebnis waren Best-Practice-Empfehlungen für eine noch besser abgestimmte Meinungsbildung und europäische Kooperation sowie taktische und strategische Ansätze zur erfolgreichen Einbringung der deutschen Position in den europäischen Diskurs. Diese sollen zukünftig in die zuständigen Arbeitskreise der DSK und ggf. die zuständigen Expert Subgroups des EDSA eingebracht werden.

IMI-Schulung durch die ZASt

12 Wo bleibt das Positive?

Wie schon in der Einleitung und auch in manchen vorhergehenden Beiträgen beschrieben, gibt es immer öfter durchaus positive Entwicklungen, die sich aus meiner Beratungs- und Kontrolltätigkeit ergeben. Da meine Mitarbeiterinnen und Mitarbeiter in den Gesprächen stets versuchen, datenschutzfreundliche Alternativen aufzuzeigen, fühlen wir uns in unserem Beratungsansatz bestärkt und freuen uns, dass dieser sich zunehmend bei der Datenverarbeitung der beaufsichtigten Stellen widerspiegelt. Wie schon im letzten Tätigkeitsbericht, will ich einige hervorgehobene Beispiele für eine solche positive Zusammenarbeit vorstellen.

12.1 Datenschutzorganisation bei der DRV Bund

Die Deutsche Rentenversicherung (DRV) Bund hat ihre Datenschutzorganisation überarbeitet und damit die Unabhängigkeit des behördlichen Datenschutzbeauftragten gestärkt.

Die DRV Bund hat eine grundlegende Neuorganisation des Datenschutzes vorgenommen und für den behördlichen Datenschutzbeauftragten eine eigene Stabsstelle geschaffen, die direkt dem Direktorium berichtet. Hierdurch wurde im Vergleich zur vorherigen Struktur eine noch deutlichere Trennung zwischen den Aufgaben des behördlichen Datenschutzbeauftragten einerseits und des operativen (administrativen) Datenschutzes andererseits erreicht. Die Verpflichtung, bei der Benennung eines Datenschutzbeauftragten gemäß Art. 38 Abs. 6 DSGVO darauf zu achten, dass weitere übertragene Aufgaben den Datenschutzbeauftragten nicht in einen Interessenkonflikt bringen können und damit seine unabhängige Stellung gefährden, wurden seitens der DRV Bund in dem erforderlichen Maße umgesetzt. Ich habe die DRV Bund während des Umstrukturierungsprozesses eng beraten und begrüße die erfolgte Reorganisation.

12.2 Datenschutzrechtliche Aspekte von Telemedienangeboten

Steter Tropfen höhlt den Stein. Sehr langsam, aber doch erkennbar, steigt bei den öffentlichen Stellen des Bundes das Bewusstsein für datenschutzrechtliche Fragestellungen bei Telemedienangeboten.

In diesem Berichtsjahr konnte ich eine wachsende Sensibilisierung und zunehmendes Bewusstsein von Behörden hinsichtlich der datenschutzrechtlichen Problematiken bei der Nutzung von Telemedienangeboten feststellen. Dies hat sich insbesondere in den zunehmenden Beratungen und erhöhtem Interesse verschiedener Behörden zu diesem Themenbereich gezeigt.

Drei Themenstellungen standen dabei im Fokus: Cookies und Cookie-Banner, Einbindung von Videos auf den Homepages der Bundesbehörden sowie der Betrieb von Facebook-Fanpages.

Die datenschutzkonforme Ausgestaltung von Cookie-Bannern wie auch die rechtlichen Grundlagen, etwa für die Reichweitenmessung, stellen fast alle verantwortliche Stellen immer wieder vor Herausforderungen. Neben mehreren Einzelberatungen habe ich deshalb insbesondere Fragestellungen zu Cookie-Bannern im Rahmen des Erfahrungsaustausches mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden vorgestellt und Empfehlungen ausgesprochen. In diesem Zusammenhang habe ich auch gezielt einige Informationstexte und FAQs auf meiner Webseite aktualisiert.[72]

Darüber hinaus wurde die für viele Telemedienanbieter sehr wichtige Arbeitsgrundlage „Orientierungshilfe Telemedien“ der DSK im Arbeitskreis Medien der DSK intensiv überarbeitet und an die neuen rechtlichen Vorgaben des TTDSG angepasst. Der Gesetzgeber möchte schon seit geraumer Zeit Regelungen zu anerkannten

72 Informationsangebot auf meiner Webseite, abrufbar unter: https://www.bfdi.bund.de/DE/Buerger/Privatwirtschaft/Telemedien/Telemedien_node.html

Diensten zur Einwilligungsverwaltung schaffen. Klare und ausgewogene Regelungen könnten die Privatsphäre von Nutzerinnen und Nutzern stärken und Cookie-Banner eindämmen. Doch eine praxistaugliche und rechtmäßige Lösung ist noch nicht in Sicht.

Die Einbindung von Videos auf Homepages der öffentlichen Stellen des Bundes erfolgt leider fast immer noch im Wesentlichen mit YouTube. Den Verantwortlichen ist die datenschutzrechtliche Problematik zwar häufig bewusst, doch wird diese meist zugunsten Bedürfnissen wie der Reichweitenmessung ignoriert. Vorbildlich verhält sich hier das Bundesministerium des Innern und Heimat, das mit Hilfe meiner Beratungen damit begonnen hat, Videos auf der Homepage nicht mehr durch YouTube, sondern ausschließlich lokal einzubinden.

Öffentliche Stellen des Bundes betreiben trotz jahrelanger Sensibilisierungsarbeit und erheblichen datenschutzrechtlichen Bedenken weiterhin Facebook-Fanpages, so dass ich nun aufsichtsrechtlich tätig werden musste.

Grundsätzlich ist anzumerken, dass neue Angebote oft deshalb zunächst datenschutzrechtlich problematisch sind, weil sie häufig mittels vorgefertigten Baukastensystemen erstellt werden, welche nicht selten von Hause aus unnötige Cookies nutzen und externe Dienste einbinden. Erst auf Ansprache wird dann schnell umgestaltet, statt die problematischen Teile von Anfang an zu vermeiden.

Ich empfehle, die Einbindung von Videos auf den Webseiten des Bundes zu überprüfen und datenschutzkonforme Alternativen zur weit verbreiteten Praxis der Einbindung mittels YouTube umsetzen.

Querverweise:

4.3.1 Verfahren Facebook Fanpages; 5.5 Dienste zur Einwilligungsverwaltung

12.3 Alternative Bereitstellung von Bundes-Apps

Apps der öffentlichen Hand sollten auch abseits der App-Stores der Betriebssystemhersteller angeboten werden.

In meinen Beratungen der Behörden zur Entwicklung von Apps habe ich in den vergangenen Jahren stets darauf hingewirkt, dass die entwickelten Apps auch über alternative vertrauenswürdige Quellen bezogen werden können. Leider musste ich feststellen, dass nicht alle Behörden meinen Empfehlungen gefolgt sind. Daher habe ich die obersten Behörden mittels Rundschreiben vom 22. Juni 2022 über die datenschutzrechtliche Wertung informiert und sie zum Handeln aufgefordert. Datenschutzrechtlich trifft die Stelle, die für die App verantwortlich ist, eine Entscheidung, über welchen Vertriebsweg das Produkt angeboten wird. Wird eine App nur über die App-Stores der Betriebssystemhersteller bereitgestellt, so müssen sich die Bürgerinnen und Bürger, die diese Apps nutzen wollen, den Prozessen dieser Unternehmen (Dritte) unterwerfen, die derzeit zwingend die Einrichtung eines Accounts vorsehen. Ebenso müssen die Geschäftsbedingungen der Store-Anbieter akzeptiert werden. Die Bereitstellung der Apps über diese Vertriebskanäle inkludiert damit eine Verarbeitung personenbezogener Daten, die für diesen Zweck nicht erforderlich ist.

Einige technisch versierte Personen haben bewusst ein freies Betriebssystem auf ihren mobilen Endgeräten installiert. Diese Personen haben keinen Account bei den Betriebssystemherstellern. Im Sinne des Open-Government-Aspektes ist jedoch auch für diese (noch kleine) Personengruppe die App bereitzustellen. Im Art. 6 Abs. 4 des Digital Markets Act ist bereits eine verpflichtende Öffnung der Stores vorgesehen. Bis zur Marktbefreiung wird es jedoch noch dauern, sodass die jetzt empfohlene Bereitstellung der Apps auf den eigenen Webseiten der Behörden eine Übergangslösung darstellt.

Eine Behörde konnte mir bereits sehr zeitnah Rückmeldung geben, dass ihr gesamtes App-Portfolie über die eigene Webseite zur Verfügung steht. Besonders gefreut hat mich, dass das Bundesministerium des Innern und für Heimat bereits prüft, inwieweit sich Apps des Bundes über ein einheitliches Bundesangebot bereitstellen lassen. Noch ist eine Entscheidung darüber nicht gefallen, doch schon das erste Feedback zeigt mir: Mit wenigen kleinen gezielten Schritten lassen sich gute datenschutzrechtliche Lösungen schaffen.

12.4 Beratung und fachlicher Austausch zum SÜG – Eine fruchtbare Ergänzung

Proaktive Beratung und fachlicher Austausch mit den verschiedensten Akteuren der Praxis ist essentiell zur Gewährleistung und Implementierung eines hohen Datenschutzniveaus im Bereich der Sicherheitsüberprüfung. Aus diesem Grund legte ich in diesem Berichtsjahr einen Fokus auf die Beratung und den fachlichen Austausch. Dies wurde von allen Beteiligten sehr positiv aufgenommen. Insbesondere bei Wirtschaftsunternehmen besteht nach meiner Einschätzung ein sehr hohes Bewusstsein für den Datenschutz.

Ergänzend zu meiner Kontrolltätigkeit im Bereich des Sicherheitsüberprüfungsgesetzes (SÜG) messe ich der Beratung einen sehr hohen Stellenwert zu. Nicht nur jede Kontrolle erfolgt in Verbindung mit einem Beratungsangebot, vielmehr nehme ich eine Beratungsaufgabe auch proaktiv wahr. Ziel ist es, die Einhaltung der datenschutzrechtlichen Vorschriften bei der Verarbeitung personenbezogener Daten nicht nur bei den kontrollierten Stellen sicherzustellen, sondern durch eine umfangreiche Beratung und Information aller Stellen schon im Vorfeld zu erreichen. Die Beachtung der datenschutzrechtlichen Vorschriften und somit der Schutz der informationellen Selbstbestimmung kann durch diesen Ansatz am effektivsten erreicht werden.

Hierzu verfolge ich neben der individuellen Beratung einzelner Stellen drei verschiedene Ansätze. Dies ist erstens der Fachdialog mit Fachanwendungsanbietern, zweitens der Austausch mit Arbeitskreisen bzw. Interessensvertretungen sowie drittens die Bereitstellung von Arbeitshilfen.

Die Verarbeitung personenbezogener Daten in Sicherheitsüberprüfungen wird zunehmend digitalisiert, so dass verschiedene elektronische Fachanwendungen Einzug halten. Ein Anbieter einer solchen Fachanwendung rief mein Beratungsangebot ab. Dies entwickelte sich zu einem für beide Seiten konstruktiven Fachdialog. Der Fachanwendungsanbieter optimierte im Laufe der Beratung seine Software, um diese den jeweiligen datenschutzrechtlichen Vorgaben des SÜG anzupassen. So erlangte ich ein besseres Verständnis von der Fachanwendung und der praktischen Arbeit mit dieser. Da die Fachanwendung von vielen kontrollierten Stellen genutzt wird, konnte ich einerseits meine Kontrolleffizienz steigern und anderseits haben die jeweiligen Nutzer der Fachanwendung die Gewissheit, dass sie eine Software nutzen, die die datenschutzrechtlichen Vorgaben des SÜG einhält.

Ich tauschte mich darüber hinaus wiederholt mit einem Arbeitskreis aus, dessen Mitglieder für die Durchführung des SÜG in Wirtschaftsunternehmen zuständig sind. Hier konnte ich nicht nur meine Anliegen platzieren, sondern insbesondere aus der Praxis erfahren, welche Probleme bei der Anwendung des Gesetzes bestehen. Der stetige Austausch mit den Anwenderinnen und Anwendern des SÜG ermöglicht es mir in Erfahrung zu bringen, welche Probleme bei der Anwendung des SÜG bestehen und insbesondere welche datenschutzrechtlichen Herausforderungen zu lösen sind. Neben meiner Kontrolltätigkeit setzt mich insbesondere der fachliche Austausch in die Lage, Empfehlungen zu geben, wie das SÜG fortzuentwickeln ist (30. TB Nr. 6.20).

Meine Erkenntnisse aus den Kontrollen, dem fachlichen Austausch sowie Rückmeldungen aus der Praxis flossen unter anderem in verschiedene Arbeitshilfen. Ich veröffentlichte in diesem Berichtsjahr Arbeitshilfen zu den datenschutzrechtlichen Anforderungen bei der Führung von Sicherheitsakten im Sicherheitsüberprüfungsverfahren sowie zu den datenschutzrechtlichen Anforderungen beim Verarbeiten personenbezogener Daten aus der Sicherheitsüberprüfung in Dateien. Die Arbeitshilfe zur Führung der Sicherheitsakte richtet sich an die jeweiligen verantwortlichen Personen in den zuständigen öffentlichen und nicht-öffentlichen Stellen. Diese werden mit zahlreichen Beispielen und datenschutzbezogenen Hinweisen für die Praxis in die Lage versetzt, die Sicherheitsakte in analoger oder digitaler Form datenschutzkonform zu führen. Ergänzt wird dies durch die Arbeitshilfe zur automatisierten Datei, die neben der Sicherheitsakte geführt werden darf. Mein Schwerpunkt liegt hier auf der Darstellung der Unterschiede zwischen den öffentlichen und nicht-öffentlichen Stellen. Der Gesetzgeber sieht hier erhebliche Unterschiede vor.

Die Arbeitshilfen ermöglichen einer Vielzahl von Anwenderinnen und Anwendern des SÜG, die eigenen Prozesse zu evaluieren und an die datenschutzrechtlichen Maßgaben anzupassen. Sie sollen laufend fortentwickelt und um weitere Themen aus der Praxis ergänzt werden.[73]

Des Weiteren versandte ich ein Rundschreiben an die Geheimschutzbeauftragten der obersten Bundesbehörden zur Weitergabe von Auskünften aus dem Bundeszentralregister sowie zur Verschlüsselung von E-Mails. Diese Rundschreiben sind ebenfalls auf meiner Homepage veröffentlicht, genau wie mehrere meiner Kontrollberichte, die von den verantwortlichen Stellen bei der Überprüfung der eigenen Prozesse herangezogen werden können.[74]

Die unterschiedlichen Beratungsansätze und der damit einhergehende Austausch mit den verschiedenen Akteuren, die entweder selbst personenbezogene Daten im Anwendungsbereich des SÜG verarbeiten oder Produkte bzw. Dienstleistungen für die verantwortlichen Stellen anbieten, haben Früchte getragen. Es freut mich, dass im Bereich des Sicherheitsüberprüfungsrechts ein großes Bewusstsein für den Datenschutz besteht. Dies gilt insbesondere für Wirtschaftsunternehmen. Positiv

73 SÜG-Arbeitshilfen, abrufbar unter: www.bfdi.bund.de/arbeitshilfen-sueg
74 SÜG-Rundschreiben, abrufbar unter: www.bfdi.bund.de/rundschreiben

hervorzuheben ist dabei, dass Anpassungen und Optimierungen auch außerhalb von Kontrollen erfolgen, um zukünftig personenbezogene Daten datenschutzkonform zu verarbeiten.

Auch zukünftig lade ich alle Akteure ein, sich mit Beratungsersuchen an mich zu wenden, um so eine datenschutzkonforme Gestaltung der entsprechenden Prozesse von Anfang an zu erreichen. Gerade Unsicherheiten, z. B. bei der Umstellung auf elektronische Anwendungen, können so am einfachsten beseitigt werden. Im Jahr 2023 werde ich die Beratung und den fachlichen Austausch weiter ausbauen. Dazu werde ich beispielsweise an der Bundesakademie für öffentliche Verwaltung eine Veranstaltung anbieten.

12.5 Protokollauswertetool für Inzoll

Im Rahmen einer Kontrolle des Zollfahndungsinformationssystems INZOLL habe ich Verbesserungsmöglichkeiten bei der Ausgestaltung der Protokollierung festgestellt. Auf mein Bestreben hin hat das Zollkriminalamt (ZKA) begonnen, die Protokollierung um ein Auswertetool zu erweitern, um Datenschutzkontrollen zukünftig besser zu gewährleisten.

In meinem letzten Tätigkeitsbericht habe ich von einer Kontrolle der Abfragen im Informationssystem des Zollfahndungsdienstes (INZOLL) berichtet (vgl. 30. TB Nr. 8.1.4). Im Rahmen dieser Kontrolle habe ich auch Einsicht in die Protokollierung genommen. Technische und inhaltliche Detailfragen der Protokollierung in INZOLL hatte ich allerdings pandemiebedingt zunächst aus meiner Bewertung ausgenommen, da hierfür ein Vor-Ort-Termin bei der Systembetreuung stattfinden sollte. Dieser konnte im Februar 2022 nachgeholt werden.

Im Vorfeld hatte ich Schwächen im Protokollierungssystem identifiziert. Insbesondere stand ein Auswertetool, das die Anzeige und Recherchierbarkeit von Protokolldaten unmittelbar vor Ort ermöglicht, für meine Kontrolle nicht zur Verfügung. Die Auswertung zu durchgeführten Abfragen musste bei der Systemadministration in Auftrag gegeben werden, was dort mit hohem manuellem Aufwand verbunden war. Auch war das Ergebnis der Auswertung kaum lesbar, da Abfragen lediglich in Form komplexer, technischer Datenbankbefehle ausgegeben wurden.

Diese Art der Protokollauswertung ist nicht ausreichend. Protokolldaten sollen darüber Auskunft geben, wer (oder was), wann, welche personenbezogenen Daten in welcher Weise verarbeitet hat. Es muss sichergestellt sein, dass die Protokolldaten für Zwecke der Datenschutzkontrolle, ohne Zwischenschaltung eines Dritten, zeitnah und praktikabel ausgewertet werden können. Ein entsprechendes Auswertetool für Protokolldaten muss hierfür zur Verfügung gestellt werden. Zudem müssen Protokolldaten auch für technische Laien verständlich sein.

Auf Grundlage dieser Anforderungen habe ich Verbesserungen bei der Protokollierung in INZOLL angeregt. Meinen Forderungen ist das ZKA unmittelbar nachgekommen. Es hat zeitnah ein Auswertetool entwickelt und zugleich in einem konstruktiven Beratungsgespräch bestehende Probleme transparent erörtert. Auf diese Weise konnte bereits eine erhebliche Verbesserung der Protokollierung erzielt werden. Eine Evaluierung wird im Rahmen meiner nächsten, turnusmäßigen Pflichtkontrolle erfolgen.

12.6 Verbesserungen im Vorgangsbearbeitungssystem BKA

Das Bundesministerium des Innern und für Heimat (BMI) hat ein aus meiner Sicht gelungenes Konzept vorgelegt, die Zweckbindung im Vorgangsbearbeitungssystem (VBS) des Bundeskriminalamts (BKA) zu verbessern. Das BMI hat das BKA damit beauftragt, dieses Konzept umzusetzen. Das begrüße ich sehr.

Im Jahr 2019 habe ich das VBS des BKA beanstandet. Ein wesentlicher Grund für die Beanstandung bestand darin, dass das VBS nicht ausreichend zwischen den verschiedenen Zwecken unterschied, zu denen die Polizeibehörde personenbezogene Daten verarbeitet. Folglich waren auch Zugriffsrechte und Recherchemöglichkeiten zu weit gefasst. Auch die Dokumentation der Rechtmäßigkeit polizeilichen Handelns habe ich als unvollständig bemängelt (28. TB Nr. 6.7.3, 29. TB Nr. 9.5.3, 30. TB Nr. 8.2.2).

Das BMI ist meinem rechtlichen Standpunkt in wesentlichen Aspekten zunächst nicht gefolgt (29. TB Nr. 9.5.3). Nach einem gemeinsamen Workshop im Dezember 2021, in dem ich das BKA bei der Aufbereitung der datenschutzrechtlichen Problemlagen im Zusammenhang mit dem VBS beraten hatte, begann das BKA, Konzepte zu erstellen, um das VBS weiterzuentwickeln (30. TB Nr. 8.2.2).

In einem weiteren Workshop im Oktober 2022 stellte das BKA ein gelungenes Konzept vor. Damit sollen die zu verschiedenen Zwecken im VBS verarbeiten personenbezogenen Daten besser getrennt werden. Dies soll dem wichtigen datenschutzrechtlichen Prinzip der Zweckbindung personenbezogener Daten Rechnung tragen. Damit sollen meine Forderungen aus dem Kontrollbericht

umgesetzt werden. Das BMI teilte mir Anfang November mit, das BKA per Erlass mit der Umsetzung des Konzepts beauftragt zu haben. Auch wenn ich die Langwierigkeit der Umsetzung meiner Forderungen kritisiert habe, erkenne ich nach wie vor die Komplexität des Unterfangens an (30. TB Nr. 8.2.2) und begrüße den ambitionierten Zeitplan des BKA von 14 Monaten, in dem dieses das VBS anpassen will.

12.7 Einlenken beim Ausländervereinsregister

Das Bundesverwaltungsamt setzt die Verarbeitung personenbezogener Daten im Ausländervereinsregister teilweise aus.

Ausländervereine und ausländische Vereinigungen können verboten werden, wenn ihr Zweck oder ihre Tätigkeit einen der Tatbestände des Art. 14 Abs. 2 Vereinsgesetz erfüllt und damit den Grundwerten der Bundesrepublik Deutschland zuwiderläuft.

Nach der „Verordnung zur Durchführung des Gesetzes zur Regelung des öffentlichen Vereinsrechts (Vereinsgesetz)“ aus dem Jahr 1966 unterliegen sie einer besonderen Anmelde- und Auskunftspflicht. Die geforderten Angaben umfassen auch personenbezogene Daten, wie z. B. Namen und Anschriften der Vorstandsmitglieder bzw. der zur Vertretung berechtigten Personen sowie bestehende Teilorganisationen in den Ländern. Die Vereinsbehörden der Länder melden die Angaben an das Bundesverwaltungsamt, welches das sogenannten Ausländervereinsregister (AVR) führt.

Bereits seit längerem habe ich das Bundesverwaltungsamt darauf hingewiesen, dass keine ausreichende Rechtsgrundlage für die Datenverarbeitung im AVR besteht. Zuletzt habe ich eine entsprechende Verbotsverfügung gemäß Art. 58 Abs. 2 lit. f) DSGVO gegenüber dem Bundesverwaltungsamt eingeleitet. Nun teilten mir sowohl das Bundesverwaltungsamt als auch das fachaufsichtsrechtlich zuständige Bundesministerium des Innern und für Heimat mit, dass ab dem 1. Januar 2023 keine neuen Mitteilungen der Vereinsbehörden in das AVR aufgenommen werden. Ausgenommen davon sind Mitteilungen, die Löschungen im Register zum Gegenstand haben. Diese Maßnahmen begrüße ich sehr. Ob sie allerdings ausreichen, eine datenschutzkonforme Datenverarbeitung im AVR zu gewährleisten, prüfe ich derzeit.

12.8 Postdienstleister stellt sich datenschutzrechtlich neu auf

In den vergangenen Jahren wurde ich auf unterschiedliche Geschäftsprozesse eines großen Postdienstleisters aufmerksam, die einer datenschutzrechtlichen Anpassung bedurften. Die in diesem Zusammenhang von mir ergriffenen Abhilfemaßnahmen gem. Art. 58 Abs. 2 DSGVO veranlassten den Verantwortlichen dazu, seine Geschäftsprozesse bei der Erbringung von Postdienstleistungen zu hinterfragen und weitreichenden, grundlegenden Überarbeitungen zu unterziehen. Erfreulicherweise hat dies dazu geführt, dass die Anzahl an Beschwerden und Datenschutzverstoßmeldungen zu diesem Unternehmen nun gesunken sind.

Seit dem Jahr 2020 wurden mir durch Beschwerden und Hinweise von Bürgerinnen und Bürgern vermehrt datenschutzrechtliche Mängel und Verstöße im Zusammenhang mit der Erbringung von Postdienstleistungen und der Bearbeitung von hierzu geltend gemachten Betroffenenrechten offenbar. Zu diesen gemeldeten Mängeln gehörten z. B. Zustelllisten, die im Freien oder in abgestellten Fahrzeugen, für Außenstehende lesbar, aufgefunden worden sind oder das Fotografieren von Sendungsempfängern ohne deren Einwilligung durch Zustellkräfte. Aufgrund dieser hierdurch gegebenen Datenschutzverstöße wie z. B. die Offenlegung personenbezogener Daten, die Erfassung personenbezogener Daten ohne Rechtsgrundlage oder die verspätete und unvollständige Erteilung von Auskünften zu personenbezogenen Daten ergriff ich Abhilfemaßnahmen gem. Art. 58 Abs. 2 DSGVO, indem ich Verwarnungen für die Vergangenheit aussprach und die Einführung eines kontinuierlichen Verbesserungsprozesses sowie eines Schulungskonzeptes für Zustellkräfte anwies.

Die notwendig gewordene datenschutzkonforme Umgestaltung der Prozesse wurde je nach Einzelfall von meinen Beschäftigten durch zusätzliche Beratungsgespräche begleitet. Zudem hat der Postdienstleister von sich aus weitreichende Veränderungen zugunsten eines sich durch das gesamte Unternehmen ziehenden Bewusstseins für Datenschutzthemen umgesetzt. Dadurch wurde sichergestellt, dass etwa neue Prozesse oder Software stets unter dem Blickwinkel des Datenschutzes betrachtet und auf ihre diesbezügliche Tauglichkeit geprüft werden. In der Folge führte der erhöhte Beratungsansatz dazu, dass die Prozesse datenschutzkonform angepasst und so weitere Maßnahmen gem. Art. 58 Abs. 2 DSGVO in diesem Zusammenhang abgewendet werden konnten.

12.9 Beratung und Aufsicht – gemeinsam mehr für den Datenschutz erreichen

Datenschutz ist komplex und streitbar zugleich. Diese Erfahrung mache ich immer wieder in meiner Beratungs- und Aufsichtspraxis. Manche Fragen im Datenschutz bedürfen einer gerichtlichen Klärung. Oft haben meine Argumente aber auch im Berichtsjahr bereits ausgereicht, um verantwortliche Stellen zu gutem Datenschutz zu bewegen.

Datenschutz muss schnell und effizient bei den Menschen ankommen. Deshalb freue ich mich besonders über Fälle, in denen meine Beratungen und Empfehlungen unmittelbar umgesetzt werden. Dies war im vergangenen Jahr etwa bei den Anforderungen an eine Identifizierung an der Störungshotline eines Telekommunikationsunternehmens der Fall. Viele Bürger hatten sich bei mir beschwert, weil sie bereits bei einer einfachen Abgabe einer Störungsmeldung nach ihren Bankdaten gefragt wurden. Nach Austausch der rechtlichen Argumente änderte die verantwortliche Stelle ihre Position und stellte ihre Prozesse datenschutzfreundlich um. Bürgerinnen und Bürger profitierten von einer schnellen Lösung in ihrem Sinne.

Datenschutzaufsicht und verantwortliche Stellen sind keine Gegenspieler. Gerade viele Unternehmen sind sensibilisiert, haben Datenschutz als Wettbewerbsfaktor erkannt und ihre Geschäftsprozesse hierauf ausgerichtet. Meine Kontrolle bestätigt sie dann darin, dass sich diese kontinuierliche Arbeit am Ende auszahlt. Denn teurer Anpassungsbedarf als Resultat einer Kontrolle entsteht so regelmäßig erst gar nicht. Ein positives Beispiel hierfür stellt die Kontrolle und Beratung der Emden Digital GmbH dar. Bei diesem Beratungs- und Kontrollbesuch zeigte sich auch der Vorteil eines Vor-Ort-Termins. Alle Entscheidungsträger waren vor Ort eingebunden. Umsetzungsvarianten wurden direkt erörtert und ich konnte unmittelbar meine Umsetzungsempfehlungen aussprechen.

Themenzuordnung nach Bundestagsausschüssen

Ausschuss für Arbeit und Soziales

- 3.2.4 Neue Entschließung der DSK zum Beschäftigtendatenschutzgesetz
- 8.7. Betriebliches Eingliederungsmanagement (BEM)

Auswärtiger Ausschuss

- 3.4 G7 Roundtable
- 3.5.1 Jahreskonferenz der Global Privacy Assembly 2022
- 9.3 Kontrollen in Auslandvertretungen in Kasachstan

Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

- 4.1.2 Forschungsdatenzentrum Gesundheit
- 4.1.3 Taskforce Forschungsdaten
- 4.1.4 Petersberger Erklärung

Ausschuss für Digitales

- 3.2.2 DSK Taskforce Souveräne Cloud
- 3.3.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Corporate Rules
- 3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield Nachfolge)
- 3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers
- 3.4 G7 Roundtable
- 3.5.1 Jahreskonferenz der Global Privacy Assembly 2022
- 4.1.2 Forschungsdatenzentrum Gesundheit
- 4.2.1 KI-Verordnung
- 4.2.2 Digital Services Act
- 4.2.3 Digital Markets Act
- 4.2.4 Data Governance Act
- 4.2.5 Data Act
- 4.2.6 Verordnung Politische Werbung
- 4.3.2 Entscheidungen europ. AB zu Google Analytics
- 5.5 Dienste zur Einwilligungsverwaltung
- 8.3 Sormas (follow up)
- 8.8 Zensus 2022
- 8.10 Digitale Datenräume und Mobilitätsdaten im Verkehrssektor
- 8.11 TrustPid – neue Wege der personalisierten Werbung
- 8.12 Videokonferenzdienste
- 8.13 Neues von der E-Mail – Zuständigkeitswechsel zum BfDI
- 8.15 Datenschutz im Smart Home
- 10.2 Aufbau Labor
- 12.2 Datenschutzrechtliche Aspekte von Telemedienangeboten
- 12.3 Alternative Bereitstellung von Bundes-Apps

Ausschuss für die Angelegenheiten der Europäischen Union

- 3.3.1 Allgemeiner Bericht zum EDSA
- 3.3.8 Verbindliche interne Datenschutzvorschriften – Neues von den Binding Corporate Rules
- 3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield Nachfolge)

3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers

4.5 Evaluierung der JI-Richtlinie und unzureichende Abhilfebefugnisse des BfDI in den Bereichen der Gefahrenabwehr und der Strafverfolgung

4.2.1 KI-Verordnung

4.2.4 Data Governance Act

4.2.5 Data Act

4.2.6 Verordnung Politische Werbung

Ausschuss für Familie, Senioren, Frauen und Jugend

8.7. Betriebliches Eingliederungsmanagement (BEM)

Finanzausschuss

5.3 Änderungen bei der Geldwäschebekämpfung und der Durchsetzung von Sanktionen

9.2 Kontrolle Aufbewahrungsvorschriften in der Finanzverwaltung

9.4.2 Pflichtkontrolle eingriffsintensiver Maßnahmen im Zollfahndungsamt München

9.4.5 PIAV-Kontrolle

Ausschuss für Gesundheit

4.1.2 Forschungsdatenzentrum Gesundheit

4.1.3 Taskforce Forschungsdaten

4.1.4 Petersberger Erklärung

5.2 Regelungen zur Bewältigung der COVID-19-Pandemie

8.2 Digitale Gesundheitsanwendungen

8.3 Sormas (follow up)

8.4 Nutzung der Krankenversichertennummer (follow up)

Haushaltsausschuss

10.2 Aufbau Labor

10.4 Personalentwicklung und Haushaltslage im Jahr 2022

10.5 Längst notwendig – das neue Verbindungsbüro des BfDI in Berlin

10.7 Gut vernetzt: Das Hauptstadtteam des BfDI

Ausschuss für Inneres und Heimat

3.2.2 DSK Taskforce Souveräne Cloud

3.2.5 Aktenvernichtungs- und Datenlöschmoratorium

3.2.6 Orientierungshilfe Werbung 2.0

3.3.4 EU-Systeme: Zentrale Koordinierung der Aufsicht im CSC

3.3.9 EU-U.S. Data Privacy Framework (Privacy Shield Nachfolge)

4.3.2 Entscheidungen europ. AB zu Google Analytics

4.3.4 Einsatz eines Content-Distribution-Network (CDN) für die Website des Zensus 2022

5.4 Hinweisgeberschutzgesetz

5.6 Neues EES- und ETIAS-Durchführungsgesetz

6.4 Transparenzgesetz

7.1 Passenger Name Records (PNR) – Grundsatzurteil des EuGH bestätigt Handlungsbedarf

7.2 Polizei 20/20 – P 20

7.3 Einschaltung Dritter bei Quellen-TKÜ und Onlinedurchsuchung

7.4 Kennzeichenerfassung Bundespolizei

7.6 Der Verfassungsschutz und das Bundesverfassungsgericht

7.7 Beanstandungen des BAMAD und des BfV aufgrund der Verletzung der Unterstützungspflicht

7.8 Personenbezogene Daten in Informationsschreiben des BfV

7.9 Endlich: eine gesetzliche Grundlage für die ZITiS

7.10 Wildwuchs bei Überprüfungsverfahren

8.6 Registermodernisierung/OZG-Umsetzung

8.8 Zensus 2022

9.3 Kontrollen in Auslandvertretungen in Kasachstan

9.4.1 Pflichtkontrolle: Verdeckte Maßnahmen beim BKA

9.4.2 Pflichtkontrolle eingriffsintensiver Maßnahmen im Zollfahndungsamt München

9.4.3 Datenübermittlung des BKA im internationalen Bereich

9.4.4 Pflichtkontrollen ATD/RED

9.4.6 Kontrolle der Abrufe von Daten im automatisierten Auskunftsverfahren

9.4.7 Funkzellendatei des Bundeskriminalamts

9.4.8 Koordinierte Kontrollen zu Ausschreibungen zur verdeckten/gezielten Kontrolle im Schengener Informationssystem

9.4.9 Datenschutzaufsicht und Beratung beim BfV

9.4.10 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst

9.4.11 Datenverarbeitung beim BND

12.2 Datenschutzrechtliche Aspekte von Telemedienangeboten

12.3 Alternative Bereitstellung von Bundes-Apps

12.6 Verbesserungen im Vorgangsbearbeitungssystem BKA

12.7 Einlenken beim Ausländervereinsregister

Ausschuss für Klimaschutz und Energie

8.15 Datenschutz im Smart Home

Rechtsausschuss

6.4 Transparenzgesetz

7.5 Verstärkte Tätigkeiten im Bereich der Strafjustizbehörden

Verkehrsausschuss

8.10 Digitale Datenräume und Mobilitätsdaten im Verkehrssektor

Verteidigungsausschuss

7.7 Beanstandungen des BAMAD und des BfV aufgrund der Verletzung der Unterstützungspflicht

9.4.10 Datenschutzaufsicht und Beratung beim Bundesamt für den Militärischen Abschirmdienst

Wirtschaftsausschuss

3.2.6 Orientierungshilfe Werbung 2.0

3.3.8 Verbindliche interne Datenschutzvorschriften - Neues von den Binding Corporate Rules

3.3.10 Leitlinien zu genehmigten Zertifizierungen und Verhaltensregeln als Instrumente für Drittstaatentransfers

3.4 G7 Roundtable

4.2.2 Digital Services Act

4.2.3 Digital Markets Act

4.3.2 Entscheidungen europ. AB zu Google Analytics

5.4 Hinweisgeberschutzgesetz

5.5 Dienste zur Einwilligungsverwaltung

8.11 TrustPid – neue Wege der personalisierten Werbung

8.12 Videokonferenzdienste

8.13 Neues von der E-Mail – Zuständigkeitswechsel zum BfDI

12.2 Datenschutzrechtliche Aspekte von Telemedienangeboten

Anlagen

Anlage 1

Kontrollierte Stellen

Acht Unternehmen zum SÜG

Auswärtiges Amt

BARMER Ersatzkasse

BKK VBU

Bundesamt für den Militärischen Nachrichtendienst

Bundesamt für die Sicherheit der nuklearen Entsorgung

Bundesamt für die Sicherheit in der Informationstechnik

Bundesamt für Familie und zivilgesellschaftliche Aufgaben

Bundesanstalt für Geowissenschaften und Rohstoffe

Bundesamt für Justiz

Bundesamt für Migration und Flüchtlinge

Bundesamt für Strahlenschutz

Bundesamt für Verfassungsschutz

Bundesamt für Wirtschaft und Ausfuhrkontrolle

Bundeskriminalamt

Bundesministerium der Verteidigung

Bundesministerium für Wirtschaft und Klimaschutz

Bundesnachrichtendienst

Bundesnetzagentur

Bundespolizeidirektion Sankt Augustin

Bundesrechnungshof

Deutsche Post AG

Deutsche Rentenversicherung Bund

DPD Deutschland GmbH

Emden Digital GmbH

Fernstraßen-Bundesamt

GEL Express Logisitik GmbH

Heiko Ulber Transporte GmbH & Co. KG

Hermes Germany GmbH

Inexio Informationstechnologie und Telekommunikation GmbH

Informationstechnikzentrum Bund

Jobcenter Deutsche Weinstraße

Jobcenter Halle an der Saale

Jobcenter Heilbronn

Jobcenter Mittelsachsen

Militärisches Nachrichtenwesen der Bundeswehr

Stiftung Zentrale Stelle Verpackungsregister

Wasserstraßen- und Schifffahrtsamt Necker

Wasserstraßen- und Schifffahrtsamt Oder-Havel

Zentrale Stelle für Informationstechnik im Sicherheitsbereich

ZF Transporte GmbH

Zollfahndungsamt Frankfurt am Main

Zollfahndungsamt München

Zollkriminalamt

Diese Liste enthält auch schriftliche Kontrollen. Manche der aufgeführten Stellen wurden mehrfach kontrolliert.

Bei den in dieser Liste genannten Stellen wurde während des Berichtszeitraums ein Kontroll- oder Beratungsgespräch vor Ort, virtuell oder in schriftlicher Form begonnen. Dies bedeutet jedoch nicht, dass alle Gesamtverfahren ebenfalls im Berichtszeitraum abgeschlossen werden konnten. Insbesondere liegt noch nicht für sämtliche Verfahren ein Abschlussbericht vor. Diese veröffentlicht der BfDI im Rahmen der rechtlichen Möglichkeiten zeitnah nach der Fertigstellung auf seiner Website unter: www.bfdi.bund.de/kontrollberichte

Anlage 2

Übersicht über Maßnahmen/Beanstandungen gegenüber öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
Bundesagentur für Arbeit	Verwarnung nach Art. 58 Abs. 2 Buchst. b) DSGVO	Verstoß gegen Art. 34 Abs. 1 lit. b) versäumter Schutz von personenbezogener Daten gegenüber Kollegen
Bundesagentur für Arbeit	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Versand des Krankengeldbescheides (ohne Einwilligung) an die Mutter der Beschwerdeführerin
Bundesamt für das Personalmanagement der Bundeswehr	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	nicht fristgerechte Beauskunftung Art. 15 DSGVO im Beschäftigungsverhältnis
Bundesamt für den Militärischen Abschirmdienst	Beanstandung nach § 16 Abs. 2 BDSG wegen Verstoß gegen § 8 MADG iVm § 14 Abs. 3 BVerfSchG	Fehlende Nachholung der Anhörung des BfDI bei Erlass einer Dateianordnung (DAO) in Form einer Sofortanordnung (SAO) nach § 8 MADG iVm § 14 Abs. 3 BVerfSchG
Bundesamt für Familie und zivilgesellschaftliche Aufgaben	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 19 Abs. 2 SÜG und § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG
Bundesamt für Justiz	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen §§ 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG; § 15a; § 17 Abs. 2 Satz 1
Bundesamt für Kartographie und Geodäsie	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 6 Abs. 1 DSGVO wegen des Einsatzes eines Online-Virenscanners (VirusTotal)
Bundesamt für Migration und Flüchtlinge	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 17 Abs. 1 lit. a DSGVO wegen Unterlassen der Löschung von Daten aus der Auswertung mobiler Datenträger
Bundesamt für Verfassungsschutz	Beanstandung nach § 16 Abs. BDSG, § 28 Abs. 2 BVerfschG	Verstoß gegen die Mitwirkungspflicht aus § 28 Abs. 2 BVerfSchG
Bundesamt für Wirtschaft und Ausfuhrkontrolle	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 19 Abs. 2 SÜG
Bundeskriminalamt	Anordnung gemäß § 69 Abs. 2 BKAG	Verstoßes gegen § 47 Nr. 1 Var. 1 BDSG wegen Datenverarbeitung ohne ausreichende Rechtsgrundlage
Bundeskriminalamt	Beanstandung gemäß § 16 Abs. 2 S. 1 BDSG	Verstoßes gegen § 3 Abs. 1 ATDG (automatisierte Übertragung von Daten ohne die Möglichkeit einer Einzelfallprüfung) sowie gegen § 11 Abs. 2 ATDG i.V.m. § 58 Abs. 2 BDSG (Verletzung von Löschpflichten)
Bundeskriminalamt	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 21 SÜG
Bundeskriminalamt	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen Art. 2 Abs. 1 i. V .m. Art. 1 Abs. 1 GG, § 19 Abs. 2 SÜG
Bundesministerium für Arbeit und Soziales	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Versand einer E-Mail Kampagne ohne Rechtsgrundlage uvm.

Stelle	Maßnahme/Beanstandung	Grund
Bundesministerium für Wirtschaft und Klimaschutz	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen §§ 19 Abs. 2, 22 Abs. 2 Nr. 1 lit. a SÜG; § 20 Abs. 1 SÜG
Bundespolizei	Beanstandung § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung
Bundespolizei	Beanstandung § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung
Bundespolizei	Beanstandung § 16 Abs. 2 BDSG	Petentenverfahren
Bundespolizeiakademie	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	nicht fristgerechte Auskunft nach Art. 15 DSGVO im Beschäftigungsverhältnis
Finanzamt Fürstenfeldbruck	Anweisung gemäß Art. 58 Abs. 2 lit. c) DSGVO	Erteilung einer unvollständigen Auskunft nach Art. 15 DSGVO
Finanzamt Homburg – Außenstelle St. Ingbert	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß wegen Versand des Steuerbescheides an Eltern obwohl Sohn volljährig war
Finanzamt Prenzlauer Berg	Warnung gemäß Art. 58 Abs. 2 lit. a) DSGVO und Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO	Versand unverschlüsselter E-Mail und damit Nichteinhaltung des nach Art. 32 DSGVO erforderlichen Schutzniveaus
Generalzolldirektion	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Verwarnung wegen Versand von Impfinformationen von 61 Personen an 89 Kontaktpunkte anderer Dienststellen per E-Mail
Informationstechnikzentrum Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 44 DSGVO wegen des Einsatzes von Cloudflare auf der Zensus-Webseite
Jobcenter Berlin Neukölln	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Offenlegung einer Information durch den Personalrat
Jobcenter Berlin Nord	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Vermischung zweier Datensätze
Jobcenter Halle (Saale)	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Anforderung von ungeschwärzten Kontoauszügen
Jobcenter Ilm-Kreis	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Anforderung von ungeschwärzten Kontoauszügen
Kommando Heer	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Art. 15 DSGVO Antrag verspäter beschieden, zudem rechtsgrundlos zunächst Auskunft abgelehnt
Luftlandeaufklärungskompanie 310	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	1. Offenlegung personenbezogener Daten auf Laufwerk, 2. verfristete Art. 33-DSGVO-Meldung, 3. zunächst keine Meldung an Betroffene; 15-210/035#0712
Panzerbrigade 12	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	elektronische Datei mit pbD des BF war im Intranet ungeschützt verfügbar
Zentrale Stelle für Informationstechnik im Sicherheitsbereich	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 2 Abs. 1 Satz 1 SÜG und § 19 Abs. 2 SÜG und § 22 Abs. 2 Satz 1 Nr. 1 SÜG
Zollfahndungsamt München	Beanstandung gemäß § 16 Abs. 2 BDSG	Keine Benennung aufgrund einer Einstufung

Stelle	Maßnahme/Beanstandung	Grund
Deutsche Rentenversicherung Knappschaft-Bahn-See	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO i.V.m. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch Sozialgesetzbuch (SGB I)
Unfallversicherung Bund und Bahn	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. a) i. V. m. Art. 9 Abs. 1 und 2 lit. a) sowie gegen Art. 6 Abs. 1 DSGVO
Deutsche Rentenversicherung Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
BKK firmus	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO i.V.m. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I)
Deutsche Rentenversicherung Bund	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO
mhplus Betriebskrankenkasse	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 13 DSGVO, Art. 7 Abs. 2 S. 1 DSGVO, Art. 5 Abs. 1 lit. b) und c) DSGVO
DAK-Gesundheit	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 9 Abs. 1 DSGVO i.V.m. § 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I)
Verwaltungs-Berufsgenossenschaft VBG	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 Abs. 1 DSGVO, Art. 15 Abs. 3 S. 3 DSGVO
Bundesanstalt für Post und Telekommunikation	Verwarnung nach Art. 58 Abs. 2 lit. b) DSGVO	Unvollständige Auskunft nach Art. 15 DSGVO, unverschlüsselte Kommunikation via E-Mail, Überschreitung der Aufbewahrungsfristen

Nicht alle der oben aufgelisteten Maßnahmen und Beanstandungen sind bisher rechtskräftig.

Übersicht über Maßnahmen/Beanstandungen gegenüber nicht-öffentlichen Stellen

Stelle	Maßnahme/Beanstandung	Grund
Ein Postdienstleistungs-unternehmen	Verwarnung (Art. 58 Abs. 2 lit. b) DSGVO)	Verstoß gegen Art. 6 Abs. 1 S. 1 und Art. 32 Abs. 1 lit. b) DSGVO wegen Anzeige der Postleitzahlen in der Sendungsverfolgung, wodurch Dritte personenbezogene Daten einsehen konnten
Ein Postdienstleistungs-unternehmen	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 17 Abs. 1 lit. d) DSGVO wegen keiner unverzüglichen bzw. vollständigen Löschung der personenbezogenen Daten
Ein Postdienstleistungs-unternehmen	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 Abs. 2 DSGVO wegen nicht ausreichender technisch-organisatorischen Maßnahmen (fehlende Identitätsprüfung bei Erteilung einer Abstellgenehmigung)
Ein Postdienstleistungs-unternehmen	Verwarnung Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 15 Abs. 1 lit. c) DSGVO, keine Informationen zu Empfängern bzw. Kategorien von Empfängern in der Auskunft
Ein Telekommunikations-dienstleistungsunternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 17 Abs. 1 lit. a) DSGVO, Missachtung der Pflicht zur Löschung personenbezogener Daten, sobald diese zweckmäßig nicht mehr notwendig sind
Ein Telekommunikations-dienstleistungsunternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 DSGVO, Unternehmen fragt bei Störungsmeldung letzte 6 Ziffern der IBAN ab
Ein Telekommunikations-dienstleistungsunternehmen	Anweisung gemäß Art. 58 Abs. 2 lit. d) DSGVO und Androhung eines Zwangsgeldes gemäß §§ 6, 11, 13 VwVG	Verstoß gegen §38 Abs. 1 S. 1 BDSG und Art. 37 Abs. 1 lit. b) DSGVO, Unternehmen benennt keinen Datenschutzbeauftragten
Ein Telekommunikations-dienstleistungsunternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO. Informationen zu offenen Forderungen von Kunden wurden telefonisch mitgeteilt, ohne dass eine vorherige Authentifizierung der Anrufer erfolgte.
Ein Telekommunikations-dienstleistungsunternehmen	Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO	Verstoß gegen Art. 32 DSGVO, Art. 6 Abs. 1 DSGVO, Weitergabe personenbezogener Daten an unbefugte Dritte ohne ausreichende Kundenauthentifizierung und unter Missachtung der technisch organisatorischen Maßnahmen
Ein Telekommunikations-dienstleistungsunternehmen	Anweisung nach Art. 58 Abs. 2 lit. c) und Androhung eines Zwangsgeldes gemäß §§ 6,11,13 VwVG	Verstoß gegen Art. 15 Abs. 1 lit. c) DSGVO, unvollständige Auskunft über die Empfänger der personenbezogenen Daten zur betroffenen Person nach Inanspruchname des Auskunftsrecht durch die betroffene Person
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 18 Abs. 1 u. 2 SÜG und § 19 Abs. 2 SÜG
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 19 Abs. 2 SÜG und § 22 Abs. 2 SÜG
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen §§ 30, 19 Abs. 2 SÜG und §§ 31, 22 Abs. 2 SÜG
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen §§ 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG; § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 51 Abs. 1 BDSG

Stelle	Maßnahme/Beanstandung	Grund
Ein Unternehmen	Beanstandung gemäß § 36 Abs. 1 SÜG i.V.m. § 16 Abs. 2 Satz 1 BDSG	Verstoß gegen § 18 Abs. 1 u. 2 SÜG und § 19 Abs. 2 SÜG

BfDI
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Leitungsstab Presse/Öffentlichkeitsarbeit
MR Hensel
R 5010

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Prof. Ulrich Kelber
R 5000

Gleichstellungsbeauftragte
OAR'n Kemper
R 1900

Behördlicher Datenschutzbeauftragter
RD Deitermann
R 1950

Interessensvertretungen

Personalrat
Vorsitzender
TB Walbröl
R 1910

Vertrauensperson der schwerbehinderten Menschen
OAR'n Thelen
R 1920

Zentrale Anlaufstelle
MR Meister
R 7100

Leitender Beamter
MinDir Müller, J. H
R 6000

Informationsfreiheit
RD'n Schlögel
R 6100

Geheim- und Sabotageschutzbeauftragter
OAR Finzelberg
R 1940

IT-Sicherheitsbeauftragter
OAR Höllen
R 1930

Ansprechperson für Korruptionsprävention, Sponsoringbeauftragter, interne Meldestelle
RD Roski
R 1960

Abteilung Z
Zentrale Aufgaben
MinDirig'n Dr. Grundmann
R 9000

- **Referat Z 1** — Personal — MR'n Dr. Kreiling — R 9100
- **Referat Z 2** — Organisation/Haushalt — MR'n Bönner — R 9200
- **Referat Z 3** — Innerer Dienst/Beschaffung — RD'n Westkamp — R 9300
- **Referat IKT** — Informations- und Kommunikationstechnik — MR Dr. Garbotz — R 9400
- **Justitiariat** — MR Peschel — R 9600

Abteilung 1
Grundsatz, Verwaltung des Bundes, Internationales
MinDirig Heyn
R 1000

- **Referat 11** — Grundsatz, nichtöffentlicher Bereich — MR Hermerschmidt — R 1100
- **Referat 12** — Finanz-/Steuerverwaltung, Rechtswesen, Parlamentarischer Bereich — MR Lenzen — R 1200
- **Referat 13** — Sozial- und Gesundheitswesen — RD Müller, T. — R 1300.
- **Referat 14** — Europäische und Internationale Angelegenheiten — MR Dr. Haupt — R 1400
- **Referat 15** — Arbeitsverwaltung, Beschäftigtendatenschutz, Verteidigung — RD Dr. Kisker — R 1500
- **Referat 16** — Innere Verwaltung, Auswärtiger Dienst — RD Faßbender — R 1600

Abteilung 2
Technologischer Datenschutz, Telekommunikation und Telemedien
MinDirig'n Jost
R 2000

- **Referat 21** — Projekte der angewandten Informatik, Telematik — TB Leopold — R 2100
- **Referat 22** — Postdienste, Wirtschaftsverwaltung — MR'n Schäfer — R 2200
- **Referat 23** — Telemedien und Messenger Dienste — MR'n Hartmann — R 2300
- **Referat 24** — Telekommunikation — RD Dr. Stadler — R 2400
- **Referat 25** — Technologischer Datenschutz, Datensicherheit — MR Dr.Bender — R 2500
- **Referat 26** — Technikentwicklung, Labor — N.N. — R 2600
- **Referat 27** — Bundesamt für Sicherheit in der Informationstechnik — N.N. — R 2700

Abteilung 3
Polizei und Nachrichtendienste
MinDirig'n Polfers
R 3000

- **Referat 31** — Grundsatz , Internationales im Bereich Polizei und Justiz — MR Behn — R 3100
- **Referat 32** — Bundeskriminalamt, Generalbundesanwalt — MR Bergemann — R 3200
- **Referat 33** — Bundesamt für Verfassungsschutz, Bundesamt für den Militärischen Abschirmdienst, Zentrale Stelle für Informationstechnik im Sicherheitsbereich — MR'n Dr. Sosna — R 3300
- **Referat 34** — Bundesnachrichtendienst, Militärisches Nachrichtenwesen, Nachrichtendienstliche Kooperationen — MR'n Mittnacht — R 3400
- **Referat 35** — Bundespolizei, Zollkriminalamt, Financial Intelligence Unit — MR'n Löwnau — R 3500
- **Referat 36** — Sicherheitsüberprüfungsgesetz — MR'n Dr. Gnedler — R 3600

Anschrift:
Dienstsitz Bonn: Graurheindorfer Str. 153, 53117 Bonn
Postfach 14 68, 53004 Bonn

Verbindungsbüro
Berlin: Friedrichstr. 50, 10117 Berlin

Erreichbarkeit:
Telefon: 0228/997799-0
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Stand: 17. Januar 2023

Abkürzungsverzeichnis

3G-Nachweise	Nachweise entweder über einen vollständigen Impfschutz gegen COVID-19, eine Genesung von einer Infektion mit COVID-19 oder einer Negativtestung auf COVID-19
AB	Aufsichtsbehörde
a. a. O.	am angegebenen Ort
a. F.	alte Fassung
AA	Auswärtiges Amt
Abs.	Absatz
AI Act	Artificial Intelligence Act
AK	Arbeitskreis
AO	Abgabenordnung
App	Application
Art.	Artikel
ATD	Anti-Terror-Datei
AVR	Ausländervereinsregister
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAFzA	Bundesamt für Familie und zivilgesellschaftliche Aufgaben
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BayVSG	Bayerisches Verfassungsschutzgesetz
BCR	Binding Corporate Rules
BCR-C	Controller Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
beBPo	besonderes elektronisches Behördenpostfach
BEM	Betriebliches Eingliederungsmanagement
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfJ	Bundesamt für Justiz
BfV	Bundesamt für Verfassungsschutz
BGleiG	Bundesgleichstellungsgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMAS	Bundesministerium für Arbeit und Soziales
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern und für Heimat
BMVg	Bundesministerium der Verteidigung
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BPol	Bundespolizei
BPolG	Bundespolizeigesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Deutscher Bundestag
BVerfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
BZR	Bundeszentralregister
CDN	Content-Distribution-Netzwerk
CEF	Coordinated Enforcement Action
CIS	Zollinformationssystem
CNIL	Commission National de L'Informatique et Libertes (französische Datenschutzbehörde)
CNPD	Commission nationale pour la protection des données (luxemburgische Datenschutzbehörde)
COVID-19-SchG	Gesetz zur Stärkung des Schutzes der Bevölkerung und insbesondere vulnerabler Personengruppen vor COVID-19
CPPA	California Privacy Protection Agency (kalifornische Datenschutzbehörde)
CSA	Child Sexual Abuse
CSAM VO	Child Sexual Abuse Material-Verordnung

CWA	Corona-Warn-App
d. h.	das heißt
DA	Data Act
DAkkS	deutsche Akkreditierungsstelle
DAO	Dateianordnung
DARP	Deutschen Aufbau- und Resilienzplan
DFFT	Data Free Flow with Trust
DGA	Data Governance Act
DiGA	digitale Gesundheitsanwendungen
DiPa	digitalen Pflegeanwendungen
DMA	Digital Markets Act
DOMUS	Personensuche in der elektronischen Akte
DPC	Data Protection Comission (irische Datenschutzbehörde)
DRV	Deutsche Rentenversicherung
DSA	Digital Services Act
DSC	Digital Services Coordinator
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DWD	Deutscher Wetterdienst
ECRIS-TCN	Systeme Europäisches Strafregisterinformationssystem für Drittstaatsangehörige und Staatenlose
EDSA	Euroäischer Datenschutzausschuss
EDSB	Europäische Datenschutzbeauftragte
EEDG	EES- und ETIAS-Durchführungsgesetz
EES	Einreise-/Ausreisesystem
EES	Europäisches Ein- und Ausreisesystem
EESDG	EES-Durchführungsgesetz
eFBS	einheitliches Fallbearbeitungssystem
eGK	elektronische Gesundheitskarte
EHDS	European Health Data Space
ePA	elektronische Patientenakte
EPRIS	European Police Records Index System
ERV	elektronischer Rechtsverkehr
ETIAS	Europäisches Reiseinformations- und -genehmigungssystem
ETIASDG	ETIAS-Durchführungsgesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-US DPF	EU-U.S. Data Privacy Framework
FAQ	engl. Frequently Asked Questions
FDP	Freie Demokratische Partei
FDR	Falldatei Rauschgift
FISG	Finanzmarktintegritätsstärkungsgesetz
FIU	Financial Intelligence Unit
FlugDaG	Fluggastdatengesetz
G7 DPA	G7 Data Protection Authorities Roundtable
GBA	Generalbundesanwalt
GDPR	General Data Protection Regulation
ggf.	gegebenenfalls
GleiB	Gleichstellungsbeauftragte
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
GSB	Geheimschutzbeauftragte/r
GwG	Geldwäschegesetz

HKV	Heizkostenverordnung
HS Bund	Hochschule des Bundes für öffentliche Verwaltung
HZI	Helmholtz-Zentrum für Infektionsforschung
IDNr	Identifikationsnummer
IDNrG	Identifikationsnummerngesetz
IFG	Informationsfreiheitsgesetz
IFK	Konferenz der Informationsfreiheitsbeauftragten
IfSG	Infektionsschutzgesetz
IMI	Binnenmarktinformationssystem
INZOLL	Informationssystem des Zollfahndungsdienstes
IoT	Internet of things
IP	Internet Protocol
IST ESG	EDSA-Expert Subgroup International Transfers
IT-PLR	IT-Planungsrat
ITZBund	Informationstechnikzentrum Bund
IWGDPT	International Working Group Data Protection in Technology
JI-Richtlinie	Richtlinie zum Datenschutz bei Polizei und Justiz
KEA	Anlassbezogene automatische Kennzeichenerfassung
KfZ	Kraftfahrzeug
KHPflEG	Krankenhauspflegeentlastungsgesetz
KI	Künstliche Intelligenz
KMU	kleine und mittlere Unternehmen
KONSENS	Koordinierte neue Software-Entwicklung der Steuerverwaltung
KVKK	Kişisel Verileri Koruma Kurumu (türkische Datenschutzbehörde)
KVNR	Krankenversichertennummer
LDA	Landesamt für Datenschutzaufsicht Bayern
Meta IE	Meta Platforms Ireland Limited
MII	Medizininformatikinitiative
MIO	Medizinische Informationsobjekte
MsbG	Messstellenbetriebsgesetz
NADIS-WN	Nachrichtendienstliches Informationssystem und Wissensnetz
NFC	Near Field Communication
NGO	Nichtregierungsorganisation
NOYB	Non-of-your-business
Nr.	Nummer
NUM	Netzwerk Universitätsmedizin
OH	Orientierungshilfe
ONI	Operative Nutzung des Internets durch verdeckte Informationserhebung durch Ausnutzung schutzwürdigen Vertrauens
OOTS	Once-Only-Technical-System
OSINT	Open Source Intelligence
OTT	Over the top
PGP	Pretty Good Privacy
PIAV	Polizeilicher Informations- und Analyseverbund
PIMS	Privacy-Information-Management-Systems
PKV	private Krankenversicherung
PNR	Passenger Name Record
RED	Rechtsextremismus-Date
RegMoG	Registermodernisierungsgesetz
RKI	Robert Koch-Institut

S.	Seite
s.	siehe
SanktDG	Sanktionsdurchsetzungsegsetz
SARS-CoV-2	Severe-Acute-Respiratory-Syndrome-Coronavirus-2
SCG	Supervision Coordination Groups
SDG VO	Single-Digital-Gateway-Verordnung
SGB	Sozialgesetzbuch
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengener Informationssystem
SIS III-VO	Verordnung (EU) 2018/1862 des europäischen Parlaments und des Rates vom 28. November 2018
SIS SCG	SIS II Supervision Coordination Group
SMGW	Smart-Meter-Gateways
SOCMINT	Social Media Intelligence
SPD	Sozialdemokratische Partei Deutschlands
StPO	Strafprozessordnung
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TF	Task Force
TI	Telematik Infrastruktur
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V
TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetzes
u. a.	unter anderem
UIG	Umweltinformationsgesetz
USA	United States of America
VBS	Vorgangsbearbeitungssystem
VeRA	Verfahrensübergreifendes Recherche- und Analysesystem
Verbund-DMS	einheitlichen Dokumentenmanagementsystems im Verfassungsschutzverbund
vgl.	vergleiche
VIS	Visa-Informationssystem
WBRL	Whistleblowing Richtlinie
z. B.	zum Beispiel
ZASt	Zentrale Anlaufstelle
ZfDG	Zollfahndungsdienstegesetz
ZfS	Zentralstelle für Sanktionsdurchsetzung
ZITiS	Zentrale Stelle für die Informationstechnik im Sicherheitsbereich
ZKA	Zollkriminalamt
ZStV	Zentrale Staatsanwaltliche Verfahrensregister

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
Internet: www.bfdi.bund.de

Bonn 2023
Dieser Bericht ist als Bundestagsdrucksache erschienen.

Bildnachweis: BfDI, Erik Liebermann, Christine Pfohlmann, Thomas Plaßmann, Ralph Ruthe

Druck:
Druckerei Franz Paffenholz GmbH
Königstraße 82
53332 Bornheim